Deutscher Bundestag **Drucksache 20/15036**

20. Wahlperiode 24.02.2025

Kleine Anfrage

der Abgeordneten Anke Domscheit-Berg, Dr. André Hahn, Gökay Akbulut, Clara Bünger, Nicole Gohlke, Dr. Gregor Gysi, Jan Korte, Ina Latendorf, Cornelia Möhring, Petra Pau, Sören Pellmann, Victor Perli, Martina Renner, Dr. Petra Sitte, Kathrin Vogler und der Gruppe Die Linke

Digitale Souveränität und Nutzung von Open Source bei Clouds der Bundesverwaltung und der Status der Deutschen Verwaltungscloudstrategie (DVS)

Die Digitalisierung der Bundesverwaltung geht zunehmend einher mit Cloud-basierten Diensten, da sich häufig Ressourcen effizienter und flexibler nutzen las-sen, von Serverkapazitäten bis zur gemeinsamen Nutzung von Open Source Soft-ware. Die Auslagerung von Daten und Arbeitsprozessen auf Clouds steigert jedoch (außer beim Eigenbetrieb) die Abhängigkeit von einzelnen Dienstleistenden, was eine Reihe von Risiken erhöhen kann, zum Beispiel hinsichtlich der Cybersicher-heit, Datenhoheit, Funktionssicherheit und Datenschutz und in vielen Konstella-tionen auch mit Blick auf die digitale Souveränität.

So haben aktuell alle in der Diskussion stehenden Hyperscaler ihren Hauptsitz im EU-Ausland und unterliegen daher spezifischen hoheitlichen Interessen und Rechtsrahmen der jeweiligen Herkunftsländer, die im Konflikt zu den Bedürfnissen der Datenverarbeitung staatlicher Stellen in Deutschland stehen können (www.bundestag.de/resource/blob/990440/baf5c0d018ff7cdbfc08edf0f4ce6e64/WD-3-105-23-pdf.pdf). Bereits die ersten Wochen der Trump-Präsidentschaft zeigen, dass große Tech-Konzerne mindestens nach Druckausübung bereit sind, die Interessen von Trump offensiv zu unterstützen und dass die Trump-Administration erhöhten politischen und wirtschaftlichen Druck auf internationale Partnerländer ausüben könnte, der mit Drohungen aus sachfremden Bereichen unterstützt wird – z. B. neue Zölle bei Durchsetzung des Digital Markets Acts (www.tagesschau.de/wirtschaft/verbraucher/trump-eu-apple-meta-google-amazon-musk-dma-100.html) oder die von J. D. Vance angedrohte Absage militärischer Unterstützung, sollte die EU das Unternehmen X wegen Verstößen gegen den DSA sanktionieren (www.fr.de/politik/musk-nato-trump-vance-militaer-unterstuetzung-eu-x-twitter-bussgeld-usa-regierung-zr-93403255.html).

Zu starke Abhängigkeiten können daher nach Ansicht der Fragestellenden ein potenziell hohes Sicherheitsrisiko für das Funktionieren der deutschen Bundesverwaltung sein. Deshalb braucht es auch für die Bundesverwaltung die Möglichkeit eines souveränen Cloud-Computings. Eine souveräne Cloud wird jedoch unterschiedlich definiert, auch hinsichtlich der Rolle von Open Source Software (OSS).

Ein sogenannter Multi-Cloud-Ansatz, bei dem Kunden aus einem Portfolio mehre-rer Cloud-Anbieter verschiedene Dienstleistungen in Anspruch nehmen, kann Vendor-Lock-In-Effekte verringern und so einen höheren Grad an digita-

ler Souve-ränität erreichen (www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/deutsche-verwaltungscloud-strategie/deutsche-verwaltungscloud-strategie-node.html). Mit OSS sind nach Ansicht der Fragestellenden darüber hinaus unabhängige Überprüfungen des Quellcodes und damit mehr Transparenz und mehr Sicherheit und außerdem eine kollaborative Nutzung und Weiterentwicklung möglich. Außerdem entfallen Lizenzkosten auf die Software.

Im November 2020 beschloss der IT-Planungsrat ein Konzeptpapier der Deutschen Verwaltungscloud (DVC)-Strategie (DVS, Beschluss 2020/54). Die darin enthaltenen Empfehlungen für OSS und deren Priorisierung sowohl für die Verwaltungscloud-Architektur als auch für angebotene Cloud-Dienste wurden unter anderem im Oktober 2022 und November 2023 bekräftigt (IT-Planungsrat-Beschlüsse 2022/47 und 2023/50), wobei eine Open-Source-Only-Vorgabe bisher nicht existiert. Eine Voraussetzung für die praktische Umsetzung bilden vor allem die vom ITZ-Bund betriebene Bundes-Cloud, die in eigenen Rechenzentren läuft und so ein großes Maß an digitaler Souveränität bietet, aber auch andere Cloud-Anbieter in Europa und Deutschland. Gleichzeitig haben US-amerikanische Hyperscaler ein Interesse daran, im Zuge der Migration der Bundesverwaltung in die Cloud in deren Betrieb einzusteigen. Dazu gibt es von Google mit T-Systems ein gemeinsames Angebot auf Basis der Google Public Cloud. Microsoft ist direkt aber auch mit der Delos-Cloud am Markt, die über die SAP-Tochter Delos betrieben wird, Oracle bietet sein Angebot direkt für die Bundesverwaltung an. Auch Amazon kündigte umfassende Cloud-Angebote für die Bundesverwaltung an. (www.wik.org/fileadmin/user_upload/Unternehmen/Veroeffentlichungen/Diskus/2024/WIK_Diskussionsbeitrag_Nr_529.pdf). Die Hyperscaler werben dabei mit besonders großem Funktionsumfang und hoher Performance

Für die DVS werden regelmäßig aktualisierte Rahmenwerke veröffentlicht und vom IT-Planungsrat beschlossen, zuletzt Version 2.5.4 vom 11. September 2023 (IT-Planungsratbeschluss 2023/50). Ein Kernbestandteil ist neben definierten DVC-Standards das im Januar 2024 gestartete DVC-Umsetzungsprojekt mitsamt Aufbau einer Koordinierungsstelle und eines Cloud-Service-Portals, über das Cloud-Anwendungen unterschiedlicher Cloud-Anbieter durch Bund, Länder und Kommunen bezogen werden können (Multi-Cloud-Strategie). Neben Bund und einigen Ländern sind daran die Förderale IT-Kooperation (FITKO) und die Genossenschaft govdigital beteiligt. Tatsächlich werden für wesentliche Komponenten der DVC jedoch Drittanbieter beauftragt, beispielsweise hat BTC im Juli 2024 den Zuschlag als „Cloud Broker“ erhalten, der den Zugang zu einem Cloud-Portfolio unterschiedlicher Anbieter für das Cloud-Service-Portal ermöglichen soll (www.tcilaw.de/govdigital-eg-vergibt-grossen-cloud-auftrag-mit-hilfe-von-tci/).

Nach Ansicht der Fragestellenden wurden im Widerspruch zu dieser Umsetzungsstrategie und der Priorisierung von OSS im Koalitionsvertrag der (ehem.) Ampel-Koalition einerseits von der Bundesregierung mit Oracle umfangreiche Rahmenverträge über insgesamt fast 4,8 Mrd. Euro und einer Laufzeit bis 2030 abgeschlossen – vermutlich mit einem erheblichen Anteil für Cloud-Services (https://dserver.bundestag.de/btd/20/096/2009641.pdf) und andererseits setzten sich Vertreter der Bundesregierung für einen umfassenden Einsatz der Delos-Cloud ein. Es gab über 40 hochrangige Lobbytreffen, bei denen es explizit um die Delos-Cloud ging und sogar Kanzler Scholz setzte sich für die Delos-Cloud auf der Ministerpräsidentenkonferenz am 20. Juni 2024 ein (https://mdb.anke.domscheit-berg.de/2024/09/microsoft_lobby/). Die Bundesagentur für Arbeit hat zudem gemeinsam mit der gesetzlichen Rentenversicherung und der deutschen Unfallversicherung ein Cloud-Broker-Portal ausgeschrieben und im Dezember 2024 Computacenter den Zuschlag dafür erteilt (www.arbeitsagentur.de/presse/

2024-49-cloud-ausschreibung-ba-drv-und-dguv-erteilen-zuschlag-an-multi-cloud-broker-computacenter), was ebenfalls im Widerspruch zum geplanten Cloud Service Portal von govdigital steht, das laut DVS als „zentraler Baustein des Gesamtvorhabens DVC“ entwickelt wird (IT-Planungsrat-Beschluss 2023/50).

Eigentlich muss in der Bundesverwaltung stets der Mustervertrag EVB-IT Cloud (www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/it-beschaffung/evb-it-bvb/basisvertraege/cloud/it-cloud-vertrag.docx) sowie die entsprechenden AGBs (www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/it-beschaffung/evb-it-bvb/basisvertraege/cloud/cloud-agb.pdf) bei allen Cloud-Ausschreibungen, die in den Anwendungsbereich eines Vertragsmusters der EVB-IT fallen, zwingend zur Anwendung kommen (vgl. Antwort auf Frage 17 in Drucksache 20/12864). Tatsächlich ist dies nach Ansicht der Fragestellenden aber nicht der Fall, wie aus der Antwort auf Frage 57 in Drucksache 20/14188 hervorgeht.

Aus Sicht der Fragestellenden erscheint es daher fraglich, ob die bisherige Multi-Cloud-Strategie ganzheitlich geplant und eingehalten wurde, ob sie den Anspruch der digitalen Souveränität erfüllen kann und ob eine Priorisierung von OSS tatsächlich stattfindet.

Wir fragen die Bundesregierung:

1. Wie definiert die Bundesregierung die Begriffe
   a) Souveräne Cloud,
   b) Private Cloud,
   c) On Premises Cloud,
   d) Föderale Cloud (DVC),
   e) Third-Party-Cloud,
   f) Public-Cloud,
   g) Hybrid Cloud,
   h) Multi-Cloud (bitte im Folgenden die genannten Begriffe stets dieser Definition zugrundeliegend verwenden)?
2. Wie bewertet die Bundesregierung (gern tabellarisch) jeweils für die in 1 a–h beschriebenen Clouds die Erfüllbarkeit der drei vom IT-Planungsrat im Beschluss 2024/11 definierten Kriterien für digitale Souveränität der
   a) Selbstständigkeit,
   b) Selbstbestimmtheit,
   c) IT-Sicherheit?
3. Welche der folgenden Kriterien sollten nach Auffassung der Bundesregierung bei Vergabeverfahren mit dem Beschaffungsziel „souveräne Cloud für die Bundesverwaltung“ jeweils wie stark berücksichtigt werden (bitte – sofern eine entsprechende Einteilung getroffen werden kann – tabellarisch jedes Kriterium mit einer von vier möglichen Bewertungen versehen: 1) Muss-Kriterium – Vergabe sollte daran gebunden sein, 2) wichtiges Kriterium mit erheblichem Einfluss auf eine Vergabeentscheidung, 3) Kriterium mit mäßigem Einfluss auf die Vergabe, 4) Kriterium ohne Einfluss auf die Vergabe)
   a) Betrieb der Cloud in einem hoheitlichen Intranet ohne Netzverbindung zum Internet oder zu externen Partnern,

b) Private-Cloud-Umgebung (entsprechend Definition in der Antwort auf 1b),

c) Third-Party-Cloud-Umgebung, (entsprechend Definition in der Antwort auf 1c),

d) anbieterunabhängiger Betrieb in einem Rechenzentrum der öffentlichen Hand,

e) Cloud-Anbieter befindet sich vollständig unter öffentlicher Kontrolle und in einer nicht-gewinnorientierten Rechtsform,

f) strukturelle Unabhängigkeit von Eigeninteressen anderer Staaten und Unternehmen (zum Beispiel technische Unmöglichkeit von illegitimer Einflussnahme oder Datenabflüssen),

g) Möglichkeit der Einsicht in alle Datenströme durch den Bund,

h) Datenverarbeitung ausschließlich im europäischen Wirtschaftsraum,

i) Hauptwohnsitz aller beim betreffenden Cloud-Service beschäftigten Mit-arbeitenden in Europa,

j) maximal 24 Prozent des Cloudanbieters und von Kooperationspartnern unter Kontrolle von Unternehmen mit Hauptsitz außerhalb der EU (vgl. französisches Cloud-Zertifizierungssystem SecNumCloud),

k) der Cloud-Stack ist OSS (die Software des Cloud-Stacks steht unter einer Open-Source-Lizenz, die auf der Liste der Open Source Initiative steht, bzw. die Software des Cloud-Stacks steht unter einer Open-Source-Lizenz, die auf der Plattform OpenCode zulässig ist),

l) alle Cloud-Anwendungen basieren auf OSS,

m) dokumentierte Referenzimplementierung für mehr Schutz vor Lock-in-Effekten,

n) Verwendung offener Standards und Schnittstellen,

o) Hoheit über Krypto-Module und -Schlüssel?

4. Warum erfolgte im Januar 2024 durch mehrere Bundesbehörden eine gemeinsame Ausschreibung für Cloud-Bedarfe, die offensichtlich vorwiegend auf die proprietären Hyperscaler Microsoft, Google und Amazon zugeschnitten war (www.evergabe-online.de/tenderdetails.html?0&id=575946) und wie will die Bundesregierung trotz Fokus dieser Ausschreibung auf den Einkauf eines Cloud-Broker-Portals verhindern, dass sowohl die DVS als auch das Cloud-Service-Portal organisatorisch und hinsichtlich der Anforderungen an die Souveränität ausgehebelt werden?

5. Inwiefern gliedert sich die Ausschreibung für den Aufbau einer Public Cloud durch das Beschaffungsamt des BMI vom Februar 2024 (www.evergabe-online.de/tenderdetails.html?5&id=597186) in die bestehende DVS und das Cloud-Service-Portal ein?

6. Welche der in Frage 3 genannten Kriterien für eine Souveräne Cloud waren laut der in Frage 4 und 5 erwähnten Ausschreibungen Bedingung für die Vergabeentscheidung und welche waren zwar nicht Bedingung, aber relevant bei der Vergabeentscheidung?

7. Hat die Bundesregierung entsprechend der IT-Strategie des Bundes – Hand-lungsfeld Cloud eine Klassifizierung der Daten des Bundes nach Kritikalität vorgenommen (www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/it-strategie/it-strategie-handlungsfeld_cloud_bf.pdf) einschließlich Zuordnung der daraus abzuleitenden Anforderungen

an Clouds, wenn nein, wann soll eine solche Klassifizierung erfolgen und ist diese Klassifizierung als verbindlich für alle Bundesbehörden geplant?

8. Welche Cloud-Anbieter und welche konkreten Cloud-Anwendungen werden voraussichtlich ab wann im Cloud-Service-Portal verfügbar sein (bitte für 2025 und 2026 die Planung je Quartal angeben, und wenn der konkrete Anbieter noch nicht absehbar sein sollte, bitte verallgemeinerte Zielstellungen angeben)?

9. Warum sind sowohl die Netze des Bundes (NdB) als auch die Register im bisherigen Rahmenwerk der DVS nicht berücksichtigt, obwohl beide nach Ansicht der Fragestellenden eine elementare Bedeutung für die Umsetzung der Deutschen Verwaltungscloud haben, oder ist die Bundesregierung der Ansicht, dass Register und NdB für die erfolgreiche Umsetzung der DVC keine besondere Rolle spielen?

   a) Welche Fortschritte bei Ausbau und Qualität der NdB wurden seit Beantwortung der schriftlichen Frage Nr. 74 vom 10. Juni 2022 (Ds 20/2170) erzielt?

   b) Welche Fortschritte zur Sicherheit der NdB wurden seit Veröffentlichung des Bundesrechnungshofberichts „Bemerkungen 2024 zur Haushalts- und Wirtschaftsführung des Bundes“ vom 11. Dezember 2024 (www.bundesrechnungshof.de/SharedDocs/Downloads/DE/Berichte/2024/hauptband-2024/gesamtband-volltext.pdf?__blob=publicationFile&v=2) erreicht, in denen der Bundesrechnungshof feststellte, dass von 106 Behörden und Einrichtungen des Bundes, die die NdB nutzen, 52 die Sicherheitsanforderungen für diese Nutzung gar nicht erfüllen und von diesen wiederum 45 Behörden und Einrichtungen des Bundes die von BDBOS bereitgestellte Lösung zur Erhöhung der Sicherheit dieser Nutzer (TLS-Proxy) unverändert seit 2022 nicht nutzen?

   c) Wie bewertet die Bundesregierung den gegenwärtigen Zustand der NdB hinsichtlich der begonnenen Transformation der Bundesverwaltung Richtung Cloud und welche Maßnahmen sowie finanziellen Mittel sollen zu einer zeitnahen Verbesserung führen?

   d) Gibt es in der Bundesverwaltung ungenutzte Kapazitäten für die Band-breite der NdB, und wenn ja, wie sollen diese aktiviert werden?

   e) Wie bewertet die Bundesregierung den derzeitigen Zustand der Registerlandschaft hinsichtlich der beabsichtigten Transformation der Bundesverwaltung in die Cloud und welche Maßnahmen und finanziellen Mittel sollen bis wann zu einer Verbesserung führen?

10. Nach welchen Kriterien wird bewertet, ob ein Transfer von Daten und Anwendungen der Bundesverwaltung in Clouds sinnvoll ist?

    a) Gibt es einen einheitlichen, verbindlichen, standardisierten und ergebnisoffenen Kriterienkatalog für eine Ja/Nein-Entscheidung, ob ein Transfer von Daten und Anwendungen des Bundes in die Cloud sinnvoll ist, und wenn ja, wo ist er veröffentlicht?

    b) Wird bei Entscheidungen für oder gegen einen Transfer in die Cloud regelmäßig die WiBe 5.0 (www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/it-beschaffung/wirtschaftlichkeitsbetrachtung/wibe5-0/wibe-fachkonzept-5-0.pdf) beziehungsweise seit ihrer Veröffentlichung im Dezember 2024 die Wirtschaftlichkeitsbetrachtung „Deutsche Verwaltungscloud“ (www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/cio-bund/steuerung-it-bund/beschluesse_

cio-board/2024_06_Beschluss_CIO_DVC_Wibe.html) zugrunde gelegt (wann wird jeweils welche WiBe eingesetzt)?

c) Warum wird in der Wirtschaftlichkeitsbetrachtung WiBe „Deutsche Verwaltungscloud“ bereits eine unbedingte Notwendigkeit des Transfers in die Cloud vorausgesetzt (die Handlungsalternative dazu wird pauschal als „keine vertretbare Option“ bezeichnet), anstatt diese Fragestellung mit zum Gegenstand der Prüfung zu machen, denn nach Ansicht der Fragestellenden haben die Kriterien der Wibe 5.0, wie „Plattform-/Herstellerunabhängigkeit“ oder „Erfüllung von Datenschutz und Informationssicherheit“, durchaus Einfluss auf die Frage, ob ein Transfer bestimmter Daten in die Cloud überhaupt zielführend ist?

11. Inwiefern kooperiert der Bund entsprechend der Multi-Cloud-Strategie derzeit mit den Bundesländern bei der Beschaffung von Clouds?

a) Wie erfolgt dabei der Austausch mit den Bundesländern zu deren aktuellen Cloud-Vorhaben, wie zum Beispiel zur Planung Niedersachsens, bezüglich der IT-Infrastruktur auf eine Kooperation mit Microsoft zu setzen (www.behoerden-spiegel.de/2024/04/30/niedersachsen-setzt-auf-teams-und-die-cloud/), auch mit Blick auf die in Frage 10 b) erwähnte Wirtschaftlichkeitsbetrachtung „Deutsche Verwaltungscloud“, in der die zentrale Beschaffung von Cloud-Services über die DVC anstatt dezentral über die einzelnen Bundesländer separat vom Bund als das sinnvollste Szenario eingeschätzt wird?

b) Welche Bedeutung hat bei diesem Bund-Länder Austausch der geplante Roll-Out von OpenDesk über das ZenDiS nach Kenntnis der Bundesre-gierung in den Bundesländern und welche Cloud-Anbieter sind der Bun-desregierung bekannt, die OpenDesk anbieten oder angekündigt haben, es anzubieten?

c) Welche Bedeutung hat bei diesem Bund-Länder Austausch das für 2029 angekündigte Auslaufen des Supports für on-premise-genutztes Micro-soft Office und die von der Bundesregierung festgestellte Bestrebung von Microsoft, die in der Bundesverwaltung „on-premise“-genutzten Microsoft-Produkte zukünftig vorrangig oder ausschließlich als eigene Cloud-Angebote fortentwickeln zu wollen, entsprechend einer sogenannten „Cloud-First-Strategie“ (vgl. Drucksache 20/12864, Vorbemerkungen der Bundesregierung)?

d) Plant die Bundesregierung, Rabatte durch längerfristige und hochvolumige Rahmenverträge mit Cloud-Anbietern, insbesondere solchen, die direkt oder indirekt Cloud-Produkte von US-Hyperscalern anbieten, (ggf. in Kooperation mit den Bundesländern) zu ermöglichen und welche Konflikte könnten durch derartige Verträge, die mit kurzfristigen finanziellen Vorteilen verbunden sein können, für die digitale Souveränität der Verwaltung entstehen (wie können diese möglichen Risiken für die digitale Souveränität nach Ansicht der Bundesregierung verringert werden)?

12. Soll entsprechend Zielstellung des ITZ-Bund die Bundescloud „zur zentralen Plattform für alle Dienste ausgebaut werden, die in der Bundesverwaltung ge-nutzt werden” (www.itzbund.de/DE/itloesungen/egovernment/bundescloud/bundescloud_node.html)?

a) Wenn ja, aus welchen Gründen wird dennoch ein Multi-Cloud-Ansatz verfolgt?

b) Wenn nein, welche Bedarfe kann die Bundescloud nach Auffassung der Bundesregierung auch perspektivisch nicht erfüllen, die andere Clouds erfüllen können?

13. Welche IT-Dienstleister sind in welchem Umfang in die Bereitstellung der Bundescloud eingebunden oder sollen eingebunden werden (bitte die jeweiligen Auftragsvolumina beziehungsweise Rahmenverträge mit Umfang, Beginn und Ende ihrer Laufzeit angeben)?

14. Was sind aus Sicht der Bundesregierung die Vor- und Nachteile einer föderierten Bundescloud, die allen deutschen und europäischen Anbietern offensteht und wenn aus Sicht der Bundesregierung die Vorteile überwiegen, plant die Bundesregierung eine solche Föderation (wenn nein, warum nicht)?

15. Welches Budget stand dem ITZ-Bund und anderen Einrichtungen des Bundes im Haushalt 2024 zur Verfügung für

a) die Bundescloud,

b) die souveräne On-Premise-Cloud (IONOS),

c) die IT-Betriebsplattform Bund,

d) für Public Clouds (jeweils für interne und externe Kosten),

e) für die hochsichere „R-VSK Cloud-Plattform“ (vgl. Ds. 20/6876) und

f) gegebenenfalls für weitere Clouds des Bundes?

16. Welches Budget steht (soweit auch ohne verabschiedeten Haushalt 2025 bezifferbar) für die in Frage 15 unter a) bis f) genannten Clouds im laufenden Jahr 2025 zur Verfügung?

17. Welche tatsächlichen Kosten sind für die in Frage 15 genannten Clouds in den Jahren 2021 bis einschließlich 2024 jeweils entstanden (bitte je Jahr und Cloud-Kategorie gemäß Frage 15 a) bis f) aufschlüsseln)?

18. Inwieweit werden mittel- und längerfristig steigende Preise sowie die eingeschränkte Flexibilität beim Wechsel von einem Cloud-Anbieter zu einem anderen (wegen damit verbundener komplexer Prozesse, Aufwand und Kosten), bei der Auswahl der Cloud-Anbieter für die Bundesverwaltung berücksichtigt, so wie es eine aktuelle Studie exemplarisch für die Lage bei öffentlichen Unternehmen kürzlich beschrieb (www.znt-berlin.com/app/uploads/2025/02/zNT_Studie_Fair-Software-Licensing-and-Cloud.pdf)?

19. Welche tatsächlichen Kosten entstanden dem Bund im Jahr 2024 einerseits für OSS-Cloud-Dienste und andererseits für Closed-Source-Cloud-Dienste (bitte nach Ressort aufschlüsseln und dabei auch Entwicklungs- und Betriebskosten unterscheiden)

a) bezogen auf Cloud-Stacks,

b) bezogen auf Anwendungen, die in Clouds laufen?

20. Welche Ergebnisse brachte das Gespräch der Bundesregierung mit Christian Klein von SAP zum Thema Delos-Cloud, das laut Antwort auf Frage 21 in Drucksache 20/14451 am 2. Dezember 2024 stattfand?

a) Gab es seitdem noch weitere vergleichbare Gespräche zur Delos-Cloud und wenn ja, zwischen wem (SAP, Delos, Microsoft) und wem (Bundesregierung) und mit welchem Gesprächsthema beziehungsweise Ziel?

b) Welche konkreten Ziele hinsichtlich des Zeitpunkts der Markteinführung, eines möglichen Roll-Outs etc. bezüglich der Delos-Cloud hat nach Kenntnis der Bundesregierung die Anbieterseite und die Bundesregierung selbst?

21. Ist das BSI in die DVS eingebunden (wenn ja, wie) und warum ist in der Cloud-Strategie des BSI vom Dezember 2024 (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2024_02.pdf) die DVS nicht einmal erwähnt?

22. Warum werden Cloud-Stacks, die nicht auf Open Source basieren, weiterhin durch Ausschreibungen des Bundes eingekauft, obwohl sie mit den Zielen „Die Mechanismen der Deutschen Verwaltungscloud fördern gezielt OS-Lösungen“ und „OSS wird für den Aufbau der Deutschen Verwaltungscloud priorisiert“ (IT-Planungsrat Beschluss 2023/50) nicht kompatibel sind?

23. Wird für den Cloud-Stack und/oder laufende und geplante Cloud-Anwendungen der Bundescloud konsequent OSS entwickelt und eingesetzt oder gibt es davon Ausnahmen (wenn es Ausnahmen gibt, warum gibt es sie und welche sind das)?

24. Wie bewertet die Bundesregierung die bestehenden und angekündigten Angebote der nachfolgend aufgelisteten Cloud-Anbieter hinsichtlich der Bereitstellung tatsächlich souveräner Clouds (entsprechend Definition in Frage 1) und von OSS-basierten Clouds

a) Microsoft

b) Delos,

c) Google/T-Systems,

d) Amazon,

e) Oracle,

f) Ionos,

g) Schwarz Gruppe (STACKIT),

h) plusserver (pluscloud),

i) Secunet/Syseleven,

j) und gegebenenfalls weiterer Anbieter (bitte argumentativ begründen)?

25. Welche konkreten Pläne verfolgt die Bundesregierung für die Nutzung des Sovereign Cloud Stack, der bis September 2024 zu 100 Prozent durch das Bundesministerium für Wirtschaft und Klimaschutz gefördert wurde, außerdem im Rahmenwerk der Zielarchitektur der DVC explizit erwähnt wird und der zum Aufbau einer OSS-Referenzimplementierung und einer OSS-Cloud für Wirtschaft und Verwaltung beitragen soll, und was plant die Bundesregierung hinsichtlich der Weiterentwicklung des Sovereign Cloud Stacks?

26. Plant die Bundesregierung, für künftige Entwicklungsaufträge und Eigenentwicklungen von Software einen Container-Ansatz oder andere Voraussetzungen für den Betrieb der Software im Sovereign Cloud Stack oder dazu kompatiblen Clouds zur Bedingung zu machen, wenn nein, warum nicht?

27. Inwiefern wird beim Aufbau einer OSS-basierten souveränen Bundescloud mit der UN kooperiert oder Erfahrungen ausgetauscht, zum Beispiel hinsichtlich der von UNICC und Canonical aufgebauten privaten Cloud auf OpenStack-Basis (www.unicc.org/news/2023/10/19/unicc-partners-wi

th-canonical-to-build-unicc-cloud/), und welchen Erfahrungsaustausch gibt es zu OSS-Cloud-Vorhaben gegebenenfalls auch mit anderen internationalen Partnern?

28. Welche Hürden gibt es für eine verstärkte Beschaffung von OSS-Cloud-Diensten durch den Bund nach Ansicht der Bundesregierung (zum Beispiel Anforderungen in Ausschreibungen wie Referenzen, Umsatz- oder Nutzen-denzahlen, die nur von Closed-Source-Cloud-Anbietenden erfüllt werden können, aber gar nicht zwingend erforderlich sind für einen sicheren und verlässlichen Cloud-Betrieb für die Bundesverwaltung) und wie könnte beziehungsweise wird die Bundesregierung diese Hürden jeweils abbauen, um die angestrebte Stärkung der digitalen Souveränität zu erreichen?

29. Wie bewertet die Bundesregierung die Aussage einer Sachverständigen in der Anhörung zu Open Source im Digitalausschuss vom 4. Dezember 2024, wonach die Delos-Cloud keineswegs „souverän“ sei, da ihr Kern die proprietäre Cloud eines US-Konzerns sei (Bianca Kastl; www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/1024966-1024966)?

30. Teilt die Bundesregierung die Auffassung des Sachverständigen Alexander Sander von der Free Software Foundation in der in Frage 29 erwähnten Anhörung, dass der Interoperable Europe Act (2024/903) die Veröffentlichung des Quellcodes als eine Voraussetzung für die Bezeichnung „Open Source“ benennt?

31. Warum ist in der aktuellen Cloud-Strategie des BSI (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2024_02.pdf) trotz nach Ansicht der Fragestellenden Widersprüchlichkeit zum Interoperable Europe Act von der „souveränen Delos-Cloud“, und von einer „AWS EU Sovereign Cloud“ die Rede und warum werden im Kapitel „Souveräne Clouds“ dieser Strategie lediglich diese zwei Beispiele für souveräne Clouds genannt, während tatsächlich souveräne und OSS-Cloud-Lösungen völlig unerwähnt bleiben?

32. Liegen dem mit Oracle im Mai 2023 geschlossenen Rahmenvertrag über 4,8 Mrd. Euro (https://ted.europa.eu/de/notice/-/detail/324505-2023) auch die EVB-IT-Cloud sowie die entsprechenden AGBs für den Einzelabruf von Leistungen zugrunde und in welchem Volumen wurden Leistungen aus diesem Rahmenvertrag in den Jahren 2023 und 2024 jeweils abgerufen (bitte aufschlüsseln nach Cloud-Services und sonstigen Leistungen)?

33. Warum wurde laut Antwort auf Frage 57 in Drucksache 20/14188 eindeutig auch Azure-Cloud von Microsoft ohne Anwendung einer EVB-IT beschafft, obwohl die EVB-IT laut Antwort auf Frage 17 in Drucksache 20/12864 verbindlich anzuwenden sind, wenn die konkrete Beschaffung in den Anwendungsbereich eines passenden Vertragsmusters (zum Beispiel die EVB-IT Cloud) fällt?

34. Ist geplant, bei der derzeit laufenden Prüfung und geplanten Überarbeitung der EVB-IT Cloud deren Verbindlichkeit für die Beschaffung von Cloud-Services zu stärken und die Beschaffung von OSS bevorzugt zu regeln, und falls nein, warum nicht?

35. Was hat das Prüfprojekt zur Microsoft-Cloud-Technologie, die der IT-Rat laut Antwort auf Frage 8 in Drucksache 20/12864 in Auftrag gab und das einen Vorbehalt für die Nutzung dieser Technologie darstellt, im Detail ergeben, und inwiefern berücksichtigte die Prüfung, dass laut Antwort auf Frage 14a in derselben Drucksache in jedem Fall eine direkte technische Verbindung zur Microsoft Corporation für den Betrieb der Delos-Cloud unvermeidlich ist (bitte auf das Prüfergebnis jeder der priorisierten Anfor-

derungen: Informationssicherheit, Datenschutz und Geheimschutz eingehen)?

a) Falls dieses Prüfprojekt des IT-Rats noch nicht abgeschlossen ist, bis wann soll der Abschlussbericht vorgelegt werden und ist eine Veröffentlichung geplant (falls keine geplant ist, bitte begründen, warum nicht)?

b) Wie bewertet die Bundesregierung die Kompromittierung der Microsoft-Cloud-Infrastruktur (durch einen erfolgreichen Angriff auf OWA, über den das Unternehmen im Juli und September 2023 sowie im März 2024 berichtete) sowie den infolgedessen erstellten Bericht des Department of Homeland Security's Safety Review Board (CSRB3, www.dhs.gov/news/2024/04/02/cyber-safety-review-board-releases-report-microsoft-online-exchange-incident-summer) und wurden die Microsoft empfohlenen Sicherheitsmaßnahmen beziehungsweise technischen Verbesserungen in dem oben genannten Prüfungsprojekt einbezogen?

36. Wie bewertet die Bundesregierung den im Dezember 2024 öffentlich bekannt gewordenen Vorfall, demzufolge es einem Forschungsteam gelang, die Multifaktor-Authentifizierung (MFA) von Microsoft Azure zu überwinden, was einen unbefugten Zugriff auf Benutzerkonten ermöglichte, einschließlich Outlook-E-Mails, Teams-Chats, die Azure Cloud sowie OneDrive-Dateien (www.oasis.security/resources/blog/oasis-security-research-team-discovers-microsoft-azure-mfa-bypass)?

37. Teilt die Bundesregierung die in den „Mindeststandards zur Nutzung externer Cloud-Services" dokumentierte Auffassung des BSI, wonach die „Risiken durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden" durch Eigenerklärungen und Vertragsklauseln im Vergabeverfahren berücksichtigt werden müssen und damit hinreichend eingegrenzt sind?

a) Wenn ja, wie können, nach Ansicht der Bundesregierung Verstöße gegen derartige Vertragsklauseln in der Praxis überprüft werden?

b) Wenn nein, schließt sich die Bundesregierung stattdessen der Feststellung im Positionspapier der Datenschutzkonferenz vom 11. Mai 2023 an (https://datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf, Kapitel 2.4), dass rein vertragliche Maßnahmen hierzu unzureichend sind, selbst wenn die Datenverarbeitung innerhalb des europäischen Wirtschaftsraumes erfolgt?

c) Wie sollen Verletzungen der technischen No-Spy-Klausel, die laut Antwort auf Frage 18 c) in Drucksache 20/12864 lediglich ein rein vertragliches Instrument ist, überhaupt nachweisbar sein, wenn Herausgabepflichten von Informationen gegenüber Drittstaaten der Geheimhaltung unterliegen (zum Beispiel durch geltendes US-Recht, dem US-Unternehmen und deren Töchter auch bei Datenverarbeitung in Europa unterliegen) und wie soll die rein vertragliche No-Spy-Klausel das Risiko der Spionage oder Überwachung praktisch verringern?

d) Ist der Bundesregierung die Feststellung der wissen-schaftlichen Dienste des Bundestages (WD 3 – 3000 – 105/23; www.bundestag.de/resource/blob/990440/baf5c0d018ff7cdbfc08edf0f4ce6e64/WD-3-105-23-pdf.pdf) bekannt, dass eine verdeckte Informationsausleitung an US-amerikanische Sicherheitsbehörden bei US-amerikanischen Cloud-Anbietern, deren Tochterunternehmen und Vertragspartnern,

auch dann nicht auszuschließen ist, wenn sich die für den Cloud-Service benötigten Serverstandorte ebenso wie die Wohnorte der Mitarbeitenden in Europa befinden und wenn ja, welche Schlüsse zieht sie daraus und welche Auswirkungen ergeben sich daraus für die DVS und das geplante Portfolio des Cloud-Service-Portals?

38. Inwiefern berücksichtigt die Bundesregierung bei der Umsetzung der DVC die Möglichkeit, dass das EU-US-Data Privacy Framework wie schon die vorherigen transatlantischen Datenschutzabkommen dieser Art keinen Bestand vor dem EuGH haben wird (vgl. Schrems I und Schrems II Urteile), insbesondere angesichts der Tatsache, dass Max Schrems als Sachverständiger im Digitalausschuss bereits am 26.6.2024 eine weitere Klage angekündigt hat (Videomitschnitt dieses Digitalausschusses, bei 1:24:40: www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/1006274-1006274) und jüngste Entwicklungen der US-Politik unter Trump die Risiken für das Abkommen weiter und deutlich erhöhen (https://noyb.eu/de/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal)?

39. Wird für alle Cloud-Anwendungen, die nicht OSS sind, eine „Exit-Strategie" gemäß IT-Strategie des Bundes – Handlungsfeld Cloud vom 2. November 2023 (www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitaler-wandel/it-strategie/it-strategie-handlungsfeld_cloud_bf.pdf) erarbeitet (wenn ja, was ist der Stand beziehungsweise der Plan dafür, und wenn nein, warum werden solche Exit-Strategien nicht für notwendig gehalten)?

40. Welche Clouds haben bisher nach Kenntnis der Bundesregierung

    a) Testate zur Erfüllung des Kriterienkatalogs Cloud Computing C5 des BSI erlangt,

    b) ein Zertifikat nach ISO 27001 erhalten,

    c) eine Freigabe für eingestufte Informationen „VS-NfD",

    d) eine Freigabe für die Vertraulichkeitsstufe „GEHEIM"?

41. Inwiefern teilt die Bundesregierung die Einschätzung des BSI in dessen aktueller Cloud-Strategie (www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2024_02.pdf?__blob=publicationFile&v=8), dass die staatliche Verwaltung Vorreiter bei der sicheren Public-Cloud-Nutzung auch für sensible Inhalte wie VS-NfD sei, und wenn ja, welche Grundlagen in der DVS gibt es für eine derartige Vorreiterrolle?

42. Was ist der Bundesregierung dazu bekannt, ob die Handhabung von Kundendaten (Übertragung, Speicherung, Verarbeitung) bei Cloud-Produkten, die auf Microsoft-, Google-, Oracle-, oder AWS-Software basieren, verschlüsselt erfolgen kann (bitte jeweils für Nutzerdaten und Metadaten getrennt beantworten)?

    a) Bei welchen der von Behörden und Einrichtungen des Bundes genutzten Clouds besteht die Möglichkeit, dass Schlüssel für den Datenzugriff in der Cloud ausschließlich auf den Endgeräten der Nutzenden erzeugt, bekannt und gespeichert werden und dazu ein quelloffenes, vollständig transparentes Verfahren genutzt werden kann?

    b) Bei welchen der von Behörden und Einrichtungen des Bundes genutzten Clouds ist Ende-zu-Ende-Verschlüsselung gewährleistet in dem Sinne, dass keine Entschlüsselung der Daten stattfinden kann (auch nicht bei deren Verarbeitung), außer auf den Endgeräten der Nutzenden (bitte für Nutzdaten und Metadaten getrennt beantworten)?

c) Wie bewertet die Bundesregierung (falls zutreffend) das Fehlen der in b) beschriebenen Ende-zu-Ende-Verschlüsselung hinsichtlich des Risikos, dass eine Informationsausleitung an Drittstaaten technisch doch möglich ist, auch im Vergleich zu rein europäischen Clouds, OSS-Cloud-Lösungen in Eigenbetrieb und Nicht-Cloud-basierten Lösungen in Eigenbetrieb?

Berlin, den 20. Februar 2025

Heidi Reichinnek, Sören Pellmann und Gruppe

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