



Aktenzeichen: Pet 1-20-06-90206-003647

Der Deutsche Bundestag hat die Petition am 06.07.2023 abschließend beraten und beschlossen:

Die Petition der Bundesregierung – dem Bundesministerium des Innern und für Heimat – als Material zu überweisen.

Begründung

Mit der Petition wird eine Stärkung der Digitalen Souveränität durch ein Digitalisierungsgesetz, welches Open Source für alle öffentlichen IT-Projekte verbindlich festlegt, gefordert.

Zur Begründung des Anliegens wird im Wesentlichen ausgeführt, dass sich Digitalisierung zwangsläufig im Spannungsfeld zwischen Innovation, Marktinteressen, Nachhaltigkeit, Datenschutz, Informationssicherheit, Souveränität und vielem mehr bewege. Die digitale Souveränität werde durch den Einsatz von geschlossenen Systemen zunehmend gefährdet, da dies zur Abhängigkeit von wenigen Anbietern führe, weil diese kein Interesse an der Interoperabilität ihrer Systeme hätten. Sobald ein Anbieter zusammen mit und für den Bund ein System entwickelt habe, der Bund allerdings an diesen Anbieter gebunden sei, sei ein Wechsel sehr teuer, da Fortschritte nicht mitgenommen werden könnten (Vendor-Lock-In). Dadurch könne der Anbieter beliebig hohe Preise abrufen und Zugeständnisse hinsichtlich der Souveränität erzwingen. Vor diesem Hintergrund werde mit der Petition die Verabschiedung eines Digitalisierungsgesetzes angeregt, das Open Source für IT-Projekte des Bundes verbindlich festlegt, um die digitale Souveränität zu fördern.

Open Source sei zwar anfangs teurer, biete jedoch zahlreiche Vorteile sowie einen großen Freiheits- und Sicherheitsgewinn. So sei Open Source anbieterunabhängig. Die Software könne weiterhin durch externe Anbieter entwickelt und gehostet werden. Ferner sei der Bund durch Open Source frei in der Gestaltung der Software. Datenschutz und Sicherheit stünden an oberster Stelle. Zudem würden freie Schnittstellen den IT-



Markt in Deutschland beflügeln. Ein weiterer Vorteil sei ein sicheres Hosting in der Cloud. Durch Open Source könnten Software-Entwickler und Hostler entkoppelt werden. Durch öffentliche Unterstützung von sicheren Open Source-Projekten würden auch Private diese Lösungen einsetzen, was das Sicherheitsniveau ebenfalls anhebe. Hinsichtlich der weiteren Einzelheiten zu dem Vorbringen wird auf die von den Petenten eingereichten Unterlagen verwiesen.

Zu der auf der Internetseite des Deutschen Bundestages veröffentlichten Eingabe liegen 531 Mitzeichnungen und 23 Diskussionsbeiträge vor. Es wird um Verständnis gebeten, dass nicht auf alle der vorgetragenen Aspekte im Einzelnen eingegangen werden kann. Der Petitionsausschuss hat der Bundesregierung Gelegenheit gegeben, ihre Ansicht zu der Eingabe darzulegen. Das Ergebnis der parlamentarischen Prüfung lässt sich unter Einbeziehung der seitens der Bundesregierung angeführten Aspekte wie folgt zusammenfassen:

Der Petitionsausschuss begrüßt zunächst das mit der Petition zum Ausdruck gebrachte Engagement, da die Gewährleistung der Digitalen Souveränität der Öffentlichen Verwaltung für ihn ebenfalls ein sehr wichtiges Anliegen darstellt.

Der Ausschuss weist darauf hin, dass Bund, Länder und Kommunen sich 2020 zum Ziel gesetzt haben, die Digitale Souveränität der Öffentlichen Verwaltung gemeinsam zu stärken.

Grundlage dieses Vorgehens ist das im IT-Planungsrat beschlossene Eckpunktepapier (Entscheidung 2020/07), welches den Rahmen bildet, Abhängigkeiten von Technologieanbietern mithilfe von Open Source sowie offenen Schnittstellen und Standards zu minimieren und hierdurch die Wechselmöglichkeit und -fähigkeit der Verwaltung zu stärken.

Weiterhin macht der Ausschuss darauf aufmerksam, dass auch im Koalitionsvertrag zwischen SPD, BÜNDNIS 90/DIE GRÜNEN und FDP für die 20. Wahlperiode bezüglich der Thematik Digitaler Staat und digitale Verwaltung u. a. Folgendes ausgeführt wird (vgl. S. 15):

[...] „Für öffentliche IT-Projekte schreiben wir offene Standards fest.

Entwicklungsaufträge werden in der Regel als Open Source beauftragt, die entsprechende Software wird grundsätzlich öffentlich gemacht.“ [...]



Zur Erreichung dieses Ziels hat das Bundesministerium des Innern und für Heimat (BMI) verschiedene Maßnahmen auf unterschiedlichen Fachgebieten angestoßen. Ein Beispiel für gelungene Transparenz ist die Umsetzung der Corona-Warn-App (gemeinsam mit dem Bundesministerium der Gesundheit): Im Sinne einer maximalen Transparenz wurden alle Bestandteile und Codes der App auf der Open Source-Plattform github veröffentlicht.

Auch bei der Umsetzung des Onlinezugangsgesetzes (OZG) sollen kritische Abhängigkeiten zu IT-Anbietern vermieden und die Akzeptanz digitaler Lösungen bei Bürgerinnen und Bürgern gesteigert werden. Bund und Länder haben sich daher selbst auferlegt, möglichst oft und gezielt in die Entwicklung und Bereitstellung von freier und quelloffener Software für OZG-Leistungen zu investieren. Dies vereinfacht nicht nur die rechtliche Nachnutzung von Basis- sowie Online-Diensten, sondern soll auch die bessere Einbindung von Start-ups/KMUs in die Digitalisierung der Verwaltung ermöglichen. Bund und Länder haben sich mit dem Beschluss des IT-Planungsrates zum Konjunkturpaket der Bundesregierung vom 9. September 2020 zu Open Source und offenen Standards als eines der sechs Grundprinzipien bei der OZG-Umsetzung bekannt.

In diesem Sinne wird auch mit der Beschaffungsstrategie (Version 1.0 – Anlage zu Beschluss Nr. 2018/14, Konferenz der IT-Beauftragten der Ressorts) für die zentralen IT-Beschaffungsstellen festgeschrieben, dass bei Beschaffung von Softwareprodukten mit der Leistungsbeschreibung Transparenz in Bezug auf Quellcode und Technologie zu fordern sein soll. Die im Jahr 2023 zu beschließende IT-Beschaffungsstrategie für die zentralen Beschaffungsstellen (V 2.0) wird das Thema Digitale Souveränität als weiteres konstitutives Ziel in der IT-Beschaffung aufgreifen und damit zum integralen Bestandteil der IT-Beschaffung machen.

Ferner stellt der Ausschuss fest, dass mit der Entscheidung 2020/54 des IT-Planungsrats die Deutsche Verwaltungscloud-Strategie beschlossen wurde. Sie schafft gemeinsame Standards und offene Schnittstellen für föderale Cloud-Lösungen. Ziel dieser Maßnahme ist die Möglichkeit einer cloudübergreifenden Nutzung von (möglichst Open Source-) Anwendungen nach dem Grundsatz „build once, run everywhere“. Zudem wurde eine zentrale Open Source-Plattform inklusive Code Repository Management



System geschaffen, um die technische Wiederverwendbarkeit von Anwendungen bzw. Quellcode zu ermöglichen, Transparenz über bereits existierende Lösungen zu schaffen und die Zusammenarbeit an Open Source-Projekten in der Öffentlichen Verwaltung zu fördern.

Ferner haben Bund, Länder und Kommunen mit der „Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung“ einvernehmlich strategische Ziele, Lösungsansätze und Maßnahmen zur Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung beschlossen (Entscheidung im IT-Planungsrat 2021/09). Als eine zentrale Maßnahme ist im Rahmen der Strategie die Etablierung eines Zentrums für Digitale Souveränität (ZenDiS) zur Förderung von Open Source-Software (OSS) in der Öffentlichen Verwaltung geplant.

Mit der im IT-Rat beschlossenen Architekturrichtlinie für die IT des Bundes – Version 2022 steht darüber hinaus ein zentrales Dokument zur Festschreibung von offenen Standards als Vorgabe für IT-Projekte in der Bundesverwaltung zur Verfügung.

Gemäß der Architekturrichtlinie für die IT des Bundes soll Open Source kontinuierlich in ihrem Einsatz ausgebaut werden. Open Source und deren Weiterentwicklung soll durch eine aktive Beteiligung an der Open Source Community gefördert werden. Open Source Software, die durch oder für die Öffentliche Verwaltung entwickelt wird, soll auf der Open CoDE Plattform der Öffentlichen Verwaltung oder entsprechenden Plattformen veröffentlicht werden.

Vor diesem Hintergrund und im Sinne der Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung empfiehlt der Petitionsausschuss im Ergebnis, die Petition der Bundesregierung – dem BMI – als Material zu überweisen, um zu erreichen, dass sie im Rahmen der Umsetzung der o. g. Maßnahmen und Strategien einbezogen wird.