Deutscher Bundestag **Drucksache 20/15138**

20. Wahlperiode 21.03.2025

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Anke Domscheit-Berg, Dr. André Hahn, Gökay Akbulut, weiterer Abgeordneter und der Gruppe Die Linke
– Drucksache 20/15036 –

Digitale Souveränität und Nutzung von Open Source bei Clouds der Bundesverwaltung und der Status der Deutschen Verwaltungscloud-Strategie

Vorbemerkung der Fragesteller

Die Digitalisierung der Bundesverwaltung geht zunehmend einher mit Cloud-basierten Diensten, weil sich häufig Ressourcen effizienter und flexibler nutzen lassen, von Serverkapazitäten bis zur gemeinsamen Nutzung von Open Source Software (OSS). 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, z. B. hinsichtlich der Cybersicherheit, Datenhoheit, Funktionssicherheit und Datenschutz und in vielen Konstellationen 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 Präsidentschaft von Donald Trump zeigen, dass große Tech-Konzerne mindestens nach Druckausübung bereit sind, die Interessen von Donald 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 Digital Services Act (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.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern und für Heimat vom 20. März 2025 übermittelt.

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

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 digitaler Souve-ränität erreichen (www.cio.bund.de/Webs/CIO/DE/digitale-losungen/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 Informationstechnikzentrum Bund (ITZBund) betriebene Bundescloud, 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-Planungsrat, Beschluss 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 (ehemaligen) Koalition der Fraktionen von SPD, BÜNDNIS 90/DIE GRÜNEN und FDP 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 (Bundestagsdrucksache 20/9641) 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 Bundeskanzler Olaf Scholz setzte sich für die Delos-Cloud auf der Ministerpräsidentenkonferenz am 20. Juni 2024 ein (mdb.anke.domscheitberg.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-c

loud-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 Ergänzende Vertragsbedingungen für die Beschaffung von IT-Leistungen (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 zu Frage 17 auf Bundestagsdrucksache 20/12864). Tatsächlich ist dies nach Ansicht der Fragestellenden aber nicht der Fall, wie aus der Antwort zu Frage 57 auf Bundestagsdrucksache 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.

Vorbemerkung der Bundesregierung

Die Bundesregierung beantwortet die im Rahmen des parlamentarischen Fragerechts angefragten Sachverhalte gegenüber dem Deutschen Bundestag grundsätzlich öffentlich, transparent und vollständig, um dem verfassungsrechtlich verbrieften Aufklärungs- und Informationsanspruch des Deutschen Bundestages zu entsprechen. Soweit erfragte Informationen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann, und gegebenenfalls alternative Formen der Informationsvermittlung zu suchen, die das Informationsinteresse des Parlaments unter Wahrung der berechtigen Geheimhaltungsinteressen der Regierung befriedigen (BVerfGE 124, 161, 193).

Nach sorgfältiger Abwägung ist die Bundesregierung zu der Auffassung gelangt, dass die Beantwortung der Kleinen Anfrage nicht durchgängig offen erfolgen kann.

Die Antworten zu den Fragen 13 und 40c werden als „VS-Nur für den Dienstgebrauch“ gemäß der Allgemeinen Verwaltungsvorschrift des Bundesministeriums des Innern zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung – VSA) eingestuft und als nicht zur Veröffentlichung in einer Bundestagsdrucksache bestimmte Anlage übermittelt.

Ursächlich hierfür ist, dass die in Frage 13 erfragten Unternehmensdaten missbräuchlich, z. B. durch gezielte Cyberangriffe, Social Engineering, o. Ä. für Maßnahmen bei den dort genannten Unternehmen in Hinblick auf Ihre Zusammenarbeit mit dem IT-Dienstleister verwendet werden könnten.

Zudem ist die IT-Infrastruktur der Bundesregierung jeden Tag einer Vielzahl unterschiedlicher Angriffe ausgesetzt. Zur Aufrechterhaltung der Staats- und Regierungsfunktion ist diese Infrastruktur angemessen zu schützen bzw. keinen unnötigen Risiken auszusetzen. Eine Beeinträchtigung oder sogar ein Ausfall aufgrund erfolgreicher Cyberangriffe muss auch in der Zukunft bestmöglich verhindert werden. Das öffentliche Preisgeben von möglichen Hochwertzielen, hier von „VS-Nur für den Dienstgebrauch“-freigegebenen Clouds, ist vor diesem Hintergrund nicht möglich; die Beantwortung der Frage 40c erfolgt daher ebenfalls eingestuft.

In Bezug auf die Fragen 15, 16, 17 und 19 ist die Bundesregierung nach sorgfältiger Abwägung zu der Auffassung gelangt, dass eine Beantwortung der Fragen für die Nachrichtendienste des Bundes nicht – auch nicht eingestuft – erfolgen kann. Die erbetenen Auskünfte sind geheimhaltungsbedürftig, weil sie Informationen enthalten, die im direkten Zusammenhang mit der Arbeitsweise und Methodik der Nachrichtendienste des Bundes stehen. Insbesondere durch eine Auskunft über das Budget im Bereich des Einsatzes und der Nutzung von Cloudtechnologien könnten Rückschlüsse auf die technische Arbeits- und Funktionsweise der Nachrichtendienste des Bundes und dessen Schutzvorkehrungen gegen Sabotageakte, Spionage und terroristische Anschläge gezogen werden. Eine Kenntniserlangung dieser Informationen durch Unbefugte wäre daher geeignet, hochrangigen staatlichen Sicherheitsinteressen schweren Schaden zuzufügen.

Eine Bekanntgabe von Einzelheiten zu Cloud-Einsatz- und Umfang sowie deren konkreter Anwendung bei den Nachrichtendiensten des Bundes würde darüber hinaus weitgehende Rückschlüsse auf technische Fähigkeiten sowie Aufklärungspotenzial und Resilienz der Nachrichtendienste des Bundes ermöglichen. Der Erfolg zukünftiger Maßnahmen könnte gefährdet und damit die Erkenntnisgewinnung beeinträchtigt werden. Diese ist zur Aufgabenerfüllung der Nachrichtendienste des Bundes jedoch unerlässlich. Aus der sorgfältigen Abwägung der Informationsrechte des Deutschen Bundestags und seiner Abgeordneten mit den negativen Folgen für die Arbeitsfähigkeit und Aufgabenerfüllung der Nachrichtendienste des Bundes sowie den daraus resultierenden Beeinträchtigungen der Sicherheit der Bundesrepublik Deutschland folgt, dass auch eine Auskunft nach Maßgabe der Geheimschutzordnung und damit einhergehende Einsichtnahme über die Geheimschutzstelle des Deutschen Bundestages ausscheidet. Eine Bekanntgabe auch gegenüber einem begrenzten Kreis von Empfängern wird dem Schutzbedarf nicht gerecht. Hieraus ergibt sich, dass die erbetenen Informationen derart schutzbedürftige Geheimhaltungsinteressen berühren, dass das Staatswohl gegenüber dem parlamentarischen überwiegt. Insofern muss ausnahmsweise das Fragerecht der Abgeordneten gegenüber den Geheimhaltungsinteressen der Bundesregierung zurückstehen.

1. Wie definiert die Bundesregierung die Begriffe

   a) Souveräne Cloud,

„Digitale Souveränität“ beschreibt „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können“ (vgl. www.cio.bund.de/Webs/CIO/DE/digitale-loesungen/digitale-souveraenitaet/digitale-souveraenitaet-node.html). In diesem Sinne werden als sogenannte souveräne Clouds alle Clouds verstanden, die es dem Bund erlauben selbstständig, selbstbestimmt und sicher tätig zu sein. Gemäß Beschluss IT-Planungsrat zur Digitalen Souveränität (Beschluss 2021/09) müssen dabei die strategischen Ziele Wechselfähigkeit, Gestaltungsfähigkeit und Einfluss auf IT-Anbieter beachtet werden.

   b) Private Cloud,

Als Private Clouds des Bundes werden Cloud-Umgebungen bezeichnet, welche durch IT-Dienstleister des Bundes bereitgestellt und betrieben und exklusiv für den Bund oder einzelne Bundesbehörden angeboten werden, sowie Cloud-Umgebungen, die im Falle, dass eine Ausnahme von der Verpflichtung zur Betriebskonsolidierung gegeben ist, in den Ressorts zur fachlichen Aufgabenwahrnehmung betrieben werden (vgl. Handlungsfeld Cloud der IT-Strategie des Bundes).

c) On Premises Cloud,

Der Begriff On-Premise Cloud drückt aus, dass die Cloud in Rechenzentren des Bundes aufgebaut ist. Es handelt sich um Private Clouds des Bundes, die durch einen Dritten organisiert und geführt werden. (vgl. www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html).

d) Föderale Cloud (DVC),

Aus Perspektive des Bundes handelt es sich bei Föderalen Clouds (DVC) um Cloud-Umgebungen der öffentlichen Verwaltung von Ländern und Kommunen, welche durch IT-Dienstleister von Ländern oder Kommunen betrieben, über die Deutsche Verwaltungscloud bereitgestellt und durch den Bund mitgenutzt werden (vgl. Handlungsfeld Cloud der IT-Strategie des Bundes).

e) Third-Party-Cloud,

Third-Party-Private-Cloud in ihrer Grundform sind Cloud-Umgebungen privater Anbieter, die von deutschen bzw. europäischen Anbietern nach deutschem Recht bereitgestellt und betrieben und vom Bund exklusiv genutzt werden (vgl. Handlungsfeld Cloud der IT-Strategie des Bundes).

f) Public-Cloud,

Public Clouds sind Cloud-Umgebungen privater Anbieter, die öffentlich verfügbar sind und auch vom Bund genutzt werden (vgl. Handlungsfeld Cloud der IT-Strategie des Bundes).

g) Hybrid Cloud,

Bei einer Hybrid-Cloud handelt es sich um ein Cloud-Architekturmodell, bei welchem mehrere Cloud-Infrastrukturen, die für sich selbst eigenständig sind und über standardisierte Schnittstellen gemeinsam genutzt werden. (vgl. www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Grundlagen/grundlagen.html).

h) Multi-Cloud

(bitte im Folgenden die genannten Begriffe stets dieser Definition zugrunde liegend verwenden)?

Bei einer Multi-Cloud handelt es sich um ein Cloud-Architekturmodell, bei welchem mehrere Cloud-Infrastrukturen, die für sich selbst eigenständig sind und separat genutzt werden. (vgl. Handlungsfeld Cloud der IT-Strategie des Bundes).

2. Wie bewertet die Bundesregierung (gern tabellarisch) jeweils für die in Frage 1a bis 1h beschriebenen Clouds die Erfüllbarkeit der drei vom IT-Planungsrat im Beschluss 2024/11 definierten Kriterien für digitale Souveränität der

   a) Selbstständigkeit,

   b) Selbstbestimmtheit,

Die Fragen 2a und 2b werden zusammen beantwortet.

Gemäß dem Strategiepapier „Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung“ (Beschluss 2021/09 des IT-Planungsrats) wurden die genannten Kriterien durch die drei strategischen Ziele Wechselfähigkeit, Gestaltungsfähigkeit und Einfluss auf IT-Anbieter konkretisiert.

Wechselmöglichkeit bedeutet, dass die Öffentliche Verwaltung die Möglichkeit einer freien Wahl bzw. eines flexiblen Wechsels zwischen IT-Lösungen, IT-Komponenten und Anbietern hat. Dies bedeutet, dass leistungsfähige und erprobte Alternativen zur Verfügung stehen, um kurzfristige Produktwechsel zu ermöglichen. IT-Architekturen, Beschaffungswege und Personalschulungen müssen darauf ausgelegt sein, ein Wechsel mit verhältnismäßigen Kosten und angemessenem Aufwand zu ermöglichen. Gestaltungsfähigkeit erfordert währenddessen, dass die Öffentliche Verwaltung die Fähigkeit hat, ihre IT (mit-)gestalten zu können. Dafür verfügt sie über die notwendigen Kompetenzen sowie (Zusammen-)Arbeitsstrukturen, um IT-Lösungen zu verstehen und bewerten zu können sowie bei Bedarf deren (Weiter-)Entwicklungen bzw. deren Betrieb sicherzustellen. Einfluss auf Anbieter besagt, dass die Öffentliche Verwaltung ihre Anforderungen und Bedarfe (z. B. hinsichtlich Produkteigenschaften, Verhandlung und Vertragsgestaltung) gegenüber Technologieanbietern artikulieren und durchsetzen kann. Neben rechtlichen Vorgaben und Rahmenbedingungen umfasst dies unter anderem die Option eines IT-Betriebs in Rechenzentren der Öffentlichen Verwaltung, die Berücksichtigung von Richtlinien zu Informationssicherheit und zum Datenschutz sowie den Einfluss auf Lizenzmodelle und die Produkt-Roadmap.

Die Bewertung einer Cloud nach den genannten Kriterien/Aspekten ist jeweils nur für einen konkreten Einzelfall möglich. Da es sich bei denen in der Anfrage beschriebenen Clouds um Archetypen handelt, ist eine Bewertung nicht möglich. Grundsätzlich kann jedes Kriterium in jedem Archetyp umgesetzt werden.

c) IT-Sicherheit?

Nach Auffassung der Bundesregierung lässt sich die Erfüllbarkeit des Kriteriums IT-Sicherheit für die in 1a bis 1h beschriebenen Clouds nicht pauschal beurteilen, da für eine Bewertung der IT-Sicherheit einer Cloud neben dem Cloud-Modell mehrere Faktoren, wie beispielsweise der Betrieb, zu berücksichtigen sind. Mit Blick auf die in einer Cloud zu verarbeitenden Daten sowie die betroffenen Prozesse bewerten die Nutzer die IT-Sicherheit grundsätzlich eigenständig entlang der drei Grundwerte der IT-Sicherheit: Vertraulichkeit, Integrität sowie Verfügbarkeit. Auf Grundlage technischer Expertise kann das Bundesamt für Sicherheit in der Informationstechnik (BSI) hierbei beratend unterstützen. Das im Beschluss 2024/11 des IT-Planungsrats genannte Kriterium IT-Sicherheit bringt zum Ausdruck, dass selbstbestimmtes und selbstständiges Handeln nur dann zu digitaler Souveränität führt, wenn die Lösungen auch sicher sind.

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 zu Frage 1b),

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

   d) anbieterunabhängiger Betrieb in einem Rechenzentrum der öffentlichen Hand,

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

   f) strukturelle Unabhängigkeit von Eigeninteressen anderer Staaten und Unternehmen (z. B. 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 Mitarbeitenden in Europa,

   j) maximal 24 Prozent des Cloud-Anbieters 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 Krypto-Schlüssel?

Die Fragen 3 bis 3o werden zusammen beantwortet.

Aktuell existiert keine von den Bedarfen des jeweiligen Beschaffungsvorgangs losgelöste abgestimmte Auffassung der einzelnen Ressorts hinsichtlich der Frage, wie die genannten Kriterien bei Vergabeverfahren mit dem Beschaffungsziel „souveräne Clouds“ gewichtet werden sollten. Je nach Zuschnitt der Aufgaben des jeweiligen Ressorts unterscheiden sich die Anforderungen an zu beschaffende souveräne Clouds. Dementsprechend differieren die Gewichtungen der Kriterien. Die folgende Tabelle stellt die Ergebnisse einer durchgeführten Ressortabfrage (inklusive Geschäftsbereichsbehörden) dar. Die in den Zellen dargestellten Ziffern stellen dabei jeweils die Anzahl zu einer Bewertung (a-o) erhaltenen Rückmeldungen dar.

	Muss-Kriterium, Vergabe sollte daran gebunden sein	wichtiges Kriterium mit erheblichem Einfluss auf eine Vergabeentscheidung	Kriterium mit mäßigem Einfluss auf die Vergabe	Kriterium ohne Einfluss auf die Vergabe
3a	2	6	10	4
3b	2	10	8	3
3c	2	8	9	3
3d	3	12	5	3
3e	3	6	9	5
3f	15	7	1	0
3)	6	6	7	4
3h	16	7	0	0
3i	5	8	7	3
3j	1	10	7	4
3k	4	11	4	4
3l	1	10	8	4
3m	5	12	3	3
3n	12	8	3	0
3o	16	6	1	0

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?

Das Rahmenwerk zur Zielarchitektur der Deutschen Verwaltungscloud 2.5 sieht die spezielle Rolle eines Integrators vor, um externe Marktangebote, dazu gehören auch proprietäre Angebote, bedarfsgerecht in die DVC einzubinden.

Bei diesen Integratoren handelt es sich um IT-Dienstleister der öffentlichen Verwaltung, die Angebote externer, d. h. verwaltungsfremder Cloud-Anbieter (z. B. Hyperscaler) gemäß den DVC-Standards konfigurieren und so rechtssicher für die Deutsche Verwaltungscloud verfügbar machen.

Dadurch wird sichergestellt, dass die Anforderungen der Verwaltung immer beachtet werden. Dies gilt auch für die Souveränitätsanforderungen. Sofern die durch das Beschaffungsamt des BMI beschafften Cloud-Broker-Dienstleistungen durch einen Integrator im Cloud-Service-Portal der DVC verfügbar gemacht werden, entspricht dies den Vorgaben der DVS.

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

Sofern die durch das Beschaffungsamt des BMI beschaffte Public Cloud Leistung durch einen Integrator im Cloud-Service-Portal der DVC verfügbar gemacht werden, entspricht dies den Vorgaben der DVS.

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

Mit der in Frage 4 erwähnten Ausschreibung wurde eine Multi-Cloud-Broker Ausschreibung vorangetrieben, welche den Leistungsumfang der DVC ergänzt. Da die BA als beschaffende Stelle kein Mitglied der govdigital eG ist, ist es ihr auch nicht möglich, Leistungen über den dort ausgeschriebenen Multicloud-Broker-Vertrag zu beziehen.

Folgende Kriterien wurden dabei als „Muss-Kriterium, Vergabe sollte daran gebunden sein“ bewertet: 3f) strukturelle Unabhängigkeit von Eigeninteressen anderer Staaten und Unternehmen (für einen Teil der anzubietenden Cloud-Provider), 3h) Datenverarbeitung ausschließlich im europäischen Wirtschaftsraum (für einen Teil der anzubietenden Cloud-Provider), 3i) Hauptwohnsitz aller beim betreffenden Cloud-Service beschäftigten Mitarbeitenden in Europa (für einen Teil der anzubietenden Cloud-Provider). Zusätzlich wurde das Kriterium 3n) offene Standards und Schnittstellen als „Kriterium mit mäßigem Einfluss auf die Vergabe“ bewertet. Alle weiteren Kriterien hatten keinen Einfluss auf die Vergabe.

Mit der in Frage 5 erwähnten Ausschreibung sollte ein Anbieter für eine „Public Cloud“-Lösung, nicht für eine souveräne Cloud im engeren Sinne, gewonnen werden. Die Auswahl der Kriterien erfolgte dementsprechend. Dabei waren folgende in Frage 3 benannten Kriterien einschlägig und wurden als Bedingung für die Vergabeentscheidung angewandt: 3f) strukturelle Unabhängigkeit von Eigeninteressen anderer Staaten und Unternehmen, 3h) Datenverarbeitung ausschließlich im europäischen Wirtschaftsraum.

Alle weiteren Kriterien der Frage 3 sind für die Public-Cloud-Ausschreibung (vgl. Frage 5) nicht einschlägig und fanden daher keine Anwendung.

7. Hat die Bundesregierung entsprechend der IT-Strategie des Bundes – Handlungsfeld 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?

Gemäß Handlungsfeld Cloud der IT-Strategie des Bundes können die Chancen von Cloud-Computing nur dann umfassend genutzt werden, wenn eine anwendungsfallbezogene Bewertung der Prozessabläufe durchgeführt und Daten sowie Meta-Daten hinsichtlich ihrer Sensibilität und Kritikalität klassifiziert werden. D. h., dass im Rahmen von Maßnahmen mit dem Ziel der Transition von Fachverfahren in die Cloud, jeweils die betroffenen Daten zu bewerten sind. Eine pauschale zentrale Klassifizierung wird nicht durchgeführt.

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)?

Auf die Anlage 1 wird verwiesen.*

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?

Um den zukünftigen Netzansprüchen der DVC gerecht zu werden, werden entsprechende leistungsfähige Weitverkehrsnetze benötigt. Die aktuelle Ausstattung der Netze des Bundes (NdB) könnte diese Anforderung nicht erfüllen. Daher wurde für das Umsetzungsprojekt DVC ein Grobkonzept erstellt, welches die Planung und Umsetzung eines Peering-Networks der DVC beschreibt. Ob dieses Konzept über den derzeit im Aufbau befindlichen Informationsverbund der Verwaltung (IVÖV) umgesetzt werden kann, wird derzeit geprüft.

Hinsichtlich der Frage zu den Registern ist festzustellen, dass die Register aus Sicht der DVC IT-Dienste darstellen. Im Rahmenwerk werden grundsätzlich keine einzelnen IT-Dienste spezifiziert. Die unter Kapitel 4.5 aufgeführten „Mögliche Softwarelösungen für den Betrieb in Cloud-Standorten“ stellen lediglich eine beispielhafte Aufzählung dar. Aus heutiger Sicht kann nachvollzogen werden, dass eine künftige Aufnahme des Begriffes Register in die Aufzählung zielführend erscheint.

a) Welche Fortschritte bei Ausbau und Qualität der NdB wurden seit der Antwort auf die Schriftliche Frage 74 auf Bundestagsdrucksache 20/2170 erzielt?

Seit der vergangenen Anfrage aus dem Jahr 2022 können folgende Fortschritte für den Ausbau der NdB gemeldet werden:

Es erfolgten der Aufbau und Betrieb der Grundschutzzone Extranet (GS/Ex) sowie die Fertigstellung dedizierter Anschlüsse. Für die Überwachung des Netzes und dem Monitoring von Angriffen wurde ein Security Operations Center (SOC) installiert. Die Planung zur Nutzung und Umsetzung von IPv6 ist abgestimmt. TLS-Proxy steht zur Verfügung und wird mit dem Firewall-Redesign im Laufe dieses Jahres allen Nutzern angeboten werden können.

Erweiterungen der mobilen Einwahllösungen wurden vorgenommen und sind z. T. noch in der Umsetzung. Weiterhin werden derzeit notwendige vertragliche Anpassungen zur Zukunftsfähigkeit der NdB vorgenommen. Auch die Thematik zur Weiterentwicklung hin zum IVÖV ist in Planung.

* Von einer Drucklegung der Anlage wird abgesehen. Diese ist auf Bundestagsdrucksache 20/15138 auf der Internetseite des Deutschen Bundestages abrufbar.

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 der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) bereitgestellte Lösung zur Erhöhung der Sicherheit dieser Nutzer (TLS-Proxy) unverändert seit 2022 nicht nutzen?

Um die Sicherheit in NdB bis zur breitflächigen Nutzung der NdB-Grundschutzzone (GS/Ex) zu gewährleisten, bot das Bundesministerium des Innern und für Heimat (BMI) den Behörden eine ergänzende IT-Lösung, den sog. TLS-Proxy als eine Übergangslösung, an. Beim TLS-Proxy handelt es sich um eine Technik, um Schadsoftware auch in verschlüsselten Internetverkehren detektieren zu können. Der Bundesrechnungshof kritisierte in seinem Bericht, dass ein Großteil der NdB-Nutzer, die die Sicherheitsanforderungen nicht erfüllen, den zentralen TLS-Proxy nicht einsetzen. Dennoch wird der TLS-Verkehr bei den meisten NdB-Nutzern bereits selbst untersucht bzw. durch die geschaffene, zentrale Lösung pilotweise detektiert. Die schrittweise Einführung des zentralen TLS-Proxys in den Wirkbetrieb ist ab Sommer 2025 geplant. Mittels einer zentralen Migration wird darauf hingewirkt, dass alle Nutzer den zentralen TLS-Proxy schnellstmöglich verwenden.

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?

Bezüglich der generellen Maßnahmen zur Verbesserung der Netze des Bundes wird auf die Antwort zu Frage 9a verwiesen. Diese Maßnahmen werden im Rahmen der im laufenden Haushalt bereitgestellten Mittel kontinuierlich überprüft und angepasst. Für die hochleistungsfähigen Rechenzentren des ITZBund wurde ein gesonderter Anschlusstyp in den Netzen des Bundes eingeführt.

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

Die Netze des Bundes bestehen aus einer Vielzahl von Anschlüssen, Netzverbindungen und Diensten. Noch mögliche Optimierungen der Kapazitäten sind nahezu erschöpft. Der weitere Ausbau der Kapazitäten stößt zunehmend an die Grenzen der veralteten Architektur der technischen Basisplattform. Die Bereitstellung von Anschlussprodukten mit hohen Anschlussbandreiten von 10 Gbit/s und mehr durch den Carrier wird ebenfalls zunehmend schwierig. Diese Hemmnisse sind die Hauptgründe für die Fokussierung des Aufbaus einer neuen technischen Basisplattform sowie der Umsetzung einer Multi-Carrier-Strategie gemäß den Zielen der Netzstrategie 2030 zur Neuerrichtung eines Informationsverbundes der deutschen Verwaltung (IVÖV).

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?

Mit dem Handlungsfeld Cloud der IT-Strategie des Bundes hat der Bund festgelegt, Cloud-Technologie umfassend für die Bundesverwaltung verfügbar zu machen. Als Zielbild für den Themenbereich Cloud wird eine Multi Cloud Bund vorgegeben, welche es der Bundesverwaltung erlauben soll, auf unterschiedliche Cloud-Umgebungen mit unterschiedlichen Eigenschaften zurückzugreifen. Eine besondere Fokussierung auf Bundesregister liegt nicht vor, sodass keine Erfassung von Maßnahmen und finanziellen Mittel im Sinne der Fragestellung vorliegt.

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?

Die Fragen 10 und 10a werden zusammen beantwortet.

Ein einheitlicher, verbindlicher, standardisierter und ergebnisoffener Kriterienkatalog, auf dessen Grundlage bewertet wird, ob ein Transfer von Daten und Anwendungen der Bundesverwaltung in Clouds sinnvoll ist, liegt nicht vor. Die Entscheidungen hierfür sind bezogen auf konkrete Anwendungsfälle herbeizuführen. Mit Beschluss des IT-Rats vom 29. Juli 2015 wurden Grundsätze für die Einrichtungen des Bundes bezüglich ihrer Planungen, Bedarfsbeschreibungen und Vergaben zur etwaigen Verwendung von Cloud-Diensten der IT-Wirtschaft nach festgelegt (vgl. www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/it-rat/beschluesse/beschluss_2015_05.pdf?__blob=publicationFile&v=1).

b) Wird bei Entscheidungen für oder gegen einen Transfer in die Cloud regelmäßig die Wirtschaftlichkeitsbetrachtung (WiBe) 5.0 (www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/digitale-loesungen/it-beschaffung/wirtschaftlichkeitsbetrachtung/wibe5-0/wibe-fachkonzept-5-0.pdf) bzw. 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 „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?

Die Fragen 10b und 10c werden zusammen beantwortet.

Eine Wirtschaftlichkeitsbetrachtung (WiBe) muss von einer Behörde durchgeführt werden, wenn sie eine Investition, eine größere Beschaffung oder ein IT-Projekt plant. Die WiBe dient dazu, die wirtschaftlichste Lösung zu identifizie-

ren sowie die Nachhaltigkeit der Maßnahme zu bewerten. Sofern die Entscheidung für oder gegen einen Transfer in die Cloud, eine Investition, ein IT-Projekt oder eine größere Beschaffung darstellt, ist eine WiBe durchzuführen.

Vor der Entscheidung zum Aufbau der Deutschen Verwaltungscloud wurde die in der Fragestellung zitierte WiBe durchgeführt. Dabei wurde davon ausgegangen, dass es mittelfristig keine vertretbare Option sein wird, bestimmte Daten nicht in die DVC zu transferieren. Die WiBe kam zu dem Ergebnis, dass der Aufbau wirtschaftlich und nachhaltig ist.

Diese damalige WiBe ist abgeschlossen und kann daher nicht mehr für Entscheidungen für oder gegen den Transfer bestimmter Daten in die Cloud verwendet werden. Die damalige Einschätzung, dass mittelfristig bestimmte Daten in die DVC transferiert werden müssen, hat keinen Einfluss auf aktuelle Entscheidungen hinsichtlich konkreter Daten.

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

Bund und Länder arbeiten im Rahmen der Umsetzung der DVS beim Aufbau der DVC eng zusammen. Das Cloud-Service-Portal der DVC bietet den angeschlossenen IT-Dienstleistern der Öffentlichen Verwaltung die Möglichkeit, Cloud-Lösungen anderer IT-Dienstleister zu beziehen und Cloud-Lösungen anderen IT-Dienstleistern zur Verfügung zu stellen.

Über den regelmäßigen Austausch zu Cloud-Fragen in der AG Cloud Computing und Digitale Souveränität des IT-Planungsrats hinaus bestehen derzeit keine unmittelbaren Kooperationen zur gemeinsamen Beschaffung von Clouds mit den Bundesländern.

a) Wie erfolgt dabei der Austausch mit den Bundesländern zu deren aktuellen Cloud-Vorhaben, wie z. B. 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 10b 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?

Cloud- und diesbezügliche Standardisierungsvorhaben von Bund und Ländern sind regelmäßig Gegenstand eines Austauschs in gemeinsamen Gremien des IT-Planungsrats. Der Bund prüft aktuell im sog. MSSC-Projekt die Nutzbarkeit der angekündigten Delos-Cloud, über die bislang in der Verwaltung on-premise genutzte Microsoft-Arbeitsplatzdienste der deutschen Verwaltung perspektivisch angeboten werden sollen. Zum MSSC-Projekt besteht ein regelmäßiger Austausch zwischen Bund und Ländern.

In der AG Cloud Computing und Digitale Souveränität des IT-Planungsrats sind alle Bundesländer vertreten, dazu gehört auch Niedersachsen. In diesem Format tauschen sich Bund und Länder zu allen Themen hinsichtlich der Deutschen Verwaltungscloud und eigener Cloud-Projekte wie bspw. dem Vorhaben aus Niedersachsen aus. Hinsichtlich der Frage zur zentralen Beschaffung von Cloud-Services über die DVC ist festzustellen, dass eine solche aus Sicht der DVC weiterhin wünschenswert ist. Derzeit befindet sich die DVC jedoch noch im Aufbau. Sofern bei einzelnen Ländern (z. B. Niedersachsen) derzeit ein dringender Bedarf an Cloud-Leistungen besteht, ist eine zeitnahe Beschaffung nachvollziehbar.

b) Welche Bedeutung hat bei diesem Bund-Länder-Austausch der geplante Roll-Out von OpenDesk über das Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) nach Kenntnis der Bundesregierung in den Bundesländern, und welche Cloud-Anbieter sind der Bundesregierung bekannt, die OpenDesk anbieten oder angekündigt haben, es anzubieten?

Die ZenDiS GmbH stellt in regelmäßigen Abständen den Sachstand zu openDesk in der AG Cloud Computing und Digitale Souveränität des IT-Planungsrats dar. Die Länder erhalten dabei die Möglichkeit der ZenDiS GmbH Fragen zu stellen. Geplante länderspezifische Rollouts haben in dem Austausch keine herausgehobene Bedeutung.

Derzeit wird openDesk durch die ZenDiS GmbH angeboten, den dafür notwendigen Betrieb verantworten die Cloud-Anbieter STACKIT GmbH und IONOS SE. Weitere privatwirtschaftliche Unternehmen prüfen den Betrieb und damit verbundene Angebote.

Darüber hinaus prüfen öffentliche IT-Dienstleister derzeit einen eigenen Betrieb von OpenDesk.

c) Welche Bedeutung hat bei diesem Bund-Länder-Austausch das für 2029 angekündigte Auslaufen des Supports für „on-premise“-genutztes Microsoft 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. Vorbemerkung der Bundesregierung auf Bundestagsdrucksache 20/12864)?

Der Austausch dient in der Sache dem Wissenstransfer zwischen Bund und Ländern. Im Kern stehen das Prüfvorgehen und die Prüfanforderungen hinsichtlich der „on-premise“-genutzten Microsoft-Produkte. Dies erfolgt je nach Bedarf in gemeinsamen Sitzungen und sonstiger geeigneter Informationsbereitstellung. Das angekündigte Auslaufen des Supports ist somit nicht nur Anlass des Projekts, sondern damit auch mittelbar Inhalt der Gespräche mit den Ländern.

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)?

Die Bundesregierung hat keine konkreten Planungen für die Ausschreibung längerfristiger und hochvolumiger Rahmenverträge mit Cloud-Anbietern, insbesondere solchen, die direkt oder indirekt Cloud-Produkte von US-Hyperscalern anbieten. Ob zukünftig ein entsprechender Bedarf für die Aufgabenerfüllung des Bundes besteht, wird fortlaufend evaluiert und etwaige Planungen daran ausgerichtet.

Das Verfahren zum Abschluss von Rahmenvereinbarungen ist vergaberechtlich vorgeschrieben. Dies schließt auch Regelungen zur zulässigen Dauer von Rahmenvereinbarungen ein. Preise und Angebotskonditionen ergeben sich im Wege des durchgeführten Wettbewerbs und Verhandlungen.

12. Soll entsprechend Zielstellung des ITZBund die Bundescloud „zur zentralen Plattform für alle Dienste ausgebaut werden, die in der Bundesverwaltung genutzt 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?

Die Fragen 12 bis 12b werden zusammen beantwortet.

Um der Fülle und Varianz der Anforderungen gerecht zu werden und ein effizientes, marktübliches Cloudproduktportfolio bei gleichzeitigem internen Ressourcenmangel anbieten zu können, wird eine Multi-Cloud Strategie verfolgt. Gemäß dieser Strategie werden standardisierte Cloudprodukte aus mehreren Clouds zur Verfügung gestellt, um den Kundenbehörden für jeden Anwendungsfall die optimale und wirtschaftlichste Lösung bieten zu können. Die Kunden des ITZBund profitieren hierbei von einer schnelleren Erschließung neuer Technologien, sowie den damit verbundenen notwendigen Weiterentwicklungen von Cloudprodukten und somit einer Zukunftssicherheit. Die Kunden des ITZBund aus der Bundesverwaltung haben vielfältige Use Cases, die sich hinsichtlich des erforderlichen Schutzniveaus der Daten, der verfügbaren Ressourcen und weiterer Kriterien unterscheiden. Um den Kundenbehörden hier differenzierte und passgenaue Angebote aus der Cloud bereitstellen zu können, verfolgt das ITZBund eine Multi-Cloud-Strategie.

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

Die gewünschten Informationen können nicht offen übermittelt werden. Auf die Begründung in der Vorbemerkung der Bundesregierung wird verwiesen. Die gewünschten Angaben werden daher in Tabellenform als Anlage 2* mit dem Vermerk „VS-Nur für den Dienstgebrauch“ übersandt.

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, und wenn nein, warum nicht?

Hier ist zu unterscheiden. Die Bundescloud ist eine zentrale Cloud-Plattform, die für die Bundesverwaltung vom ITZBund betrieben wird. Sie bietet verschiedene IT-Dienste an, darunter Computing-Services und Datenspeicherung. Bei der Bundescloud handelt es sich um eine einzelne Cloud und nicht um eine föderierte Cloud, da hier gerade nicht mehrere unabhängige Cloud-Dienste zusammengekoppelt werden, um gemeinsam genutzte Ressourcen zur Verfügung zu stellen.

Die Bundesregierung sieht verschiedene Vorteile einer föderierten Cloud. Sie sichert die digitale Souveränität, da Nutzer nicht von einzelnen Anbietern abhängig sind. Durch die einer föderierten Cloud inhärente Interoperabilität kön-

* Das Bundesministerium des Innern und für Heimat hat die Antwort als „VS-Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

nen verschiedene Cloud-Anbieter nahtlos zusammenarbeiten, was Flexibilität und Skalierbarkeit erhöht. Zudem führt die gemeinsame Nutzung von Ressourcen zu Kostenersparnissen und kann helfen, dem IT-Fachkräftemangel der Verwaltung zu begegnen. Die Bundesregierung fördert mit der DVC einen solchen föderierten Ansatz.

15. Welches Budget stand dem ITZBund 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) Public Clouds (jeweils für interne und externe Kosten),

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

    f) ggf. weitere Clouds des Bundes?

Auf die Anlage 3 wird verwiesen.*

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

Auf die Anlage 4 wird verwiesen.*

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

Auf die Anlage 5 wird verwiesen.*

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)?

Die EVB-IT Vertragsmuster sehen umfassende Möglichkeiten für die Beendigung von Leistungsbeziehungen vor. In den EVB-IT Cloudvertrag können verschiede Leistungen für das „Migration out“ vereinbart werden. Zudem umfassen die EVB-IT Cloud verschiedene Regelungsmöglichkeiten für die Nachnutzung von Daten sowie Datenexport.

* Von einer Drucklegung der Anlage wird abgesehen. Diese ist auf Bundestagsdrucksache 20/15138 auf der Internetseite des Deutschen Bundestages abrufbar.

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?

Auf die Anlage 6 wird verwiesen.*

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

Es wird auf die Vorbemerkung in der Antwort auf die Schriftliche Frage 21 des Abgeordneten Matthias Hauer (CDU/CSU) auf Bundestagsdrucksache 20/14451 verwiesen.

    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 bzw. Ziel?

Eine Verpflichtung zur Erfassung sämtlicher geführter Gespräche – einschließlich Telefonate und elektronischer Kommunikation – bzw. deren Ergebnissen besteht nicht, und eine solche umfassende Dokumentation wurde auch nicht durchgeführt (siehe dazu die Vorbemerkung der Bundesregierung in der Antwort auf die Kleine Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/1174). Zudem werden Gesprächsinhalte nicht protokolliert. Die nachfolgenden Ausführungen bzw. aufgeführten Angaben erfolgen auf der Grundlage der vorliegenden Erkenntnisse sowie vorhandener Unterlagen und Aufzeichnungen. Diesbezügliche Daten sind somit möglicherweise nicht vollständig.

Datum	Gesprächsthema/ Ziel	Teilnehmende (SAP, Delos, Microsoft)	Teilnehmende (Bundesregierung)
22.01.2025	Allgemeiner Austausch, u. a. Delos-Cloud	Brad Smith (Microsoft)	BM Dr. Kukies
05.12.2024	Lizenzmodell SAP und Delos-Cloud	Hr. Saueressig (SAP) und Hr. Hagl (SAP)	Staatssekretärin Prof. Dr. Luise Hölscher

    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 hat die Bundesregierung selbst?

Die Cloud der Delos GmbH ist ein Marktangebot. Der Bundesregierung sind die firmeninternen Ziele der Delos GmbH bzgl. des Roll-Outs etc. nicht bekannt. Das MSSC-Projekt ist ein Prüfprojekt in welchem überprüft werden soll, ob das Marktangebot der Delos-Cloud die Anforderungen der Bundesregierung

* Von einer Drucklegung der Anlage wird abgesehen. Diese ist auf Bundestagsdrucksache 20/15138 auf der Internetseite des Deutschen Bundestages abrufbar.

erfüllen kann. Auf Basis des Prüfergebnisses wird die Bundesregierung über den Bezug von Leistungen aus der Delos-Cloud entscheiden.

21. Ist das Bundesamt für Sicherheit in der Informationstechnik (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?

Das BSI war von Beginn an bei der DVS beratend beteiligt. Aktuell ist das BSI im Themenkreis 5 „Informationssicherheit und Datenschutz“ sowie im „Architektur-Board“ vertreten. Mit Blick auf den genannten Artikel auf der BSI-Webseite wird die DVS bzw. die DVC unter nationale Cloud-Anbieter subsummiert.

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?

Die Ausschreibungen des Bundes richten sich nach den festgestellten Bedarfen der Behörden des Bundes. Im Rahmen der Bedarfsdefinition sind die unterschiedlichsten Anforderungen an den Beschaffungsgegenstand zu berücksichtigen, u. a. auch Cloud-Stacks, die keine Open Source-Lösung sind.

23. Wird für den Cloud-Stack und bzw. 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)?

Der Einsatz von OSS spielt bei der Entwicklung und dem Betrieb der Bundescloud eine sehr wichtige Rolle. Die Bundescloud ist eine Eigenentwicklung des Bundes und keine gekaufter Cloud-Stack. Wo möglich wird OSS eingesetzt, wo nötig kann auch davon abgewichen werden. Entscheidend dafür sind die funktionalen und nicht funktionalen Anforderungen – aus der Bundesverwaltung –, die zu erfüllen sind. In der Bundescloud betrifft dies in erster Linie spezielle Themen wie die Virtualisierungsschicht, in der auch proprietäre Software eingesetzt wird. Vereinzelt gibt es auch Systeme, die mit Windows betrieben werden; für diese liegen entsprechende Anforderungen vor, hier Betrieb eines Windows Update Servers für das Patchen von Windows Betriebssystemen, die durch den Kunden in der Bundescloud bestellt werden können.

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

Bei der Frage, ob es sich bei den Cloud-Angeboten um souveräne Clouds im Sinne der o. g. Definition (Frage 2) handelt, sind jeweils die strategischen Ziele zur Stärkung der Digitalen Souveränität die Wechselfähigkeit, die Gestaltungsfähigkeit und der Einfluss auf IT-Anbieter zu bewerten.

Die Bewertung der Wechselfähigkeit von Cloud-Angeboten kann nicht pauschal durchgeführt werden, da die Bewertung von den zu wechselnden Diens-

ten und Daten abhängt. Sofern bei der Softwareentwicklung auf cloud-agnostische Ansätze geachtet wird, sollte ein Wechsel zwischen verschiedenen Clouds grundsätzlich möglich sein. Dies ist deshalb der Fall, da eine solche Software nicht an eine spezifische Cloud-Plattform gebunden ist, sondern standardisierte Schnittstellen und Technologien nutzt. Sofern sie z. B. auf Container-Technologien, wie Docker oder Kubernetes basiert, die eine einheitliche und portable Laufzeitumgebung bieten, reduziert sich der Migrationsaufwand. Anders kann sich die Sachlage darstellen, wenn die zu wechselnden Anwendungen eine tiefe Integration in das Cloud-Ökosystem des Anbieters (z. B. Nutzung von Anbieterspezifischen Services wie bspw. Verzeichnis- oder exklusive Datenbankdienste) aufweisen. Auch dies ist aber letztlich keine Frage der angebotenen Cloud, sondern der Nutzung des Cloud-Ökosystems des Anbieters. Da die genannten Cloud-Dienste jeweils standardisierte Schnittstellen und Dienste anbieten, ist die Wechselfähigkeit kein geeignetes Kriterium, um die Digitale Souveränität einzelner Cloud-Plattformen allgemein zu bewerten.

Ähnliches gilt für das Kriterium Gestaltungsfähigkeit. Dieses erfordert, dass die Verwaltung ihre IT mitgestalten und bei Bedarf weiterentwickeln kann. Alle in der Frage genannten Clouds ermöglichen es, IaaS-, PaaS- und SaaS-Angebote selbst zu betreiben. Es obliegt den IT-Dienstleistern zu entscheiden, bis zu welchem Fertigungsgrad sie selbst Leistungen erbringen bzw. Verantwortung übernehmen. Wenn bspw. ein IT-Dienstleister nur die IaaS-Angebote nutzt, kann er auf diesen aufbauend eigene Softwarelösungen erstellen, betreiben und weiterentwickeln. Somit ist auch die Gestaltungsfähigkeit kein geeignetes Kriterium, um die Digitale Souveränität einzelner Cloud-Plattformen allgemein zu bewerten.

Bei dem Kriterium des Einflusses auf den Anbieter geht es um die Frage, ob die Verwaltung in der Lage ist, bei Verhandlung und Vertragsgestaltung ihre Anforderungen und Bedarfe, bspw. den Betrieb in eigenen Rechenzentren oder den Einfluss auf Lizenzmodelle und die Produkt-Roadmap durchzusetzen. Kriterien dafür können bspw. eine mögliche Kapitalbeteiligung des Bundes, ein hoher Umsatzanteil der öffentlichen Verwaltung hinsichtlich des Konzernumsatzes und ein Firmensitz in Deutschland (Jurisdiktion) sein. Bei der Bewertung des Umsatzanteils wird als Referenz die kürzlich erfolgte Ausschreibung des ITZBund im Cloud-Bereich herangezogen. Für den vergebenen Rahmenvertrag an die IONOS SE wurde eine Obergrenze von 410 Millionen Euro für fünf Jahre vereinbart. Als Größenordnung entspräche das circa 80 Millionen pro Jahr.

a) Microsoft,

Die Bundesregierung geht bei der Frage 24a davon aus, dass es sich um das Public Cloud Angebot von Microsoft (Azure) handelt. Der Vertragspartner wäre die Microsoft Ireland Operations Ltd., welche keinen Firmensitz in Deutschland hat. Der Bund ist an dieser nicht beteiligt. Der Jahresumsatz der Microsoft Ireland Operations Ltd. betrug ausweislich des letzten verfügbaren Geschäftsberichts 2023 circa 70 Mrd. US-Dollar. Bei einer möglichen Beauftragung durch die Verwaltung gemäß der o. g. Referenz wäre von keinem hohen Umsatzanteil für Cloud-Leistungen auszugehen. Der Einfluss auf den IT-Anbieter wäre somit gering.

b) Delos,

Der Vertragspartner wäre die DELOS GmbH, welche ihren Firmensitz in Deutschland hat. Der Bund ist an dieser nicht beteiligt. Eigentümer der DELOS GmbH ist die SAP SE. Der Jahresumsatz der SAP SE betrug ausweislich des letzten verfügbaren Geschäftsberichts 2024 circa 34 Mrd. Euro. Bei einer mög-

lichen Beauftragung durch die Verwaltung gemäß der o. g. Referenz wäre von keinem hohen Umsatzanteil für Cloud-Leistungen auszugehen. Der Einfluss auf den IT-Anbieter wäre etwas höher, da das Unternehmen einen Firmensitz in Deutschland hat.

c) Google/T-Systems,

Die Bundesregierung geht bei der Frage 24c davon aus, dass es sich um das Angebot „T-Systems Sovereign Cloud powered by Google Cloud“ handelt.

Der Vertragspartner wäre die T-Systems International GmbH, welche ihren Firmensitz in Deutschland hat. Eigentümer ist die Deutsche Telekom AG, an welcher der deutsche Staat 27 Prozent der Anteile hält. Der Jahresumsatz betrug ausweislich des letzten verfügbaren Geschäftsberichts 2024 circa 116 Mrd. Euro. Bei einer möglichen Beauftragung durch die Verwaltung gemäß der o. g. Referenz wäre von keinem hohen Umsatzanteil für Cloud-Leistungen auszugehen. Der Einfluss auf den IT-Anbieter wäre durch die Beteiligung und den Firmensitz in Deutschland relativ hoch.

d) Amazon,

Der Vertragspartner wäre die Amazon Web Service Germany GmbH, welche ihren Firmensitz in Deutschland hat. Der Bund ist an dieser nicht beteiligt. Eigentümer ist die Amazon.com Inc. Der Jahresumsatz der Amazon.com Inc. betrug ausweislich des letzten verfügbaren Geschäftsberichts 2023 circa 575 Mrd. Euro. Bei einer möglichen Beauftragung durch die Verwaltung gemäß der o. g. Referenz wäre von keinem hohen Umsatzanteil für Cloud-Leistungen auszugehen. Der Einfluss auf den IT-Anbieter wäre somit nicht sehr hoch, da er sich lediglich daraus ergibt, dass das Unternehmen einen Firmensitz in Deutschland hat.

e) Oracle,

Der Vertragspartner wäre die Oracle Deutschland B.V. & Co. KG, welche ihren Firmensitz in Deutschland hat. Der Bund ist an dieser nicht beteiligt. Eigentümer ist die Oracle Cooperation. Der Jahresumsatz der Oracle Cooperation betrug ausweislich des letzten verfügbaren Geschäftsberichts 2023 circa 50 Mrd. Euro. Bei einer möglichen Beauftragung durch die Verwaltung gemäß der o. g. Referenz wäre von keinem hohen Umsatzanteil für Cloud-Leistungen auszugehen. Der Einfluss auf den IT-Anbieter wäre somit nicht sehr hoch, da er sich lediglich daraus ergibt, dass das Unternehmen einen Firmensitz in Deutschland hat.

f) Ionos,

Der Vertragspartner wäre die IONOS SE, welche ihren Firmensitz in Deutschland hat. Der Bund ist an dieser nicht beteiligt. Hauptanteilseigner ist die United Internet AG. Der Jahresumsatz der United Internet AG betrug ausweislich des letzten verfügbaren Geschäftsberichts 2024 circa 6,2 Mrd. Euro. Bei einer möglichen Beauftragung durch die Verwaltung gemäß der o. g. Referenz wäre von keinem hohen Umsatzanteil für Cloud-Leistungen auszugehen. Der Einfluss auf den IT-Anbieter wäre somit nicht sehr hoch, da er sich lediglich daraus ergibt, dass das Unternehmen einen Firmensitz in Deutschland hat.

g) Schwarz Gruppe (STACKIT),

Der Vertragspartner wäre die STACKIT GmbH Co. KG, welche ihren Firmensitz in Deutschland hat. Der Bund ist an dieser nicht beteiligt. Sie ist Teil der

Schwarz Gruppe. Der Jahresumsatz der Schwarz Gruppe betrug ausweislich des letzten verfügbaren Geschäftsberichts 2024 circa 167 Mrd. Euro. Bei einer möglichen Beauftragung durch die Verwaltung gemäß der o. g. Referenz wäre von keinem hohen Umsatzanteil für Cloud-Leistungen auszugehen. Der Einfluss auf den IT-Anbieter wäre somit nicht sehr hoch, da er sich lediglich daraus ergibt, dass das Unternehmen einen Firmensitz in Deutschland hat.

h) plusserver (pluscloud),

Der Vertragspartner wäre die PlusServer GmbH, welche ihren Firmensitz in Deutschland hat. Der Bund ist an dieser nicht beteiligt. Der Jahresumsatz der PlusServer GmbH betrug ausweislich des letzten verfügbaren Geschäftsberichts 2021 circa 94 Mio. Euro. Bei einer möglichen Beauftragung durch die Verwaltung gemäß der o. g. Referenz wäre von einem hohen Umsatzanteil für Cloud-Leistungen auszugehen. Der Einfluss auf den IT-Anbieter wäre somit relativ hoch, da er sich sowohl aus einem vergleichsweise hohen Umsatzanteil sowie daraus ergäbe, dass das Unternehmen einen Firmensitz in Deutschland hat.

i) Secunet/Syseleven und

j) ggf. weiterer Anbieter

(bitte argumentativ begründen)?

Die Bundesregierung geht bei der Frage 24i davon aus, dass es sich um das Cloud Angebot von SysEleven handelt.

Der Vertragspartner wäre die SysEleven GmbH welche ihren Firmensitz in Deutschland hat. Der Bund ist an dieser nicht beteiligt. Eigentümer ist die secunet Security Networks AG. Der Jahresumsatz der secunet Security Networks AG betrug ausweislich des letzten verfügbaren Geschäftsberichts 2023 circa 394 Mio. Euro. Bei einer möglichen Beauftragung durch die Verwaltung gemäß der o. g. Referenz wäre von einem relativ hohen Umsatzanteil für Cloud-Leistungen auszugehen. Der Einfluss auf den IT-Anbieter wäre somit relativ hoch, da er sich sowohl aus einem vergleichsweise hohen Umsatzanteil sowie daraus ergäbe, dass das Unternehmen einen Firmensitz in Deutschland hat.

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?

Die Nutzung des Sovereign Cloud Stack wurde im Rahmen des Umsetzungsprojektes der DVC pilotiert. Eine weitere Nutzung wird derzeit eruiert. Das Förderprojekt Sovereign Cloud Stack ist abgeschlossen. Eine weitere Förderung durch den Bund ist aktuell nicht vorgesehen.

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?

Der Beauftragte der Bundesregierung für Informationstechnik hat mit der IT-Architekturrichtlinie Bund in der technischen Vorgabe Nummer 10 den Betrieb auf standardisierten Betriebsumgebungen verbindlich empfohlen. Zu den standardisierten Betriebsumgebungen gehört u. a. auch der Sovereign Cloud Stack. Die weitere Ausgestaltung der Vorgaben zu Betriebsumgebungen ist in den Fortschreibungen der IT-Architekturrichtlinie Bund eingeplant. Die Anwendung und Wirksamkeit der Vorgaben haben die jeweiligen Bedarfsträger sicherzustellen.

27. Inwiefern wird beim Aufbau einer OSS-basierten souveränen Bundescloud mit der UN (United Nations) kooperiert oder werden Erfahrungen ausgetauscht, z. B. hinsichtlich der von UNICC (United Nations International Computing Centre) und Canonical aufgebauten privaten Cloud auf Open-Stack-Basis (www.unicc.org/news/2023/10/19/unicc-partners-with-canonical-to-build-unicc-cloud/), und welchen Erfahrungsaustausch gibt es zu OSS-Cloud-Vorhaben ggf. auch mit anderen internationalen Partnern?

Zwischen dem ITZBund und der UN findet kein Austausch zum United Nations International Computing Centre (UNICC) statt. Austausche mit IT Dienstleistern der öffentlichen Verwaltung haben in den letzten Jahren mit mehreren europäischen Ländern wie bspw. Frankreich, Dänemark und Österreich stattgefunden und sind auch zukünftig weiterhin geplant. Austausche fanden darüber hinaus auch mit Ländern außerhalb Europas statt, bspw. mit Kanada.

28. Welche Hürden gibt es für eine verstärkte Beschaffung von OSS-Cloud-Diensten durch den Bund nach Ansicht der Bundesregierung (z. B. Anforderungen in Ausschreibungen wie Referenzen, Umsatz- oder Nutzendenzahlen, 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 bzw. wird die Bundesregierung diese Hürden jeweils abbauen, um die angestrebte Stärkung der digitalen Souveränität zu erreichen?

Die Bundesregierung sieht keine spezifischen Hürden in der Beschaffung von OSS-Cloud-Diensten. Dies setzt voraus, dass entsprechende Open Source-Cloud-Dienste am Markt verfügbar sind und Unternehmen existieren, die erforderliche Betriebs- und Pflegeleistungen übernehmen. Aufgrund der durch § 16a des E-Government-Gesetzes geschaffenen Soll-Vorschrift hinsichtlich des Vorrangs von Open Source Software geht die Bundesregierung davon aus, dass die Beschaffung von Open Source Software in der Bundesverwaltung zunehmen wird.

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, weil ihr Kern die proprietäre Cloud eines US-Konzerns sei (Bianca Kastl; www.bundestag.de/ausschuesse/a23_digitales/Anhoerungen/1024966-1024966)?

Die von der Sachverständigen genutzte Definition für Digitale Souveränität weicht von der im IT-Planungsrat beschlossenen Definition ab. Digitale Souveränität wird nach Maßgabe des IT-Planungsrates definiert als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können.“ Daraus werden, wie oben bereits dargestellt, die drei strategischen Ziele Wechselfähigkeit, Gestaltungsfähigkeit und Einfluss auf IT-Anbieter abgeleitet. Es ist Aufgabe des Prüfprojekts MSSC zu bestimmen, inwiefern die Nutzung der Delos Cloud die Anforderungen des Bundes erfüllt. Es ist weiterhin festzuhalten, dass nach Einschätzung der Bundesregierung die Verwendung proprietärer Software oder einzelner proprietärer Softwarekomponenten nicht zwangsläufig zur Einschränkung der digitalen Souveränität führt.

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?

Ja. Die Bundesregierung teilt die Auffassung, dass die Veröffentlichung des Quellcodes die zwingende Voraussetzung zur Bezeichnung als Open Source ist. Die Definition wird durch die Open Source Initiative (OSI) festgelegt. Danach muss der Quellcode öffentlich zugänglich sein.

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?

Die Cloud-Strategie des BSI zielt auf die sichere Nutzung von Clouds ab und darauf, wie das Sicherheits-Potenzial von Cloud-Computing gefördert werden kann. Die Cloud-Strategie des BSI definiert dafür Ziele, denen sich das BSI in diesem Komplex besonders widmet. Die Nennung von zwei Beispielen im Artikel des BSI-Magazins ist keine abschließende Liste der Clouds, mit denen sich das BSI beschäftigt.

Mit Blick auf den genannten Interoperable Europe Act (IEA) besteht keine Widersprüchlichkeit, da es im IEA nicht um eine OSS-Infrastruktur geht, sondern um Interoperabilität von (Verwaltungs-) Anwendungen. In Abhängigkeit der technischen Ausgestaltung können (Verwaltungs-) Anwendungen von Cloud-Anbietern dabei unterschiedlich unterstützt werden.

32. Liegen dem mit Oracle im Mai 2023 geschlossenen Rahmenvertrag über 4,8 Mrd. Euro (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 nach Cloud-Services und sonstigen Leistungen aufschlüsseln)?

Dem mit Oracle im Mai 2023 geschlossenen Rahmenvertrag 21728 liegen die EVB-IT Cloud sowie die dazugehörigen AGBs zugrunde.

Aus der Rahmenvereinbarung wurden im Jahr 2023 Cloud-Services i. H. v. 180 000 Euro (netto) abgerufen, im Jahr 2024 betrugen die Abrufe 548 000 Euro (netto).

Sonstige Leistungen wurden i. H. v. 52 795 207,76 Euro (netto) im Jahr 2023 abgerufen. Im Jahr 2024 beliefen sich die Abrufe für sonstige Leistungen auf 83 455 405,79 Euro (netto).

33. Warum wurde laut Antwort auf die Schriftliche Frage 57 der Abgeordneten Anke Domscheit-Berg (Gruppe Die Linke) auf Bundestagsdrucksache 20/14188 eindeutig auch Azure-Cloud von Microsoft ohne Anwendung einer EVB-IT beschafft, obwohl die EVB-IT laut Antwort zu Frage 17 auf Bundestagsdrucksache 20/12864 verbindlich anzuwenden sind, wenn die konkrete Beschaffung in den Anwendungsbereich eines passenden Vertragsmusters (z. B. die EVB-IT-Cloud) fällt?

Die Anwendung eines einzelnen EVB-IT Vertragsmusters war in dem oben benannten Fall aus fachlichen Gründen nicht möglich. In einer Bestellung zu einem Enterprise Agreement müssen ggf. verschiedene Lizenzmodelle (On-Premise-Lizenzen mit dauerhaften Nutzungsrechten, On-Premise-Abonnements und Cloud-Services) miteinander kombiniert werden. Hierfür ist kein passendes Vertragsmuster vorhanden, sondern es müssen vielmehr drei verschiedene EVB-IT Vertragsmuster Anwendung finden, namentlich Überlassung Typ-A, Überlassung Typ-B und EVB-IT Cloud. Daher wurde eine Kombination der entsprechenden Anforderungen aus diesen drei EVB-IT Vertragsmustern in einer Vereinbarung zusammengeführt.

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 wenn nein, warum nicht?

Die verbindliche Anwendung der EVB-IT ergibt sich im Bund aus der Verwaltungsvorschrift zu § 55 der Bundeshaushaltsordnung (BHO). Danach sind die EVB-IT zu berücksichtigten. Aufgrund der Ausnahmeregelung in § 112 BHO gilt dies nicht für die dort genannten Träger wie z. B. der gesetzlichen Krankenversicherung, der sozialen Pflegeversicherung oder der gesetzlichen Rentenversicherung. Das Berücksichtigungsgebot erstreckt sich nur auf Fälle, die von den EVB-IT Verträgen abgedeckt sind. Bei komplexen Beschaffungen oder neuen Technologien ist daher eine Ergänzung oder Abweichung zulässig. Der EVB-IT Cloudvertrag ist derzeit nicht als Rahmenvereinbarung ausgestaltet. Die Cloudrahmenvereinbarung wird derzeit von der AG EVB-IT im Dialog mit der Beschaffungspraxis entwickelt und im Rahmen des aktuellen Reviews des Cloudvertrages mit der Digitalwirtschaft verhandelt. Derzeit ist daher bei der Beschaffung von Cloudleistungen als Rahmenvereinbarung eine Anpassung oder Abweichung erforderlich.

Alle EVB-IT Verträge wurden für eine leichtere Beschaffung von Open Source-Software und von Dienstleitungsprodukten für Open Source-Software verbessert. Diese Neufassungen sind derzeit in intensiver Verhandlung mit der Digitalwirtschaft. Nach erfolgreichem Abschluss der Abstimmungen werden die verbesserten EVB-IT für die Beschaffung bereitgestellt. Die Frage, ob ein Beschaffungsbedarf mit Open Source-Software gedeckt werden soll, ist dem Vergabeverfahren vorgelagert. Die EVB-IT Verträge können auch in vergaberechtlicher Hinsicht hier kein proprietäres Produkt diskriminierten. Es ist zudem zu beachten, dass die EVB-IT Verträge für die gesamte öffentliche Hand von Bund, Ländern und Kommunen bereitgestellt werden und daher die Interessen aller Nutzenden berücksichtigen müssen.

35. Was hat das Prüfprojekt zur Microsoft-Cloud-Technologie, die der IT-Rat laut Antwort zu Frage 8 auf Bundestagsdrucksache 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 zu Frage 14a auf Bundestagsdrucksache 20/12864 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 Anforderungen: Informationssicherheit, Datenschutz und Geheimschutz eingehen)?

Das Prüfprojekt ist noch nicht abgeschlossen.

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

Das Prüfprojekt unterteilt sich in zwei Phasen und endet mit Abschluss der Prüfphase 2 (Testbetrieb). Die aktuelle Planung sieht vor, dass die Prüfungen bis Ende 2026 abgeschlossen werden. Es wird ein Abschlussbericht erarbeitet. Die Veröffentlichung des Abschlussberichts ist nicht geplant, sofern Interna der Partner im Prüfprojekt im Abschlussbericht enthalten sind. Im Rahmen der Prüfungen im Prüfprojekt werden auch die Anforderungen des Bundes an von Dritten betriebene private Cloud detailliert, diese Detaillierungen werden veröffentlicht.

b) Wie bewertet die Bundesregierung die Kompromittierung der Microsoft-Cloud-Infrastruktur (durch einen erfolgreichen Angriff auf Outlook Web Access [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 bzw. technischen Verbesserungen in dem oben genannten Prüfungsprojekt einbezogen?

Die Bundesregierung teilt die Bewertung des BSI im Bericht zur Lage der IT-Sicherheit in Deutschland 2024. Auf Grundlage u. a. des Berichts des Cyber Safety Review Board (CSRB) hat das BSI sich unmittelbar nach dem Vorfall intensiv mit den technischen Hintergründen auseinandergesetzt und Microsoft gem. § 7a BSIG verpflichtet Informationen zu relevanten Schutzmechanismen zu veröffentlichen. Die Bundesregierung nimmt die im CSRB-Bericht an Microsoft sowie andere Cloud-Anbieter gerichteten empfohlenen Sicherheitsmaßnahmen zur Kenntnis und berücksichtigt diese im Prüfprojekt zur Delos-Cloud. Die von Microsoft auf Grundlage des CSRB-Berichts umgesetzten Maßnahmen

werden zudem nach Rücksprache mit dem BSI auch in die künftige Delos-Cloud übernommen.

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)?

Mit Blick auf den genannten Vorfall teilt die Bundesregierung die Bewertung des BSI, dass die Multifaktor-Authentifizierung in diesem Fall entgegen internationaler Empfehlungen umgesetzt wurde. Vor dem Hintergrund, dass Sicherheitslücken bei Cloud-Anbietern in der Regel viele Nutzer betreffen und somit als kritisch einzustufen sind, steht das BSI – analog zu dem in Frage 35b genannten Vorfall – zu den im CSRB-Bericht empfohlenen Maßnahmen sowie deren Umsetzung mit Microsoft im Austausch.

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 (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 zu Frage 18c auf Bundestagsdrucksache 20/12864 lediglich ein rein vertragliches Instrument ist, überhaupt nachweisbar sein, wenn Herausgabepflichten von Informationen gegenüber Drittstaaten der Geheimhaltung unterliegen (z. B. 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 Wissenschaftlichen Dienste (WD) des Deutschen 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, wenn ja, welche Schlüsse zieht sie daraus, und welche Auswirkungen ergeben sich daraus für die DVS und das geplante Portfolio des Cloud-Service-Portals?

Die Fragen 37 bis 37d werden zusammen beantwortet.

Im Rahmen des Mindeststandards des BSI zur Nutzung externer Cloud-Dienste (in der Version 2.1 vom 15. Dezember 2022) verweist das BSI u. a. auch auf die Pflicht zur Einhaltung nicht-technischer Regelungen durch Behörden und Einrichtungen des Bundes bei einer Cloud-Nutzung, wie etwa den hier zitierten Vergabe-Erlass des BMI aus 2014. Auf Grundlage des hier seitens BSI zitierten Erlasses des BMI werden für Vergabeverfahren, u. a. auch für die Cloud-Nutzung, eine Prüfung für die Verwendung einer Eigenerklärung sowie einer Vertragsklausel gefordert mit dem Ziel, den später ggf. notwendigen Nachweis eines vertragswidrigen Verhaltens, etwa durch nicht offengelegte Informationsabflüsse an ausländische Sicherheitsbehörden, zu ermöglichen. Darüber hinaus teilt die Bundesregierung die Auffassung der wissenschaftlichen Dienste des Bundestags, dass ein rein vertragliches Instrument allein, keinen ausreichenden Schutz vor unerwünschten Informationsausleitungen bietet. Mit Blick auf die Umsetzung der DVS sowie zur Unterstützung der Behörden und Einrichtungen des Bundes bei einer sicheren Cloud-Nutzung setzt die Bundesregierung neben zentralen Anforderungen und Prüfungen gem. BSIG auf umfangreiche Beratungsangebote des BSI sowie den direkten Austausch im Rahmen der IT-Governance des Bundes.

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 Europäischen Gerichtshof (EuGH) haben wird (vgl. Schrems-I- und Schrems-II-Urteile), insbesondere angesichts der Tatsache, dass Max Schrems als Sachverständiger im Digitalausschuss bereits am 26. Juni 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 (noyb.eu/de/us-cloud-soon-illegal-trump-punches-first-hole-eu-us-data-deal)?

Wie in der Antwort zu Frage 4 erläutert, können externe Angebote des Marktes nur über die besondere Rolle des Integrators in die DVC eingebunden werden. Dabei obliegt es den Integratoren die Anforderungen der Verwaltung sowie alle gesetzlichen Vorgaben umzusetzen. Aufgrund der Rechtsbindung der Verwaltung (Artikel 20, Absatz 3 des Grundgesetzes) kann davon ausgegangen werden, dass sich die IT-Dienstleister der Verwaltung an alle rechtlichen Vorgaben halten – dazu gehören selbstverständlich auch die Datenschutzregeln der EU unter Berücksichtigung der jeweils aktuellen Urteile der europäischen Gerichte.

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 bzw. der Plan dafür, und wenn nein, warum werden solche Exit-Strategien nicht für notwendig gehalten)?

Gemäß Handlungsfeld Cloud der IT-Strategie des Bundes ist neben privaten Clouds des Bundes die Anbindung von weiteren Cloud-Umgebungen vorgesehen. Bei deren Integration sind die Vorgaben der Architekturrichtlinie des Bundes und der Deutschen Verwaltungscloud-Strategie anzuwenden sowie die Gaia-X-Prinzipien zu berücksichtigen. Um sicherzustellen, dass die staatliche Handlungsfähigkeit nicht durch externe Eingriffe in die IT-Bereitstellung und den IT-Betrieb eingeschränkt oder sogar verhindert wird sowie um Lock-in Ef-

fekte zu vermeiden, sind Exit-Strategien zu erarbeiten. D. h., Exit-Strategien sind nicht je Cloud-Anwendung, sondern nur hinsichtlich der zugrundeliegenden Cloud-Technologie notwendig. Hinsichtlich der (Weiter-)Entwicklung von Fachverfahren hin zu Cloud-Anwendungen sind ebenfalls die oben genannten Vorgaben einzuhalten. Hierdurch sollen unter anderem Wechselfähigkeit der Cloud-Anwendungen zwischen unterschiedlichen Cloud-Technologien gewährleistet werden.

40. Welche Clouds haben bisher nach Kenntnis der Bundesregierung

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

Mit Blick auf die der Bundesregierung bekannten C5-Testate wird auf die Webseite http://www.c5-attestations.com verwiesen.

b) ein Zertifikat nach ISO 27001 erhalten,

Zertifikate nach „ISO 27001 auf Basis von IT-Grundschutz“ des BSI werden auch für Cloud-Anbieter auf der BSI-Seite (www.bsi.bund.de/dok/6617462) aufgeführt. Eine Liste der Cloud-Anbieter die ein solches Zertifikat haben, führt das BSI nicht. Nach Kenntnis der Bundesregierung existiert keine vollständige Liste aller ISO 27001-Zertifikate. Die Zertifizierungsstellen veröffentlichen jedoch oft die von ihnen ausgestellten Zertifikate.

c) eine Freigabe für eingestufte Informationen „VS-NfD“ (Verschlusssache-Nur für den Dienstgebrauch),

Die gewünschten Informationen können nicht offen übermittelt werden. Zur Begründung wird auf die Vorbemerkung der Bundesregierung verwiesen. Die gewünschten Angaben werden daher in Anlage 7* mit dem Vermerk „VS-Nur für den Dienstgebrauch“ übersandt.

d) eine Freigabe für die Vertraulichkeitsstufe „GEHEIM“?

Mitteilungen zu freigegebener Cloud-VS-IT für die Verarbeitung von VS der Geheimhaltungsgrade „VS-Vertraulich“ oder höher liegen dem BSI derzeit nicht vor.

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-Nur für den Dienstgebrauch“ sei, und wenn ja, welche Grundlagen in der DVS gibt es für eine derartige Vorreiterrolle?

Aus Sicht der Bundesregierung vereint das BSI für eine sichere Cloud-Nutzung wichtige Expertise und stellt diese der öffentlichen Verwaltung zur Verfügung. Wenngleich die Nutzer grundsätzlich eigenständig über die Nutzung bzw. Nicht-Nutzung von Cloud-Computing entscheiden, können u. a. durch die Beratung des BSI Vorteile für die IT-Sicherheit in der öffentlichen Verwaltung nutzbar gemacht werden.

* Das Bundesministerium des Innern und für Heimat hat die Antwort als „VS-Nur für den Dienstgebrauch“ eingestuft. Die Antwort ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Bei der Erarbeitung der DVS war den Beteiligten bewusst, dass die Speicherung und Verarbeitung eingestufter Informationen in der Cloud zukünftig ermöglicht werden soll. Dementsprechend wurde an herausgehobener Stelle das strategische Ziel „Sicherstellung und Stärkung von Datenschutz und Informationssicherheit“ formuliert.

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 Nutzerdaten und Metadaten getrennt beantworten)?

Auf die Anlage 8 wird verwiesen.*

    c) Wie bewertet die Bundesregierung (wenn zutreffend) das Fehlen der in Frage 42b 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?

Aus Sicht der Bundesregierung müssen, sofern für den betroffenen (Cloud-)Dienst keine Ende-zu-Ende-Verschlüsselung möglich ist, u. a. technische Maßnahmen ergriffen werden, um einen unerwünschten Zugriff bzw. eine Informationsausleitung weitestgehend nachweislich zu verhindern. Dieser Grundsatz gilt ebenso für rein europäische Clouds, OSS-Cloud-Lösungen in Eigenbetrieb sowie Nicht-Cloud-basierte Lösungen in Eigenbetrieb. Auf Grundlage einer u. a. sicherheitstechnischen, wirtschaftlichen sowie funktionalen Bewertung entscheiden nutzende Behörden und Einrichtungen des Bundes grundsätzlich eigenständig über den Einsatz von Cloud-Computing.

* Von einer Drucklegung der Anlage wird abgesehen. Diese ist auf Bundestagsdrucksache 20/15138 auf der Internetseite des Deutschen Bundestages abrufbar.

Anlage 1

Zu 8.

Verfügbare Services (Stand: 27.02.2025):

Service	**Serviceanbieter**	**Verfügbar seit / ab**
Dataport	dDataBox	01.09.2024
Dataport	dDataBox (Testversion)	01.09.2024
Dataport	DIPASaaS	01.09.2024
Dataport	dReservierung	01.09.2024
Dataport	dReservierung Testbetrieb	01.09.2024
Dataport	dMessenger	01.09.2024
Dataport	Terminfinder	01.09.2024
DVZ-MV	INTERAMT.kompakt	01.09.2024
DVZ-MV	INTERAMT.professional	01.09.2024
DVZ-MV	INTERAMT.data	01.09.2024
IT.NRW	NRW.Genius.Translate	30.09.2024
IT.NRW	Conceptboard by IT.NRW Demo	30.09.2024
LGLN	KI Gebäudeerkennung	30.09.2024
Komm.ONE	I-KFZ-4	30.09.2024
OWL IT	Kritzel (Outlook Signaturen)	30.09.2024
Betrieb für Informationstechnologie Bremerhaven (BIT)	Hallenbuchungsplan	01.12.2024
Betrieb für Informationstechnologie Bremerhaven (BIT)	Hallenbuchungsplan Demozugang	01.12.2024
Dataport	dMessenger Testversion	01.12.2024
GovConnect	pmPayment	09.12.2024
GovConnect	pmOrdnungsmanager	16.12.2024
GovConnect	pmOWI-App	24.01.2025
GovConnect	pmOWI-App Lite	18.12.2024
LDBV / IT-DLZ Bayern	Geodigitalisierungskomponente	27.01.2025
Komm.ONE	Chatbot für Kommunen und Landkreise	10.02.2025
Bundesdruckerei	Zertifikate	28.02.2025
Bundesdruckerei	Zentrale Siegelinfrastruktur	28.02.2025
Bundesdruckerei	Fernsignatur	28.02.2025
ekom21	esina21	28.02.2025
AKDB	OK.KOMM	28.02.2025
AKDB	Signaturservice	28.02.2025
Komm.ONE	Virtuelles Amt	28.02.2025
Komm.ONE	eRecruiting	28.02.2025
Dataport	dLernmanagementsystem - Moodle	28.02.2025
Dataport	BigBlueButton	28.02.2025
Dataport	KaaS (Kubernetes as a Service	28.02.2025
DVZ-MV	PZM-Prozessmanagement	28.02.2025
DVZ-MV	Online Whiteboard	28.02.2025

GovConnect	pmHundManager: Hundeverwaltung	15.03.2025
GovConnect	pmHundManager: digitale Hundemarke	15.03.2025
GovConnect	pmHundManager: Hundesteuer	15.03.2025

Services in Prüfung/Abstimmung (Stand 27.02.2025):

Hinweis: Für Services, welche in Prüfung/Abstimmung sind, kann keine verbindliche Zusage bzgl. der Aufnahme in das Cloud-Service-Portal der Deutschen Verwaltungscloud oder hinsichtlich der zeitlichen Verfügbarkeit getroffen werden. Die Prüfungen bzgl. der Aufnahme von Services sind aktuell noch Einzelfalluntersuchungen.

Service	**Servicekategorie**
API Hub	Datenintegration und APIs
ARIS for FIM	Prozessautomatisierung & Prozessmanagement
ARIS Process Mining	Prozessautomatisierung & Prozessmanagement
Axon Ivy	Low Code/No Code Plattformen
Bbvl – Beteiligungsmanagement	Organisationsmanagement
BIS	Recht & Ordnung
BundesMessenger	Kommunikationslösungen
Cert4Trust	Digitale Signaturen
CIVENTO	Prozessautomatisierung & Prozessmanagement
CVS as a Service	Querschnittsleistungen
dAmtshilfe	Organisationsmanagement
dConnector	Datenintegration und APIs
DDOCUSCAN	Dokumentenmanagement
dEvent	Organisationsmanagement
DiAs PIK Chassis	Ein- & Auswanderung
dKulturVideo	Bildung
DMS MACH AG (eAkte)	Organisationsmanagement
dOnlinezusammenarbeit	Kommunikationslösungen
dProjectTracking	Projektmanagement
dVirtuellerRundgang	Bildung
dWebService	Hosting und Compute
dWorkflow	Workflow-Automatisierung
EPAY21	Zahlungsabwicklung
eRechnung	Zahlungsabwicklung
eWaffe	Querschnittsleistungen
Feedbacksammler	Querschnittsleistungen
Flüchtlingskompass	Ein- & Auswanderung
Generische Antragstrecke/ Ende-zu-Ende (GAnS/E2E)	Prozessautomatisierung & Prozessmanagement
Generisches Antrags-Formular (GAnF)	Prozessautomatisierung & Prozessmanagement
Generisches Widerspruchsformular	Prozessautomatisierung & Prozessmanagement
GovManager	Prozessautomatisierung & Prozessmanagement
KAI	Datenanalyse und KI
KDO Multi-Messaging-Gateway (Bebpo)	Workflow-Automatisierung
KDO-Agent	Workflow-Automatisierung

KDO-Connect	Kollaborationstools
KDO-IAM	Identitätsmanagement
KDO-Kombox	Kollaborationstools
KDO-Kommune365	Betrieb von Fachverfahren
KDO-Meeting	Kommunikationslösungen
KI-Tool zum Untertiteln von Videos	Datenanalyse und KI
KIVAN - Verwaltungssoftware für Kitas, Träger und Kommunen	Querschnittsleistunngen
KommSafe	Speicherplatz und Datenbanken
Kubernetes as a Service	Hosting und Compute
Kubernetes as a Service (OpenShift)	Hosting und Compute
Kubernetes as a Service (Rancher)	Hosting und Compute
Masterportal Geodaten	Smart City Lösungen
Messenger-Dienst	Kommunikationslösungen
Modul F	Low Code/No Code Plattformen
NRW.desk	Büroanwendungen
OK.CASH	Zahlungsabwicklung
OK.FINN	Finanzmanagement
OK.PERS+	Personalmanagement
OpenDesk	Büroanwendungen
Opferschutz SGB XIV	Recht & Ordnung
OSCI-Postfach	Büroanwendungen
OZG Cloud	Portale und Antragsmanagement
pmINSPIRE: Geodaten-Management	Smart City Lösungen
pmOnline GovManager: Verwaltungsmanagement	Recht & Ordnung
pmOnline: GovForms: Digitale Formular-Dienste	Portale und Antragsmanagement
pmOnline: Online-Dienste	Portale und Antragsmanagement
pmOrdnungsManager: Ordnungsmanagement	Recht & Ordnung
pmPrüfung: Prüfungsmanagement	Organisationsmanagement
pmZEMA: Zentrales Meldewesen	Recht & Ordnung
Readyplace	Personalmanagement
Rückkanal	Prozessautomatisierung & Prozessmanagement
Sachbearbeitungskomponente mit Rückkanal	Prozessautomatisierung & Prozessmanagement
SecureBox	Kollaborationstools
Signaturservice	Digitale Signaturen
SozP2Cloud	Querschnittsleistungen
Unterlagen App	Dokumentenmanagement
VAMS	Querschnittsleistungen
Vaultwarden Passworttresor	Security-Services
Virtual Machine as a Service	Hosting und Compute
VOIS|BONUS	Identitätsmanagement
VOIS|Hund	Querschnittsleistungen
Votemanager	Recht & Ordnung
Workspace One	Kollaborationstools
Zugang zum VS-NfD fähigen Netz des Bundes	Netzwerk und VPN

Anlage 3

Zu 15.

Ressort	Behörde	Bundescloud	souveräne On-Premise-Cloud (IONOS)	IT-Betriebsplatt-form Bund	Public Clouds interne Kosten	Public Clouds externe Kosten	hochsichere „R-VSK Cloud-Plattform“ (vgl. BT-Drs. 20/6876)	weitere Clouds des Bundes
BMI		0,00 €	0,00 €	0,00 €	0,00 €	10.661,00 €	0,00 €	0,00 €
BMI	BKA	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	8.000.000,00 €
BMI	BpB	0,00 €	0,00 €	0,00 €	0,00 €	500.000,00	0,00 €	0,00 €
BMI	ZITiS	0,00 €	0,00 €	0,00 €	0,00 €	20.000,00 €	0,00 €	15.000.000,00 €
AA	AA	0,00 €	0,00 €	0,00 €	0,00 €	4.760.000,00 €	86.950.008,00 €	2.945.587,00 €
BMAS		0,00 €	0,00 €	0,00 €	0,00 €	65.777,70 €	0,00 €	0,00 €
BMDV	DWD	0,00 €	2.500,00 €	0,00 €	295.000,00 €	150.000,00 €	0,00 €	0,00 €
BMEL	MRI	0,00 €	0,00 €	0,00 €	0,00 €	75.000,00 €	0,00 €	0,00 €
BMEL	BfR	0,00 €	0,00 €	0,00 €	0,00 €	8.000,00 €	0,00 €	0,00 €
BMEL	BLE	0,00 €	0,00 €	0,00 €	0,00 €	80.000,00 €	0,00 €	0,00 €
BMEL	FLI	0,00 €	0,00 €	0,00 €	0,00 €	10.341,58 €	0,00 €	0,00 €
BMEL	BVL	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	8.871,91 €
BMF	ITZBund / BMF	108.023.867,74 €	15.629.810,41 €	116.815.721,88 €	0,00 €	1.100.000,30 €	0,00 €	0,00 €
BMFSFJ	BMFSFJ	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	61.266,67 €
BMJ	BMJ	0,00 €	0,00 €	0,00 €	0,00 €	26.357,04 €	0,00 €	0,00 €
BMJ	DPMA	0,00 €	120,00 €	0,00 €	0,00 €	0,00 €	0,00 €	- €
BMUV		0,00 €	0,00 €	0,00 €	0,00 €	177.204,09 €	0,00 €	- €
BMWK	BGR	0,00 €	0,00 €	0,00 €	5.000,00 €	35.000,00 €	0,00 €	- €
BMWK	PTB	0,00 €	0,00 €	0,00 €	0,00 €	138.216,00 €	0,00 €	- €
BMWK	BNetzA	0,00 €	0,00 €	0,00 €	0,00 €	30.733,75 €	0,00 €	- €
BMWSB	BMWSB	0,00 €	0,00 €	0,00 €	0,00 €	20 T€	0,00 €	- €
BMZ	BMZ	0,00 €	0,00 €	0,00 €	0,00 €	61.000,00 €	0,00 €	- €

	BPA	0,00 €	0,00 €	4.000,00 €	0,00 €	800.000,00 €	0,00 €	- €

Anlage 4

Zu 16.

Ressort	Behörde	Bundescloud	souveräne On-Premise-Cloud (IONOS)	IT-Betriebs-plattform Bund	Public Clouds interne Kosten	Public Clouds externe Kosten	hochsichere „R-VSK Cloud-Plattform“ (vgl. BT-Drs. 20/6876)	weitere Clouds des Bundes
BMI	BAMF	0,00 €	0,00 €	0,00 €	0,00 €	366.277,39 €	0,00 €	0,00 €
BMI	BKA	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	10.000.000,00 €
BMI	bpb	0,00 €	0,00 €	0,00 €	0,00 €	500.000,00 €	0,00 €	0,00 €
BMI	BKG	0,00 €	0,00 €	863.000,00 €	0,00 €	0,00 €	0,00 €	0,00 €
BMI	ZITiS	0,00 €	0,00 €	0,00 €	0,00 €	20.000,00 €	0,00 €	13.000.000,00 €
AA		0,00 €	0,00 €	0,00 €	0,00 €	5.260.660,00 €	66.740.675,00 €	3.729.500,00 €
BMAS		0,00 €	0,00 €	0,00 €	0,00 €	87.727,85 €	0,00 €	0,00 €
BMBF		0,00 €	0,00 €	140.000,00 €	0,00 €	0,00 €	0,00 €	0,00 €
BMDV	DWD	0,00 €	2.500,00 €	0,00 €	295.000,00 €	150.000,00 €	0,00 €	0,00 €
BMEL	MRI	0,00 €	0,00 €	0,00 €	0,00 €	75.000,00 €	0,00 €	0,00 €
BMEL	BfR	0,00 €	0,00 €	0,00 €	0,00 €	8.000,00 €	0,00 €	0,00 €
BMEL	BLE	0,00 €	0,00 €	0,00 €	0,00 €	80.000,00 €	0,00 €	0,00 €
BMEL	FLI	0,00 €	0,00 €	0,00 €	0,00 €	10.341,58 €	0,00 €	0,00 €
BMF	ITZBund/ BMF	79.385.502,42 €	18.052.931,00 €	143.918.318,08 €	0,00 €	0,00 €	0,00 €	0,00 €

BMJ		0,00 €	0,00 €	0,00 €	0,00 €	26.357,04 €	0,00 €	0,00 €
BMJ	DPMA	0,00 €	120,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
BMUV		0,00 €	0,00 €	0,00 €	0,00 €	178.069,41 €	0,00 €	0,00 €
BMWK	BGR	0,00 €	0,00 €	0,00 €	0,00 €	90.000,00 €	0,00 €	0,00 €
BMWK	PTB	0,00 €	0,00 €	0,00 €	0,00 €	162.300,00 €	0,00 €	0,00 €
BMWK	BNetzA	0,00 €	0,00 €	0,00 €	0,00 €	20.819,55 €	0,00 €	0,00 €
BMWSB		0,00 €	0,00 €	0,00 €	0,00 €	4 T€	0,00 €	0,00 €
BMZ		0,00 €	0,00 €	0,00 €	0,00 €	165.000,00 €	0,00 €	0,00 €
	BPA	0,00 €	0,00 €	7.000,00 €	0,00 €	535.000,00 €	0,00 €	0,00 €

Anlage 5

Zu 17.

2021:

Ressort	Behörde	Bundescloud	souveräne On-Premise-Cloud (IONOS)	IT-Betriebs-plattform Bund	Public Clouds interne Kosten	Public Clouds externe Kosten	hochsichere „R-VSK Cloud-Plattform“ (vgl. BT-Drs. 20/6876)	weitere Clouds des Bundes
BMI	BKA	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	ca. 10.000.000 €
BMI	bpb	0,00 €	0,00 €	0,00 €	0,00 €	471,222,04€	0,00 €	0,00 €
BMI	ZITiS	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	8.800.000 €
AA		0,00 €	0,00 €	0,00 €	0,00 €	485.048,44 €	25.825.524,00 €	0,00 €
BMDV		0,00 €	0,00 €	0,00 €	0,00 €	617,11 €	0,00 €	0,00 €
BMDV	DWD	0,00 €	2.500,00 €	0,00 €	295.000,00 €	150.000,00 €	0,00 €	0,00 €
BMDV	BSH	0,00 €	0,00 €	0,00 €	0,00 €	35.862,86 €	0,00 €	0,00 €
BMEL	MRI	0,00 €	0,00 €	0,00 €	0,00 €	65.000,00 €	0,00 €	0,00 €
BMEL	BfR	0,00 €	0,00 €	0,00 €	0,00 €	6.715,74 €	0,00 €	0,00 €
BMEL	FLI	0,00 €	0,00 €	0,00 €	0,00 €	11.543,00 €	0,00 €	0,00 €
BMEL	BVL	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	11.098,40 €
BMF	ITZBund/ BMF	10.695.519,45 €	0,00 €	78.564.817,98 €	0,00 €	0,00 €	0,00 €	0,00 €

BMJ		0,00 €	0,00 €	0,00 €	0,00 €	13.944,00 €	0,00 €	0,00 €
BMJ	DPMA	0,00 €	119,96 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
BMUV		0,00 €	0,00 €	0,00 €	0,00 €	19.000,25 €	0,00 €	0,00 €
BMWK	PTB	0,00 €	0,00 €	0,00 €	0,00 €	82.642,00 €	0,00 €	0,00 €
BMZ		0,00 €	0,00 €	0,00 €	0,00 €	15.000,00 €	0,00 €	0,00 €
	BPA / NC	0,00 €	0,00 €	0,00 €	0,00 €	191.996,46 €	0,00 €	0,00 €
	BPA / SAC	0,00 €	0,00 €	0,00 €	0,00 €	98.110,88 €	0,00 €	0,00 €
BMAS		0,00 €	0,00 €	0,00 €	0,00 €	29.522,82 €	0,00 €	0,00 €

2022:

Ressort	**Behörde**	**Bundescloud**	**souveräne On-Premise-Cloud (IONOS)**	**IT-Betriebs-plattform Bund**	**Public Clouds interne Kosten**	**Public Clouds externe Kosten**	**hochsichere „R-VSK Cloud-Plattform“ (vgl. BT-Drs. 20/6876)**	**weitere Clouds des Bundes**
BMI	BKA	0,00 €	0,00 €	0,00 €	0,00 €	10.000,00 €	0,00 €	ca. 10.000.000€
AA		0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	74.664.727,00 €	8.632,26 €
BMDV	BMDV	0,00 €	0,00 €	0,00 €	0,00 €	2.051,13 €	0,00 €	0,00 €
BMDV	DWD	0,00 €	2.500,00 €	0,00 €	295.000,00 €	150.000,00 €	0,00 €	0,00 €
BMDV	BSH	0,00 €	0,00 €	0,00 €	0,00 €	58.953,98 €	0,00 €	0,00 €

BMEL	MRI	0,00 €	0,00 €	0,00 €	0,00 €	70.000,00 €	0,00 €	0,00 €
BMEL	BfR	0,00 €	0,00 €	0,00 €	0,00 €	9.560,30 €	0,00 €	0,00 €
BMEL	FLI	0,00 €	0,00 €	0,00 €	0,00 €	11.543,00 €	0,00 €	0,00 €
BMEL	BVL	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	11.402,18 €
BMF	ITZBund/ BMF	17.594.925,57 €	0,00 €	56.501.011,87 €	0,00 €	0,00 €	0,00 €	0,00 €
BMJ		0,00 €	0,00 €	0,00 €	0,00 €	15.076,00 €	0,00 €	0,00 €
BMJ	DPMA	0,00 €	120,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
BMUV		0,00 €	0,00 €	0,00 €	0,00 €	58.274,66 €	0,00 €	0,00 €
BMWK	PTB	0,00 €	0,00 €	0,00 €	0,00 €	116.984,00 €	0,00 €	0,00 €
BMZ		0,00 €	0,00 €	0,00 €	0,00 €	20.000,00 €	0,00 €	0,00 €
	BPA / NC	0,00 €	0,00 €	0,00 €	0,00 €	383.992,92 €	0,00 €	0,00 €
	BPA / SAC	0,00 €	0,00 €	0,00 €	0,00 €	98.110,88 €	0,00 €	0,00 €
BMAS		0,00 €	0,00 €	0,00 €	0,00 €	50.890,30 €	0,00 €	0,00 €

2023:

Ressort	Behörde	Bundescloud	souveräne On-Premise-Cloud (IONOS)	IT-Betriebs-plattform Bund	Public Clouds interne Kosten	Public Clouds externe Kosten	hochsichere „R-VSK Cloud-Plattform“ (vgl. BT-Drs. 20/6876)	weitere Clouds des Bundes
BMI	BKA	0,00 €	0,00 €	0,00 €	0,00 €	9.000,00 €	0,00 €	ca. 7.000.000€
AA		0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	89.082.472,00 €	1.518.856,82 €
BMDV	BMDV	0,00 €	0,00 €	0,00 €	0,00 €	2.686,67 €	0,00 €	0,00 €
BMDV	DWD	0,00 €	2.500,00 €	0,00 €	295.000,00 €	150.000,00 €	0,00 €	0,00 €
BMDV	BSH	0,00 €	0,00 €	0,00 €	0,00 €	87.389,53 €	0,00 €	0,00 €
BMEL	MRI	0,00 €	0,00 €	0,00 €	0,00 €	75.000,00 €	0,00 €	0,00 €
BMEL	BfR	0,00 €	0,00 €	0,00 €	0,00 €	8.555,88 €	0,00 €	0,00 €
BMEL	FLI	0,00 €	0,00 €	0,00 €	0,00 €	11.543,00 €	0,00 €	0,00 €
BMEL	BVL	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	12.552,98 €
BMEL		0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	53.920,09 €	0,00 €
BMF	ITZBund/ BMF	88.201.490,88 €	333.914,33 €	45.579.994,94 €	0,00 €	0,00 €	0,00 €	0,00 €
BMFSFJ	BMFSFJ	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	61.266,67 €
BMJ		0,00 €	0,00 €	0,00 €	0,00 €	22.917,00 €	0,00 €	0,00 €
BMJ	DPMA	0,00 €	120,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €

BMUV		0,00 €	0,00 €	0,00 €	0,00 €	113.943,56 €	0,00 €	0,00 €
BMWK	BGR	0,00 €	0,00 €	0,00 €	0,00 €	30.000,00 €	0,00 €	0,00 €
BMWK	PTB	0,00 €	0,00 €	0,00 €	0,00 €	116.493,00 €	0,00 €	0,00 €
BMWSB		0,00 €	0,00 €	0,00 €	0,00 €	75.000,00 €	0,00 €	0,00 €
BMWSB		0,00 €	0,00 €	0,00 €	0,00 €	19.573,45 €	0,00 €	0,00 €
BMWSB		0,00 €	0,00 €	0,00 €	0,00 €	4.000,00 €	0,00 €	0,00 €
BMZ		0,00 €	0,00 €	0,00 €	0,00 €	30.000,00 €	0,00 €	0,00 €
	BPA / Besu	0,00 €	0,00 €	0,00 €	0,00 €	167.932,80 €	0,00 €	0,00 €
	BPA / NC	0,00 €	0,00 €	0,00 €	0,00 €	383.992,92 €	0,00 €	0,00 €
	BPA / SAC	0,00 €	0,00 €	0,00 €	0,00 €	27.893,13 €	0,00 €	0,00 €
BMAS		0,00 €	0,00 €	0,00 €	0,00 €	68.862,45 €	0,00 €	0,00 €
BMG		0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	695.000,00 €

2024:

Ressort	**Behörde**	**Bundescloud**	**souveräne On-Premise-Cloud (IONOS)**	**IT-Betriebs-plattform Bund**	**Public Clouds interne Kosten**	**Public Clouds externe Kosten**	**hochsichere „R-VSK Cloud-Plattform“ (vgl. BT-Drs. 20/6876)**	**weitere Clouds des Bundes**
BMI		0,00 €	0,00 €	0,00 €	0,00 €	10.745,00 €	0,00 €	0,00 €

BMI	BKA	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	ca. 8.000.000€
AA		0,00 €	0,00 €	0,00 €	0,00 €	4.760.000,00 €	86.950.007,85 €	2.945.586,88 €
BMDV		0,00 €	0,00 €	0,00 €	0,00 €	3.920,28 €	0,00 €	0,00 €
BMDV	DWD	0,00 €	2.500,00 €	0,00 €	295.000,00 €	150.000,00 €	0,00 €	0,00 €
BMDV	BSH	0,00 €	0,00 €	0,00 €	0,00 €	97.402,21 €	0,00 €	0,00 €
BMEL	MRI	0,00 €	0,00 €	0,00 €	0,00 €	75.000,00 €	0,00 €	0,00 €
BMEL	BfR	0,00 €	0,00 €	0,00 €	0,00 €	5.246,09 €	0,00 €	0,00 €
BMEL	FLI	0,00 €	0,00 €	0,00 €	0,00 €	10.341,58 €	0,00 €	0,00 €
BMEL	BVL	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	8.871,91 €
BMEL		0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	37.650,41 €	0,00 €
BMEL	BLE	0,00 €	0,00 €	0,00 €	0,00 €	72.384,89 €	0,00 €	0,00 €
BMF	ITZBund/ BMF	84.557.857,65 €	9.915.893,18 €	84.737.948,22 €	0,00 €	1.100.000,31 €	0,00 €	0,00 €
BMFSFJ	BMFSFJ	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	61.266,67 €
BMJ		0,00 €	0,00 €	0,00 €	0,00 €	26.357,04 €	0,00 €	0,00 €
BMJ	DPMA	0,00 €	120,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €
BMUV		0,00 €	0,00 €	0,00 €	0,00 €	97.204,09 €	0,00 €	0,00 €
BMWK	BGR	0,00 €	0,00 €	0,00 €	0,00 €	35.000,00 €	0,00 €	0,00 €
BMWK	BNetzA	0,00 €	0,00 €	0,00 €	0,00 €	9.914,25 €	0,00 €	0,00 €

BMWK	PTB	0,00 €	0,00 €	0,00 €	0,00 €	138.216,00 €	0,00 €	0,00 €
BMWSB		0,00 €	0,00 €	0,00 €	0,00 €	19.315,17 €	0,00 €	0,00 €
BMZ		0,00 €	0,00 €	0,00 €	0,00 €	61.000,00 €	0,00 €	0,00 €
	BPA	0,00 €	0,00 €	4.000,00 €	0,00 €	630.000,00 €	0,00 €	0,00 €
BMAS		0,00 €	0,00 €	0,00 €	0,00 €	65.777,70 €	0,00 €	0,00 €
BMG		0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	0,00 €	845.000,00 €

Anlage 8

Zu 42.

Nutzerdaten:

Ressort	Behörde	Cloud-Produkt	Übertragung	Speicherung	Verarbeitung
AA	AA	Microsoft Azure	Ist bekannt	Ist bekannt	Ist bekannt
BMBF	BMBF	AWS AWS-API	Ja	Nicht zutreffend	Teilweise
BMBF	BMBF	AWS Backup	Ja	Ja	Ja
BMBF	BMBF	AWS CodeBuild	Ja	Ja	Teilweise
BMBF	BMBF	AWS Console	Ja	Nicht zutreffend	Teilweise
BMBF	BMBF	AWS Directory Services	Ja	Teilweise	Teilweise
BMBF	BMBF	AWS EBS	Ja	Ja	Teilweise
BMBF	BMBF	AWS EC2	Ja	Nicht zutreffend	Teilweise
BMBF	BMBF	AWS Glue	Ja	Nicht zutreffend	Teilweise
BMBF	BMBF	AWS RDS	Ja	Ja	Teilweise
BMBF	BMBF	AWS Route 53 DNS	Ja	Nicht zutreffend	Teilweise
BMBF	BMBF	AWS S3	Ja	Ja	Teilweise
BMBF	BMBF	AWS Security Groups	Ja	Nicht zutreffend	Teilweise
BMBF	BMBF	AWS Step Functions	Ja	Ja	Teilweise
BMBF	BMBF	AWS VPC Router	Ja	Nicht zutreffend	Teilweise
BMBF	BMBF	AWS VPN Client Endpoints	Ja	Nicht zutreffend	Teilweise
BMBF	BMBF	AWS Workspace	Ja	Nicht zutreffend	Teilweise
BMBF	BMBF	Cisco Webex	Ja	Ja	Teilweise
BMBF	BMBF	Conceptboard	Ja	Ja	Teilweise
BMBF	BMBF	Trend Micro Vision One	Ja	Ja	Teilweise
BMBF	BMBF	Zenkit	Ja	Ja	Teilweise
BMDV	BSH	MS Azure/O365	ja	unbekannt	vertraglich ausgeschlossen
BMEL	FLI	Sharefile	AES 256	AES 256	AES 256
BMEL	BVL	KIPITZ	Public-Cloud-Lösung	Die Kommunikation erfolgt über das Rechenzentrum von	Verschlüsselung wird per Zertifikat und HTTPS sichergestellt. Zusätzlich

				Microsoft Azure, das die C5-Kriterien erfüllt und entsprechend zertifiziert ist.	greifen die Sicherheitseinstellungen des BVL für Web-Anwendungen.
BMVg	BAAINBw	Google Distributed Cloud – air gapped (GDC-A)	ja	ja	nein
BMWK	BAM	Office 365 E3	Ja	Ja	Nein
	BPA	Microsoft Azure	Ja	Ja	Ja
	BPA	SAP BTP	Ja	Unbekannt	Unbekannt
BMBF	BMBF	AWS AWS-API	Ja	Nicht zutreffend	Teilweise
BMBF	BMBF	AWS Backup	Ja	Ja	Ja
BMBF	BMBF	AWS CodeBuild	Ja	Ja	Teilweise
BMBF	BMBF	AWS Console	Ja	Nicht zutreffend	Teilweise

Meta-Daten:

Ressort	**Behörde**	**Cloud-Produkt**	**Übertragung**	**Speicherung**	**Verarbeitung**
AA	AA	Microsoft Azure	Ist bekannt	Ist bekannt	Ist bekannt
BMBF	BMBF	AWS AWS-API	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS Backup	Ja	Unbekannt	Ja
BMBF	BMBF	AWS CodeBuild	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS Console	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS Directory Services	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS EBS	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS EC2	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS Glue	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS RDS	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS Route 53 DNS	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS S3	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS Security Groups	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS Step Functions	Ja	Unbekannt	Teilweise

BMBF	BMBF	AWS VPC Router	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS VPN Client Endpoints	Ja	Unbekannt	Teilweise
BMBF	BMBF	AWS Workspace	Ja	Unbekannt	Teilweise
BMBF	BMBF	Cisco Webex	Ja	Nein	Teilweise
BMBF	BMBF	Conceptboard	Ja	Unbekannt	Teilweise
BMBF	BMBF	Trend Micro Vision One	Ja	Unbekannt	Teilweise
BMBF	BMBF	Zenkit	Ja	Unbekannt	Teilweise
BMDV	BSH	MS Azure/O365	ja	unbekannt	vertraglich ausgeschlossen
BMEL	FLI	Sharefile	AES 256	AES 256	AES 256
BMVg	BAAINBw	Google Distributed Cloud - air gapped (GDC-A)	ja	nein	nein
BMWK	BAM	Office 365 E3	Ja	Ja	Nein
	BPA	Microsoft Azure	Ja	Ja	Ja
	BPA	SAP BTP	Ja	Unbekannt	Unbekannt

Zu 42a)

Ressort	**Behörde**	**Clouds gemäß Anforderungen aus 42a)**
AA	AA	Nicht nativ, nur mit Zusatzsoftware
BMBF	BMBF	AWS
BMBF	BMBF	Cisco Webex
BMBF	BMBF	Conceptboard
BMBF	BMBF	Trend Micro Vision One
BMBF	BMBF	Zenkit
BMDV	BSH	Nicht nativ, nur mit Zusatzsoftware bleibt der private Schlüssel lokal
BMEL	MRI	1
BMUV	Ressort	je nach Einordnung / exakter Spezifikation eventuell bei umwelt.info CloudFerro

BMI	BKA	Polizei-Service-Plattform (PSP)
BMI	BPOL	AWS-Software (VAULT-Storage)

Zu 42b)

Nutzerdaten:

Ressort	**Behörde**	**Clouds gemäß Anforderungen aus Frage 42b)**
BMBF	BMBF	Cisco Webex
BMDV	BSH	genutzte Produkte garantieren kein echtes peer2peer Verschlüsseln, nur vertraglich die Nutzung ausgeschlossen!
BMEL	MRI	1
BMUV	Ressort	Open Telekom Cloud
BMI	BPOL	AWS-Software (VAULT-Storage)

Meta-Daten:

Ressort	**Behörde**	**Clouds gemäß Anforderungen aus Frage 42b)**
BMDV	BSH	genutzte Produkte garantieren kein echtes peer2peer Verschlüsseln, nur vertraglich die Nutzung ausgeschlossen!
BMI	BPOL	AWS-Software (VAULT-Storage)

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