Bundesverband IT-Mittelstand e.V. • Schiffbauerdamm 40 • 10117 Berlin

Dr. Oliver Grün
Bundesverband IT-Mittelstand e.V. (BITMi)
Präsident & Vorstandsvorsitzender
Berlin, den 03.12.2024

STELLUNGNAHME
Öffentliche Anhörung des Ausschusses für Digitales zum Thema „Open Source“ am 04.12.2024

Ausgangslage: Deutschland ist digital abgehängt und abhängig

Bei der digitalen Transformation ist unser Land inzwischen mit einer doppelten Herausforderung konfrontiert: In wesentlichen Bereichen, wie etwa der Verwaltungsdigitalisierung, ist die Bundesrepublik gegenüber anderen Nationen inzwischen schlicht abgehängt (DESI 2024). Der Anteil unserer Wirtschaft an der globalen digitalen Wertschöpfung schwindet in dramatischem Tempo (IW Köln 2021). Gleichzeitig gehört Deutschland zur Gruppe derjenigen Länder, die weltweit am zweitstärksten abhängig sind von digitalen Technologien aus dem Ausland (Mayer, Lu 2022). Dieser Zustand ist alarmierend und wird absehbar Folgen für unseren Wohlstand in einer zunehmend digitalen Welt mit sich bringen (Draghi-Bericht 2024). Wie leicht zudem einseitige Abhängigkeiten in strategisch wichtigen Domänen auch unsere politische Handlungsfähigkeit einschränken können, wurde bei den Gasengpässen infolge des russischen Angriffs auf die Ukraine deutlich. Vor diesem Hintergrund ist es von großer strategischer Bedeutung, dass die **digitale Souveränität** heute und in Zukunft das Leitmotiv für die digitalpolitische Agenda Deutschlands und Europas sein muss.

In der deutschen und europäischen Debatte um digitale Souveränität hat sich weitgehend ein Begriffsverständnis durchgesetzt, das die Frage nach **technologischer Selbstbestimmung**, also der Abbau einseitiger technologischer Abhängigkeiten insbesondere von Tech-Konzernen aus dem Nicht-EU-Ausland in den Mittelpunkt stellt. Dieses Verständnis von Souveränität entspricht auch der Auffassung des BITMi: Deutschland und Europa müssen in die Lage kommen, die digitale Transformation in allen wesentlichen Bereichen nach eigenen Wertvorstellungen und mithilfe von eigenen vertrauenswürdigen Lösungen „made in Germany/Europe“ zu **gestalten**. Dies umfasst mehrere Facetten, bzw. Erfüllungsmerkmale:

- **Digitale Resilienz**: Wir müssen nicht alles selbst entwickeln – das wäre schwer möglich und auch ökonomisch kaum sinnvoll. Aber in allen Kernbereichen der digitalen Transformation müssen Staat, Wirtschaft und Gesellschaft voll Handlungsfähig bleiben. Zu diesen Kernbereichen zählt etwa die digitale Infrastruktur unserer Verwaltung, die nicht von außereuropäischen Tech-Konzernen abhängen darf.

- **Digitale Wertschöpfung**: Der Wohlstand der Zukunft wird im digitalen Raum erwirtschaftet. Deutschlands ökonomische Entwicklung hängt daher

Hauptgeschäftsstelle:

Bundesverband
IT-Mittelstand e.V. (BITMi)
Pascalstraße 6
52076 Aachen
Deutschland

Telefon +49 241 1 89 05 58
Telefax +49 241 1 89 05 55

Hauptstadtbüro:

Bundesverband
IT-Mittelstand e.V. (BITMi)
Haus der
Bundespressekonferenz
Schiffbauerdamm 40
10117 Berlin
Deutschland

Telefon +49 30 22 60 50 05
Telefax +49 30 22 60 50 07

www.bitmi.de
kontakt@bitmi.de

Bankverbindung:
Konto 359 703
BLZ 390 500 00
Sparkasse Aachen
BIC AACSDE33
IBAN DE04 3905 0000
0000 3597 03

Vereinsregister Köln
43 VR 10055

Präsident und
Vorstandsvorsitzender:
Dr. Oliver Grün

USt.-IdNr DE 122662582

entscheidend davon ab, ob es uns gelingt eigene digitale Geschäftsmodelle zu etablieren und damit global Wettbewerbsfähig zu sein. Wenn wir digitale Lösungen nur noch aus Übersee einkaufen, wird dies nicht gelingen. Doch gerade im wichtigen Business-to-Business- (B2B) und Business-to-Government- (B2G) -Bereich haben wir noch die Chance, uns erhebliche Marktanteile zu sichern.

- **Datensouveränität**: Dies umfasst die technische Hoheit sowie die vollständige Kontrolle von Individuen, Organisationen und des Staats über die Erfassung, Speicherung, Verarbeitung und Nutzung ihrer Daten auszuüben.

Für die Einhaltung dieser Erfüllungsmerkmale ist es zudem in erster Linie entscheidend, dass sich Anbieter digitaler Lösungen **im europäischen Wirtschaftsraum angesiedelt** sind und sich dem **Zugriff des europäischen Rechtsregimes** nicht entziehen können. Keine Rolle spielt dafür hingegen das jeweilige Lizenzmodell des Anbieters, da dieses eher individuellen Ansprüchen auf der Nachfrageseite zu genügen hat.

Heimische Digitalwirtschaft in ihrer ganzen Breite nutzen

Deutschland muss dringend wieder zu wirtschaftlicher Stärke finden. Unser Wohlstand und unsere Produktivität hängen heute in bedeutendem Maße von einem starken IT-Sektor als Querschnittsindustrie zur Realisierung der digitalen Transformation ab. Wir müssen unser Land deutlich schneller digitalisieren – aber ohne uns dabei immer weiter in einseitige technologische Abhängigkeiten von Technologiekonzernen aus Übersee zu begeben. Der BITMi macht sich deshalb dafür stark, dass Deutschland die Innovationskraft seiner zahlreichen kleinen und mittelständischen Digitalunternehmen besser nutzt, um ein eigenes Angebot an Lösungen für alle wesentlichen Teile der digitalen Transformation zu schaffen. Die gute Nachricht: Auf dem Weg zu diesem Ziel können wir auf eine vielfältige und innovationsstarke Landschaft an Softwarelösungen und -anbietern zurückgreifen, um Souveränität herzustellen. **Wahr ist aber auch: Die meisten Anbieter in Deutschland sind proprietäre („Closed Source“) Hersteller** Die Mehrheit dieser Unternehmen – nach Erhebungen des BITMi sind es **etwa 85% der Anbieter** – bietet proprietäre Softwarelösungen an, die spezifisch auf die Bedürfnisse ihrer Kunden zugeschnitten sind. Diese Lösungen zeichnen sich oft durch hohe Zuverlässigkeit, vertraglich abgesicherte Wartung und umfassenden Support aus. Gleichzeitig gibt es in der deutschen Digitalwirtschaft – wenn auch zu einem deutlich geringeren Anteil – Akteure im Bereich der Open Source Software (OSS), die ebenfalls wichtige Beiträge zur technologischen Vielfalt leisten. Beide Gruppen – proprietäre und Open Source-Anbieter – sind unverzichtbar, um die digitale Infrastruktur in Deutschland zu gestalten und zu betreiben.

Klar ist deshalb aus Sicht des BITMi: Beide Ansätze – Open Source und proprietäre Modelle – können durch einen **pragmatischen**, **technologieoffenen** Ansatz einander ergänzen und erheblich dazu beitragen, das gemeinsame Ziel der digitalen Souveränität zu erreichen. Dazu braucht es ein Verständnis für die komplementären Stärken beider Ansätze und eine klare strategische Ausrichtung, die auf Zusammenarbeit setzt:

1. **Technologieoffene Beschaffungspolitik**: Der Fokus sollte darauf liegen, die besten Lösungen zu fördern – unabhängig vom Lizenzmodell. Anstatt OSS oder proprietäre Software ideologisch zu bevorzugen, sollte jede Lösung

2. anhand ihrer Fähigkeit bewertet werden, die Anforderungen an digitale Souveränität, Sicherheit und Wirtschaftlichkeit zu erfüllen.
3. **Förderung offener Standards**: Offene Standards sind eine Brücke zwischen beiden Ansätzen. Sie stellen sicher, dass Software – ob offen oder proprietär – interoperabel ist und Nutzer Wahlfreiheit behalten. Ein starker Fokus auf Standards kann verhindern, dass geschlossene Systeme isoliert oder zu monopolartigen Strukturen führen.
4. **Anerkennung der Stärken beider Ansätze**: Digitale Souveränität ist zu wichtig, um ideologisch geführt zu werden. OSS bietet Transparenz, Anpassbarkeit und Sicherheit in spezifischen Szenarien, während proprietäre Software Haftung, kommerziellen Support und Investitionen in Innovation garantiert. Beide Ansätze haben ihre Daseinsberechtigung und sollten koexistieren, um ein vielfältiges, resilientes und souveränes digitales Ökosystem zu schaffen.

Angesichts des erheblichen Rückstands bei der digitalen Transformation in nahezu allen Bereichen, ist deshalb entscheidend: Wir müssen unsere Digitalwirtschaft in ihrer ganzen Breite aktivieren, wenn wir uns aus dieser Situation herausarbeiten wollen.

Nutzen und Grenzen von Open Source im Kontext der digitalen Souveränität

Bei der Frage, inwieweit Open Source Software die digitale Souveränität stärken kann, ist es wichtig, zu differenzieren. Zweifellos bietet sie in spezifischen Kontexten klare Vorteile. Die Offenheit des Quellcodes ermöglicht Transparenz, Anpassbarkeit und prinzipiell ein erhebliches Maß an Kontrolle über digitale Infrastrukturen. Dennoch ist es essenziell, die Diskussion sachlich und differenziert zu führen, da auch OSS nicht frei von Nachteilen und Grenzen ist.

Vertreter der Open Source Community argumentieren häufig, dass der Grad an technologischen Abhängigkeiten von Anbietern aus den USA und China ein bedenkliches Ausmaß erreicht hat. Diese Analyse ist korrekt und durch Studien unterfüttert. In der Schlussfolgerung wird jedoch eine möglichst vollständige Abkehr (insbesondere bei der Digitalisierung der Verwaltung) von allen proprietären Anbietern gefordert – selbst dann, wenn diese deutsch/europäisch sind – und stattdessen eine flächendeckende Nutzung von OSS empfohlen. Als Begründung wird angeführt, dass nur OSS „echte digitale Souveränität“ ermöglicht, da proprietäre Software immer mit einer Abhängigkeit von einem privaten Anbieter einhergehe, denn nur dieser kenne den Quellcode und könne Updates bereitstellen. Auf diese Weise wird digitale Souveränität mit OSS gleichgesetzt. Diese Gleichsetzung ist problematisch, da es wie oben skizziert den größten Teil unserer mittelständisch geprägten Digitalwirtschaft ausklammert. **Fakt ist: Wir sind nicht abhängig vom proprietären Cloudanbieter aus dem Schwarzwald und werden es vermutlich nie sein – sondern von marktbeherrschenden Tech-Riesen wie Microsoft, Oracle et. al**. Wenn wir digitale Souveränität wollen und unsere Abhängigkeit von amerikanischen Großkonzernen verringern möchten, dann müssen wir unsere Digitalwirtschaft in der ganzen Breite befähigen und beflügeln – nicht nur OSS als einen geringfügigen Teil dieses Sektors.

Open Source Software vs. Closed Source Software in der Verwaltung

Ein oft genannter Vorteil von OSS ist die Möglichkeit, den Quellcode unabhängig zu prüfen und anzupassen. Dies kann besonders in der öffentlichen Verwaltung von Bedeutung sein, da hier Sicherheitsaspekte und die Anpassbarkeit an spezifische

Anforderungen eine zentrale Rolle spielen. Allerdings wird häufig übersehen, dass die Offenheit des Codes allein nicht ausreicht, um die digitale Souveränität zu gewährleisten. Es fehlt bei OSS an einer zentralen Instanz, die für Haftung und langfristige Wartung verantwortlich ist. In der Praxis müssen öffentliche Verwaltungen oft auf externe Dienstleister zurückgreifen, um Betrieb, Sicherheit und Weiterentwicklung sicherzustellen, was neue Abhängigkeiten schaffen kann – auch von kommerziellen OSS-Anbietern wie Red Hat oder SUSE.

Im Vergleich dazu bieten proprietäre Softwarelösungen klar definierte Support-Verträge und Haftungsregelungen, die gerade im staatlichen Kontext für den Staat als Kunden von Vorteil sind. Eine Sicherstellung des Zugriffs auf den Quellcodes für den Staat als Kunden, aber nicht für die Öffentlichkeit, kann bei proprietärer Software durch Quellcodehinterlegung bei Dritten Stellen (Escrow Services) wie dem TÜV problemlos ebenfalls sichergestellt werden. Beide Modelle haben ihre Stärken, und eine technologieoffene Haltung bei der Vergabe ist entscheidend, um die besten Lösungen für den jeweiligen Anwendungsfall zu finden.

Öffentliche Vergabe technologieoffen gestalten

Der Staat ist der größte IT-Einkäufer in Deutschland. Er beschafft permanent mit öffentlichen Geldern auch proprietäre Produkte – von der simplen Büroausstattung bis hin zu militärischem Großgerät. Die Forderung, für die öffentliche Verwaltung ausschließlich offene Software nach dem Grundsatz „Public Money? Public Code!“ einzukaufen, greift zu kurz und würde den Großteil der deutschen Digitalwirtschaft entscheidend benachteiligen und deren Erfindungen und Innovationen ausschließen. Diese besteht überwiegend aus mittelständischen Unternehmen, die proprietäre Software entwickeln und wichtige Beiträge zur Innovationskraft leisten. Eine technologieoffene Vergabepolitik gewährleistet, dass sowohl Open Source als auch proprietäre Lösungen gleichberechtigt berücksichtigt werden. Ziel sollte sein, die **besten** Lösungen für die jeweiligen Anforderungen zu wählen – unabhängig davon, ob sie von der Lizenzierungsseite auf Open Source oder Closed Source basieren – solange sie die digitale Souveränität stärken und der Lizenz-Anbieter sich nicht dem europäischen Rechtsraum entziehen kann.

Ein pauschaler Fokus auf OSS birgt das Risiko, dass Innovationen und wirtschaftliche Potenziale proprietärer Anbieter ungenutzt bleiben. Es ist daher essenziell, bei der Vergabe nicht nur kurzfristige Lizenzkosteneinsparungen zu betrachten, sondern auch langfristige Faktoren wie Haftung, Support und Kompatibilität mit bestehenden Systemen.

Sicherheitsaspekte beim Einsatz offener Software

Ein häufig genannter Vorteil von OSS ist die Transparenz des Quellcodes, die es ermöglicht, Schwachstellen schneller zu erkennen und zu beheben. In der Theorie erhöht dies die Sicherheit, da viele Entwickler und Sicherheitsexperten den Code prüfen können. In der Praxis kann dies jedoch auch zu neuen Herausforderungen führen. Die Offenheit des Quellcodes erlaubt auch böswilligen Akteuren, etwa Hackergruppen oder fremden Geheimdiensten, die Softwarearchitektur und Detail-

Arbeitsweise der Softwarenutzer zu sichten, potenzielle Schwachstellen zu analysieren und gezielte Angriffe vorzubereiten. Dieses Risiko ist besonders im Kontext der öffentlichen Verwaltung mit sensiblen Daten und kritischen Infrastrukturen problematisch.

Im Gegensatz dazu durchlaufen proprietäre Softwarelösungen oft umfangreiche Sicherheitsprüfungen durch den Hersteller, der zudem vertraglich verpflichtet ist,

Sicherheitsupdates oder auch Software-Quellcodehinterlegungen als Investitionsschutz für den Auftraggeber bereitzustellen. Bei OSS liegt die Verantwortung für die Sicherheit oft bei der Community oder beim Nutzer selbst, was zusätzliche personelle und finanzielle Ressourcen erfordert.

Herausforderungen bei Haftungsfragen

Ein wesentlicher Unterschied zwischen OSS und proprietärer Software liegt in der Haftung. Bei proprietären Lösungen haftet der Anbieter für die Funktionalität und Sicherheit der Software, was gerade in kritischen Bereichen wie der öffentlichen Verwaltung ein wichtiges Kriterium ist. OSS hingegen bietet keine zentrale Instanz, die für Fehler oder Sicherheitsprobleme haftbar gemacht werden kann. Nutzer müssen entweder selbst für Wartung und Sicherheit sorgen oder auf externe Dienstleister zurückgreifen, was neue Abhängigkeiten schaffen und die Betriebskosten erhöhen kann.

Diese fehlende Haftungsstruktur kann im staatlichen Kontext erhebliche Risiken mit sich bringen, da hier klare Verantwortlichkeiten gefordert sind. Eine umfassende Strategie zur Stärkung der digitalen Souveränität sollte daher die Haftungsfrage bei OSS-Projekten explizit adressieren. Soweit versucht wird, die Haftungsnachfrage im Nachgang auch bei OSS-Projekten zu regeln, folgt daraus dieselbe Abhängigkeit zum Anbieter, also zu klar definierten sogenannten „OSS-Herstellern“, wobei schon in der Wortkombination ein Widerspruch zum Verständnis des Open Source liegt, welcher oftmals im Vergleich zum Wikipedia-Ansatz als Gemeinschaftswerk von Vielen für Viele angesehen wird.

Open und Closed Source im Kontext von Interoperabilität

Ein verbreitete Fehlannahme ist, dass Interoperabilität ausschließlich durch OSS gewährleistet werden kann. Tatsächlich wird Interoperabilität primär durch die Nutzung **offener Standards** ermöglicht, die sowohl in Open Source als auch in proprietärer Software implementiert werden können. Selbst Anbieter wie Microsoft oder Adobe unterstützen ebenfalls offene Standards wie das Open Document Format (ODF) oder PDF/A, um die Zusammenarbeit mit anderen Systemen sicherzustellen. Gleichzeitig garantiert die Offenheit des Quellcodes bei OSS nicht automatisch eine bessere Interoperabilität, insbesondere wenn unterschiedliche Projekte divergierende Standards verwenden. Für die öffentliche Verwaltung sollte der Fokus daher auf der Förderung offener Standards liegen, unabhängig davon, ob die eingesetzte Software Open Source oder proprietär ist.

Digitale Souveränität: Selbstbestimmung erfordert Wahlfreiheit

Digitale Souveränität basiert letztlich auf der **Wahlfreiheit und Angebotsvielfalt**. Technologische Vorfestlegungen bieten keine tragfähigen Lösungen, um Unabhängigkeit zu erreichen. Vielmehr müssen wir die Angebotsvielfalt vergrößern und dafür sorgen, dass sowohl proprietäre als auch Open Source-Lösungen zu einem starken, wettbewerbsfähigen Markt beitragen. Die Fähigkeit, zwischen verschiedenen

Technologien und Anbietern wählen zu können, ist ein wesentlicher Faktor, um langfristig Resilienz und Unabhängigkeit zu sichern. Die digitale Souveränität Deutschlands und Europas erfordert deshalb einen ganzheitlichen Ansatz, der die gesamte Breite der technologischen Möglichkeiten einbezieht. Open Source Software ist ein wichtiger Bestandteil dieser Strategie, aber bei weitem nicht die alleinige Lösung. Proprietäre Anbieter spielen eine zentrale Rolle, insbesondere bei der Entwicklung maßgeschneiderter, sicherer und zuverlässiger Lösungen. Eine politische Bevorzugung von Open Source würde den größten Teil der deutschen Digitalwirtschaft benachteiligen und unsere Innovationskraft langfristig schwächen.

Angesichts der digitalen Rückständigkeit Deutschlands ist es dringend erforderlich, die Digitalwirtschaft in ihrer gesamten Vielfalt zu stärken. Nur durch eine technologieoffene Haltung, die sowohl proprietäre als auch Open Source-Lösungen fördert, können wir die digitale Transformation erfolgreich gestalten und unsere Souveränität sichern. Dies erfordert eine klare strategische Ausrichtung, die Innovation, Wettbewerb und wirtschaftliches Wachstum gleichermaßen fördert. Der Schlüssel liegt in einem pragmatischen, ideologiefreien Ansatz, der die besten Lösungen für die Herausforderungen der digitalen Zukunft identifiziert und unterstützt.