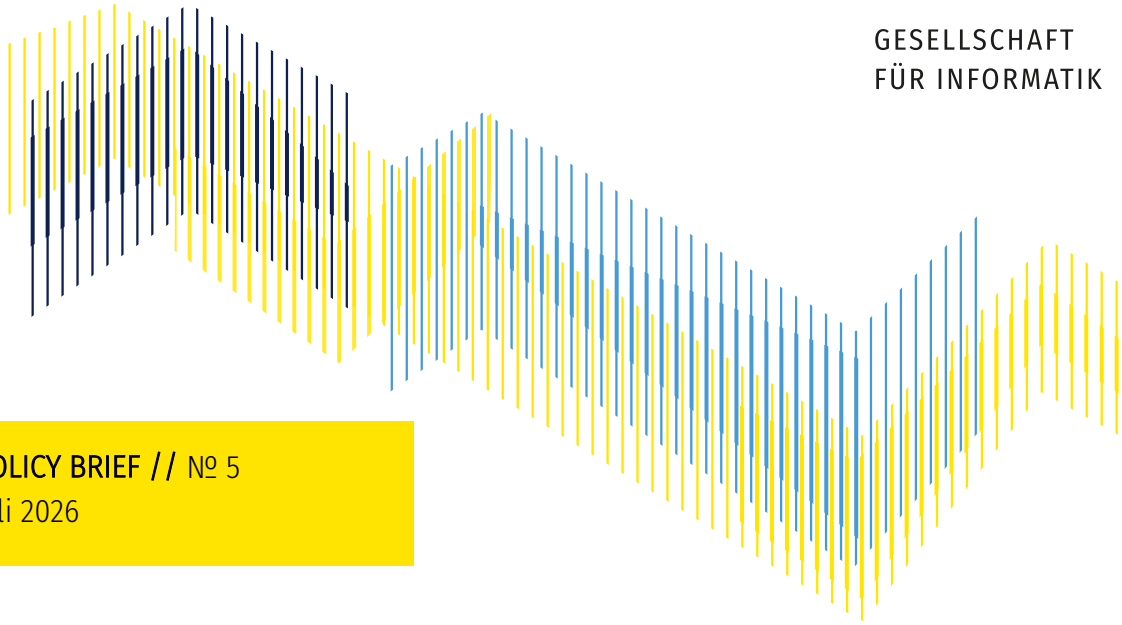

GESELLSCHAFT
FÜR INFORMATIK

POLICY BRIEF // № 5
Juli 2026

Anerkennung und Besserstellung von Open-Source-Software-Stewards

Peter Schoo[1], Maximilian Kroker[2], Harald Wehnes[3], Julian Kunkel[4], Tanja Krins[5], Katika Kühnreich[6], Daniel Loebenberger[7], Stefan Schulte[8], Christian Janiesch[9]

Die Cyberresilienz-Verordnung (Cyber Resilience Act, CRA) der EU etabliert einen umfassenden regulatorischen Rahmen für die Cybersicherheit von Produkten mit digitalen Elementen und definiert dabei auch die Verantwortlichkeiten von Herstellern entlang des gesamten Lebenszyklus dieser Produkte [1]. Die diesbezügliche, Ende 2027 kommende Rechtslage wurde bereits dargestellt [2]. Hier nun geht es um die Auswirkung des CRA auf das Ökosystem von Open-Source-Software (OSS) [3], konkret um die im CRA Artikel 24 neu definierte Rolle der OSS-Stewards („Verwalter quelloffener Software"), die juristischen Personen vorbehalten und die für alle Hersteller von Software, die OSS-Komponenten beinhaltet, von Bedeutung ist.

CRA und das OSS-Ökosystem

Vom CRA betroffen sind alle Produkte mit digitalen Komponenten, bei denen die beabsichtigte oder vorhersehbare Nutzung eine logische oder physische Verbindung zu einem Gerät oder Netzwerk umfasst und die in der EU hergestellt oder in die EU importiert werden. Für Unternehmen bedeutet der CRA, dass sie bereits ab September 2026 erste Anforderungen erfüllen müssen, insbesondere die Pflicht zur Meldung von Schwachstellen als erster Bestandteil des CRA.

Heute baut die Mehrheit der deutschen Unternehmen auf dem OSS-Ökosystem auf: Rund 73 Prozent setzen entsprechende Komponenten ein. Dabei verwenden etwa 67 Prozent der Unternehmen diese sogar ohne Anpassung des Quellcodes. Obwohl na-

[1] Mitglied des PAK „Digitale Souveränität"
[2] Junior-Fellow der GI
[3] Sprecher des PAK „Digitale Souveränität"
[4] Sprecher des AK „Open Source"
[5] Mitglied des Fachbereichs „Informatik in Recht und öffentlicher Verwaltung"
[6] Sprecherin der Fachgruppe „Internet und Gesellschaft"
[7] Sprecher des Fachbereichs „Sicherheit"
[8] Sprecher der Fachgruppe „Kommunikation und Verteilte Systeme"
[9] Mitglied des Fachbereichs „Wirtschaftsinformatik"

hezu alle Unternehmen Sicherheit, Funktionalität und regulatorische Vorgaben als zentrale Auswahlkriterien für OSS-Komponenten nennen, beteiligt sich nur etwa die Hälfte dieser Unternehmen an der Weiterentwicklung von OSS. [4]

Ein Steward ist im Sinne des CRA eine juristische Person, die Open-Source-Software systematisch und dauerhaft unterstützt sowie deren Weiterentwicklung und langfristige Nutzbarkeit sicherstellt, ohne diese selbst auf dem Markt als kommerzielles Produkt bereitzustellen. Die Rolle betrifft insbesondere freie Open-Source-Software, etwa zur Integration in kommerzielle Produkte oder Dienste anderer und dabei Anforderungen des CRA an Sicherheit, Verantwortlichkeit und Compliance erfüllt. Ein Unternehmen kann je nach Softwareprojekt gleichzeitig sowohl Steward als auch Hersteller sein.

OSS-Stewards

An der Schnittstelle im OSS-Ökosystem zwischen Wirtschaft, Verwaltung und Gesellschaft wird den Stewards eine besondere Verantwortung zugewiesen [5]. Mit dem CRA sind sie verpflichtet, eine Cybersicherheitsstrategie zu entwickeln und nachvollziehbar zu dokumentieren. Ziel ist es, sowohl die Entwicklung sicherer Produkte mit digitalen Elementen zu fördern, als auch den wirksamen Umgang mit Schwachstellen sicherzustellen und dabei den einschlägigen Melde- und Kooperationspflichten zu entsprechen. Sie übernehmen somit eine zentrale Funktion für die Sicherheit und Stabilität von CE gekennzeichneten Produkten aus dem OSS-Ökosystem heraus.

Vor diesem Hintergrund sollte die Rolle der Stewards normativ anerkannt, geschützt und gestärkt werden. Aktuell sieht der Gesetzgeber jedoch nur vor, dass diese Rolle nicht gewinnorientiert ausgeübt werden darf, und bietet kein spezifisches Kompensationsschema für diese Aufgaben an. Dies bedeutet einen nicht unerheblichen Entwicklungs- und Pflegeaufwand, da von Stewards bereitgestellte Komponenten nach dem Stand der Technik gesichert sein und Schwachstellen kontinuierlich sowie fristgerecht behoben werden müssen.

Bisher wenig strategische Relevanz zugewiesen

Die in der EU jetzt einzuführenden Stewards werden in den USA häufig als Open-Source-Organisationen nach 501(c)(3) (klassische gemeinnützige Organisationen, die offene Technologie als öffentliches Gut fördern) oder 501(c)(6) (branchenorientierte Konsortien zur Koordination von Unternehmen, Standardisierung und Ökosystem-Aufbau) eingeordnet. Dabei sind sie in den USA kein Nischenphänomen, sondern weit verbreitet, schaffen und erhalten systemrelevante Infrastrukturen für die digitale Zukunft und formen somit eine strategische Ressource. Während eine europäische Industriepolitik für die Digitalwirtschaft OSS als strategischen Hebel begreifen könnte (sie senkt Einstiegshürden, beschleunigt Innovation und ermöglicht es europäischen Akteuren, sich auf zukunftsweisende Technologien zu konzentrieren) [6], spielt selbst für das BMFTR Gemeinnützigkeit nur eine administrativ-rechtliche Rolle (z. B. bei Vergütung oder Förderbedingungen) und wird nicht als eigenständiges, innovationspolitisches Konzept gesehen. [7]

Allerdings setzt sich vor dem Hintergrund, dass die USA nicht nur den Weltmarkt für Software dominieren, sondern auch für OSS ein attraktiver Standort sind [8], in Europa langsam die Einsicht durch, dass OSS eine entscheidende Rolle für die digitale Zukunft einnimmt. Die Europäische Kommission [9] und das BMDS [10] unterstützen dies bereits durch Initiativen wie DC-EDIC und in Deutschland konkret mit ZenDiS und der Sovereign Tech Agency [11].

Doch dieser gute Anfang wird der Aufgabe von OSS und der Rolle von Stewards nicht gerecht: Die Finanzierung erfolgt meist nur projektbasiert und die Steward-Rolle bleibt nicht nachhaltig hervorgehoben. Für eine resiliente digitale Gesellschaft, wie sie durch den CRA geformt wird, sind diese jedoch wesentliche Aufgaben, die alle Bereiche der digitalen Gesellschaft – Wissenschaft, Wirtschaft, Verwaltung und letztlich auch die Zivilgesellschaft – perspektivisch prägen und beeinflussen.

Handlungsempfehlungen

Die wirtschaftliche Bedeutung von OSS-Stewards liegt nicht nur in der Bereitstellung von Software, sondern auch in der Förderung von Innovation und digitaler sowie technologischer Souveränität. Damit sind sie ein unverzichtbarer Bestandteil für die Zukunftsfähigkeit der deutschen und europäischen Wirtschaft im digitalen Zeitalter [12].

Die heutigen Organisationen, die zukünftig als agierende Open-Source-Software-Stewards erkannt werden und dabei wichtige Aufgaben für Wirtschaft und Gesellschaft übernehmen, existieren in vielfältigen Rechtsformen, die in einer Anerkennung ihrer Funktion umfassend einbezogen werden müssen. Daraus folgt:

Handlungsempfehlung 1: Der Gesetzgeber sollte sicherstellen, dass die im CRA definierte Rolle der Stewards im deutschen Recht so eingerichtet wird, dass sich bestehenden Open-Source-Organisationen – unabhängig von ihrer jetzigen Rechtsform – darin wiederfinden und damit ihre Rolle als Verwalter quelloffener Software offiziell anerkannt wird, um den Zugang zu Förderungen und rechtlicher Absicherung zu vereinfachen.

Die Gemeinwohlorientierung und Gemeinnützigkeit von Stewards sind anzuerkennen und zu stärken, etwa durch steuerliche Besserstellung wie zum Beispiel eine erweiterte Spendenabzugsfähigkeit oder reduzierte Abgaben für gemeinnützige Open-Source-Projekte. Zudem sollten die Möglichkeiten ausgebaut werden, Stiftungen durch öffentliche Mittel oder Matching-Funds verbessert zu fördern, wenn damit die Unterstützung gemeinnütziger OSS-Organisationen ausgeweitet werden. Auch eine direkte öffentliche Finanzierung über Förderprogramme ist dabei ein wichtiger Schritt. Rechtliche Privilegien, etwa Haftungsbeschränkungen für Stewards oder vereinfachte Gründungsprozesse für OSS-Organisationen, könnten die Arbeit zusätzlich absichern. Anreize für Unternehmen wie Steuererleichterungen für Firmen, die OSS-Projekte nachhaltig unterstützen, würden die Zusammenarbeit stärken. Zudem sollte OSS als kritische Infrastruktur anerkannt und in nationale Cybersicherheitsstrategien eingebunden werden. Schließlich ist der Aufbau von Bildungskapazitäten, etwa durch staatlich geförderte Ausbildungsprogramme für OSS-Schaffende, entscheidend, um langfristig Fachkräfte zu sichern.

Handlungsempfehlung 2: Um ihre Rolle wirksam auszufüllen, sollte die Politik OSS-Stewards durch rechtliche Klarheit (z. B. Haftungsprivilegien), finanzielle Förderung (z. B. direkte öffentliche Mittel, steuerliche Anreize, nachhaltige Förderung gemeinwohlorientierter Pflege) und institutionelle Unterstützung (z. B. Einbindung in Cybersicherheitsstrategien) gezielt stärken.

Die steuerliche Behandlung von OSS-Stewards entspricht derzeit nicht ihrer gesellschaftlichen und wirtschaftlichen Bedeutung. Im Steuerrecht besteht ein nationaler Gestaltungsspielraum, der von anderen EU-Staaten bereits genutzt wird, und genau dieser Spielraum sollte genutzt werden. Zumal der Koalitionsvertrag die Modernisierung des Gemeinnützigkeitsrechts angekündigt hat, um es an das digitale Zeitalter anzupassen. Da der EU-Gesetzgeber mit dem CRA Open-Source-Software-Stewards eine wesentliche Rolle bei der Cybersicherheit zuweist, kann kaum noch argumentiert werden, dass diese Tätigkeit „rein privatwirtschaftlich“ sei. Dennoch fehlt bisher eine klare steuerrechtliche Einordnung, die ihre gemeinnützigen Tätigkeiten angemessen würdigt und finanzielle Anreize schafft.

Handlungsempfehlung 3: Der Gesetzgeber sollte die steuerliche Anerkennung von OSS-Stewards als gemeinnützig stärken, indem er die Förderung digitaler Gemeingüter und digitaler Teilhabe sowie die Sicherheit und Resilienz digitaler Infrastrukturen in die Positivliste des § 52 AO aufnimmt, Tätigkeiten zur Absicherung der digitalen Lieferkette gemäß CRA per Anwendungserlass als Zweckbetrieb definiert (mit der Folge: keine Körperschaftsteuer, keine Gewerbesteuer und ggf. reduzierte Umsatzsteuer) und die Ehrenamtspauschale auf ein Digitales Ehrenamt ausweitet, um Expertinnen und Experten steuerfrei zu entlohnen.

LITERATUR

[1] Regulation of the European Parliament and of the Council on Horizontal Cybersecurity Requirements for Products with Digital Elements and amending regulations (Eu) No 168/2013 and (Eu) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CONSIL:PE_100_2023_REV_1, Abruf vom 15.05.2026 (DE VERSION): https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32024R2847

[2] GI-Radar 391: Der Digital Resilience Act, https://gi-radar.de/391-der-digital-resilience-act/

[3] Unlocking the power of digital commons: Data cooperatives as a pathway for data sovereign, innovative and equitable digital communities, https://www.mdpi.com/2673-6470/3/3/11

[4] Open Source Monitor 2025, https://www.bitkom.org/Bitkom/Publikationen/Studie-Open-Source-Monitor

[5] Über die Stewards, https://navigator.cranis.eu/cra/de/for-opensource/stewards

[6] Digitale Souveränität: Europas digitale Zukunft entsteht nicht in Silos, https://background.tagesspiegel.de/digitalisierung-und-ki/briefing/europas-digitale-zukunft-entsteht-nicht-in-silos

[7] Pläne der Bundesregierung für ein Innovationsfreiheitsgesetz und zum Rückbau der Forschungsbürokratie, https://dserver.bundestag.de/btd/21/034/2103458.pdf

[8] Commit für das Gemeinwohl, https://inf.gi.de/13/commit-fuer-das-gemeinwohl

[9] Commission Implementing Decision (EU) 2025/2170 of 29 October 2025 setting up the European Digital Infrastructure Consortium for Digital Commons (DC-EDIC), http://data.europa.eu/eli/dec_impl/2025/2170/oj

[10] Digitale Souveränität in der Wirtschaft - Bundesministerium für Digitales und Staatsmodernisierung, https://bmds.bund.de/themen/digitale-souveraenitaet/digitale-souveraenitaet-in-der-wirtschaft

[11] DC EDIC Gründung, https://www.zendis.de/en/newsroom/press/eu-digital-commons-consortium-dc-edic-officially-founded

[12] EU-Studie: Open Source stärkt die Wirtschaft und die technologische Unabhängigkeit, https://osb-alliance.de/verbands-news/eu-studie-open-source-staerkt-die-wirtschaft-und-die-technologische-unabhaengigkeit

Über die Gesellschaft für Informatik

Die Gesellschaft für Informatik e.V. (GI) ist die größte Fachgesellschaft für Informatik im deutschsprachigen Raum. Seit 1969 vertritt sie die Interessen der Informatikerinnen und Informatiker in Wissenschaft, Gesellschaft und Politik und setzt sich für eine gemeinwohlorientierte Digitalisierung ein. Mit 14 Fachbereichen, über 30 aktiven Regionalgruppen und unzähligen Fachgruppen ist die GI Plattform und Sprachrohr für alle Disziplinen in der Informatik.

GESELLSCHAFT FÜR INFORMATIK E.V. (GI)

Geschäftsstelle Berlin
Weydingerstraße 14-16
10178 Berlin
Tel: +49 1767 322 404 3

Ansprechpartner:
Nikolas Becker
Bereichsleitung Politik & Wissenschaft

Mail: nikolas.becker@gi.de
Tel: +49 (0)1767 322 404 3
Web: www.gi.de