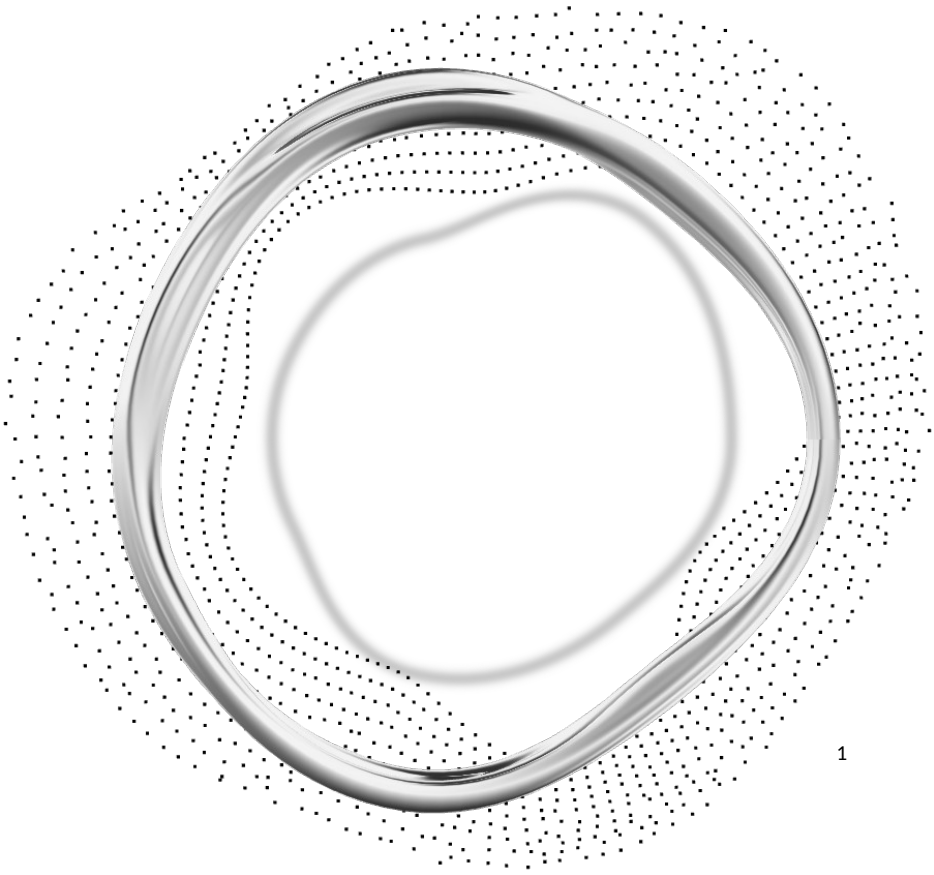
Stellungnahme Anhörung „Open Source“ im Ausschuss für Digitales

Jutta Horstmann, Vorsitzende der Geschäftsführung des Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS), 04.12.2024



1. Vorbemerkung

Alltag, Freizeit, Gesundheit, Beruf: Ohne digitale Technologien wäre das Leben, wie wir es heute kennen, nicht möglich.

Was viele nicht wissen: **Immer häufiger sind es quelloffene Lösungen, die im Hintergrund dafür sorgen, dass Digitalisierung funktioniert.** So basiert beispielsweise nahezu die gesamte Software-Infrastruktur des Internets auf Open Source. Auch aus der Wirtschaft ist Open Source nicht mehr wegzudenken. Zahlreiche große Unternehmen, darunter z.B. Mercedes Benz, bekennen sich offen zur Nutzung von Open Source und tragen aktiv zu Open-Source-Projekten bei.

Damit verglichen hinkt die Verwaltung beim Einsatz von Open Source deutlich hinterher. Der Großteil der öffentlichen IT-Investitionen geht nach wie vor in proprietäre Lösungen, die meist von wenigen Tech-Konzernen aus Übersee kommen. Über die Jahre sind auf diese Weise kritische Abhängigkeiten entstanden, die die Digitale Souveränität unseres Staates und seine Handlungsfähigkeit – und damit letztlich die Daseinsvorsorge – gefährden. Besonders stark sind die Abhängigkeiten im Bereich des PC-Arbeitsplatzes sowie bei Datenbank- und Virtualisierungslösungen. Bei Cloud-Technologien und KI können vergleichbare Abhängigkeiten durch den bewussten Einsatz offener Lösungen und Modelle noch verhindert werden.

Um kritische Abhängigkeiten aufzulösen und dem Staat die Kontrolle über seine IT wiederzugeben, erklärte der **IT-Planungsrat 2021 die Stärkung der Digitalen Souveränität zum gemeinsamen Ziel von Bund, Ländern und Kommunen** (Beschluss: Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung). Als wesentlicher Hebel wurde „ein **vermehrter Einsatz von Open-Source-Software** (OSS)“ identifziert.

Die Verwaltung bei diesem Wandel zu befähigen, ist eine der Kernaufgaben des **Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS)**, das 2022 von Bundesministerium des Innern und für Heimat (BMI) gegründet wurde. Als Kompetenz- und Servicezentrum informiert das ZenDiS, baut Wissen auf und befähigt die Verwaltung, Open-Source-Lösungen zu beschaffen, zu teilen und zu betreiben – vieles davon geschieht über die

Plattform openCode. Zudem verschafft das ZenDis der Verwaltung einen einfachen Zugang zu modernen, leistungsfähigen und skalierbaren Open-Source-Lösungen, die gemeinsam mit der Wirtschaft entstehen und bereitgestellt werden und die Bedarfe der öffentlichen Hand in besonderem Maße erfüllen (Beispiele: openDesk, openConference). Die Verwaltung kann diese i. d. R. über eine Inhouse-Vergabe ohne Ausschreibung beziehen.

2. Zu den Fragen

Frage 1) Welche Vor- und Nachteile hat Open Source-Technologie allgemein und besonders im Hinblick auf technische, sicherheitsrelevante, konzeptionelle, soziale, finanz-, außenpolitische und gesellschaftliche Aspekte? Welche der genannten Vor- und Nachteile kommen besonders zum Tragen, wenn Open Source-Technologien im staatlichen Kontext eingesetzt werden?

Antwort auf Frage 1) Open-Source-Lösungen bieten zahlreiche **Vorteile**, die sich nicht nur auf Wirtschaft und Gesellschaft, sondern gerade auch im staatlichen Kontext positiv auswirken. Sie zeichnen sich durch freie Nutzung, Anpassung und Verbreitung aus, fördern Innovation und unterstützen Transparenz. Ein wesentlicher Vorteil ist die Unabhängigkeit von Anbietern und die damit einhergehende Stärkung der Digitalen Souveränität.

Technisch überzeugt Open Source durch offenen Code, der Sicherheitsprüfungen durch unabhängige Expert:innen ermöglicht („security by transparency“). Schwachstellen können schneller erkannt und behoben werden, was ein schnelles Reagieren auf Sicherheitsvorfälle ermöglicht und damit hohe Sicherheitslevel unterstützt.

Neben den Vorteilen im Bereich Cybersecurity gibt es weitere sicherheitsrelevante Vorteile von Open-Source-Software. Sie **schützt die Bürger:innen** nachprüfbar vor dem Abfließen von Daten an ausländische Akteure und Regierungen und vor der Kompromittierung ihrer Grundrechte (z. B. freie Wahlen) durch Einflussnahme aus dem Ausland.

Gleichzeitig **schützt sie auch die Öffentliche Verwaltung** vor der Einflussnahme durch ausländische Akteure, indem die (Androhung von) Abschaltung von für das Verwaltungshandeln relevanten digitalen Lösungen kein Druckmittel mehr darstellt.

Die Stärken von Open Source zeigen sich daher auch in der **Wechselfähigkeit**: Der Staat wird nicht an ein einzelnes Unternehmen gebunden (kein Vendor-Lock-in), kann flexibel auf Marktveränderungen reagieren und Systeme an spezifische Anforderungen anpassen.

Open Source ermöglicht **Nachnutzung**: Einmal entwickelte Lösungen können innerhalb der Verwaltung und sogar föderal übergreifend geteilt und gemeinsam weiterentwickelt werden. Diese Synergien steigern die Effizienz, erhöhen das Tempo bei der Verwaltungsdigitalisierung und verhindern teure Mehrfachentwicklungen.

Auch **gesellschaftlich und sozial** bringt Open Source Vorteile: Die Transparenz gegenüber Bürger:innen stärkt das **Vertrauen in staatliche IT-Lösungen**, da diese überprüfbar und nachvollziehbar sind. Spätestens beim Einsatz von KI in der Verwaltung wird dies eine entscheidende Rolle spielen. Gleichzeitig bieten der offene Quellcode und die freie Verfügbarkeit eine Chance für lokale Unternehmen und Entwickler:innen, Innovationen beizusteuern, wodurch die **heimische Wirtschaft gefördert** wird und ein breiterer gesellschaftlicher Mehrwert entsteht.

Darüber hinaus stärkt Open Source die Position Deutschlands in der **Außenpolitik**. Sie löst Abhängigkeiten und damit **Erpressungspotenziale** auf und ist in der Lage, kritische Szenarien in Bezug auf den Zugang zu digitalen Technologien wirksam zu verhindern. Dass einseitige Abhängigkeiten nicht nur in der Theorie entsprechende Risiken bergen, wissen wir spätestens seit dem Angriffskrieg Russlands auf die Ukraine und den damit einhergehenden Engpässen bei der Gasversorgung in Deutschland.

Ein weiterer außenpolitisch relevanter Aspekt ist, dass die kollaborative Entwicklung, der Austausch und die Nachnutzung von Open-Source-Software die **europäische Zusammenarbeit** fördern und die Digitale Souveränität Europas insgesamt stärkt.

Die größte **Herausforderung** liegt in der **unzureichenden Finanzierung** kritischer Open-Source-Infrastrukturkomponenten. Dies betrifft am Ende Open-Source-Lösungen genauso wie auch proprietäre Software, da auch proprietäre Lösungen vielfach auf Open-Source-Komponenten basieren. Der Staat könnte hier durch gezielte Förderung eine stabilisierende Rolle übernehmen. Der Grundstein hierzu wurde bereits mit der Einrichtung der Sovereign Tech Agency gelegt, die gezielt in kritische Komponenten investiert.

Frage 2) Welche Voraussetzungen und Infrastrukturen braucht der erfolgreiche Einsatz von Open Source-Technologien im staatlichen Kontext?

Antwort auf Frage 2) Neben einer entschiedenen Open-Source-Strategie, verlässlichen politischen und rechtlichen Rahmenbedingungen und einer nachhaltigen Finanzierung bedarf es vor allem einer **zentralen Koordination, eines Wissensaufbaus und einer Befähigung**.

Die Voraussetzungen hierfür wurden mit der Gründung des **ZenDiS** geschaffen. Als zentrales Service- und Kompetenzzentrum befähigt das ZenDiS sowohl Bund, als auch Länder und Kommunen bereits heute zum erfolgreichen Einsatz von Open Source und baut wertvolles Wissen auf.

Das ZenDiS **berät** zu Ausschreibungen und Lizenzen, etabliert Best Practices und bietet der Verwaltung einen niedrigschwelligen Zugang zu professionellen **Open-Source-Anwendungen**, wie beispielsweise die Office & Collaboration Suite openDesk oder eine souveräne Videokonferenzlösung, die bestehende, unsichere Systeme im Bund ablösen wird. Hierzu fördert das ZenDiS die Zusammenarbeit zwischen Staat und Open-Source-Anbietern und ermöglicht so einen schnellen Zugang zu Innovationen (mehr zum Thema Innovation in unserer Antwort auf Frage 14).

Die vom ZenDiS im Auftrag des IT-Planungsrats bereitgestellte und betriebene **Plattform openCode** dient als zentraler Ort für Kollaboration, Wissensvermittlung und Beratung. Sie bildet einen rechtssicheren Rahmen für die Zusammenarbeit von Verwaltungseinrichtungen an gemeinsamen Open-Source-Projekten – und dies auch föderal übergreifend –, bietet Entwicklungswerkzeuge, Compliance-Checks sowie ein Lizenzclearing. Mehr als 5.000 Nutzende machen davon bereits heute in rund 2.000 Projekten Gebrauch.

Ein weiterer zentraler Hebel ist das **Vergaberecht**: Bestehende Gesetze im Bereich eGovernment und Beschaffung müssen so ausgestaltet sein, dass es perspektivisch eine **Verpflichtung (Muss) zum Einsatz quelloffener Technologien** gibt. Da dies nicht sofort realisierbar ist, sollte für eine Übergangsperiode ein klarer **Open-Source-Vorrang** kodifiziert werden. Mit dem OZG 2.0 wurde hier bereits ein wichtiger Schritt getan. Allerdings entfaltet das OZG keine Wirkung auf die interne IT des Staates, wo jedoch die kritischsten

Abhängigkeiten und damit die höchsten Risiken in Bezug auf Digitale Souveränität bestehen. Um dies zu ändern, braucht es eine Novellierung des Vergaberechts mit einem klaren Open-Source-Vorrang, der im derzeitigen Referentenentwurf für das **Vergabetransformationspaket** leider nicht angelegt ist.

Mehr Rechtssicherheit bei der Beauftragung bzw. Nutzung von Open-Source-Leistungen böten darüber hinaus speziell auf diesen Fall zugeschnittenen **EVB-IT**. Vorschläge zu deren Ausgestaltung liegen bereits seit Längerem vor, die entsprechende EVB-IT-Novelle steht jedoch noch aus.

Das **ZenDiS** spielt eine entscheidende Rolle für einen erfolgreichen Umstieg der Öffentlichen Verwaltung auf Open-Source und benötigt daher eine langfristige Finanzierung unabhängig von der jährlichen Haushaltsplanung. Darüber hinaus müssen innerhalb der ÖV Mittel nicht nur für die Einführung von Open-Source-Software, sondern auch für die langfristige Wartung und Weiterentwicklung bereitgestellt werden.

Zudem sollte ein **fixer Prozentsatz der Mittel für öffentliche IT-Projekte an Open Source** gebunden sein, um den Anteil offener Lösungen auf Basis offener Standards und Schnittstellen und damit auch die Interoperabilität und die Wechselfähigkeit innerhalb der Verwaltungs-IT insgesamt zu erhöhen und Integrationsaufwände perspektivisch zu reduzieren. Langfristiges Ziel muss ein Open-Source-only-Ansatz sein.

Frage 3) Können Sie Beispiele für Open Source-Projekte nennen, die in den vergangenen Jahren besonders zum Gemeinwohl beigetragen haben und welche Erfolgsfaktoren und Best Practices lassen sich aus diesen Projekten ableiten?

Im Gegenzug: Woran scheitern Open Source-Projekte und Projekte, die auf Open Source-Technologien aufbauen häufig? Welche Fallstricke sehen Sie?

Antwort auf Frage 3) Open Source-Projekte tragen weltweit erheblich zum Gemeinwohl bei. Sie fördern Transparenz, Sicherheit und den Zugang zu Technologien und Wissen und standen im Juli dieses Jahres entsprechend im Mittelpunkt einer eigens zum Thema Open Source und Gemeinwohl („OSPOs for Good“) organisierten Konferenz der Vereinten Nationen, zu deren Erfolg das ZenDiS wesentlich beitrug.

Wikipedia ist sicherlich das prominenteste Beispiel. Die größte freie Enzyklopädie der Welt macht Menschen in aller Welt unabhängig von ihrer Herkunft und finanziellen Mitteln Wissen frei zugänglich. Etwa eine Milliarde Aufrufe pro Monat verzeichnen allein deutschsprachige Wikipedia-Einträge. Ihr Erfolg basiert auf der kollaborativen Arbeit von Freiwilligen und einer klaren Governance, die aus einem Regelwerk und einem offenen, aber moderierten Beitragssystem besteht.

Server, Supercomputer, mobile Geräte und nahezu die gesamte Internet-Infrastruktur basieren heute auf dem **Open-Source-Betriebssystem Linux**. Erfolgsfaktoren sind eine starke Entwickler:innen-Community, der modulare Aufbau und kontinuierliche Innovation durch Beiträge (Contributions) von Einzelpersonen, aus Wirtschaft und Institutionen.

Projekte wie der **Tor-Browser, Signal und GnuPG** spielen eine zentrale Rolle bei sicherer Kommunikation und dem Schutz von Demokratien. Sie ermöglichen anonymes Surfen und schützen Menschen in repressiven Regimen oder Journalist:innen und Whistleblower vor Überwachung und Verfolgung. **Erfolgsfaktoren** sind ein klarer Fokus auf Sicherheit und Datenschutz, die konsequent offenen Entwicklung, ein großes Community-Engagement und Vertrauen durch Audits.

Android ist ein weiteres Beispiel. Das Open-Source-Betriebssystem hat einen Markt für mobile Open-Source-Derivate ermöglicht, darunter auch die Entwicklung des FairPhones.

Gemeinsame **Erfolgsfaktoren** sind: Klare Zielsetzung und Governance, Transparenz und Offenheit, starke Communities, nachhaltige Finanzierung sowie technologische Exzellenz.

Zu den größten **Hemmnissen** zählen Rechtsunsicherheiten v. a. in Bezug auf Lizenzen.

Mit seinen Angeboten agiert das **ZenDiS** entlang dieser Best Practices und ermöglicht Akteur:innen innerhalb der ÖV die Überwindung von Hemmnissen.

So entsteht die Office & Collaboration Suite **openDesk** in einem co-kreativen Prozess mit einer professionellen Anbieter- und Entwickler:innen-Community. Das Projekt folgt einer klaren Zielsetzung – der Auflösung kritischer Abhängigkeiten in der Verwaltung beim PC-Arbeitsplatz – und zeichnet sich durch eine klare Governance und Steuerung aus, in deren Zentrum jeweils das ZenDiS steht. Die Finanzierung wird sowohl durch beauftragte Entwicklungs- und Anpassungsleistungen, als auch durch Subscriptions – also

Nutzungsentgelte – abgesichert.

openDesk ist eines der derzeit rund 2.000 Projekte, die bereits auf **openCode** entwickelt werden. Es nutzt die Plattform als Entwicklungsinfrastruktur und rechtssicheren Rahmen für die Zusammenarbeit zwischen Staat und Anbieter-Ökosystem. Ein zentraler gesellschaftlicher Nutzen von openCode ist die freie **Nachnutzung** von Lösungen innerhalb der Verwaltung, aber auch darüber hinaus. Damit kommen staatliche Investitionen gemäß dem Grundsatz „Public Money, Public Code" wieder der Gesellschaft zugute.

openDesk zeigt, dass das Interesse daran erheblich ist. Die Lösung wird nicht nur von Ministerien und weiteren Behörden nachgefragt, sondern auch von zahlreichen NGOs, Bildungseinrichtungen, Unternehmen und Vereinen, die sich eine offene, souveräne Arbeitsplatz- und Kollaborationslösung wünschen.

Frage 4) Für wie relevant halten Sie das Problem des „Open-Washings", in Anlehnung an „Greenwashing", also vermeintliche Open Source Entwicklung, die dann schlussendlich doch wieder in proprietärem Code endet? Welche anderen Probleme sehen Sie bei der Entwicklung von Open Source Technologien?

Antwort auf Frage 4) Mit zunehmender Popularität von Open-Source-Software gewinnt auch das Problem des „Open-Washings" an Bedeutung. Konkret äußert sich dies darin, dass Unternehmen **Open Source als Marketinginstrument** nutzen, ohne echte Offenheit und die damit einhergehenden Vorteile von Transparenz, Nachnutzung und dem freien Zugang zu Innovationen zu bieten. Zudem entstehen auf diesem Weg neue Abhängigkeiten.

Ein ähnliches Phänomen ist das **„Souveränitäts-Washing"** insbesondere im Zusammenhang mit Cloud-Angeboten.

Die vom ZenDiS betriebene Plattform **openCode** ist der Schlüssel, um Open-Washing bei öffentlichen Open-Source-Projekten wirksam zu verhindern. Durch Unterstützung beim „Open-Source-Stellen" und Lizenzclearing gelangen nur Projekte auf die Plattform, die die Kriterien an echtes Open Source erfüllen.

Darüber hinaus **berät das ZenDiS die ÖV** bei der präzisen Formulierung von Open-Source-

Ausschreibungen und plant die Bereitstellung eines **Souveränitätschecks**, mit dem öffentliche Auftraggeber ihre Projekte automatisiert entlang klarer Souveränitätskriterien überprüfen können.

Frage 5) In welchem Zusammenhang stehen Open Source-Technologien und Fragen der digitalen Souveränität und wäre eine Bevorzugung von Open Source-Technologien in diesem Zusammenhang erstrebenswert – wo liegen konkret die Chancen und Risiken?

Antwort auf Frage 5) Open Source ist das effektivste Werkzeug zur Erreichung der Souveränitätsziele der Öffentlichen Verwaltung.

Im Gegensatz zu proprietären Systemen ermöglichen Open-Source-Lösungen **Wechselfähigkeit, Gestaltungsfähigkeit und Einflussnahme** und stellen damit eine nachhaltige Handlungsfähigkeit der Verwaltung in ihren Rollen als Nutzerin, Bereitstellerin und Auftraggeberin von digitalen Angeboten sicher.

Ein Umschichten der öffentlichen Ausgaben für IT in Open-Source-Projekte und Open-Source-Lösungen mittels eines verpflichtenden **Open-Source-Vorrangs** mit klar definierten, sehr eng abgegrenzten Ausnahmemöglichkeiten ist daher nicht nur für OZG-Leistungen geboten, sondern insbesondere auch für Projekte der internen IT.

Die Herausforderung liegt darin, die **ÖV umfassend für den Einsatz von Open-Source-Software zu befähigen** – von der Markterkundung bis zur Beschaffung, von Exit- und Migrationsstrategien bis zur Unterstützung der Einführung mit passendem Change-Management für die Belegschaft, von der Kollaboration über staatliche Ebenen hinweg bis zur Nachnutzung, von Lizenz-Clearing bis zu Security-Checks.

Das **ZenDiS** ist kompetenter Partner, um diese Herausforderungen mit und für die Verwaltung zu lösen.

Frage 6) Welche Vorteile oder Herausforderungen für die Verwaltungsdigitalisierung ergeben sich durch die Nutzung von Open Source-Technologien?

Antwort auf Frage 6) Open Source ist geeignet, die Verwaltungsdigitalisierung insgesamt zu **beschleunigen** und den Zugang zu **Innovationen** zu erleichtern (siehe auch Antwort auf Frage 14). Darüber hinaus ermöglicht Open Source die **Anpassung** von Lösungen an die spezifischen und sehr heterogenen Sicherheits-, Betriebs- und funktionalen Anforderungen innerhalb der Verwaltung und erlaubt grundsätzlich ein **schnelles, kontrolliertes Reagieren auf Sicherheitsvorfälle und Cyberangriffe** durch die Möglichkeit, Schwachstellen eigenständig zu identifizieren und zu beheben (Unabhängigkeit vom Patch-Management der Hersteller). **openCode** bildet hierfür die ideale Plattform.

Die Nutzung von Open-Source-Lösungen **verhindert Vendor-Lock-ins** und damit zusammenhängende Risiken wie Kontrollverlust und unkontrolliert steigende Lizenzkosten. Die Nachnutzung und Weiterentwicklung bestehender Open-Source-Lösungen ist **kosteneffizient** und erhöht das Tempo bei der Verwaltungsdigitalisierung.

Herausforderungen liegen in der gängigen **Vergabepraxis**, die auf „Kauf", „Miete" oder „Entwicklung" ausgelegt ist, jedoch nicht auf die Weiterentwicklung bzw. Mitarbeit an gemeinschaftlichen Projekten von mehreren Beteiligten (Contribution) bzw. die Ausschreibung von Dienstleistungen rund um die lizenzfreie Nutzung von Open Source.

Hier gilt es, die nötigen Kompetenzen aufzubauen und, wo nötig, für Klarheit im Vergaberecht sowie die entsprechenden Standardverträge (Stichwort: **EVB-IT Open Source)** zu sorgen. Mit dem **ZenDiS** hat die Verwaltung einen Akteur geschaffen, der diese Aufgaben übernimmt und beratend tätig ist.

Frage 7) Welche Vergabekriterien sollten im Vergaberecht mit Blick auf die Beschaffung digitaler Produkte und Dienstleistungen reformiert werden und welche Gründe sprechen dafür oder dagegen, hier einen Mindestanteil von Open Source-Technologien einzuführen?

Antwort auf Frage 7) In der Vergabeverordnung für öffentliche Aufträge lässt sich der grundsätzliche **Open-Source-Vorrang** operationalisieren, der in **§ 16a eGovG** verankert ist

(„*Zur Steigerung der digitalen Souveränität sollen die Behörden des Bundes offene Standards nutzen und vorrangig Software mit offenem Quellcode einsetzen. Wird eine genutzte Software weiterentwickelt, so ist der weiterentwickelte Quellcode unter eine geeignete Software- und Open Source-Lizenz zu stellen und zu veröffentlichen, soweit der Veröffentlichung keine zwingenden sicherheitsrelevanten Gründe entgegenstehen und dies lizenzrechtlich zulässig ist. Die Software soll auch als Referenzimplementierung veröffentlicht werden.*“).

Dazu eignen sich vor allem die Vorgaben zur Leistungsbeschreibung (§ 31 und § 32 VgV) und zum Zuschlag (§ 58 VgV).

Mit Blick auf die **Vorgaben zur Leistungsbeschreibung** halten wir es für notwendig, verbindlich in der Leistungsbeschreibung solche Anforderungen aufzuführen, die die Digitale Souveränität stärken, bspw. die Nutzung offener Standards und Schnittstellen sowie quelloffener Code.

Mit Blick auf die **Vorgaben zum Zuschlag** halten wir es für notwendig, den Effekt der Software auf die Digitale Souveränität (Kriterien: Wechselfähigkeit, Gestaltungsfähigkeit und Möglichkeit der Einflussnahme auf Anbieter) als eigenständiges Kriterium für die Beurteilung von Angeboten zu etablieren. Dabei sollte die Beurteilung der **Wirtschaftlichkeit** mögliche **Folgekosten** mit einbeziehen, die sich aus einem etwaigen Lock-in-Effekt ergeben, sodass die wirtschaftlichen Auswirkungen auf andere Akteure aus der Öffentlichen Verwaltung (Nachnutzung von Software) berücksichtigt werden.

Um den für eine effiziente, wirtschaftliche und souveräne Verwaltungsdigitalisierung nötigen Wandel von der Beschaffung proprietärer Lösungen hin zu Open Source tatsächlich zu realisieren, halten wir einen schrittweise steigenden, verpflichtenden **Open-Source-Mindestanteil** bei Beschaffungsvorgängen und Rahmenverträgen für dringend geboten. Denkbar ist eine moderate Verpflichtung in Höhe von 20 Prozent in 2025 mit dem Ziel, bis 2035 die vollständige Umstellung in der Beschaffung vollzogen zu haben.

Mit dem **ZenDiS** steht der Verwaltung ein interner Partner zu Seite, der bei dieser Transformation begleiten und unterstützen kann.

Frage 8) Wie bewerten Sie die Fragen der Cybersicherheit im Kontext von Open-Source-Technologien, insbesondere mit Blick auf den Einsatz in öffentlichen Verwaltungen?

Antwort auf Frage 8) Cybersicherheitsaspekte betreffen alle IT- und Digitalisierungsprojekte und dies ganz unabhängig davon, ob es sich um proprietäre Closed-Source-Systeme oder Open-Source-Lösungen handelt.

Im Gegensatz zu proprietären Lösungen erlauben Open-Source-Lösungen aufgrund des öffentlich einsehbaren und bearbeitbaren Quellcodes jedoch grundsätzlich eine **schnelle Identifikation und Behebung von Sicherheitslücken**.

Im Vergleich zu proprietären Systemen, bei denen die Nutzenden vom Patch-Management der Hersteller mit unter Umständen langen Reaktionszeiten und späten Updates abhängig sind, kann die Verwaltung mit Open-Source-Software **Sicherheitslücken eigenständig oder durch externe Dienstleister schneller beheben**. Bei schweren Cyberssicherheitsvorfällen kann dies direkte, positive Auswirkungen auf die nationale Sicherheit haben.

Zusätzlich besteht bei Open Source die Möglichkeit, **Sicherheitsanforderungen regelmäßig automatisiert oder teilautomatisiert zu prüfen** und die Software jederzeit an spezifische oder sich ändernde Sicherheitsbedürfnisse in der Verwaltung anzupassen.

Letztlich wird mit dem zunehmend konsequenten Einsatz von Open Source im Zusammenspiel mit der **Plattform openCode** erstmals überhaupt die Erstellung eines **Echtzeit-Lagebildes zu Bewertung der Cybersicherheitslage in der Verwaltung** denkbar. Hierzu ist das **ZenDiS mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI)** im Austausch.

Frage 9) Welche Herausforderungen beim Thema Skalierung und Rollout von Open Source Software Projekten im staatlichen Einsatz sind Ihnen begegnet und welche strukturellen Maßnahmen schlagen Sie vor, um diesen zu begegnen?

Antwort auf Frage 9) Die erste Herausforderung ist die vorherrschende, **komplexe IT-Landschaft in der Verwaltung** mit ihrer großen Anzahl proprietärer Systeme, die keine offenen Standards und Schnittstellen nutzen.

Das daraus resultierende **Fehlen von Interoperabilität** verursacht regelmäßig **hohe Integrationsaufwände** – und dies ganz unabhängig davon, ob eine Open-Source-Lösung oder ein proprietäres System integriert werden soll. Durch einen konsequenten Umstieg hin zu Lösungen basierend auf **offenen Standards und Schnittstellen** können diese Integrationsaufwände deutlich reduziert werden. Bei der Beschaffung neuer Lösungen sind offene Standards und Schnittstellen als Mindestanforderung daher zwingend geboten. Bei Open-Source-Software sind diese grundsätzlich vorhanden.

Darüber hinaus braucht die Einführung jeder neuen Lösung ein **nachhaltiges Konzept für Betrieb und Wartung**, um die hohen Anforderungen der Verwaltung an Verfügbarkeit, Sicherheit und Nutzerfreundlichkeit zu erfüllen. Es ist daher wichtig, bei der anvisierten (Nach)nutzung einer Open-Source-Software **Betrieb, Pflege, Patch Management und Support mitzudenken** und entsprechende Dienstleistungen zu beschaffen.

Strukturell sehen wir den Aufbau bzw. die Stärkung entsprechender **Kompetenzzentren** als zentralen Erfolgsfaktor. Sie unterstützen die Behörden bei der Einführung und Skalierung von Open Source, schulen Mitarbeitende und bauen wichtiges Know-how sowohl im Bereich der IT als auch in der Beschaffung auf. Gleichzeitig halten sie den Kontakt zum Open-Source-Ökosystem und sorgen mit Contributions (Entwicklungsbeiträgen) dafür, dass sich Verwaltungsprojekte gegenseitig befruchten. Neben dem **ZenDiS als föderal übergreifend agierende und zentral koordinierende Stelle** gibt es schon heute in vielen Bundesländern und Kommunen entsprechende Einrichtungen.

Ein wichtiges Element neben lokalen Kompetenzzentren ist der bundesweite, behördenübergreifende Austausch. Die vom ZenDiS betriebene Plattform **openCode** bietet hierfür die notwendigen Tools und Services und ermöglicht eine rechtssichere Zusammenarbeit über alle föderalen Ebenen hinweg.

Frage 10) Welche vergaberechtlichen und verwaltungsrechtlichen Möglichkeiten werden derzeit nicht ausreichend genutzt, um den Einsatz von Open Source Software im staatlichen Bereich zu fördern und proprietäre Software perspektivisch durch quelloffene Alternativen zu ersetzen?

Welche zusätzlichen gesetzlichen Vorgaben wären wünschenswert, um diesen Übergang zu unterstützen?

Antwort auf Frage 10) Bei der Beschaffung von Software lassen sich **zwei Leistungsarten** unterscheiden: Zum einen die **Lieferung des Produkts Software** beziehungsweise die Überlassung des Rechts, die Software zu nutzen (Lizenzen). Zum anderen sämtliche **Dienstleistungen**, die im Zusammenhang mit der Software erbracht werden.

Open-Source-Lizenzen überlassen das Recht, die jeweilige Software zu nutzen, weiterzuentwickeln und weiterzugeben, **ohne dass dafür Lizenzgebühren anfallen** – einer der wesentlichen Unterschiede zu proprietärer Software. Insofern lässt sich argumentieren, dass die **Beschaffung von Open-Source-Software an sich nicht unter das Vergaberecht fällt**.

Im Detail wurde das bereits 2010 in einem Leitfaden betrachtet, der für das IDABC-Programm (Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Business and Citizens) der Europäischen Union erstellt wurde.

Wenn eine Öffentliche Verwaltung sich dafür entscheidet, eine Open-Source-Software zu nutzen, kann sie diese demnach **ohne Ausschreibung aus einer frei zugänglichen Quelle – zum Beispiel openCode – herunterladen**. Vom Vergaberecht betroffen sind dann lediglich die von Unternehmen zu erbringenden **Dienstleistungen, die entsprechend ausgeschrieben werden müssen**.

Bislang geht die Öffentliche Verwaltung allerdings nur ausnahmsweise den Weg, eine Open-Source-Software als gegebene Tatsache zu deklarieren und dann entsprechende Dienstleistungen auszuschreiben. In der Regel werden die Lieferung des Produkts Software und die entsprechenden Dienstleistungen gemeinsam ausgeschrieben. In der Leistungsbeschreibung sind dann die Anforderungen aufgeführt, die erfüllt werden müssen. Das umfasst in der Regel neben den funktionalen auch technische und organisatorische

Spezifikationen. So weist etwa der IDABC-Leitfaden explizit darauf hin, dass **offene Standards als Teil der technischen Spezifikationen** festgelegt werden dürfen.

Eine gesetzliche Klarstellung, wonach die Nutzung von freier Software ohne Ausschreibung und Vergabe ausdrücklich erlaubt ist, kann also helfen.

Derzeit besteht jedoch die Gefahr, dass das Gegenteil der Fall ist: In der Bundesverwaltung gibt es eine Diskussion um die **Bedeutung von § 63 BHO**. § 63 BHO regelt den Erwerb und die Veräußerung von Vermögensgegenständen durch den Bund und es gibt die Lesart, wonach das „Teilen" von Open-Source-Software einer Veräußerung gleichkommt und deshalb **genehmigungspflichtig** sein könnte. Dies wäre ein entscheidender **Wettbewerbsnachteil** für den Einsatz von Open-Source-Software. Demgegenüber steht die – überzeugende – Interpretation, wonach Open-Source-Software immer nur mit Ziel erworben bzw. beauftragt wird, sie auch anderen Nutzenden zugänglich zu machen, das **„Teilen" also selbstverständlicher Bestandteil des Erwerbs** ist.

Auch hier kann also eine gesetzliche Klarstellung helfen. Dies gilt ebenso in Bezug auf Exportregelungen.

Frage 11) Welche Auswirkungen und Folgen sehen Sie voraus für den Fall, dass die Entwicklung und der Betrieb quelloffener Software als gemeinnütziger Zweck in der Abgabenordnung aufgenommen wird? Halten Sie dies für wünschenswert?

Antwort auf Frage 11) In klarer Abgrenzung zu kommerziellen Open-Source-Angeboten, wäre es wünschenswert, dass **nicht gewinnorientierte Open-Source-Projekte** die Möglichkeit erhalten, ihre Arbeit als **gemeinnützig** anerkennen zu lassen. Dies würde die wichtige Arbeit von Communities in Deutschland stärken.

Frage 12) Welche institutionellen Strukturen, wie z. B. Stiftungen oder NGOs wären im Bereich der Open Source Förderung wünschenswert und welche Aufgaben oder Ziele sollten diese hypothetischen Strukturen erreichen?

Antwort zu Frage 12) Statt neue institutionelle Strukturen zu schaffen, sollten **bestehende Einrichtungen wie das ZenDiS und die Sovereign Tech Agency verstetigt und gestärkt** und ihre Arbeit noch stärker im Kontext europäischer Initiativen („Interoperable Europe Act" etc.) verankert werden. Außerdem sollten **bestehende Stiftungen und Vereine wie die Linux Foundation oder die FSFE unterstützt** werden.

Die gemeinsame Arbeit **über nationalstaatliche Grenzen hinweg** verschafft einen noch besseren Zugang zu Innovationen und trägt zu einer wirtschaftlichen Stärkung europäischer Anbieter bei, indem öffentliche Investitionen in heimische Märkte fließen. Zudem sorgt sie für Sichtbarkeit auf EU-Ebene und geht potenziell mit zusätzlichen Finanzierungsmöglichkeiten einher. Grundsätzlich gilt: Die Antwort auf die zunehmende geopolitische Destabilisierung kann nur pan-europäisch erfolgen, was eine **Vernetzung europäischer Akteur:innen** zwingend erfordert.

Frage 13) Sollte auf Bundesebene ein Open-Source-Advisory-Board initiiert werden, von dem aus auch OS-Entwicklungen monitored werden, um Probleme wie in der Vergangenheit (Log4j-Attacke) zu minimieren?

Antwort auf Frage 13) Die Einrichtung eines zusätzlichen Gremiums halten wir für nicht erforderlich. Das ZenDiS verfügt über die nötigen fachlichen Kompetenzen und kann bei entsprechender Beauftragung diese Aufgabe übernehmen und bei Bedarf weitere relevante Akteur:innen (wie z. B. die STA) involvieren. Zu **Sicherheitsfragen** arbeitet das ZenDiS bereits heute eng mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen. Ziel ist, die Plattform **openCode** so weiterzuentwickeln, dass sie nicht nur zur Basis für eine **sichere und souveräne Softwarelieferkette** für die Verwaltung und für vielfältige Kooperationsprojekte wird, sondern erstmals auch die Möglichkeit bietet, **Lagebilder in Echtzeit** zu erstellen. Dies würde die Handlungsfähigkeit der Verwaltung bei Cybersicherheitsvorfällen signifikant verbessern. Erste Werkzeuge zum Lizenz- und

Sicherheitsscan sind bereits im Probebetrieb und werden sukzessive ausgebaut.

Frage 14) Inwiefern könnte Open Source-Software als Katalysator für innovative Ansätze in der Verwaltung fungieren? Welche neuen Dienstleistungen oder Modelle könnten durch Open Source realisiert werden, um die Bürger besser zu bedienen?

Antwort auf Frage 14) Open-Source-Projekte zeichnen sich durch **Transparenz und die Vernetzung** unterschiedlicher Akteure aus. Damit ermöglichen sie völlig neue Formen der technologischen wie auch prozessualen Zusammenarbeit zwischen Verwaltungseinrichtungen untereinander – und dies rechtssicher und föderal übergreifend –, aber auch mit Unternehmen, Forschung, NGOs und Zivilgesellschaft. Eine **neue Kultur der Zusammenarbeit** entsteht, die viel stärker ein i**nnovatives Gestalten** ermöglicht.

Lösungen können **co-kreativ** gemeinsam entwickelt und verbessert werden. Das erhöht **Innovationsgeschwindigkeit** und Akzeptanz.

Darüber hinaus bietet Open-Source-Software die Möglichkeit, auf bestehenden Lösungen aufzubauen, die von anderen Verwaltungen erfolgreich eingesetzt werden – und dies sogar **über nationalstaatliche Grenzen** hinweg. Das spart zeitliche wie finanzielle Ressourcen und **beschleunigt Innovation**. Durch die Öffnung in Richtung Bürger:innen, Nutzende und Entwickler:innen-Communities werden **bürgerfreundlichere und praxisnähere Lösungen** erreicht.

Frage 15) Bei der Entwicklung von Open Source Software (OSS) kann durchaus auch unbemerkt Schad-Software eingebaut werden, z. B. ist dann von sogenannter Protestware die Rede. Wie sicher ist OSS im Vergleich zu proprietärer Software, gibt es dazu empirische Befunde, wer haftet für etwaige Folgeschäden und mit welcher Zunahme von Protestware rechnen Sie, angesichts des allgegenwärtigen Aktivismus der sogenannten Zivilgesellschaft?

Antwort auf Frage 15) Bei Open-Source-Software ist der **Quellcode grundsätzlich öffentlich** zugänglich. Sicherheitstechnisch bietet dies einen entscheidenden Vorteil

gegenüber proprietären Lösungen. Denn jede:r - und nicht nur die Entwickler:innen oder der Anbieter der Software selbst - kann **Sicherheitslücken erkennen, öffentlich machen und auch schließen**. Nutzende von Open-Source-Software sind daher unabhängig von Patches, die von den Herstellern bereit gestellt werden müssen. Dass dies entscheidend sein kann, zeigen Beispiele aus der jüngeren Vergangenheit wie die massiven Sicherheitsproblem mit den Master-Keys zur Microsoft-Cloud. Große Open-Source-Projekte wie Linux oder Kubernetes mit ihren starken Entwickler:innen-Communities bzw. Herstellern schaffen häufig **schneller Abhilfe**.

Das Einschleusen von unerwünschtem Code in Open-Source-Projekten wiederum kann wirksam verhindert werden, u. a. durch **Code-Reviews**, bei denen Änderungen von mehreren Entwickler:innen überprüft werden, oder durch **automatisierte Code-Analyse-Tools**. Auch die Verwendung von **digitalen Signaturen und Hashes** zur Verifizierung von Code-Änderungen trägt dazu bei, Manipulationen zu verhindern.

Darüber hinaus helfen **klare Governance-Strukturen** mit Regeln für die Genehmigung von Pull Requests und eine aktive Community, die auf verdächtige Änderungen aufmerksam macht.

Ebenso zentral ist das **Monitoring von Abhängigkeiten** auf unsichere oder kompromittierte Bibliotheken. Dafür baut das ZenDiS **openCode** derzeit zu einer zentralen Stelle für die Öffentliche Verwaltung aus, über die Qualitäts- und Sicherheitsüberprüfungen automatisiert vorgenommen und das Einschleusen von Schadcode perspektivisch wirksam verhindert werden können.

Haftungsrisiken wiederum können über **bilaterale Verträge** mit den Anbietern professioneller Open-Source-Lösungen gelöst werden. Bei openDesk haftet das ZenDiS als Anbieter/Bereitsteller der Software.

Frage 16) Die Bildgenerierungssoftware Stable Diffusion ist eine quelloffene Lösung, die ähnlich gute und verblüffende Ergebnisse liefert wie ihre proprietären Pendants; gleiches gilt für den Textgenerator Mistral. Wäre es aus Ihrer Sicht möglich, im Bereich generativer KI mit quelloffenen Lösungen die sich abzeichnenden Oligopole der großen Technologiekonzerne zu brechen?

Antwort auf Frage 16) Die größte Herausforderung für generative KI ist der **Zugang zu den nötigen, sehr energieintensiven und damit teuren Rechenleistungen**. Diese können meist nur von großen Technologiekonzernen bereitgestellt werden.

Insofern ist **Stable Diffusion** ein hochspannendes Beispiel, weil das Modell mit dem Ziel entwickelt wurde, generative **KI zu demokratisieren** und so energiesparend auszugestalten, dass sie auf herkömmlicher Nutzer:innen-Hardware (Smartphone, Tablets) läuft. Damit ist eine quelloffene Lösung wie Stable Diffusion durchaus in der Lage, sich abzeichnende Oligopole aufzubrechen. Mit seinem innovativen Ansatz war Stable Diffusion einer von drei Nominierten des diesjährigen Deutschen Zukunftpreises von Bundespräsident Frank-Walter Steinmeier.

Der aus gesellschaftlicher Sicht wohl größte Vorteil von Open-Source-KI besteht in der **Transparenz**. Quellcode und Trainingsdaten können offen eingesehen werden, was für Vertrauen sorgt und **Risiken wie Bias und Manipulation minimiert** und damit eine ethische Nutzung im Einklang mit europäischen Werten erlaubt.

Daneben besteht ein wesentlicher Vorteil von quelloffenen KI-Modellen darin, dass sie **prinzipiell bei jedem geeigneten Provider bzw. in jedem geeigneten Rechenzentrum betrieben werden können**, also auch in geschützten Umgebungen. Zudem sind sie leicht zu beschaffen und wegen ihrer offenen Schnittstellen leicht zu implementieren.

Ein wichtiger Hebel liegt in der **(über-)staatlichen Finanzierung** bzw. Unterstützung vielversprechender Modelle wie beispielsweise des jüngst veröffentlichten „Teuken-7B“ – einer quelloffenen Alternative zu ChatGPT aus Deutschland, da die Betriebskosten die finanziellen Möglichkeiten einzelner Unternehmen oder Forschungseinrichtungen in Europa in der Regel übersteigen.

Das **ZenDis** als zentraler Akteur zur Befähigung der ÖV für die Digitale Souveränität und den

Einsatz von Open Source wird im kommenden Jahr einen strategischen und technologischen Schwerpunkt auf das Thema Künstliche Intelligenz setzen, um seinem Auftrag auch in Bezug auf diese Technologie gerecht zu werden.

Eine entsprechende Finanzierung bzw. Beauftragung vorausgesetzt, werden wir **Open Source KI im Kontext der Digitalen Souveränität der Öffentlichen Verwaltung** evaluieren, relevante Technologien identifizieren, Strategien für den Einsatz empfehlen und beratend unterstützen. Darüber hinaus können wir die Auswahl und den Betrieb geeigneter Modelle zentral für die Öffentliche Verwaltung übernehmen. Ebenfalls wird der Einsatz von KI in unseren Produkten openDesk und openConference vorbereitet.

Frage 17) Welche Barrieren sehen Sie gegen einen höheren Einsatz von Open Source bei staatlichen Stellen, und wie bewerten Sie insbesondere folgende Barrieren:

- **„harte“ Lock-In-Effekte zum Beispiel durch technische Abhängigkeiten, wenn Hardware nur mit bestimmter Software läuft, oder Software nur mit bestimmter proprietärer Software interoperabel ist,**
- **weiche Abhängigkeitsfaktoren wie Gewöhnungseffekte, mangelnde IT-Kompetenz im Einkauf, was zur Verlängerung von Rahmenverträgen oder mehr Einkauf von Vertrautem führt, weil man Alternativen nicht kennt oder ihre Risiken überschätzt,**
- **mangelnde IT-Kompetenz im Betrieb, weil es weniger Erfahrung mit Open-Source-Dienstleistenden gibt,**
- **Folgen von Lobbyismus großer Hersteller proprietärer Software,**
- **fehlende Transparenz zum Einsatz von Open Source und proprietärer Software,**
- **mangelnde strategische Weitsicht beziehungsweise Überschätzung von kurzfristigem Nutzen bei Unterschätzung langfristiger Risiken?**

Antwort auf Frage 17) Die genannten Barrieren sind allesamt relevant. Von der Bedeutung her sehen wir die folgende Reihenfolge (absteigend sortiert):

1. mangelnde strategische Weitsicht

2. weiche Abhängigkeitsfaktoren
3. Folgen von Lobbyismus
4. fehlende Transparenz
5. mangelnde IT-Kompetenz im Betrieb
6. „harte“ Lock-in-Effekte

Dabei ist das **Fehlen einer umfassenden Strategie** für den Einsatz von Open Source in der Öffentlichen Verwaltung sicher am schwerwiegendsten. Der IT-Planungsrat hat 2021 mit dem oben zitierten Strategiepapier eine gute Grundlage vorgelegt, um dies zu adressieren. Diese muss – sich an die rapiden technologischen Entwicklungen anpassend und vorausdenkend – **weitergeführt und ihre Umsetzung anhand von Kennzahlen überprüfbar** gemacht werden.

Insgesamt erfordert die Überwindung dieser Barrieren ein Z**usammenspiel aus technischer Unterstützung, rechtlicher Klarheit und kulturellem Wandel.** Mit der Gründung des **ZenDiS** wurde der Öffentlichen Verwaltung in Deutschland ein starker Partner an die Seite gestellt, der sie gezielt zum erfolgreichen Einsatz von Open Source befähigt – von der Beschaffung bis zum Betrieb. Dazu zählt letztlich auch die Beratung zu Exit-Strategien, das Aufzeigen von Migrationspfaden hin zu Open-Source-Lösungen sowie das für eine größtmögliche Akzeptanz erforderliche Change-Management bei den Anwender:innen.

Frage 18) Inwiefern kann eine Stärkung der Verbreitung von Open Source Anwendungen auch positive soziale Effekte haben und Grundrechte fördern, und welche Rolle spielen dabei und generell eine hohe Interoperabilität und Maßnahmen zur Erleichterung der Nachnutzung bereits existierender Open Source Software?

Antwort auf Frage 18) Open Source ermöglicht Menschen und Organisationen unabhängig von ihrem Einkommen bzw. ihren finanziellen Mitteln den **Zugang zu moderner Technologie**. Da Open Source auch auf älterer Hardware funktioniert und zudem keine Lizenzkosten nach sich zieht, trägt sie nicht nur zur **Nachhaltigkeit**, sondern auch zur Nutzbarkeit für einkommensschwächere Bürger:innen bei und damit zur **digitalen Teilhabe**.

Der frei zugängliche Quellcode und die kollaborative Arbeitsweise in Open-Source-Projekten ermöglichen es, unabhängig von kostenpflichtigen Bildungsangeboten **Programmier- und IT-Kenntnisse zu erwerben** und stärkt die Chancengleichheit. Zudem können Open-Source-Projekte gezielt **barrierefrei** gestaltet werden, um **Inklusion** für alle Menschen zu fördern, unabhängig von ihren Fähigkeiten.

Maßnahmen wie die vom ZenDiS betriebene Plattform **openCode**, die eine einfache Nachnutzbarkeit zum Ziel haben, spielen dabei eine wichtige Rolle. Konkret macht openCode Software-Lösungen, die durch die Verwaltung beauftragt und – finanziert über Steuergelder – für diese entwickelt wurden, letztlich allen Bürger:innen, aber auch kleinen Unternehmen, NGOs oder Vereinen zugänglich.

3. Über das ZenDiS

Das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) wurde 2022 durch das Bundesministerium des Innern und für Heimat (BMI) gegründet. Als Kompetenz- und Servicezentrum unterstützt das ZenDiS die Öffentliche Verwaltung auf Ebene von Bund, Ländern und Kommunen dabei, ihre Handlungsfähigkeit im digitalen Raum langfristig abzusichern – vor allem, indem kritische Abhängigkeiten von einzelnen Technologieanbietern aufgelöst werden. Dazu konzentriert sich das ZenDiS in der ersten Ausbaustufe darauf, den Einsatz von Open-Source-Software in der Öffentlichen Verwaltung voranzutreiben. Das ZenDiS ist eine GmbH und liegt derzeit zu 100 Prozent in der Hand des Bundes. Eine Beteiligung der Länder ist in Vorbereitung. Sitz des ZenDiS ist Bochum.

4. Über die Expertin

Jutta Horstmann ist eine erfolgreiche Unternehmerin und Digitalexpertin, die sich für Digitale Souveränität, Nachhaltigkeit und Open-Source-Software einsetzt. Als Geschäftsführerin der ZenDiS GmbH unterstützt sie die Öffentliche Verwaltung in Deutschland dabei, ihre digitale Unabhängigkeit durch innovative Open-Source-Lösungen zu stärken. Mit über 25 Jahren Erfahrung in der IT-Branche hat Jutta Horstmann Unternehmen erfolgreich aufgebaut und transformative Veränderungen vorangetrieben. In ihrer Zeit als COO und CTO bei der eyeo GmbH trieb sie das Wachstum und die technologische Innovation des Unternehmens voran. Als gefragte Rednerin auf internationalen Konferenzen teilt Jutta Horstmann ihre Einblicke zu Führung, digitaler Transformation und der Zukunft von Open-Source-Technologien. Seit Oktober 2024 ist sie Vorsitzende der Geschäftsführung des ZenDiS.