Deutscher Bundestag **Drucksache 21/5689**

21. Wahlperiode 29.04.2026

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Ruben Rupp, Robin Jünger, Alexander Arpaschi, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 21/5161 –

Zum Einkauf von IT-Gütern im Bereich des Bundes

Vorbemerkung der Fragesteller

Die Digitalisierung der öffentlichen Verwaltung schreitet voran und erfordert den kontinuierlichen Einsatz moderner Softwarelösungen in allen Bereichen des Bundes. Die Beschaffung von Software durch die Bundesregierung und nachgeordnete Behörden stellt dabei einen erheblichen Kostenfaktor im Bundeshaushalt dar und hat zugleich weitreichende Auswirkungen auf die digitale Souveränität Deutschlands, die IT-Sicherheit kritischer Infrastrukturen sowie die Abhängigkeit von einzelnen Anbietern und deren Herkunftsländern.

Angesichts der zunehmenden geopolitischen Spannungen und der wachsenden Bedeutung von Cybersicherheit ist es nach Auffassung der Fragesteller von besonderem öffentlichem Interesse, einen umfassenden Überblick über die im Bundesbereich eingesetzte Software zu erhalten. Dies betrifft insbesondere Fragen nach der Herkunft der Softwareanbieter, der finanziellen Aufwendungen für Lizenzgebühren und Wartungsverträge sowie der Verteilung der Softwareprodukte auf die einzelnen Ressorts, Behörden und nachgeordneten Einrichtungen.

Die Transparenz über die IT-Beschaffung des Bundes ist in den Augen der Fragesteller eine wesentliche Voraussetzung für die parlamentarische Kontrolle der Haushaltsführung sowie für eine fundierte Bewertung der strategischen Ausrichtung der Bundes-IT.

Vorbemerkung der Bundesregierung

Die Beantwortung der Fragen 1, 4, 12, 15 bis 18 und 20 kann aus Gründen des Staatswohls nicht – auch nicht in eingestufter Form – erfolgen. Die Beantwortung der Fragen 2, 3, 5 und 10 kann aus Gründen des Staatswohls nur in Teilen erfolgen.

Eine detaillierte Auflistung der im Bereich des Bundes eingesetzten Softwareprodukte – einschließlich Produktbezeichnungen, Kategorien und Einsatzzwecken – würde in ihrer Gesamtheit eine Zusammenstellung von Angriffsvektoren darstellen. Es muss potentiellen Angreifern verborgen bleiben, welche Softwareprodukte in welchen Behörden aktuell eingesetzt werden.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums für Digitales und Staatsmodernisierung vom 28. April 2026 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

Eine Aufschlüsselung nach Ressorts oder Behörden würde Rückschlüsse auf die Sicherheitserheblichkeit verarbeiteter Daten zulassen und so gezielte Angriffe auf einzelne Teile der Bundesregierung vereinfachen. Werden produktspezifische Sicherheitslücken bekannt, könnten Angreifer diese unmittelbar ausnutzen, sofern bekannt ist, in welcher Behörde das betroffene Produkt zum Einsatz kommt. Dies gefährdet die Arbeitsfähigkeit und die gesetzliche Aufgabenerfüllung der betroffenen Stellen erheblich. Die Kenntnis über Softwarestände versetzt Angreifer in die Lage, gezielt nach Schwachstellen zu suchen, für die noch keine Sicherheitsupdates existieren (Zero-Day-Exploits), wodurch die Behörden einem Angriff ungeschützt ausgesetzt wären. Eine Beantwortung würde außerdem Informationen über die technische Ausstattung preisgeben, die für fremde Nachrichtendienste von erheblichem Interesse sind. Dies würde die Gefahr von Cyberspionage-Aktivitäten gegen staatliche Einrichtungen deutlich erhöhen.

Eine VS-Einstufung und Hinterlegung der angefragten Informationen in der Geheimschutzstelle des Deutschen Bundestages würde ihrer erheblichen Brisanz im Hinblick auf die Aufgabenerfüllung der Behörden des Bundes nicht ausreichend Rechnung tragen, weil insoweit auch ein geringfügiges Risiko des Bekanntwerdens unter keinen Umständen hingenommen werden kann (vgl. BVerfGE 124, 78 [139]).

Bereits geringe Kenntnisse über eingesetzte Produkte oder Softwareentwicklungen ermöglichen es Angreifern, konkrete Angriffsvektoren abzuleiten. Dies gilt insbesondere unter Einsatz künstlicher Intelligenz, die zur Analyse aggregierter Darstellungen genutzt werden kann. Durch die Veröffentlichung sensibler Informationen über die Sicherheitsarchitektur wäre die in langjährigen Prozessen erarbeitete Resilienz der Informationstechnik des Bundes zudem erheblich gefährdet.

Cyberkriminelle und staatliche Akteure professionalisieren ihre Arbeitsweise. Sie sind technisch auf dem neusten Stand und agieren aggressiv. Längst haben sie Strukturen für ihre kriminellen Dienstleistungen etabliert. Deutschland setzt der Bedrohung eine tragfähige Cybersicherheitsarchitektur entgegen. Diese Cybersicherheitsarchitektur muss unter allen Umständen funktionsfähig bleiben.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet die Sicherheitslage in den fünf Dimensionen Bedrohung, Angriffsfläche, Gefährdung, Schadwirkung und Resilienz, wobei die Resilienz den vier anderen Dimensionen positiv entgegenwirkt (vgl. www.bsi.bund.de/DE/Service-navi/Publikationen/Lagebericht/lagebericht_node.html).

In allen Dimensionen hat sich die IT-Sicherheitslage deutlich verschärft:

Der russische Angriffskrieg auf die Ukraine führt unmittelbar zu vermehrten Attacken auf Partner der Ukraine (u. a. Deutschland) durch russlandfreundliche Cybergruppierungen oder auch mutmaßlich staatliche Stellen. Dabei müssen ebenfalls Sekundäreffekte zur Zerstörung von IT-Infrastruktur berücksichtigt werden.

Die stetig wachsende Komplexität der IT-Landschaft mit zunehmender Vernetzung von Behörden untereinander, mit Unternehmen, Bürgern sowie Cloud-Diensten erweitert die Wirkungsbreite von Angriffen auf einzelne Institutionen. Gleichzeitig erwartet die Bevölkerung zu Recht einen auch mit IT funktionierenden Rechtsstaat und einen Fortschritt der Digitalisierung der öffentlichen Verwaltung.

Bereits wenige Kenntnisse über mögliche Schwachstellen reichen Cyberkriminellen oder staatlichen Akteuren aus, um die gesamte IT-Infrastruktur von Behörden unbrauchbar zu machen.

Darüber hinaus spielen bedeutende technische Entwicklungen bösartigen Akteuren im digitalen Raum in die Karten. Beispielsweise kann heute in einer noch vor kurzer Zeit kaum absehbaren Qualität künstliche Intelligenz genutzt werden, um aus der (auch aggregierten) Darstellung von Produkten oder Offenlegung von aktuellen Softwareentwicklungen konkrete Angriffsvektoren abzuleiten. In der Folge würde sich die Lage in allen vier Dimensionen Bedrohung, Angriffsfläche, Gefährdung und Schadwirkung dramatisch verschlechtern. Die Sicherstellung der Staats- und Regierungsfunktion wäre massiv gefährdet. Anders als in der Beantwortung der Drucksache 20/9641 kann daher nicht auf die konkreten Softwareprodukte eingegangen werden.

Da bereits ein geringfügiges Risiko des Bekanntwerdens dieser Informationen die Handlungsfähigkeit der Bundesverwaltung gefährden könnte, muss das parlamentarische Fragerecht hinter der Pflicht zur Aufrechterhaltung der Staats- und Regierungsfunktion sowie dem Schutz der kritischen Informationsinfrastrukturen zurückstehen.

1. Welche Softwareprodukte (einschließlich Betriebssysteme, Anwendungssoftware, Datenbanksysteme, Sicherheitssoftware und Spezialsoftware) werden aktuell im Bereich des Bundes eingesetzt, und um welche Art von Software handelt es sich jeweils (bitte nach Produktbezeichnung, Softwarekategorie und Haupteinsatzzweck aufschlüsseln)?

Auf die Vorbemerkung wird verwiesen.

2. Von welchen Herstellern bzw. Anbietern werden die in Frage 1 erfragten Softwareprodukte bezogen (bitte nach Produktbezeichnung, Herstellername, Unternehmenssitz und Herkunftsland des Unternehmens aufschlüsseln)?

Auf die Vorbemerkung wird verwiesen. Es werden Softwareprodukte unterschiedlicher Hersteller eingesetzt. Diese haben ihren Unternehmenssitz in Deutschland, innerhalb der EU, z. B. in Frankreich und auch außerhalb der EU, u. a. in Australien, Großbritannien, Japan, Kanada, und den Vereinigten Staaten.

3. Welche finanziellen Aufwendungen sind dem Bund für die in Frage 1 erfragten Softwareprodukte in den Jahren 2020 bis 2025 entstanden (bitte nach Produktbezeichnung, jährlichen Lizenzkosten, Wartungs- und Supportkosten sowie einmaligen Anschaffungskosten aufschlüsseln)?

Auf die Vorbemerkung wird verwiesen. In den Jahren 2020 bis 2025 wurden in der Bundesverwaltung für die in der Frage 1 erfragten Softwareprodukte insgesamt etwa 3,126 Mrd. Euro verausgabt.

Davon

- im Jahr 2020 in der Summe rund 350,5 Mio. Euro für
  - jährliche Lizenzkosten: 65 Mio. Euro
  - jährliche Wartungs- und Supportkosten: 212 Mio. Euro
  - einmalige Anschaffungskosten: 73, 5 Mio. Euro
- im Jahr 2021 in der Summe rund 393,5 Mio. Euro für
  - jährliche Lizenzkosten: 96,5 Mio. Euro
  - jährliche Wartungs- und Supportkosten: 201 Mio. Euro

– einmalige Anschaffungskosten: 96 Mio. Euro
• im Jahr 2022 in der Summe rund 483,5 Mio. Euro für
– jährliche Lizenzkosten: 118,5 Mio. Euro
– jährliche Wartungs- und Supportkosten: 268 Mio. Euro
– einmalige Anschaffungskosten: 97 Mio. Euro
• im Jahr 2023 in der Summe rund 680 Mio. Euro für
– jährliche Lizenzkosten: 127,5 Mio. Euro
– jährliche Wartungs- und Supportkosten: 470 Mio. Euro
– einmalige Anschaffungskosten: 82,5 Mio. Euro
• im Jahr 2024 in der Summe rund 616 Mio. Euro für
– jährliche Lizenzkosten: 187 Mio. Euro
– jährliche Wartungs- und Supportkosten: 325 Mio. Euro
– einmalige Anschaffungskosten: 104 Mio. Euro
• im Jahr 2025 in der Summe rund 602,5 Mio. Euro für
– jährliche Lizenzkosten: 247,5 Mio. Euro
– jährliche Wartungs- und Supportkosten: 240 Mio. Euro
– einmalige Anschaffungskosten: 115 Mio. Euro

4. Welchen Ressorts, Bundesbehörden, nachgeordneten Einrichtungen oder sonstigen Stellen des Bundes werden die in Frage 1 erfragten Softwareprodukte jeweils zur Nutzung bereitgestellt (bitte nach Produktbezeichnung und nutzender Stelle aufschlüsseln)?

Auf die Vorbemerkung wird verwiesen.

5. Welche Vertragslaufzeiten gelten für die jeweiligen Softwarelizenzen und Wartungsverträge, und wann laufen diese Verträge aus (bitte nach Produktbezeichnung, Vertragsbeginn, Vertragsende und etwaigen Verlängerungsoptionen aufschlüsseln)?

Auf die Vorbemerkung wird verwiesen. Die durchschnittliche Vertragslaufzeit aller Verträge in der Bundesverwaltung variiert zwischen einem und vier Jahren. Die Laufzeiten der Verträge sind sehr unterschiedlich. Es gibt Verträge, die bereits in 2026 auslaufen, aber auch welche, die erst in 2031 auslaufen.

6. Über welche Beschaffungswege wurden die Softwareprodukte erworben (bitte nach Direktvergabe, öffentlicher Ausschreibung, Rahmenvertrag oder sonstigem Beschaffungsweg aufschlüsseln)?

Die Bundesregierung erwirbt nach Auswertung der über eForms-Bekanntmachungen zugänglichen Daten Softwareprodukte über folgende Vergabeverfahren, die alle im Wege der öffentlichen Ausschreibung durchgeführt werden:

– Offenes EU-weites Verfahren,
– Verhandlungsverfahren ohne Teilnahmewettbewerb (§ 17 VgV),
– Verhandlungsverfahren mit Teilnahmewettbewerb (§ 17 VgV),

– Nichtoffenes Verfahren (§ 16 VgV).

Im Ergebnis dieser Vergabeverfahren werden ca. 32 Prozent der Verträge als Rahmenvereinbarungen geschlossen. Eine Rahmenvereinbarung ist eine Vertragsart, mit der lediglich eine Höchstgrenze von Leistungen vereinbart wird, bis zu der ein einzelvertraglich vereinbarter Mittelabfluss stattfinden kann.

7. Bestehen bei den eingesetzten Softwareprodukten vertragliche oder technische Abhängigkeiten (sogenannte Lock-in-Effekte), die einen Wechsel zu alternativen Produkten erschweren oder verhindern, und wenn ja, bei welchen Produkten, und in welcher Form?

Auf die Vorbemerkung wird verwiesen. Digitale Souveränität ist für die Bundesregierung essentiell. Eine wichtige Rolle spielen dabei Studien, die unter Federführung des BMI in den Jahren 2019 (Strategische Marktanalyse zur Reduzierung von Abhängigkeiten von einzelnen Software-Anbietern) und 2021 (Analyse der Abhängigkeit der Öffentlichen Verwaltung von Datenbankprodukten) sowie durch das BMDS 2025 (Digitale Souveränität und große Sprachmodelle in der Bundesverwaltung) initiiert wurden.

8. Wie hoch ist der Anteil der Softwareprodukte, die von Herstellern mit Sitz in der Europäischen Union stammen, im Vergleich zu Produkten aus Drittstaaten (bitte prozentual und absolut nach Herkunftsregion und Kostenvolumen aufschlüsseln)?

Der durchschnittliche Anteil der Softwareprodukte in der Bundesverwaltung von Herstellern mit einem Firmensitz in der Europäischen Union liegt bei 41 Prozent. Die angefragte Aufschlüsselung des Kostenvolumens nach Herkunftsregion wird nicht automatisch erhoben. Die Beantwortung der Frage ist mit einem unverhältnismäßig hohen Aufwand an Personal- und Zeiteinsatz verbunden und ist daher nicht zumutbar.

9. Wie hoch ist der Anteil der eingesetzten Software, die von Herstellern mit Sitz in den Vereinigten Staaten von Amerika stammt, und welches Kostenvolumen entfällt auf diese Produkte?

Der durchschnittliche Anteil der Softwareprodukte in der Bundesverwaltung von Herstellern mit einem Firmensitz in den Vereinigten Staaten liegt bei 46 Prozent. Die angefragte Aufschlüsselung des Kostenvolumens nach Herkunftsregion wird nicht automatisch erhoben. Die Beantwortung der Frage ist mit einem unverhältnismäßig hohen Aufwand an Personal- und Zeiteinsatz verbunden und ist daher nicht zumutbar.

10. Welche Softwareprodukte werden ggf. von Herstellern bezogen, deren Unternehmenssitz sich in Staaten befindet, die nicht Mitglied der NATO oder der Europäischen Union sind (bitte nach Produktbezeichnung, Hersteller und Herkunftsland aufschlüsseln)?

Auf die Vorbemerkung wird verwiesen. Der durchschnittliche Anteil der Softwareprodukte in der Bundesverwaltung von Herstellern mit einem Firmensitz in Staaten, die kein Mitglied der NATO sind, liegt bei 4 Prozent.

11. Inwiefern berücksichtigt die Bundesregierung ggf. bei der Softwarebeschaffung Aspekte der digitalen Souveränität, und welche konkreten Kriterien werden hierbei angelegt?

Die Bundesregierung verfolgt digitale Souveränität als strategisches Leitprinzip ihrer IT-Beschaffung. Kriterien wie Anbieterwechsel, Betriebsunabhängigkeit, Sicherheitsanforderungen und Datenhaltung werden kontextbezogen in Vergabeverfahren integriert. Der gesetzlich verankerte Vorrang von Open-Source-Software (§ 16a E-Government-Gesetz) stärkt die Systemoffenheit und eröffnet europäischen Anbietern bessere Marktzugangschancen.

12. Welche Open-Source-Softwareprodukte werden im Bereich des Bundes ggf. eingesetzt (bitte nach Produktbezeichnung, Einsatzzweck und nutzender Stelle aufschlüsseln)?

Auf die Vorbemerkung wird verwiesen.

13. Wie hoch ist der Anteil von Open-Source-Software am gesamten Softwarebestand des Bundes (bitte prozentual nach Anzahl der Produkte und nach Kostenvolumen aufschlüsseln)?

Der durchschnittliche Anteil der Open-Source-Software am gesamten Softwarebestand in der Bundesverwaltung liegt bei 13 Prozent. Die angefragte Aufschlüsselung des Kostenvolumens wird nicht automatisch erhoben. Die Beantwortung der Frage ist mit einem unverhältnismäßig hohen Aufwand an Personal- und Zeiteinsatz verbunden und ist daher nicht zumutbar.

14. Welche Maßnahmen ergreift die Bundesregierung ggf., um den Einsatz von Open-Source-Software im Bundesbereich zu fördern, und welche konkreten Ziele verfolgt sie hierbei?

Der gesetzlich verankerte Vorrang von Open-Source-Software (§ 16a E-Government-Gesetz) stärkt die Systemoffenheit und eröffnet europäischen Anbietern bessere Marktzugangschancen.

Zu den bisher initiierten Maßnahmen der Bundesregierung zählen u. a. die Gründung des ZenDiS. Zweck des ZenDiS ist die Förderung der Digitalen Souveränität der Bundesrepublik Deutschland. Zu den Aufgaben des ZenDiS gehört die Information und Beratung der öffentlichen Verwaltung sowie eigene Tätigkeiten bei der Entwicklung, Beschaffung, Einführung und Förderung der Nutzung von Open Source Software. Das ZenDiS wird zur Entwicklung und Förderung von Open-Source-Lösungen innerhalb der Verwaltung beitragen und die Weiterentwicklung von openDesk (OSS basierte Arbeitsplatzlösung) und openCode und Innovationen im Open-Source-Bereich für die Verwaltung vorantreiben. Unabhängig von einem Einsatz in der Bundesverwaltung unterstützt die Sovereign Tech Agency die Weiterentwicklung und Absicherung digitaler Basistechnologien.

15. Bei welchen der eingesetzten proprietären Softwareprodukte existieren nach Kenntnis der Bundesregierung funktional gleichwertige Open-Source-Alternativen, und aus welchen Gründen werden diese nicht eingesetzt?

Auf die Vorbemerkung wird verwiesen.

16. Welche Softwareprodukte im Bereich des Bundes wurden einer Sicherheitsprüfung oder Zertifizierung durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterzogen (bitte nach Produktbezeichnung und Art der Prüfung bzw. Zertifizierung aufschlüsseln)?

Auf die Vorbemerkung wird verwiesen.

17. Bei welchen eingesetzten Softwareprodukten bestehen nach Kenntnis der Bundesregierung potenzielle Sicherheitsrisiken aufgrund der Herkunft des Herstellers oder aufgrund bekannter Sicherheitslücken?

Auf die Vorbemerkung wird verwiesen.

18. Welche Maßnahmen ergreift die Bundesregierung ggf., um sicherzustellen, dass die eingesetzte Software keine sog. Hintertüren oder unerwünschten Datenabflüsse an Dritte ermöglicht?

Auf die Vorbemerkung wird verwiesen.

19. Welche strategischen Ziele verfolgt die Bundesregierung bei der Softwarebeschaffung für die kommenden fünf Jahre, insbesondere im Hinblick auf digitale Souveränität, Kosteneffizienz und Herstellerunabhängigkeit?

Die Bundesregierung verfolgt bei der Software-Beschaffung in den nächsten fünf Jahren die nachfolgenden strategischen Ziele:

- Digitale Souveränität: Mehr Unabhängigkeit von einzelnen (v. a. außereuropäischen) Anbietern durch strategischeren Einkauf bei europäischen Anbietern und Einsatz von Open Source.
- Staat als Ankerkunde: Strategischer Einkauf bei Start-ups und Steigerung von deren Anteil am Einkaufsvolumen sowie bei kleinen und mittelständischen Unternehmen (KMU), um lokale Anbieter industriepolitisch zu stärken und gezielt Innovationen zu fördern.
- Herstellerunabhängigkeit: Förderung offener Standards und Schnittstellen um Vendor Lock-ins zu vermeiden und den Wechsel von Anbietern zu erleichtern.
- Kosten & Effizienz: Senkung langfristiger Kosten durch weniger Lizenzabhängigkeiten, stärkere Wiederverwendung und Betrachtung von Total Cost of Ownership im Produktlebenszyklus.
- Reduktion von Zykluszeiten: Schnellere Beschaffung und Entwicklung durch dynamische Verfahren, besseres Warengruppenmanagement sowie AI unterstützte Vergabeprozesse.

20. Plant die Bundesregierung, bestehende Softwareprodukte durch alternative Lösungen zu ersetzen, und wenn ja, welche Produkte betrifft dies, und aus welchen Gründen?

Auf die Vorbemerkung wird verwiesen.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333