



**ÖFFENTLICHE ANHÖRUNG
„OPEN SOURCE“**

**STELLUNGNAHME
FREE SOFTWARE FOUNDATION EUROPE (FSFE)**

November, 2024

AM MITTWOCH, 4. DEZEMBER 2024,
14:15 - 16:15 UHR,
PAUL LÖBE HAUS



Was ist Freie Software?

Die Grundprinzipien Freier Software (auch bekannt als Open Source) sind schnell erklärt: es handelt sich um Software, die allen das Recht gibt, das Programm für jeden Zweck zu verwenden, zu verstehen, zu verbreiten und zu verbessern. Werden diese vier Freiheiten den Nutzern durch eine Lizenz gewährt, handelt es sich um Freie Software. Software hingegen, die eine oder mehrere dieser Freiheiten nicht vollständig einräumt, wird „proprietär“ genannt. Anerkannte Lizenzlisten werden von der Free Software Foundation¹ (FSF), der Open Source Initiative² (OSI) und dem Debian Projekt³ geführt.

Im Folgenden wird der Begriff „Freie Software“ verwendet, der als Synonym zu „Open Source“ gebräuchlich ist. Die Stellungnahme nimmt Bezug auf den übermittelten Fragenkatalog.

Status quo: Der Staat im Lock-In

Ein Blick auf den heutigen Stand der Digitalisierung zeigt: Verwaltungen in Deutschland und ganz Europa geraten in immer tiefgreifendere Abhängigkeiten von proprietären Softwareanbietern, oft solche aus nichteuropäischen Ländern. Allein in Deutschland werden für Software des US-Konzerns Oracle knapp 4,7 Mrd. Euro in einem einzigen Rahmenvertrag für sieben Jahre aufgewendet. Der US-Konzern Microsoft erhält über zwei Rahmenverträge 1,3 Mrd. Euro.⁴ Diese Zahlen stehen beispielhaft für tiefgreifende Abhängigkeiten, die im nächsten Jahrzehnt weiter zementiert werden, falls der Staat nicht strategisch gesteuert.

Die Abhängigkeit von einzelnen proprietären Anbietern verhindert staatliche Souveränität im Bereich digitaler Infrastrukturen. Proprietäre Software ermöglicht keine Kontrolle über die Systeme im Kern unserer digitalen Infrastruktur. Ohne den Hersteller

1 <https://www.gnu.org/licenses/license-list.html>

2 <https://opensource.org/licenses>

3 <https://wiki.debian.org/DFSGLicenses>

4 https://mdb.anke.domscheit-berg.de/wp-content/uploads/231205_KA_OpenSource-Beschaffungswesen-Antwort-BuReg_Geschwaerzt.pdf und <https://mdb.anke.domscheit-berg.de/2023/12/pressemitteilung-bund-hat-milliarden-fur-rahmenvertrage-mit-us-konzernen-aber-nur-05-prozent-fur-open-source/>



ist es unmöglich, Änderungen an der Software vorzunehmen. Gerade bei Sicherheitsvorfällen oder einem Konkurs des Herstellers wird dies zu einem kritischen Problem, einhergehend mit einer Unterminierung des Vertrauens in staatliche Handlungsfähigkeit im Digitalbereich. Aber auch im Alltag öffentlicher Verwaltungen erweist sich proprietäre Software als Hemmnis, da sie nicht den eigenen Bedarfen entsprechend angepasst werden kann. So entspricht die Software vor allem den wirtschaftlichen Bedürfnissen des Herstellers, der ggf. ganz andere Märkte im Blick hat, und nicht den strategischen und technischen Zielen der Beschaffer im öffentlichen Sektor.

Interoperabilität ist häufig nur im Produktuniversum des Herstellers gegeben. Offene Standards und offene Schnittstellen sucht man vergebens. Interoperabilität zu offenen Standards und offene Schnittstellen, die auch mit Freier Software kompatibel sind, sind nicht gegeben. Für die öffentliche Verwaltung führt das zur Abhängigkeit vom Hersteller, zum Vendor Lock-in.

Regierungen und Verwaltungen tragen Untersuchungen zufolge mit bis zu 27 % zum Umsatz von Softwareherstellern bei. Dieser Umsatz wird jedoch vorwiegend durch proprietäre Software von großen Technologieunternehmen außerhalb Europas generiert. Europäische Unternehmen, die auf Freie Software setzen, können hier einen entscheidenden Unterschied machen und mehr Eigenständigkeit ermöglichen, kommen aber mangels strategischer Beschaffung nicht ausreichend zum Zuge.

Zwar reift in Europa und in Deutschland zunehmend die Erkenntnis, dass Freie Software für die Herstellung digitaler Souveränität unverzichtbar ist, konkrete Bemühungen erfolgen jedoch bisher oft viel zu zögerlich oder bleiben ganz aus. Obwohl die Ampel-Koalition in ihrem Koalitionsvertrag das Prinzip „Public Money? Public Code!“ verankert hatte, suchte man bis zuletzt vergebens nach einer Strategie der Regierung, um Abhängigkeiten zu lösen statt zu zementieren und um digitale Souveränität herzustellen statt sie weiter zu untergraben.

Die Initiative, über das Zentrum für digitale Souveränität der öffentlichen Verwaltung (ZenDiS) Freie-Software-Alternativen für den produktiven Einsatz in der Verwaltung zur Verfügung zu stellen, ist positiv hervorzuheben. Dabei gilt es darauf zu achten, dass es sich auch tatsächlich vollständig um Freie Software ohne proprietäre Elemente handelt. Sonst besteht die Gefahr, dass eine proprietäre Abhängigkeit durch eine neue



proprietäre Abhängigkeit ersetzt wird. Zudem müssen perspektivisch auch Fachverfahren integriert werden. Diese strategische Neuausrichtung bedarf einer angemessenen Finanzierung. Statt Milliarden in Rahmenverträge für proprietäre Software von Oracle und Microsoft zu lenken, müssen die nötigen Mittel umgelenkt und zur Verfügung gestellt werden, um die Unabhängigkeit und Souveränität der öffentlichen Verwaltung herzustellen und nachhaltig zu sichern.

Die Code-Sharing-Plattform Open CoDE, ebenfalls vom ZenDiS betrieben, kann und sollte hierbei eine zentrale Rolle spielen. Auf dieser Plattform können Freie-Software Projekte für die Verwaltung zentral gesammelt, (weiter-)entwickelt und zur Verfügung gestellt werden. Auf Situationen wie während der Corona-Krise, als schnell rechtssichere, vertrauenswürdige Tools für neue unvorhergesehene Situationen, wie in dem Fall den Einsatz im Home-Office, ist man somit in Zukunft besser vorbereitet.

Der Weg zur Unabhängigkeit durch Freie Software

Um proprietären Lock-In-Effekte der Öffentlichen Verwaltung durch Freie Software erfolgreich begegnen zu können, bedarf es eines Grundverständnisses von den Möglichkeiten und Besonderheiten Freier Software. Die vier Freiheiten, die Software für jeden Zweck verwenden zu können, den Code zu verstehen und untersuchen zu können, die Software verändern und sie nach Belieben weitergeben zu können, sind grundsätzlich durch jede Freie-Software-Lizenz garantiert. Anders als bei proprietärer Software muss also kein öffentliches Geld für Nutzungslizenzen aufgewendet werden, sondern die öffentliche Verwaltung schreibt Entwicklung, Maintenance, Betrieb und Support aus oder ist in einem oder mehreren dieser Bereiche selbst aktiv.

Freie Software findet sich überall, wird überall eingesetzt und von allen vertrieben – vom Milliarden-Unternehmen über kleinste, kleine und mittlere Unternehmen, gemeinnützige Vereine, Stiftungen, öffentliche Verwaltungen bis hin zu Privatpersonen. Um die Code-Entwicklung kümmern sich vor allem mittelständische Unternehmen, Industriestiftungen und große Konzerne Hand in Hand, um Freie-Software-Komponenten in ihre Organisationen und Produkte zu integrieren, die sich dann in unseren Autos, Kühlschränken, Fernsehgeräten oder in der staatlichen Infrastruktur

wiederfinden. Dabei können alle Akteure selbst entscheiden, welche Kompetenzen sie selbst für verschiedene Komponenten aufbauen.

Öffentliche Verwaltungen im Freie-Software-Ökosystem

In diesem Geflecht muss sich die Öffentliche Verwaltung zurecht finden und agieren – in immer wieder verschiedenen Rollen, sei es als Contributor oder Maintainer, Steward oder Hersteller, Sponsor oder User. Eine enge und regelmäßige Zusammenarbeit der Öffentlichen Verwaltung sowie Entscheidungsträgern mit den relevanten Stakeholdern, insbesondere mit der Zivilgesellschaft, ist daher dringend geboten. Denn bei dem Einsatz von Freier Software gerät man schnell in Kontakt mit etablierten Entwicklern und Entwickler-Communities, die keine Marktteilnehmer sind und dennoch zum Funktionieren des Marktes beitragen. Mit diesen strategisch zu interagieren und ihre Perspektiven bei der Gesetzgebung und Regulierung zu berücksichtigen, ist in Hinblick auf eine sichere Infrastruktur von Vorteil.

So muss sichergestellt werden, dass Verantwortung bei den Herstellern und Betreibern liegt. Sie sind in der Pflicht, fair mit den entsprechenden Entwicklern und deren Communities zusammenzuarbeiten und diese auch mit den nötigen Ressourcen zu unterstützen. Gerade in Momenten, in denen sich die Öffentliche Verwaltung in einer dieser Rollen wiederfindet oder von Freier Software profitiert, müssen entsprechende Mittel langfristig und nachhaltig zur Verfügung gestellt werden, um Entwickler und deren Communities zu unterstützen.

Staatliche Akteure, die Öffentliche Verwaltung und Entscheidungsträger sind gefordert, Verständnis und Fähigkeiten auf- und auszubauen, um das Freie-Software-Ökosystem besser zu verstehen und sich daran zu beteiligen. Es wird immer wieder Konstellationen geben, in denen staatliche Stellen Teil der Projekte werden, mit diesen interagieren und kollaborieren oder sogar selbst zum zentralen Akteur werden. Im weltweiten Freie-Software-Ökosystem kooperieren verschiedene Akteure in verschiedenen Rollen, um das Funktionieren von Technologien zu gewährleisten. Diese verschiedenen Rollen tragen zur Resilienz des Systems bei und ermöglichen Unabhängigkeit, Transparenz, Sicherheit und Kontrolle.

Wer ohne Gewinnerzielungsabsicht zu Software für die Allgemeinheit beiträgt, die etwa einer sicheren Infrastruktur und damit dem Gemeinwohl dient, dem sollte auch die Möglichkeit einer Anerkennung dieser Arbeit als gemeinnützig offen stehen. Zudem



muss die Nutzbarkeit der Lösungen für die Zivilgesellschaft gefördert werden. Von der Software auf Open CoDE kann und sollte die ganze Gesellschaft Nutzen haben, zuerst das Ehrenamt – so kann beispielsweise auch der Freiwilligen Feuerwehr und dem Arbeiter-Samariter-Bund der Weg in die digitale Souveränität geebnet werden.

Digitale Souveränität

Digitale Souveränität bedeutet, Technologien eigenständig und unabhängig und sicher einzusetzen. Freie Software ist zentral, um Selbstbestimmung, Transparenz und Handlungsfähigkeit langfristig sicherzustellen. Sämtliche Ressourcen können selbst beschafft und neue Anforderungen schnell erfüllt werden. Das ZenDiS zeigt, wie innerhalb kürzester Zeit mit begrenzten Mitteln erste erfolgreiche Schritte in Richtung Aufbau digital souveräner Alternativen möglich sind. Auf Basis bestehender Freier-Software-Produkte wurde eine plattformunabhängige, vollintegrierte Alternative zu proprietären Office-Umgebungen geschaffen, die länderübergreifend ausfallsicher von deutschen Verwaltungen genutzt werden kann. Dank der Infrastruktur von Open CoDE, wo nur Freie Software zugelassen ist, steht die Software direkt zur Verfügung und ermöglicht eine rechtssichere ad-hoc Beschaffung.

Digitale Souveränität schafft staatliche Handlungsfähigkeit durch Lösungen, die weder plattform- noch gerätespezifisch sind. Elementar ist die Möglichkeit, Software unabhängig vom Hersteller, den eigenen Bedürfnissen entsprechend auf der eigenen Hardware ausführen zu können. Erste Verfahren auf Grundlage des Digital Markets Act legen offen, wie weit der Weg dahin noch ist: Nutzerinnen von Apple-Smartphones und -Tablets können keine alternativen App Stores installieren, da Apple als Gatekeeper auftritt. Vergleichbare Lock-ins gibt es in proprietären Ökosystemen in großer Zahl. Konsequenz auf Offene Standards, Offene Schnittstellen und Freie Software zu setzen ermöglicht, diese Lock-ins zu vermeiden und zu umgehen.

Dieses Vorgehen ist entscheidend für Interoperabilität – innerhalb der Öffentlichen Verwaltung aber auch in der Kooperation mit externen Dritten. Es ermöglicht den reibungslosen Austausch von Daten, verbessert die Zusammenarbeit zwischen Einrichtungen, mit internationalen Partnern und entlastet auch Drittorganisationen und alle Nutzer digitaler Technologie. Anwendungen und Apps müssen plattformunabhängig zur Verfügung gestellt werden, so dass diese ohne Abhängigkeiten

zu proprietären Anbietern ausgeführt und genutzt werden können, und ohne, dass deren allgemeinen Geschäftsbedingungen oder zusätzlichen Nutzungsaufgaben wie etwa der Preisgabe personenbezogener Daten zugestimmt werden muss.

Transparenz und Vertrauen

Vertrauen in Technik spielt eine bedeutende Rolle bei der Digitalisierung, um die Akzeptanz bei den Menschen im Land zu ermöglichen. Nachvollziehbarkeit, Sicherheit und besonders der Schutz personenbezogener Daten, die durch den Staat verarbeitet werden sollen, sind ausschlaggebend für die Entscheidung der Menschen, ob sie eine Technologie nutzen oder nicht. Transparenter Code macht nachvollziehbar, wie rechtliche Vorgaben im Bereich des Datenschutzes umgesetzt werden, und ermöglicht dadurch, dieses Vertrauen herzustellen. Anwendungen, die in der staatlichen Infrastruktur oder etwa von Ermittlungs- und Militäreinrichtungen eingesetzt werden, müssen unter der eignen Kontrolle stehen. Freie Software ermöglicht eine bessere Steuerungsfähigkeit im IT-Bereich und stärkt dadurch die Resilienz staatlicher IT-Infrastrukturen.

Resiliente Lieferketten

Da der Zugang zu Freier Software offen gestaltet ist, ist sie entsprechend weit verbreitet. Lieferketten können schnell unübersichtlich werden, was Sicherheitsprobleme mit sich bringen kann. Die schiere Massen an Projekten führt dazu, dass immer wieder Projekte oder Teile von Projekten in neuen, weiteren Projekten aufgehen, die wiederum in Abhängigkeiten zu anderen Projekten stehen. Sicherheitslücken können dann durch unterschiedliche im Umlauf befindliche Versionen schwer zu identifizieren sein. Zudem können Abhängigkeiten von Projekten auftreten, die nicht mehr oder nicht den Bedürfnissen entsprechend gepflegt werden.

Um dieser Herausforderung zu begegnen hat sich FSFE bereits zum Beginn der Debatte um den Cyber Resilience Act (CRA) dafür eingesetzt, die Gesetzgebung entsprechend dieser Realitäten auszurichten. Die entsprechende Ausnahme und Einführung der Steward-Rolle trägt dem Rechnung. Nun gilt es in der Implementierung, entsprechend zielgenau überall dort zu unterstützen, wo Unterstützung nötig ist, und an den Stellen Unterstützung einzufordern, wo Akteure auf den Vorleistungen Dritter, die nicht Hersteller sind, aufbauen und davon profitieren. Dies liegt auch im eigenen Interesse, da sich der Staat selbst in verschiedenen Rollen wiederfinden wird, etwa über das ZenDiS in der Steward-, aber auch Manufacturer-Rolle. Zudem wird die vorgeschriebene Software



Bill of Materials (SBOM) mehr Aufschluss über Abhängigkeiten geben, die dann gezielt adressiert werden müssen. Insbesondere die Umsetzungsphase des CRA wird daher von entscheidender Bedeutung dafür sein, wie die Freie-Software-Landschaft künftig aussieht und welche Rolle Deutschland und Europa darin einnehmen werden. Ziel muss sein, diejenigen zielgenau in die Pflicht zu nehmen, die signifikant von Freier Software profitieren, während Alternativen, die Souveränität, Unabhängigkeit und Kontrolle garantieren, auch von staatlicher Seite sowie vom Markt selbst unterstützt werden.

Sicherheit durch Freie Software

Freie Software ist nicht per se sicherer als proprietäre Software, bietet im Vergleich zu letzterer aber viele Möglichkeiten, um Produkte deutlich sicherer zu gestalten. So besteht die Möglichkeit, den Code auch extern ohne Vertragsschwierigkeiten oder Abhängigkeiten untersuchen und ändern zu lassen – bedarfsweise auch ohne Rückfrage beim Hersteller oder Verkäufer. Das Recht, die Software den eigenen Bedürfnissen entsprechend anzupassen, umfasst natürlich auch das Identifizieren und Schließen von Sicherheitslücken, jeweils ohne Abhängigkeiten. Dass der Code öffentlich ist und Entwickler sich mit guter Arbeit einen Namen über ihr Projekt hinaus machen können, ist auch die Qualität und Dokumentation des Codes bei Freier Software oft deutlich besser als in proprietären Produkten. So sind Neuerungen des Herstellers besser überprüfbar, und es kann verhindert werden, dass ein Hersteller ungewollte Funktionen eingeschleust. Das Konzept „Security through Obscurity“ ist durch entsprechende Skandale hinreichend widerlegt.

Gleichwohl führt die Offenheit Freier Software auch immer wieder zu Abspaltungen. Diese sogenannten „Forks“ in Freie-Software-Projekten sind weder ungewöhnlich noch Anlass zur Sorge, sondern ermöglichen Agilität, Innovation und Wettbewerb. Gleichwohl gibt es Forks, die von den Freiheiten Freier Software profitieren und diese für wenig freiheitliche Ziele einsetzen. Nach der Abspaltung des Verschwörungs- und Hasspropagandanetzwerk „truth.social“ vom restlichen Fediverse entschieden sich viele andere Fediverse-Serverbetreiber gegen eine Integration mit diesem Netzwerk und gegen die Zusammenarbeit auf technischer Ebene. Auch skurrile Linux-Distributionen aus Russland müssen – und sollten – nicht in Deutschland oder Europa eingesetzt

werden, entsprechender Code sollte nicht in hiesigen Unternehmen und öffentlichen Verwaltungen zur Anwendung kommen.

Gleichzeitig müssen Entwickler-Communities, die für Code-Sicherheit sorgen, unterstützt werden. Dies wird nur über die Zusammenarbeit mit diesen Communities sowie mit zivilgesellschaftlichen Akteuren gehen. Wie schnell und robust diese auch in Krisenzeiten agieren können, wenn die nötige Ressourcen zur Verfügung stehen, hat man nicht zuletzt in der Corona-Krise gesehen. Entsprechende beratende und mitentscheidende Gremien, wie etwa ein Open-Source-Advisory-Board, müssen entsprechend balanciert besetzt werden. Es dürfte zudem hilfreich sein, nachhaltige Gesprächskanäle zu den verschiedenen Akteuren aufzubauen und diese zu unterstützen. Dabei gilt es, deren etablierte Arbeitsweisen und Strukturen besser zu verstehen und sich anzupassen, um Reibungsverluste zu vermeiden.

Erfolgreiche Arbeitsweisen aus der IT-Security können hier auch leiten: Schwachstellenmanagement wird international mit Hilfe von Freier Software begegnet. Projekte wie MISP des Luxemburgischen CERT CIRCL verdeutlichen Arbeitsweisen und die Relevanz von Freier Software im Bereich IT-Security.

Wenn die Implementierung des CRA durch reformierte Beschaffungsvorgaben und einen Fonds zur Unterstützung Freier Software flankiert wird, bietet sie gute Möglichkeiten, eine resiliente, souveräne Infrastruktur mit vergleichsweise geringem Aufwand zu realisieren.

Herausforderung Openwashing

Rund um die Ausschreibung und den Einsatz von Freier Software kommt es immer häufiger zu Fällen von Openwashing. Openwashing bezeichnet eine Reihe von Praktiken und Strategien, durch die Unternehmen, Organisationen oder Projekte den irreführenden Anschein erwecken, Freie Software zu entwickeln, anzubieten oder auf andere Weise zu unterstützen. Es handelt sich um eine Form des Etikettenschwindels zur Erzielung von Marktvorteilen. Oft wird diese Praxis auch von Lobbyisten genutzt, um Interessen zu verschleiern und Vorteile in der Gesetzgebung und Regulierung zu erhalten.

Openwashing ist eine Herausforderung für die Kontrollierbarkeit technische Infrastrukturen und dadurch auch für öffentliche Verwaltungen. Openwashing



verwässert die klare Definition von Freier Software und erweckt den Anschein von Offenheit und Kontrolle, während es die Abhängigkeit von proprietären Systemen und Herstellern verstärkt. Dies widerspricht dem Ziel digitaler Souveränität und stiftet Verwirrung um diesen Begriff.

Öffentliche Verwaltungen und IT-Dienstleister sind gefordert, die Bedeutung von Freier Software für digitale Souveränität zu verstehen und vorbildhaft zu agieren, indem sie eigenes Openwashing vermeiden. Wird mit öffentlichen Mitteln Openwashing unterstützt, unterminiert das nicht nur digitale Souveränität, sondern schadet dem Vertrauen der Menschen in staatliches Handeln und in die Demokratie.

Verwaltungen müssen in der Lage sein, Freie Software von proprietären Lösungen unterscheiden. Dazu bedarf es rechtlichen und technischen Fachwissens bzw. guter Beratung z.B. durch ZenDiS. Fehlentscheidungen zugunsten vermeintlich offener Lösungen führen zu Abhängigkeiten, höheren Kosten und eingeschränkter Kontrolle. Sie schaden dem Vertrauen in Freie Software, verursachen langfristige Mehrkosten für Steuerzahler und erschweren die effiziente Haushaltsprüfung.

Behörden und Regierungen sollten durch den Austausch mit zivilgesellschaftlichen Akteuren zu Themen wie Freie-Software-Beschaffung, Lizenzrecht und Openwashing Kompetenzen aufbauen und dieses Wissen in öffentliche Verwaltungen transferieren. Die Etablierung verlässlicher Infrastrukturen wie Open CoDE kann zusätzliche Sicherheit bieten. Es sollten Ausschreibungskriterien entwickelt werden, die Openwashing sanktionieren und problematische Akteure frühzeitig erkennen lassen. Im gesamten Vergabeverfahren sollte Openwashing als problematische Praxis mitgedacht und z.B. auch die Marktposition, Kommunikation und bisheriges Verhalten von Bietenden berücksichtigt werden. Vergaben sollte stets darauf abzielen, Wechselfähigkeit sicherzustellen. Monitoring von Openwashing-Fällen und die Erleichterung von Whistleblowing ermöglichen Transparenz und Lerneffekte.

Um Missverständnisse zu vermeiden sollte der Staat daher von Openwashern häufig genutzte Formulierungen wie „Enterprise Edition“, „enterprise-fähig“ usw. vermeiden und Freie Software eher unter dem Begriff „verwaltungs-ready“ den Behörden und Einrichtungen verfügbar machen.

Public Money? Public Code!

Viele der angesprochenen Vorteile lassen sich nutzen und die meisten der angesprochenen Herausforderungen lassen sich lösen, wenn künftig anders beschafft wird – strategisch mit dem Ziel, digitale Souveränität durch Freie Software zu befördern. Das Prinzip „Public Money? Public Code!“ ist dabei als Leitlinie zu verankern: Mit öffentlichen Geldern beschaffter Code muss unter einer Freie-Software-Lizenz, etwa über Open CoDE, zur Verfügung gestellt werden. Statt sich immer weiter in die Abhängigkeitsspirale gegenüber einzelnen Anbietern zu begeben, muss Freie Software beschafft werden. Es gilt, Software zu beschaffen, die den eigenen Bedürfnissen entsprechend angepasst werden kann und welche die vollständige Kontrolle digitaler Infrastrukturen ermöglicht – auch langfristig. Wenn Software beschafft wird, die nicht diesen Kriterien entspricht, muss dies entsprechend schriftlich und öffentlich begründet sowie vom Rechnungshof überprüft werden. Durch das Bereitstellen der Software auf Open CoDE kann zudem ad-hoc und ohne großen Vergabeprozess Software beschafft, an eigene Bedürfnisse angepasst und eingesetzt werden. Dies hilft nicht nur, die Handlungsfähigkeit der Verwaltung auch in (IT-)Krisen herzustellen und zu erhalten, sondern unterstützt ebenso einen Bürokratieabbau im öffentlichen Beschaffungswesen.

Kollaborationen können grenzüberschreitend für den Aufbau digital souveräner Alternativen genutzt werden und mittel- bis langfristig Kosten sparen. Freie Software orientiert sich an den Nutzenden – statt proprietäre Software voller Sonderlocken zu beschaffen, welche im Einsatz durch die Öffentliche Verwaltung gar nicht gebraucht werden, kann durch die Beschaffung Freier Software den eigenen Bedürfnissen und Ansprüchen zielgenau entsprochen werden.

Bei der Implementierung des Interoperable Europe Act, aber auch bei der Reform des Beschaffungswesens wird es darum gehen, Prozesse und Regulierungen so aufeinander abzustimmen, dass sie tatsächlich Interoperabilität über offene Standards und Schnittstellen ermöglichen und dem Ökosystem Freie Software nicht schaden. Sichere, innovative Technik entsteht durch Kollaboration und Kooperation.

Es braucht ein adaptiertes Rollenverständnis der Verwaltung, dass die eigenen Nutzenden in Blick hat und Beschaffungen nutzt, um so Abhängigkeiten schrittweise aufzulösen. Vorhandene finanzielle Mittel werden gezielt in Freie Software gelenkt und haben dadurch einen nachhaltigen Effekt für Innovation, für den IT-Standort Europa,



aber auch für die Allgemeinheit. Darüber hinaus sollten Migrationspläne hin zu Freier Software unter strategischen Gesichtspunkten erstellt, Alternativen aufgebaut und ausgerollt werden. Nutzende sind über Open CoDE einzubinden.

Nicht zuletzt stärkt und verbessert der Aufbau von Alternativen die Verhandlungsposition öffentlicher Verwaltungen im Beschaffungsprozess – auch gegenüber großen Unternehmen, die bisher eine beherrschende Marktstellung innehatten und diese zur Preisbildung nach ihren Vorstellungen genutzt haben.

Freie Software als Chance für die Gesellschaft

Die konsequente Verfolgung des Ziels „Public Money? Public Code!“, eine zielgenaue Implementierung des IEA und des CRA sowie die Bereitstellung von Ressourcen für Freie Software haben neben den genannten direkten Vorteilen Spill-Over-Effekte, die positiv für Staat, Wirtschaft und Gesellschaft sind. Neben dem Aufbrechen von innovationshemmenden Marktkonzentrationen und der damit gewonnenen Unabhängigkeit, die allen Marktteilnehmern zu gute kommt, werden auch Grundrechte gestärkt. Resiliente Software, der vertraut werden kann, hilft Journalisten in ihrer praktischen Arbeit, lässt Transparenz und Kontrolle zu, um die Einhaltung rechtlicher Vorgaben, etwa im Bereich Privatsphäre und Datenschutz zu sichern. Freie Software kann Partizipation im digitalen Zeitalter ermöglichen und unterstützen, beispielsweise durch entsprechende Anwendungen, die Menschen in Entscheidungsprozesse besser einbinden wie Consul oder Decidim, oder durch den gezielten Abbau von Barrieren und durch inklusive Gestaltung von Programmen und Diensten. Gerade solche Projekte bedürfen der Unterstützungen, auch über bisher unkonventionelle Wege wie beispielsweise in der der Stadt München, die Projekte über Sponsoring unterstützt.

Nachhaltige Bildung für die Fachkräfte von morgen

Studien zeigen zudem, dass durch das konsequente Beschaffen von Freier Software die Anzahl von Firmengründungen und Beschäftigten in dem Bereich ansteigt, insbesondere bei Kleinen und mittleren Unternehmen in der Region. Neben der Stärkung des Mittelstands stärkt Freie Software Innovationen und Forschung und ermöglicht vor allem jungen Menschen früh des Erwerb tiefgreifenden technischen Sachverstandes und einen selbstbestimmten Umgang mit Technik. Gerade im Bildungsbereich gilt es, statt



Produkttrainings den grundlegenden Umgang mit Technik, dahinterliegende Konzepte sowie die Möglichkeiten der Gestaltung von Technologie zu vermitteln, um schon früh Interesse zu wecken und Kompetenzen zu schulen und so dem Mangel an qualifizierten Fachkräften nachhaltig zu begegnen. Zu verhindern ist, dass Schülerinnen und Schüler durch Vorgaben und proprietäre Software an Schulen in die Ökosysteme proprietärer Hersteller mit ihren Beschränkungen und Lock-In-Effekten gezwungen werden. Es muss möglich sein, für schulische Aufgaben die Software der eigenen Wahl zu verwenden, ohne proprietäre Nutzungslizenzen akzeptieren zu müssen und ohne an der Installation alternativer Freie-Software-Anwendungen gehindert zu werden, welche die Produktivität steigern und Lerneffekte verbessern können. Schulen sind bei der Umsetzung einer künftigen Digitalbildungsstrategie, die Freie Software als Arbeitsmittel nutzt und auf den souveränen Umgang mit Technik abzielt, zu unterstützen. Auch außerschulische Lernangebote dieser Art sollten in Hinblick auf den Fachkräftemangel, gerade auch im kommunalen Bereich, gefördert werden.