Deutscher Bundestag **Drucksache 19/10826**

19. Wahlperiode 13.06.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Stephan Thomae, Benjamin Strasser, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/10307 –

Nutzung externer Cloud-Anbieter und Aufbau eigener Cloud-Infrastrukturen durch die Bundesregierung

Vorbemerkung der Fragesteller

Die Bundespolizei speichert Bodycam-Aufnahmen in Amazons AWS-Cloud (vgl. Antwort der Bundesregierung auf die Schriftliche Frage 28 des Abgeordneten Benjamin Strasser auf Bundestagsdrucksache 19/8180). Nach Ansicht der Fragesteller sollten die Bundespolizei und die anderen deutschen Sicherheitsbehörden eigentlich sachlich und personell ausreichend ausgestattet sein, um solche sensiblen Daten auch ohne externe Anbieter auf dem nötigen Sicherheitsniveau zu speichern und zu verarbeiten. Laut der Antwort der Bundesregierung auf die Mündliche Frage 34 des Abgeordneten Konstantin von Notz (vgl. Plenarprotokoll 19/88) kommt allerdings durch die ausgewählte Hardware des Anbieters Motorola und die auf die Hardware abgestimmte Cloud-Architektur allein AWS als Cloud-Dienst in Betracht. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), Ulrich Kelber, hält die Speicherung von Bodycam-Daten in der Amazon Cloud für rechtswidrig und forderte die Bundesregierung auf, zu einem deutschen Cloud-Anbieter umzusteigen (Quelle: www.noz.de/deutschland-welt/politik/artikel/1685384/bundespolizei-geraet-wegen-speicherung-von-bodycam-aufnahmen-unter-druck).

Das Informations Technik Zentrum Bund (ITZBund) lässt momentan die sogenannte Bundescloud entwickeln. Aus der dazugehörigen Ausschreibung „Software und Dienstleistungen für die Bundescloud“ aus dem Jahr 2016 geht hervor, dass die Bundescloud zunächst für bis zu 350 000 Nutzer ausgestaltet werden, aber weiter skalierbar sein soll. Die Bundescloud soll für ihre Nutzer als „BCBox“ angeboten werden (Quelle: www.itzbund.de/Restricted/DE/Ausschreibungen/O1912-Z4-1519-2017/Download_Vergabeunterlagen.html).

Auf dem Digitalgipfel der Bundesregierung 2018 in Nürnberg wurde die digitale Souveränität als Regierungslinie verabschiedet (Quelle: www.de.digital/DIGITAL/Redaktion/DE/Digital-Gipfel/Download/2018/p2-digitale-souveraenitaet-und-kuenstliche-intelligenz.pdf?__blob=publicationFile&v=5). Digitale Souveränität wird in mehreren Kontexten auf das Prinzip der eigenständigen Handlungsfähigkeit in verschiedenen Bereichen der Digitalisierung zurückgeführt,

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 11. Juni 2019 übermittelt.

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

unter anderem in den Bereichen Staat und Verwaltung. Bedenkt man dies, so wirft nach Ansicht der Fragesteller generell die Nutzung von externen Anbietern für Cloud-Dienste durchaus Fragen auf.

Im Jahr 2017 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Anforderungskatalog Cloud Computing (C5) herausgegeben, der als Prüfstandard für Cloud-Dienste gelten soll. Das Bundesministerium für Wirtschaft und Energie (BMWi) war (Mit-)Initiator des Trusted Cloud Labels und des Prüfstandards „Trusted Cloud Datenschutz-Profil für Cloud-Dienste“ (TCDP). Das Trusted Cloud Label wird vom Kompetenznetzwerk Trusted Cloud e. V. herausgegeben und verwaltet, das TCDP von der Stiftung Datenschutz.

Vorbemerkung der Bundesregierung

Der Begriff Cloud wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) (in Anlehnung an die Definition vom NIST) eindeutig definiert. In der Wirtschaft wird der Begriff Cloud häufig sehr unscharf verwendet. So werden mittlerweile auch normale Web-Dienste als Cloud-Dienste bezeichnet werden. Ob es sich bei angebotenen Diensten im Internet dabei tatsächlich um einen Cloud-Dienst handelt ist für die Kundinnen und Kunden nicht immer zweifelsfrei feststellbar. Die Fragestellerinnen und Fragesteller zielen insbesondere auf die Kriterien für eine sichere Verwendung von Cloud-Diensten im Sinne des Datenschutzes und Informationssicherheit, daher bezieht sich die Bundesregierung bei dieser Antwort sowohl auf echte Cloud-Dienste, als auch Cloud-ähnliche Web-Dienste.

1. In welchen Bereichen nutzt die Bundesregierung, unter anderem für die Sicherheitsbehörden, externe Anbieter für Cloud-Dienste?

   a) Welche Anbieter werden in den jeweiligen Bereichen genutzt?

   b) Welche Aufgaben werden genau an die Anbieter ausgelagert (beispielsweise laufender Betrieb, Archiv etc.)?

Die Fragen 1, 1a und 1b werden gemeinsam beantwortet.

Bei ihrer Erhebung hat die Bundesregierung die Nutzung von Cloud-Diensten in den folgenden Bereichen festgestellt:

Bereich	**Datenaustausch mit Externen (insbesondere außerhalb der Bundesverwaltung)**
Genutzte Anbieter	•]init[• Adobe • befine Solutions • BGE • Citrix • Deutschen Bodenkundlichen Gesellschaft • Deutsches Institut für Bautechnik • Deutsches Institut für Normung • DLR • Dropbox • Geologische Bundesanstalt (Österreich) • Google • GRS • iDGard • IMTB Consulting • Lawrence Berkeley National Laboratory • Leibniz-Zentrum für Agrarlandschaftsforschung • Microsoft • o3spaces • PlanView • swistopo • Telindus • TU Braunschweig • TU Clausthal • VDI/VDE Innovation und Technik • WeTransfer • Zentrum für Informationsverarbeitung NRW
Ausgelagerte Aufgaben	Laufender Betrieb von Austauschplattformen zur Datenhaltung, Backup, Recovery, Archivierung, Kundenmanagement, Servicemanagement.
Servicemodelle	SaaS, PaaS, IaaS

Bereich	**Öffentlichkeitsarbeit, Social Media und Webseitenpflege**
Genutzte Anbieter	• Facelift bbt • CleverReach • Mindlap
Ausgelagerte Aufgaben	Bereitstellung von Werkzeugen zum Management und Analyse von eigenen Social-Media-Kanälen und zur themenbezogenen Recherche und Analyse von in den sozialen Medien und dem Web.
Servicemodelle	SaaS

Bereich	**Schulungen**
Genutzte Anbieter	• Adobe • Articulate • Liveplace • Qualitus • eStar GmbH • Sozialpädagogisches Institut Berlin
Ausgelagerte Aufgaben	Bereitstellung und Betrieb von eLearning-Plattformen
Servicemodelle	SaaS, PaaS

Bereich	**Kollaboration**
Genutzte Anbieter	• ACP IT Solutions • Brainloop • COYO • Google • IT.NRW • Microsoft • Sozialpädagogisches Institut Berlin • think project!
Ausgelagerte Aufgaben	Bereitstellung von Datenaustauschplattformen mit Kollaborationsfunktionalität
Servicemodelle	SaaS
Bereich	**Bibliotheksmanagement**
Genutzte Anbieter	• ExLibris • Elsevier • Schweitzer Connect • Bibliotheca • Doctor Doc
Ausgelagerte Aufgaben	Bereitstellung und Betrieb von Katalog und Recherchewerkzeugen
Servicemodelle	SaaS

Bereich	**Forschung und forschungsnahe Aufgaben**
Genutzte Anbieter	Government of Canada, Natural Resources Canada Writelatex Illumina NCBI Brockmann Consult
Ausgelagerte Aufgaben	Unterschiedliche forschungsnahe Aufgaben
Servicemodelle	SaaS

Bereich	**IT-Infrastruktur**
Genutzte Anbieter	AWS Dunkel GmbH CDS Gromke Cisco DFN Hetzner Online Host Europe Kroll Discovery Microsoft NetApp Oracle
Ausgelagerte Aufgaben	Laufender Betrieb, insbesondere Server-, Netzwerk und Speicherbereitstellung
Servicemodelle	IaaS, PaaS

Bereich	**Conferencing**
Genutzte Anbieter	Adobe BlueJeans Network Cisco LogMeIn Vitero Zoom Video Communications
Ausgelagerte Aufgaben	Betrieb und Bereitstellung von Web- und Videokonferenzräumen mit Teilnehmenden außerhalb der Bundesverwaltung
Bereich	**Softwareentwicklung**
Genutzte Anbieter	Atlassian Avono EM-Software GmbH GitHub iff Berlin PDV GmbH Zentrum für Umweltforschung Werum AG
Ausgelagerte Aufgaben	Bereitstellung von Ticketsystemen und Repositories.
Servicemodelle	PaaS und SaaS

Außerhalb der oben genannten Bereiche, werden die folgenden Anbieter im Servicemodell IaaS genutzt (ausgelagerte Aufgabe in Klammer):

- TrendMicro (Virenschutz)
- haufe (Dokumenterstellung)
- Tableau (Datenvisualisierung)
- iLOQ (Schließsystemmanagement)

c) Werden Software-, Plattform- oder Infrastruktur-Dienste (SaaS, PaaS oder IaaS) verwendet?

Welche dieser Dienste-Kategorien werden in welcher Form bei der Verwendung der AWS-Cloud durch die Bundespolizei genutzt?

Siehe Tabellen in der Antwort zu Frage 1.

2. Welche der Cloud-Dienste werden aufgrund eigenständiger Verträge mit den Anbietern genutzt, welche der Dienste werden im Zusammenhang mit einer angeschafften Hard- bzw. Software-Lösung oder bereits bestehenden Rahmenverträgen genutzt?

Im Sinne der Frage wird „eigenständige Verträge“ als Verträge verstanden, die nicht aus einem Rahmenvertrag abgerufen wurden. Diese Dienste sind entweder in eigenen Vergabeverfahren ausgeschrieben worden, sind in bereits bestehenden Verträgen enthalten oder es handelt sich um eine Mitnutzung von Cloud-Diensten, die durch Dritte bezogen und durch Behörden der Bundesverwaltung mitgenutzt werden. Bei mitgenutzten Cloud-Diensten wird als Vertragspartner hier die Stelle angegeben, die die Mitnutzungsmöglichkeit eingeräumt hat. Bei mitgenutzten Diensten, die von Stellen bereitgestellt werden, die dem Vergaberecht unterliegen (z. B. Landesbehörden) kann es sein, dass der Abruf bei diesen Stellen auf Grundlage eines Rahmenvertrags geschieht. Die nutzenden Stellen in der Bundesverwaltung treten dabei allerdings nicht als Rahmenvertragsnutzerinnen auf. Die genutzten und mit-genutzten Cloud-Dienste, die nicht aus einem Rahmenvertrag abgerufen wurden, sind im Folgenden angegeben (bereitstellender Anbieter in Klammern):

- Adobe Cloud (Adobe)
- Adobe Connect (Adobe)
- Alfresco (IMTB Consulting)
- Auto-Support (NetApp)
- AWS EC2 (Accenture)
- Base Space (Illumina)
- Bibliotheca (Bibliotheca)
- bitbucket (Atlassian)
- Blue Jeans (BlueJeans Network)
- BSCW (Fraunhofer Institut)
- Centex (Baden-Württemberg)
- Cisco Meraki MDM (Cisco)

- CleverReach (CleverReach)
- Connect Webinars (Adobe)
- COYO Cloud (COYO GmbH)
- CryptShare (befine Solutions)
- Cumulus (CDS Gromke)
- Decovalex (Lawrence Berkeley National Laboratory)
- DIN Livelink (Deutsches Institut für Normung)
- Diverse Cloud-Dienste (DFN)
- Diverse DLR Cloud-Dienste (DLR)
- Doctor Doc (Doctor-Doc)
- Dropbox (Dropbox)
- Facelift (facelift bbt)
- GitHub (GitHub)
- GitLab (iff Berlin)
- GitLab (UFZ)
- Google Docs (Google)
- Google Drive (Google)
- GoToMeeting (LogMeIn)
- Gremienportal (Deutsches Institut für Bautechnik)
- GRS-Ccloud (GRS)
- Hetzner Cloud (Hetzner Online)
- IDGuard Standard (iDGard)
- Ilias (Qualitus GmbH)
- iLOQ S10 Management Softwar (iLOQ Oy)
- Jira (Avono)
- Kroll Discovery (Kroll)
- Mendeley (Elsevie)r
- Meraki MDM (Cisco)
- NCBI (NCBI)
- netmind (Mindlap)
- O3Spaces (O3Spaces)
- Office 365 (ACP IT Solutions GmbH)
- Office 365 (Microsoft)
- Office Online (Microsoft)
- One Drive (Microsoft)
- Oracle Cloud (Oracle)

- Overleaf (Writelatex)
- ownCloud (BGE)
- ownCloud (DBE / BGE)
- ownCloud (Deutschen Bodenkundlichen Gesellschaft)
- ownCloud (Geologische Bundesanstalt Österreich)
- ownCloud (GRS)
- ownCloud (Leibniz-Zentrum für Agrarlandschaftsforschung)
- ownCloud (TU Clausthal)
- PDV Helpline Cloud (PDV GmbH)
- Plone (VDI/VDE IT)
- Precise Point Positioning (Government of Canada, Natural Resources Canada)
- Primo (ExLibris)
- Project Mont Terri (swistopo)
- ProjectPlace (PlanView)
- Projekt 365 (Microsoft)
- Redmine (EM-Software GmbH)
- S3 (AWS)
- Saba (Liveplace)
- Schweitzer Connect (Schweitzer)
- Sciebo (Zentrum für Informationsverarbeitung NRW)
- SFX (ExLibris)
- Sharepoint (]init[)
- SharePoint (Microsoft)
- Social Media Monitoring Tool Facelift brand building technologies GmbH (Facelift bbt)
- Storyline (Articulate)
- Synology Office (Sozialpädagogisches Institut Berlin)
- Tableau Public (Tableau)
- think project! (think project! GmbH)
- vCloud (Dunkel GmbH)
- Virtuelle Server (Host Europe)
- Visio 365 (Microsoft)
- vitero (vitero)
- VPN (CITRIX)
- Webex (Cisco)

- WeTransfer (WeTransfer)
- Zeugnis Manager (Haufe)
- Zoom (Zoom Video Communications)

Die folgenden Cloud-Dienste wurden aus einem Rahmenvertrag abgerufen:

- IT-Lösung der Fa. Motorola für die Bodycam
- DENEQUA Online-Unterweisung (eStar)
- Trac-System (Werum)
- Virenschutz Office Scan (TrendMicro)
- Ilias
- Teamrooms (Brainloop)
- Azure Entwicklungsplattform (Microsoft)
- Azure Data Lake (Microsoft)
- WebEx Events (Cisco)
- Calvalus (Brockmann Consult)

Die folgenden Cloud-Dienste stehen im Zusammenhang mit der Beschaffung von Hard- oder Software:

- IT-Lösung der Fa. Motorola für die Bodycam (Bundespolizei)
- Adobe Creative Cloud
- Illumina Base Space (Max Rubner-Institut)
- AWS S3 im Zuge der Bereitstellung der DWD Warn-App
- iLOQ S10 Management Software

3. Warum hat sich die Bundesregierung in den jeweiligen Konstellationen für die Nutzung externer Anbieter und gegen die Nutzung eigener Speicherinfrastruktur entschieden (bitte die einzelnen Bereiche und Nutzungsfälle externen Anbieter auflisten)?

   a) Lag es mehrheitlich eher an fehlender eigener Speicherinfrastruktur oder an fehlendem Know-how in der Bundesregierung?

   b) Warum war in den jeweiligen Fällen die „Bundescloud“ des ITZBund nicht als Speicherort geeignet, oder aus welchen anderen Gründen wurde diese nicht ausgewählt?

Die Fragen 3 bis 3b werden gemeinsam beantwortet.

Die Übersicht der genutzten Cloud-Dienste (siehe Antwort zu Frage 1) macht deutlich, dass die Bundesverwaltung vollwertige Dienste nutzt, die über die Bereitstellung einer bloßen Speicher-Infrastruktur hinausgehen. Die Frage lässt sich daher für alle Bereiche ohne Aufschlüsselung nach Bereich und Nutzungsfall beantworten. Der Nutzung von Cloud-Diensten geht ein fachlicher Bedarf einer Behörde voraus. Dieser Bedarf soll nach dem Beschluss des IT-Rats „Kriterien für die Nutzung von Cloud Diensten der IT-Wirtschaft durch die Bundesverwaltung“ (siehe Antwort zu Frage 4c) nach Möglichkeit zuerst durch bundeseigene Dienstleister gedeckt werden. Ist dies nicht oder nicht wirtschaftlich möglich, kann unter

bestimmten Voraussetzungen (siehe Antwort zu Frage 4c) ein externer Cloud-Dienst beschafft werden. Die in der Antwort zu Frage 1 genannten Cloud-Dienste können nicht aus der Bundescloud bezogen werden (vgl. Antwort zu Frage 14), da diese Dienste nicht in der Bundescloud zur Verfügung stehen. Dies liegt insbesondere daran, dass die Bundescloud für die Bearbeitung von Verschlusssachen (VS) bis zum Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ (VS-NfD) ausgelegt ist. Daher ist die Bundescloud nur aus den VS-Netzen des Bundes (NdB) erreichbar und insbesondere nicht an das Internet angeschlossen.

Die meisten verwendeten Cloud-Dienste zielen explizit auf den Austausch mit Dritten ab, die keinen Zugang zu den VS-Netzen des Bundes haben. Die Bundesregierung evaluiert zurzeit die Bereitstellung von Cloud-Diensten im Internet. Dazu wird auf die Antwort zu Frage 13 verwiesen.

4. Welche Verträge wurden durch Ausschreibungen vergeben (bitte jeweiligen Link zur Ausschreibung angeben)?

a) In welchem Verfahren wurden die übrigen Aufträge vergeben?

Die Fragen 4 und 4a werden gemeinsam beantwortet.

Die Verträge werden grundsätzlich durch Ausschreibung vergeben. Davon wurde zugunsten einer freihändigen Vergabe abgewichen, wenn das Auftragsvolumen unterhalb der vorgegebenen Schwellenwerte liegt. Die Übersicht aller Verträge mit Verweisen auf die Ausschreibungsunterlagen zu den in der Antwort zu Frage 1 genannten Cloud-Diensten kann nicht innerhalb der Frist zur Beantwortung der Kleinen Anfrage erstellt werden. Die Bundesregierung kommt ihrer Informationspflicht über die Veröffentlichung von Ausschreibungen auf www.evergabe-online.de nach.

b) Welche Ausschreibungen zur Vergabe sind noch geplant?

Eine Übersicht über alle geplanten Ausschreibungen kann nicht innerhalb der Frist zur Beantwortung der Kleinen Anfrage erstellt werden. Die Bundesregierung kommt ihrer Informationspflicht über die Veröffentlichung von Ausschreibungen auf www.evergabe-online.de nach.

c) Welches sind die verfahrensleitenden Kriterien der Bundesregierung für die Ausschreibung von Cloud-Diensten?

Cloud-Dienste externer IT-Dienstleister können durch Bundesbehörden ausgeschrieben und genutzt werden, falls kein entsprechender Cloud-Dienste in der Bundescloud angeboten wird und der „Mindeststandard des BSI zur Nutzung externer Cloud-Dienste[1]“, der Beschluss des IT-Rats „Kriterien für die Nutzung von Cloud Diensten der IT-Wirtschaft durch die Bundesverwaltung“[2], sowie des darauf aufbauenden Beschlusses des IT-Planungsrats „Vorgehensweise und Kriterien zu Inanspruchnahme und Beschaffung von Cloud-Diensten der IT-Wirtschaft“[3], eingehalten werden.

[1] www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.pdf
[2] www.cio.bund.de/Web/DE/Politische-Aufgaben/IT-Rat/Beschluesse/Tabelleninhalte/beschluss_2015_05.html
[3] www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/21_Sitzung/14_Anlage1_Cloud-Computing.pdf

5. Welche Kriterien gibt es, um kritische und sensible Daten nicht zur Speicherung und Verwendung an einen Cloud-Anbieter auszulagern?

   Welche Daten gelten aus Sicht der Bundesregierung als kritisch oder sensibel?

Für die Stellen des Bundes hat das BSI nach dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik § 8 einen Mindeststandard zur Nutzung externer Cloud-Dienste erstellt (siehe Frage 4, Verweis [1]). Dort ist der Prozess geregelt, den eine Behörde durchlaufen muss, um einen Cloud-Dienst zu beschaffen und Daten auszulagern. Teil dieses Prozesses ist eine Datenkategorisierung und eine anschließende Risikoanalyse. Es sind vier Kategorien festgelegt:

Kategorie 1 „Privat- und Geschäftsgeheimnisse gemäß StGB § 203“, Kategorie 2 „Personenbezogene Daten“, Kategorie 3 „Verschlusssachen gemäß VSA“ und Kategorie 4 „sonstige Daten“. Der Mindeststandard schreibt fest, dass ein Cloud-Anbieter mindestens alle C5-Basisanforderungen erfüllen muss und dass diese vertraglich zugesichert sein müssen. Davon muss sich die Behörde durch den C5-Prüfbericht einen eigenen Eindruck verschaffen. Aus der Datenkategorisierung und der Risikoanalyse ergibt sich, welche weiteren Regularien die Behörde bei der Cloud-Beschaffung einhalten muss und welche weiteren (über C5 hinausgehende) Anforderungen die Behörde an den Cloud-Anbieter stellen muss. Dazu gehören insbesondere die Anforderungen CD.08 zur Festlegung der Gerichtsbarkeit, CD.09 zur Lokation der Daten und CD.10 das Thema „Offenbarungspflichten und Ermittlungsbefugnisse fremdstaatlicher Institutionen“.

Es handelt sich hierbei um Einzelfallentscheidungen in der Verantwortung der jeweiligen Behörde. Sollte der oben skizzierte und im Mindeststandard festgelegte Prozess ergeben, dass gegen gültige Regelungen verstoßen oder ein zu großes Risiko mit der Cloud-Nutzung verbunden ist, liegt es in der Verantwortung der Behörde eine entsprechende Entscheidung gegen die Cloud-Nutzung zu treffen.

6. Wie schätzt die Bundesregierung die Relevanz von Meta-Daten im Kontext von Cloud-Diensten ein?

Meta-Daten sind von hoher Relevanz, da durch sie Rückschlüsse auf die Tätigkeit des Cloud-Kundinnen und Kunden gezogen werden können.

   a) Wie wird sichergestellt, dass kein unbefugter Zugriff auf Meta-Daten bei den verwendeten externen Anbietern stattfindet?

Der C5-Standard regelt in den Anforderungen RB-11, PI-05 und DLL-01 den Umgang mit Meta-Daten bei der Cloud-Nutzung. Dies sind Basisanforderungen des C5, somit ist durch ein C5-Testat sichergestellt, dass der Cloud-Anbieter diese Anforderungen erfüllt. Der in der Antwort zu Frage 5 genannte Mindeststandard fordert, dass der Cloud-Anbieter die Einhaltung aller C5-Basisanforderungen (also auch der drei genannten) vertraglich zusichern muss und er demnach bei Verstoß mit den Konsequenzen bei Vertragsbruch rechnen muss. Wenn die Risikoanalyse gemäß unter dem in Antwort auf Frage 5 genannten Mindeststandard zum Beispiel eine besondere Gefährdung durch Meta-Daten ergibt, kann die Behörde zusätzlich gemäß CD.06 eigene Prüfrechte beim Cloud-Anbieter vereinbaren.

b) Welchen Zugriff und welche Nutzung bzw. Verwertung von Meta-Daten erlaubt die Bundesregierung den momentan genutzten externen Cloud-Anbietern?

Die Anforderung RB-11 des C5-Standards legt fest, dass Cloud-Anbieter Meta-Daten nur für Abrechnungszwecke, Störungs- und Sicherheitsvorfallsbehandlung nutzen dürfen. Eine kommerzielle Nutzung ist ausgeschlossen. Ferner sind Meta-Daten zu löschen, wenn sie zur Erreichung dieser drei Ziele nicht mehr gebraucht werden. Der Zeitraum, in dem Metadaten gespeichert werden ist vom Cloud-Anbieter festgelegt.

Er steht im angemessenen Zusammenhang mit den Zwecken, die mit der Sammlung der Metadaten verfolgt werden. Zusätzlich verpflichtet die Anforderung DLL-01 den Cloud-Anbieter, dass er alle Regelungen des C5 und insbesondere diese Regelung zum Umgang mit Meta-Daten auch mit allen Unterauftragnehmenden vereinbart. Die Anforderung PI-05 regelt zusätzlich, dass beim Austausch von Hardware alle Daten von dieser Hardware (insbesondere auch Meta-Daten) gelöscht werden.

c) Wie ist der Zugriff auf Meta-Daten mit den jeweiligen Anbietern geregelt?

Auf die Antworten zu den Fragen 6a und 6b wird verwiesen.

7. Setzt die Bundesregierung bei der Nutzung ihrer Cloud-Dienste (eigene und externe) intelligente Such- und Erkennungssysteme, z. B. unter Einsatz von Künstlicher Intelligenz (KI), ein?

Nein. Einige Cloud-Angebote bieten Suchfunktionen an, diese basieren aber nach Information der Bundesregierung nicht auf künstlicher Intelligenz.

a) Falls ja, verwendet die Bundesregierung hierfür eigens erstellte oder selbst angeschaffte KI-Anwendungen oder verwendet die Bundesregierung von den externen Anbietern bereitgestellte KI-Anwendungen?

Auf die Antwort zu Frage 7 wird verwiesen.

b) Falls ja, wie stellt die Bundesregierung sicher, dass die externen Anbieter nicht für eigene Zwecke KI-Anwendungen nutzen, um die gespeicherten Daten oder deren Meta-Daten auszuwerten?

Eine kommerzielle Nutzung von Metadaten wird durch die C5 Anforderungen RB-11 ausgeschlossen. Dennoch existieren Anwendungsszenarien, bei denen der Einsatz von KI-Anwendungen für die Auswertung von Metadaten gemäß den C5 Anforderungen erlaubt ist und sinnvoll sein kann (z. B. im Rahmen der Detektion von Sicherheitsvorfällen durch den Cloud Anbieter).

Bei der Nutzung von Cloud-Angeboten, die für eine Veröffentlichung von Daten im Internet genutzt werden wird grundsätzlich davon ausgegangen, dass externe diese Daten für eigene Zwecke nutzen könnten.

8. Wie stellt die Bundesregierung sicher, dass die auf externe Cloud-Dienste ausgelagerten Daten die nötige Mobilität (beispielsweise durch Schnittstellen) besitzen?

Auf die Antworten zu den Fragen 4c und 5 wird dabei insbesondere auf die C5 Anforderungen PI-01 bis PI-05 verwiesen.

a) Welche Vorkehrungen wurden getroffen, um ggf. den Anbieter ohne eine Dienstunterbrechung wechseln zu können?

Im Rahmen der Anwendung des Mindeststandards zur Nutzung externer Cloud-Dienste muss die Datenrückgabe aufgrund von Anforderung CD.13 explizit vertraglich mit dem Cloud-Anbieter vereinbart werden. Die C5 Anforderungen PI-01 bis PI-04 unterstützen diesen Prozess.

b) Wie wird darüber hinaus die Unabhängigkeit vom Anbieter sichergestellt?

Auf die Antwort zu Frage 4c wird verwiesen.

c) Inwiefern wird künftig bei der Anschaffung von Hardware oder anderer IT-Infrastrukturen sichergestellt, dass die Interoperabilität mit eigenen Cloud-Diensten gewährleistet ist?

Im Kabinettbeschluss „Grobkonzept IT-Konsolidierung“ vom 20. Mai 2019 hat die Bundesregierung beschlossen, die IT des Bundes zusammenzuführen. Im Rahmen des Projekts IT-Konsolidierung Bund wurde gemeinsam mit dem Verbund der IT-Dienstleister des Bundes ein strategisches und technisches Architekturboard eingerichtet um die IT-Architektur abzustimmen. So soll insbesondere sichergestellt, dass bestehende Cloud- und klassische Plattformen beim weiteren Ausbau der Infrastruktur berücksichtigt werden.

9. Hält die Bundesregierung die Speicherung von Daten in der AWS-Cloud entgegen der Äußerung des BfDI Ulrich Kelber für rechtmäßig?

Bei der Nutzung der Cloudlösung von AWS zur Speicherung von Daten, werden die deutschen Datenschutzstandards eingehalten. Siehe dazu auch die Antwort zu Frage 10.

10. Wie stellt die Bundesregierung bei der Verwendung amerikanischer externer Anbieter technisch und rechtlich sicher, dass die durch den CLOUD Act bestehenden Befugnisse nicht dazu verwendet werden, Daten in die USA zu übertragen?

Wie wird dies konkret im Falle der Verwendung von AWS sichergestellt?

Wie in den Antworten zu den Fragen 4c, 5 und 6 dargestellt werden rechtliche und technisch-organisatorische Maßnahmen zum Schutz der Daten getroffen. Im Falle der Verwendung von AWS ist eine Vereinbarung zur Auftragsdatenvereinbarung geschlossen worden. Weitere Schutzmaßnahmen sind auf Grundlage des sog. „Trusted Cloud Datenschutz-Profil“ (TCDP) sowie des § 9 des Bundesdatenschutzgesetzes (BDSG) alte Fassung und dessen Anlage vereinbart. Das BSI wurde bei der Beschaffung beteiligt und hat festgestellt, dass die Vorgaben aus dem Mindeststandard zur Nutzung externer Cloud-Dienste erfüllt sind.

11. Wird bei der Verwendung von Office-Anwendungen durch die Bundesregierung das Produkt „OneDrive“ von Microsoft genutzt?

    Falls ja,

Die Bundesanstalt für Gewässerkunde, die Bundesanstalt für Materialforschung und -prüfung und das Max-Rubner-Institut nutzen OneDrive.

a) werden die Daten verschlüsselt?

b) wie werden Meta-Daten geschützt?

Die Fragen 11a und 11b werden gemeinsam beantwortet.

Es gelten die in Antwort zu Frage 4c, 5 und 6 beschriebenen Anforderungen. Eine darüber hinausgehende Verschlüsselung wird nicht vorgenommen.

c) wie wird technisch und rechtlich sichergestellt, dass keine unrechtmäßigen Datenübertragungen in Drittländer stattfinden?

Auf die Antworten zu den Fragen 4c, 5 und 6 wird verwiesen.

12. Wurde nach Kenntnis der Bundesregierung bei der Beschaffung der Bodycams durch die Bundespolizei auch die Softwarelösung zur Verwaltung der entstehenden Daten evaluiert?

Dedizierte Ausschlusskriterien in Bezug auf die Verwaltungssoftware gab es nicht. Die sog. Systemlösung, bestehend aus Hard- und Software, wurde sachgemäß nach ganzheitlich erhobenen und in Einklang gebrachten funktionalen sowie nicht-funktionalen Anforderungen ausgewählt und beschafft.

a) Gab es für die Auswahl einer geeigneten Lösung Ausschlusskriterien in Bezug auf die Verwaltungssoftware für die Daten?

   War beispielsweise die Möglichkeit zur Verarbeitung biometrischer Daten ein solches Kriterium?

Dedizierte Ausschlusskriterien in Bezug auf die Verwaltungssoftware gab es nicht. Die Verarbeitung biometrischer Daten ist nicht vorgesehen und war daher keine funktionale Anforderung.

b) Wurde die Möglichkeit einer späteren Migration der angefallenen Daten in eine eigene Speicher-Infrastruktur (beispielsweise die „Bundescloud“) evaluiert?

Schätzt die Bundesregierung dies als technisch möglich ein?

Wie viel würde eine solche Migration nach Einschätzung der Bundesregierung kosten?

Wurde für diesen Zweck ein Fixpreis mit dem Anbieter vereinbart?

Die Möglichkeit einer späteren Migration der angefallenen Daten in eine eigene Speicher-Infrastruktur (z. B. in der Bundescloud) wurde mit positivem technischem Ergebnis evaluiert. Neben den Daten sind jedoch auch die Software und damit die Systemlösung zu betrachten, deren Migrierbarkeit einer erweiterten Evaluierung bedürfen, die derzeit durchgeführt wird. Die konkreten Kosten für eine Migration sind unter anderem von der jeweiligen Zielumgebung abhängig, insofern kann zum jetzigen Zeitpunkt keine konkrete Schätzung erstellt werden. Ein Festpreis wurde nicht vereinbart.

13. Auf welchen Ebenen und an welchen Stellen werden nach Kenntnis der Bundesregierung derzeit staatliche Cloud-Infrastrukturen auf- oder ausgebaut?

a) In welchem Umfang sind diese geplant?

b) Wann sollen diese fertiggestellt sein?

Die Fragen 13 bis 13b werden gemeinsam beantwortet.

Das Informationstechnik Zentrum Bund (ITZBund) baut die Bundescloud für die Bundesverwaltung auf. Die Bundescloud ist seit Mitte 2017 online und kann von den Bundesbehörden genutzt werden. Die Bundescloud ist für die Verarbeitung für VS-NfD ausgelegt. Im Umfang richtet sich der Aufbau der Bundescloud nach den Anforderungen der Kundenbehörden innerhalb der sicheren Netze des Bundes (NdB). Siehe dazu auch die Antwort zu Frage 14.

Die BWI evaluiert im Rahmen der IT-Konsolidierung Bund den Aufbau von Bundescloud-Anteilen im Internet. Der Umfang dieses Vorhabens orientiert sich dabei an den Anforderungen der Bundesbehörden nach Cloud-Diensten die für Bürgerinnen, Bürger, die Wirtschaft und weitere Externe erreichbar sind.

Das Bundesministerium der Verteidigung (BMVg) führt derzeit vorbereitende Maßnahmen für den ab dem Jahr 2021 beginnenden Aufbau einer eigenständigen Cloud-Infrastruktur mit einem On-Premise Betrieb durch die BWI GmbH in den Rechenzentren der Bundeswehr durch. Für das BMVg kommt ausschließlich eine sog. Private Cloud Lösungsarchitektur in Frage, um insbesondere die nationalen Anforderungen an die Informationssicherheit (IT-Sicherheit, Datenschutz) und Militärische Sicherheit sowie spezifische Anforderungen (u. a. Autarkie, Verlegefähigkeit) für die IT im Einsatz erfüllen zu können. Die geplanten On-Premise Cloud-Infrastruktur umfasst alle zentralen IT-Services des Geschäftsbereichs BMVg. Sie stellt auf Grundlage einer herstellerunabhängigen Multi-Cloud-Architektur die erforderlichen IT-Services, Daten und Informationen höchstverfügbar und bedarfsgerecht allen Nutzern im Geschäftsbereich BMVg zur Verfügung. In einer ersten Ausbaustufe wird zunächst eine Grundbefähigung realisiert. Die derzeitigen Planungen sehen vor, dass diese bis zum Jahr 2027 abgeschlossen sein werden. Die Maßnahmen zum weiteren Ausbau hin zu einer vollständigen Befähigung werden erst nach Vorliegen praktischer Erfahrungen aus der Grundbefähigung und damit zu einem späteren Zeitpunkt festgelegt.

Das Auswärtige Amt (AA) baut die Diplo-Cloud für die Auslands-IT auf. Diese Umfasst die Cloud-Infrastruktur in den Rechenzentren und Liegenschaften im Ausland. Fertigstellung ist für 2021/2022 geplant.

Die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) baut Cloud-Infrastruktur für die interne Verwendung in verschiedenen Projekten mit besonderem Schutzbedarf auf. Eine erste Inbetriebnahme ist im dritten Quartal 2019 geplant.

Das Bundeskriminalamt (BKA) baut eine Cloud als Polizei Service Plattform für das Programm Polizei 2020 auf. Diese Cloud soll die Liefermodelle IaaS, PaaS und SaaS umfassen. Der Aufbau erfolgt programmbegleitend in Teilmengen, ein konkretes Fertigstellungsdatum kann daher derzeit nicht benannt werden.

c) An welcher Stelle sind entsprechende Projekte der Bundesregierung in der Umsetzungsstrategie der Bundesregierung zur Gestaltung des digitalen Wandels zu finden?

Die Umsetzungsstrategie digitaler Wandel konzentriert sich auf Schwerpunktvorhaben, die die Ministerien identifiziert haben. Die Bundescloud ist dort als Maßnahme der Dienstekonsolidierung vertreten (Seite 155). Bezüge zur Cloud des AA finden sich an mehreren Stellen (Seite 29, 37, 49, 78).

14. Wie weit ist die Entwicklung der „Bundescloud“ fortgeschritten?

An welchen Nutzerkreis soll sich die „Bundescloud“ und die Anwendung „BCBox“ richten?

Zu welchem Zweck sollen die Anwendungen verwendet werden können?

Der Aufbau der Bundescloud wurde mit dem Kabinettbeschluss zur IT-Konsolidierung Bund vom 20. Mai 2015 beschlossen. Seit Mitte 2017 ist die Bundescloud innerhalb des sicheren Behördennetzes (Netze des Bundes) online. Derzeit bietet die Bundescloud die folgenden Cloud-Dienste für die Bundesbehörden:

- BundescloudBox: Sicheres Speichern von Daten in der Cloud und selbstbestimmter, ressortübergreifender Austausch.
- BundescloudEntwicklungsplattform: Etablierte, auf einander abgestimmte, serverbasierte Tools und Services zur Unterstützung der Softwareentwicklung
- BundescloudLaufzeitumgebung: Laufzeitumgebung bestehend aus Web-, Application- und Datenbankserver für den Betrieb von Fachverfahren.
- BundescloudServer: virtuelle Maschinen mit Betriebssystem, Storage und Netzwerkstrukturen.

Das Dienste-Angebot wird im Rahmen der IT-Maßnahme Bundescloud am Bedarf der Bundesbehörden ständig weiterentwickelt. Nutzungskreis für die Bundescloud sind alle Bundesbehörden der unmittelbaren Bundesverwaltung mit Zugang zu den Netzen des Bundes (NdB). Die Bundesbehörden werden derzeit sukzessive an die Bundescloud angeschlossen.

15. Wird die Bundescloud nur verwaltungsintern Verwendung finden?

Oder wird die Bundescloud auch im Rahmen der Digitalisierung der Verwaltungsleistungen zur Anwendung kommen?

Die Bundescloud ist für die Verarbeitung von Verschlusssachen bis zum Geheimhaltungsgrad VS-NfD ausgelegt. Daher ist ein Zugriff außerhalb von VS-NfD-Netzen nicht möglich. Derzeit wird mit den bundeseigenen IT-Dienstleistern evaluiert, ob außerhalb einer VS-NfD-Zone weitere Cloud-Infrastrukturen aufgebaut werden sollen.

16. Wurde der C5-Prüfstandard vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt?

Wenn nein, von wem wurde dieser entwickelt?

Wurden vom BSI hierzu externe Dienstleister in Anspruch genommen?

Wenn ja, welche?

Der C5 wurde vom BSI entwickelt. Da die Prüfung nach C5 durch Wirtschaftsprüfer anhand internationaler Prüfstandards der Wirtschaftsprüfer stattfindet (siehe dazu Antwort zu Frage 18c), hat das BSI für die Entwicklung des C5 auf einen Dienstleister zugegriffen. Bei dem dazugehörigen Vergabeverfahren hat die Wirtschaftsprüfungsgesellschaft PriceWaterhouseCoopers (PwC) Deutschland den Zuschlag erhalten.

17. Wurden die Kriterien für das Trusted Cloud Label und den TCDP-Prüfstandard durch das BMWi entwickelt?

Wenn nein, von wem wurden diese entwickelt?

Wurden vom BMWi bzw. dem Kompetenznetzwerk Trusted Cloud e. V. und der Stiftung Datenschutz hierzu externe Dienstleister in Anspruch genommen?

Wenn ja, welche?

Die Kriterien für das Trusted Cloud Label wurden eigenständig vom Kompetenznetzwerk Trusted Cloud e. V. entwickelt. Hierbei wurden Stakeholdergruppen sowohl von Anbieterseite als auch von Anwenderseite und der Wissenschaft einbezogen. Ebenso wurden existierende internationale Standards (z. B. ISO 27001/2/17) und existierende Cloud Zertifizierungen (z. B. CSA, Eurocloud StarAudit) berücksichtigt. Der Kriterienkatalog wird gemäß der aktuellen Anforderungen laufend vom Kompetenznetzwerk Trusted Cloud e. V. in Abstimmung mit den zuvor genannten Stakeholdergruppen weiterentwickelt.

Die Kriterien für das TCDP wurden von der Arbeitsgruppe Rechtsrahmen unter Leitung von Prof. Dr. Georg Borges im Rahmen des Trusted Cloud Forschungsprogramms erarbeitet. Die Mitglieder der Arbeitsgruppe können unter https://tcdp.de/index.php/hintergrund/ag-rechtsrahmen freizugänglich eingesehen werden.

18. Wie viele und welche Anbieter sowie einzelne Cloud-Dienste sind nach Kenntnis der Bundesregierung nach dem Trusted Cloud Label oder dem C5- und TCDP-Prüfstandard zertifiziert?

Mit dem Trusted Cloud Label sind aktuell 35 Cloud Dienste von 32 Anbietern versehen. Weiterhin sind 17 Dienstleister gelistet, die Cloud-basierte Dienstleistungen anbieten (Beratungsdienstleistungen). Nach TCDP 1.0 sind aktuell sechs Dienste von zwei Anbietern zertifiziert. Bezüglich der erteilten C5-Testate wird auf die Antwort zu Frage 18c verwiesen.

a) Werden die Zertifizierungen nach dem Trusted Cloud Label durch das Kompetenznetzwerk Trusted Cloud e. V. vorgenommen?

Falls ja, wie viel Budget ist in welchem Einzelplan an welcher Stelle für das Haushaltsjahr 2019 hierfür eingeplant?

Falls nein, wer übernimmt die Zertifizierungen, und welche Kosten verursacht dies für die öffentliche Hand?

Die Prüfung und Vergabe des Labels Trusted Cloud obliegt dem Kompetenznetzwerk Trusted Cloud e.V. Die Kosten für die Zertifizierung trägt der Antragsteller.

b) Werden die Zertifizierungen nach dem TCDP-Prüfstandard durch die Stiftung Datenschutz vorgenommen?

Falls ja, wie viel Budget ist in welchem Einzelplan an welcher Stelle für das Haushaltsjahr 2019 hierfür eingeplant?

Falls nein, wer übernimmt die Zertifizierungen, und welche Kosten verursacht dies für die öffentliche Hand?

Da die TCDP Zertifizierung auf dem BDSG a. F. fußt, werden aktuell keine TCDP Zertifizierungen mehr durchgeführt. Die Kosten für die Zertifizierung hatte vormals der antragstellende Cloud-Anbieter zu tragen. Entsprechend der Verfahrensordnung zum TCDP wurden die Entgelte im Vertrag mit dem Cloud-Anbieter festgelegt.

c) Werden die Zertifizierungen nach dem C5-Prüfstandard durch das BSI vorgenommen?

Falls ja, wie viel Budget ist in welchem Einzelplan an welcher Stelle für das Haushaltsjahr 2019 hierfür eingeplant, und wie viele Planstellen sind hierfür vorgesehen?

Falls nein, wer übernimmt die Zertifizierungen, und welche Kosten verursacht dies für die öffentliche Hand?

Beim C5 findet keine Zertifizierung, sondern eine sogenannte Attestierung statt. Bei einer Zertifizierung gibt es den Auditor, den zu Prüfenden und eine Zertifizierungsstelle, die auf der Grundlage eines Auditberichts des Auditors ein Zertifikat an den zu Prüfenden ausstellt. Bei einer Attestierung fehlt diese Zertifizierungsstelle; der Auditor stellt das Testat direkt an den zu Prüfenden aus. Beim C5 wird das Testat durch einen Wirtschaftsprüfer ausgestellt, der dafür ein Audit und einen Auditbericht gemäß internationaler Wirtschaftsprüfernormen – dem International Standard on Assurance Engagements (ISAE) 3000 und 3402 – durchführt und erstellt. Da es eine Attestierung ist, ist das BSI an dem gesamten Prozess von Audit und Berichterstattung nicht beteiligt, da dies bilateral zwischen Cloud-Anbieter und Wirtschaftsprüfer erfolgt. Der Cloud-Anbieter entscheidet über die Bekanntgabe einer erfolgreichen C5-Prüfung – auch gegenüber dem BSI – nach

eigenem Ermessen. Dem BSI liegt daher keine vollständige Liste von C5-Testaten vor, das BSI verweist dazu auf die Veröffentlichungen der Cloud-Anbieter. Da das BSI keine C5-Prüfungen durchführt, hat das BSI weder Budget noch Planstellen für C5-Prüfungen im Haushaltsjahr 2019 vorgesehen. Da C5-Prüfungen vom Cloud-Anbieter beauftragt werden, entstehen keine direkten Extrakosten für die öffentliche Hand. Die Kosten der Attestierung sind in den Preisen für den Cloud-Dienst bereits eingepreist. Die genaue Kostenkalkulation hierzu ist dem BSI nicht bekannt.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.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.betrifft-gesetze.de
ISSN 0722-8333