IT-PLANUNGSRAT

Frankfurt
25.11.2026

Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur

Version 4.0.0

Version	Datum	Autor	Aktion
1.0	29.10.2021	AG Cloud Computing und Digitale Souveränität	Beschluss 2021/46 in der 36. Sitzung IT-Planungsrat
2.0	10.11.2022	AG Cloud Computing und Digitale Souveränität	Beschluss 2022/47 in der 39. Sitzung IT-Planungsrat
2.5	03.11.2023	AG Cloud Computing und Digitale Souveränität	Beschluss 2023/50 in der 42. Sitzung IT-Planungsrat
3.0	26.03.2025	Architekturboard der Deutschen Verwaltungscloud	Beschluss 2025/15 in der 46. Sitzung IT-Planungsrat
4.0	25.11.2026	Architekturboard der Deutschen Verwaltungscloud	Beschluss in der 51. Sitzung IT-Planungsrat

Impressum

Herausgeber

FITKO (Föderale IT-Kooperation)

Zum Gottschalkhof 3

60594 Frankfurt am Main

E-Mail: poststelle@fitko.de

Ansprechpartner

FITKO (Föderale IT-Kooperation)

Adresse: siehe oben

E-Mail: dvc@fitko.de

Stand

November 2026

Nachdruck, auch auszugsweise, ist genehmigungspflichtig.

Inhaltsverzeichnis

Präambel **5**

1 Einführung **7**

1.1 Zielsetzung und Aufbau des Dokuments 10

1.2 Geltungsbereich und Zielgruppe des Dokuments 11

1.3 Weiterentwicklung des Dokuments 11

2 Rahmenbedingungen der Deutschen Verwaltungscloud **13**

2.1 Nahestehende Vorhaben 13

2.2 Relevante Vorgaben und Richtlinien der Öffentlichen Verwaltung 17

2.3 Digitale Souveränität für die DVC 19

2.4 Datenklassifizierung in der Öffentlichen Verwaltung 20

3 Geschäftsarchitektur der Deutschen Verwaltungscloud **23**

3.1 Produktmanagement-Modell der FITKO 23

3.2 Zusammenarbeitsmodell 24

3.3 Rollen und Akteure in der Deutschen Verwaltungscloud 25

3.3.1 Rollen auf der Kundenseite 25

3.3.2 Rollen auf der Anbieterseite 27

3.3.3 Prinzip der geteilten Verantwortung 30

3.3.4 DevSecOps in der DVC und der Öffentlichen Verwaltung 31

3.4 DVC-Ökosystem 32

3.5 Vertragsmodelle 33

3.6 Einbindung von verwaltungsexternen Anbietern 36

4 Technische Architektur der Deutschen Verwaltungscloud **37**

4.1 Reduktion von Abhängigkeiten 39

4.2 Steigerung der Effizienz und Effektivität in Entwicklung, Inbetriebnahme und Betrieb 41

4.2.1 Entwicklung und Inbetriebnahme 41

4.2.2 Betrieb 43

4.2.3 Angebot von Cloud-Services 45

4.3 Sicherstellung und Stärkung von Datenschutz und Informationssicherheit 48

4.4 Optimierung von Datenaustausch, -speicherung und -nutzung zwischen Bund, Ländern und Kommunen 53

5 Reifegradmodell der Deutschen Verwaltungscloud 55

6 Weiterführende Informationen 58

6.1 Glossar 58

6.2 Dokumentation der Fortschreibung 65

6.2.1 Initiales Rahmenwerk der Zielarchitektur (Version 1.0) 65

6.2.2 Anmerkungen zur ersten Fortschreibung (Version 2.0) 65

6.2.3 Anmerkungen zur zweiten Fortschreibung (Version 2.5) 66

6.2.4 Anmerkungen zur dritten Fortschreibung (Version 3.0) 66

6.2.5 Anmerkungen zur vierten Fortschreibung (Version 4.0) 68

6.3 Ausblick auf die Version 4.1 70

Präambel

Mit der Deutschen Verwaltungscloud (DVC) wird das Ziel verfolgt, die Digitalisierung der Öffentlichen Verwaltung voranzutreiben und die Digitale Souveränität Deutschlands zu stärken. Zusammen mit anderen Initiativen auf Bundes-, Landes- und Kommunalebene soll sie zum Rückgrat einer zukunftsfähigen Verwaltung werden. Im Mittelpunkt stehen dabei die Bedürfnisse der Bürgerinnen und Bürger, der Wirtschaft sowie der Verwaltungsmitarbeitenden, die von einer modernen Öffentlichen Verwaltung profitieren sollen.

Die Digitalisierung bietet das Potenzial, die Öffentliche Verwaltung effizienter, innovativer und resilienter zu gestalten. Die DVC trägt dazu bei, dass die Öffentliche Verwaltung auf allen föderalen Ebenen schnell und einfach auf sichere und leistungsfähige Cloud-Services zugreifen kann und so von den Vorteilen der gegenwärtigen Cloud-Transformation profitiert. Für den Erfolg der DVC ist die flächendeckende und effiziente Nutzung souveräner Cloud-Services in Bund, Ländern und Kommunen zentral.

Mit der DVC wird ein selbstbestimmter Weg zu Cloud-Services für die Verwaltungen realisiert, indem Wechselmöglichkeiten geschaffen, die eigene Gestaltungsfähigkeit gefördert und der Einfluss auf IT-Anbieter gefestigt wird. Dafür werden auf dem Marktplatz Deutschland Digital (MDD) Cloud-Service-Angebote des DVC-Portfolios nach DVC-Mindeststandards angeboten. Verwaltungsexterne Anbieter können dabei als Softwarelieferanten und Cloud-Service-Lieferanten für die Fertigung von DVC-Services eingebunden werden. Diese Dienste stehen den Verwaltungen und ihren IT-Dienstleistern auf Bundes-, Landes- und Kommunalebene über einheitliche Vertragsmodelle für eine rechtskonforme Beschaffung zur Verfügung.

Zurzeit existieren bereits zahlreiche Cloud-Lösungen innerhalb der föderalen Verwaltungsebenen von Bund, Ländern und Kommunen. Aufgrund fehlender Standardisierung und dezentraler Beschaffung sind bestehende föderale Cloud-Lösungen bisher oft nur eingeschränkt interoperabel, kompatibel und Verwaltungsebenen-übergreifend nutzbar.

Mit der DVC, einem föderalen Multi-Cloud-Ökosystem, wird ein einheitlicher rechtlicher, organisatorischer und technischer Rahmen geschaffen. Dieser trägt maßgeblich dazu bei, dass Cloud-Service-Angebote standardisiert und ressourcenschonend entwickelt, betrieben, angeboten und von den Verwaltungen des Bundes, der Länder und der Kommunen sowie deren öffentlichen IT-Dienstleistern beschafft und genutzt werden können.

Die Architektur der Deutschen Verwaltungscloud ist integraler Bestandteil des Deutschland-Stacks und folgt den Vorgaben der übergreifenden Deutschland-Architektur zur Cloud-Infrastruktur. Als souveränes Cloud-Fundament des Deutschland-Stacks stellt die DVC die technologische Basis für interoperable, standardisierte und wechselfähige Cloud-Services bereit, auf denen der Deutschland-Stack aufbaut. Sie liefert zentrale Bausteine für den Betrieb von Infrastruktur-, Plattform- und Software-as-a-Service-Angeboten (IaaS, PaaS, SaaS), die den Anforderungen an digitale Souveränität, Sicherheit und föderale Interoperabilität genügen. Dadurch fügt sich die DVC-Architektur im Themenfeld Cloud-Infrastruktur stimmig in die Deutschland-Architektur ein. Die DVC ermöglicht so die technische Umsetzung übergreifender Verwaltungsdienste und trägt maßgeblich zur Schaffung eines einheitlichen, souveränen und europäisch anschlussfähigen digitalen Ökosystems für Bund, Länder und Kommunen bei.

1 Einführung

Die Stärkung der Digitalen Souveränität[1] für die IT der Öffentlichen Verwaltung ist ein gemeinsames Ziel von Bund, Ländern und Kommunen in Deutschland. Die IT der Öffentlichen Verwaltung ist aufgrund ihrer Bedeutung für die staatliche Handlungsfähigkeit in besonderem Maße schutzbedürftig.[2] Um die Digitale Souveränität nachhaltig zu wahren und kontinuierlich zu stärken, formulierte der IT-Planungsrat 2020 drei strategische Ziele: Wechselmöglichkeit, Gestaltungsfähigkeit sowie Einfluss auf Anbieter.[3]

Im Zuge der Umsetzung der Strategie zur Stärkung der Digitalen Souveränität hat der IT-Planungsrat (IT-PLR) die „Deutsche Verwaltungscloud-Strategie" (DVS) verabschiedet[4] und damit die konzeptionelle Grundlage für die „Deutsche Verwaltungscloud" (DVC) geschaffen. Im Fokus der DVS steht die übergreifende Etablierung und Nutzung von Standards für (bestehende) föderale Cloud-Lösungen der Öffentlichen Verwaltung.[5]
Bund, Länder und Kommunen haben im Rahmen der DVS allgemeine Anforderungen an die DVC festgelegt. Anhand dieser Anforderungen wurden die nachfolgenden Eckpunkte für die Zielarchitektur sowie für die anschließende Umsetzung spezifiziert:

- **Verteilter IT-Betrieb**: Es wird ein verteilter Betrieb der DVC in Rechenzentren von Bund, Ländern und Kommunen angestrebt. Hierbei soll gewährleistet sein, dass Cloud-Service-Kunden zwischen den Services der verschiedenen Anbieter auf einfache Weise wechseln können, um eine Multi-Cloud-Strategie zu ermöglichen. Die föderale Cloud-Infrastruktur soll durch die Öffentliche Verwaltung und deren IT-Dienstleister bereitgestellt und betrieben werden. Die Einbindung von Cloud-Services verwaltungsexterner Anbieter wird dabei grundsätzlich unterstützt.
- **Allgemeine Verfügbarkeit von Cloud-Services**: Angebotene Cloud-Services in XaaS-Servicemodellen (z. B. IaaS, PaaS, SaaS) innerhalb der DVC sollen für Organisationen der

---

1 Digitale Souveränität wird hier definiert als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können".

2 Eine formale Einordnung einzelner Systeme oder Einrichtungen als Kritische Infrastruktur richtet sich nach den jeweils einschlägigen gesetzlichen Kriterien.

3 Beschluss 2021/09 – Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung: Strategische Ziele, Lösungsansätze und Maßnahmen zur Umsetzung, in: IT-Planungsrat, 17.03.2021, Link zur Strategie, S. 6.

4 Beschluss 2020/54 – Deutsche Verwaltungscloud-Strategie – Föderaler Ansatz, in: IT-Planungsrat, 28.10.2020, Link zum Beschluss.

5 Ebenso ist die Schaffung föderaler Cloud-Strukturen für Bund, Länder und Kommunen ein zentrales Element des 9-Punkte-Plans des Beauftragten der Bundesregierung für Informationstechnik. 9-Punkte-Plan für ein digitales Deutschland, in: Bundesministerium des Innern und für Heimat, Link zum 9-Punkte-Plan

Öffentlichen Verwaltung aus Bund, Ländern und Kommunen nutzbar sein. Entstehende Erweiterungen und Anpassungen eines Services bei einem Teilnehmenden der DVC sollen durch die Cloud-Service-Kunden nachgenutzt werden können.

- **Einsatz von Open-Source-Software (OSS)**: OSS[6] wird für den Aufbau der DVC priorisiert[7]. Innerhalb der DVC betriebene Cloud-Services müssen nicht auf OSS basieren, Lock-in-Effekte[8] sollen jedoch verhindert, die Nachnutzung ermöglicht und risikomindernde Maßnahmen zur Reduzierung der Wahrscheinlichkeit und der negativen Auswirkungen von Lock-in-Effekten eingeplant und umgesetzt werden.
- **Zentrale Verwaltung von Cloud-Services in einem Cloud-Service-Portal (CSP)**: Die Suche, Bestellung, Änderung der Serviceleistung und Kündigung von Cloud-Services der DVC erfolgt über ein zentrales Cloud-Service-Portal, das perspektivisch in den Verwaltungsnetzen verfügbar gemacht werden soll. Die angebotenen Services werden in einen systematisch strukturierten Servicekatalog eingeordnet und detailliert beschrieben. Der spätere Zugriff durch die Cloud-Service-Kunden erfolgt direkt auf die Cloud-Service-Instanz des Anbieters, die nach der Bestellung im Cloud-Service-Portal bereitgestellt wird. Das Cloud-Service-Portal der DVC ist in den Marktplatz Deutschland Digital (MDD) überführt worden und wird dort weiter ausgebaut[9] (Beschluss 2025/08 des IT-PLR).
- **Gemeinsame Weiterentwicklung:** Zur Kooperation an öffentlichen Entwicklungsprojekten und zur Weiterentwicklung wesentlicher Softwarekomponenten (z. B. Standard-Images oder Policies[10] für den Betrieb von Containern[11]) soll die Open-Source-Plattform der Öffentlichen Verwaltung „openCode"[12] genutzt werden, auf der Repositories für (OS-)Softwareprojekte angelegt und gepflegt werden können.

---

6 Open Source Initiative: Link.

7 Eine Priorisierung von OSS bedeutet nicht, dass proprietäre Lösungen grundsätzlich ausgeschlossen werden. Der Einsatz eines proprietären Software-Stacks ist innerhalb der DVC möglich. Es müssen jedoch Schnittstellen entsprechend den gemeinsamen Standards geschaffen werden.

8 „Lock-in-Effekt" beschreibt die Zwangsbindung, die es dem Kunden wegen entstehender Wechselkosten und sonstiger Wechselbarrieren erschwert, das Produkt, den Service oder den Anbieter zu wechseln.

9 Beschluss 2025/08 des IT-PLR, Link

10 Ergebnisbericht – Deutsche Verwaltungscloud-Strategie – Proof-of-Concept, in: IT-Planungsrat, 22.04.2022, Link zum Bericht.

11 IG BVC, in: Software, Link.

12 openCode: Die Open-Source-Plattform der öffentlichen Verwaltung, Link.

Transformation der föderalen IT-Landschaft durch die DVC: Die Deutsche Verwaltungscloud unterstützt die digitale Transformation der Öffentlichen Verwaltung, wobei die folgende Abbildung den Ist- und den Zielzustand darstellt.

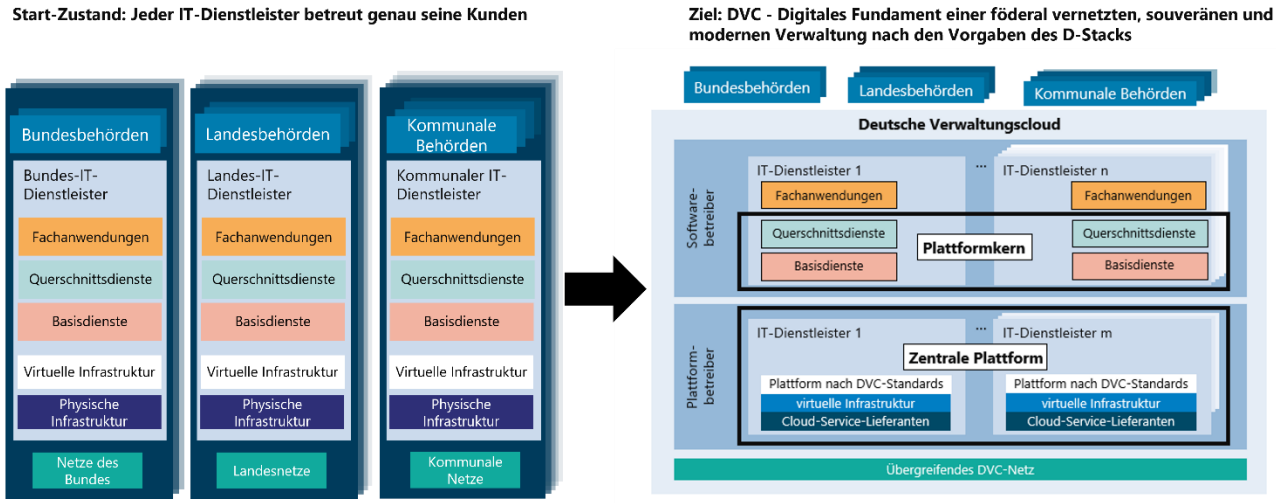

Abbildung 1: Transformation der föderalen IT-Landschaft durch die DVC

IT-Services sollen künftig nicht mehr einzeln von einem IT-Dienstleister nur für dessen eigene Kunden hergestellt und betrieben werden, wie links in der Abbildung dargestellt. Stattdessen sollen sie als hoch automatisierte Cloud-Services allen Behörden von Bund, Ländern und Kommunen zur Nutzung angeboten werden. Dadurch werden folgende Mehrwerte erwartet:

- **Beschaffung:** Schneller und einfacher ausschreibungsfreier Bezug von „Verwaltungsleistungen as a Service“ über den Marktplatz Deutschland Digital und damit eine Reduzierung der Markterkundungs- und Ausschreibungskosten.
- **Herstellung:** Softwarelieferanten können sich auf die Umsetzung von fachlichen Anforderungen fokussieren. Für die DVC entwickelte Software ist auf allen DVC-Plattformen lauffähig.
- **Integration:** Reduktion der Integrationsaufwände durch standardisierte Basis- und Querschnittsdienste.
- **Betrieb:** Senkung der Summe der Betriebs- und Weiterentwicklungskosten, da gleichartige Verfahren nicht mehr separat bei vielen IT-Dienstleistern betrieben werden, sondern ein Service von einem oder wenigen Cloud-Service-Anbietern für alle Kunden betrieben wird.

Zur Realisierung dieser Mehrwerte müssen zukünftig IT-Services für die Verwaltung nach klaren Standards und Regeln beauftragt, beschafft, hergestellt, integriert und betrieben werden. Ebenso muss eine Arbeitsteilung zwischen den IT-Dienstleistern (in Abstimmung mit ihren Trägern) ausdifferenziert werden, um die Potenziale zu heben.
Mit dem Rahmenwerk der Zielarchitektur der Deutschen Verwaltungscloud werden in diesem Dokument die Grundlagen für diese Transformation geschaffen.

1.1 Zielsetzung und Aufbau des Dokuments

Ziel des vorliegenden Dokuments „Rahmenwerk der Zielarchitektur" ist es, die Deutsche Verwaltungscloud zu beschreiben sowie Prinzipien für die Ausgestaltung und Weiterentwicklung der technischen Architektur der DVC und der in der DVC angebotenen Cloud-Services zu formulieren. Die Prinzipien unterstützen die im Eckpunkte-[13] und Strategiepapier[14] angestrebte offene, modulare und interoperable Ausrichtung der IT-Architektur der Öffentlichen Verwaltung.
Der Fokus des Rahmenwerks der Zielarchitektur liegt auf der Schaffung einer Grundlage zum standardisierten Betrieb bestehender und zukünftiger Cloud-Services, um Wechselmöglichkeiten herzustellen beziehungsweise den Wechsel zu vereinfachen.

Die Inhalte des vorliegenden Rahmenwerks der Zielarchitektur sind wie folgt gegliedert:

- **Kapitel 1** „Einführung" beschreibt die Zielsetzung und den Aufbau des Dokuments, den Geltungsbereich und die Zielgruppe.
- **Kapitel 2** „Rahmenbedingungen der DVC" beschreibt abzugrenzende Vorgaben und Vorhaben innerhalb der Öffentlichen Verwaltung.
- **Kapitel 3** „Geschäftsarchitektur der DVC" erläutert die grundsätzlichen Elemente der DVC, das Rollen-/Zusammenarbeitsmodell, das DVC-Ökosystem, die Vertragsmodalitäten sowie Aspekte der Einbindung von verwaltungsexternen Anbietern.
- **Kapitel 4** „Technische Architektur der DVC" definiert Prinzipien der technischen Architektur für die Weiterentwicklung der DVC und der in der DVC angebotenen Cloud-Services.
- **Kapitel 5** „Reifegradmodell der DVC" beschreibt den Aufbau und die Anwendung des Reifegradmodells für Cloud-Service-Anbieter und Cloud-Services im Rahmen der DVC.

---

[13] Beschluss 2020/19 – Stärkung der Digitalen Souveränität der öffentlichen Verwaltung – Eckpunkte – Ziel und Handlungsfelder, in: IT-Planungsrat, 04.05.2020, Link zum Eckpunktepapier.

[14] Beschluss 2021/09 – Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung: Strategische Ziele, Lösungsansätze und Maßnahmen zur Umsetzung, in: IT-Planungsrat, 17.03.2021, Link zum Beschluss.

- **Kapitel 6** „Weiterführende Informationen" enthält ein Glossar der wichtigsten Begriffe und zeigt die Veränderungen zwischen den Versionen im Rahmen der kontinuierlichen Weiterentwicklung des vorliegenden Dokuments auf.

1.2 Geltungsbereich und Zielgruppe des Dokuments

Mit dem Beschluss Nr. 2021/46 des IT-Planungsrats wurden die Architektur der Deutschen Verwaltungscloud sowie die entsprechenden Standards übergreifend für Bund, Länder und Kommunen sowie für deren IT-Dienstleister gültig.

Die im Rahmen der DVC formulierten Vorgaben zur Architektur richten sich vor allem an die bestehenden sowie auch neu zu schaffenden föderalen Cloud-Angebote der Öffentlichen Verwaltung (und dabei insbesondere an die beteiligten IT-Dienstleister).

Bei Teilnahme an der Deutschen Verwaltungscloud ist die Umsetzung der Minimalkriterien des DVC-Reifegradmodells[15] in der jeweils aktuell gültigen Version seitens der Cloud-Service-Anbieter verpflichtend. Sowohl für Cloud-Service-Anbieter als auch für Cloud-Service-Kunden gelten für alle Bestellungen über den MDD einheitliche Vertragsbedingungen (CS-AGB).

Jede Version der Minimalkriterien wird mit einem Wirksamkeitsdatum veröffentlicht. Für bereits autorisierte Cloud-Services gilt bei einer Anhebung von Minimalkriterien eine mit der Veröffentlichung bekanntgegebene Übergangsfrist; die Autorisierung bleibt bis zu deren Ablauf bestehen.

1.3 Weiterentwicklung des Dokuments

Das Dokument „Rahmenwerk der Zielarchitektur" wird anlassbezogen und iterativ weiterentwickelt und mit einem Beschluss im Rahmen der Governance der Deutschen Verwaltungscloud verabschiedet. Anschließend wird der IT-Planungsrat informiert. Bei wesentlichen Änderungen des Rahmenwerks soll es zu einem Beschluss durch den IT-Planungsrat kommen.

Neben dem Rahmenwerk der Zielarchitektur werden das Reifegradmodell[16], die Detailstandards (mit ihren Blaupausen) sowie die Leitfäden (mit ihren Checklisten) der DVC iterativ weiterentwickelt. Da es sich bei dem Reifegradmodell und den Detailstandards um detaillierte

[15] Minimalkriterien der Cloud-Services der Deutschen Verwaltungscloud - Gültige Fassung, Link.
[16] Cloud-Service-Reifegradmodell in aktueller Fassung, Link.

Ausarbeitungen der im Rahmenwerk definierten Prinzipien handelt und sie häufigeren Änderungszyklen unterliegen, wird der IT-Planungsrat über die Änderungen informiert, ohne dass ein Beschluss notwendig ist.

Die kontinuierliche Weiterentwicklung der DVC gewährleistet eine stets zeitgemäße Ausrichtung und erlaubt eine flexible Anpassung an sich ändernde Anforderungen und Rahmenbedingungen, wie beispielsweise Technologieentwicklungen.

2 Rahmenbedingungen der Deutschen Verwaltungscloud

Die im Rahmen der Deutschen Verwaltungscloud festgelegten Vorgaben betten sich in bereits bestehende Vorgaben und Richtlinien für IT-Lösungen auf unterschiedlichen föderalen Ebenen ein. Gleichzeitig muss das Vorhaben zur Umsetzung der DVC klar von anderen Initiativen im Bereich Cloud-Computing und Verwaltungsdigitalisierung abgegrenzt werden. Zu diesem Zweck werden nachfolgend nahestehende Vorhaben und relevante Vorgaben der Öffentlichen Verwaltung erläutert.

2.1 Nahestehende Vorhaben

Folgende Vorhaben mit Bezug zur Öffentlichen Verwaltung und mit Fokus auf Cloud-Computing sind mit ihren wesentlichen Aspekten bei der Entwicklung der Zielarchitektur berücksichtigt worden:

- **Deutschland-Architektur:** Die Deutschland-Architektur ist die Enterprise-Architektur der deutschen Verwaltung und bildet einen kohärenten Ordnungsrahmen für die zielgerichtete Steuerung und systematische Beschreibung gemeinsamer Geschäftsfähigkeiten und ihre Unterstützung durch die IT in Bund, Ländern und Kommunen. Die D-Architektur gestaltet einen modularen und interoperablen Plattformansatz basierend auf den strategischen Zielen von Bund, Ländern und Kommunen. Sie deckt sowohl Ende-zu-Ende-Prozesse für Verwaltungsleistungen (für Verwaltungskunden) als auch verwaltungsinterne Prozesse (für Verwaltungsmitarbeitende) ab. Die Deutschland-Architektur regelt das Zusammenspiel der von ihr beschriebenen Bausteine sowohl untereinander als auch nach außen (mit externen Systemen/Bausteinen). Dazu gehört eine wirksame Steuerungsstruktur, um die Deutschland-Architektur auf Basis der strategischen Zielsetzungen kontinuierlich weiterzuentwickeln. Die Architekturarbeit in der DVC wird sich an der Deutschland-Architektur ausrichten.
- **Deutschland-Stack:** Der D-Stack realisiert Bausteine der D-Architektur in Lösungsarchitekturen und stellt ein souveränes Angebot von Infrastruktur und IT-Lösungen sowohl für die unmittelbare als auch für die mittelbare Verwaltung in Bund, Ländern und Kommunen sowie den öffentlichen Sektor dar. Der D-Stack trägt zum modularen und interoperablen Plattformansatz der Deutschland-Architektur bei, indem er wiederverwendbare Lösungsbausteine bereitstellt, welche die Prinzipien der D-Architektur erfüllen und entsprechende Funktionalitäten bereitstellen sowie bundesweit integrierbar und interoperabel mit Externen (bspw. EU-Systeme) sind. Dazu gehört ein wirksames IT-Portfoliomanagement, um den D-Stack im Rahmen der Deutschland-Architektur und unter Berücksichtigung

technologischer Innovationen bedarfsgerecht weiterzuentwickeln. Die DVC als Funktionsbaustein des Deutschland-Stacks stellt selbst kein Multi-Cloud-Resource-Management bereit. Sie führt bestehende Cloud-Plattformen der Öffentlichen Verwaltung sowie ausgewählter souveräner Anbieter über angeglichene Zugangsbedingungen – ein gemeinsames Netz und vergleichbare Betriebsplattformen – zusammen und schafft so interföderale Synergien. Weiterhin sind wesentliche DVC-Standards Teil des Deutschland-Stacks (IT-PLR Beschluss B-2026/03-IT).[17] Berührt sind dabei insbesondere die Funktionsbausteine ‚Cloud-Infrastruktur', ‚Netze', ‚Entwicklung und Bereitstellung' sowie ‚Marktplatz'. Die genaue Abgrenzung und Zuordnung der DVC zu den Funktionsbausteinen des Deutschland-Stacks wird zwischen dem FITKO-Produkt DVC und den für den Deutschland-Stack verantwortlichen Stellen abgestimmt und in der nächsten Fortschreibung des Rahmenwerks dokumentiert.

- **Netzverbund Deutschland (NV-DE):** Der Netzverbund Deutschland (NV-DE) ist der Arbeitstitel zur Errichtung eines sicheren und cloudfähigen Austauschnetzes für die interföderale Zusammenarbeit auf Basis der Weiterentwicklung des Vertrages Netze des Bundes. Die DVC ist mit ihren Vernetzungsaktivitäten integraler Bestandteil des NV-DE.
- **Cloud-Lösungen von Bund, Ländern und Kommunen**: Es sind bereits verschiedene Cloud-Lösungen auf den unterschiedlichen Verwaltungsebenen von Bund, Ländern und Kommunen (z. B. Bundescloud, Justizcloud oder Bildungscloud) im Einsatz oder befinden sich in der Entwicklung.
- **Cloud-Lösungen verwaltungsexterner Anbieter**: In Reaktion auf die Souveränitätsanforderungen in der Öffentlichen Verwaltung werden neue verwaltungsexterne Cloud-Lösungen für die Nutzung in der Öffentlichen Verwaltung durch Marktanbieter entwickelt (z. B. Delos Cloud oder vergleichbare umgangssprachlich „souveräne" Cloud-Umgebungen). Während sie technologisch beispielsweise auf Hyperscaler-Technologien basieren, sollen die Anforderungen der Öffentlichen Verwaltung durch technische, organisatorische und rechtliche Maßnahmen (z. B. vollständig autonomer Betrieb innerhalb des Europäischen Wirtschaftsraums) erfüllt werden. Die Integration solcher Lösungen in die DVC ist eine Forderung der Deutschen Verwaltungscloud-Strategie. Daher werden Aktivitäten zum Aufbau von Betriebsplattformen mit ausgewählten privatwirtschaftlichen Anbietern durchgeführt.
- **Cloud-Broker**: Organisationen der Öffentlichen Verwaltung nutzen Cloud-Broker-Modelle (z. B. gd.Cloud-Broker oder zukünftig Multi-Cloud-Broker der Bundesanstalt für Arbeit, der

[17] IT-Planungsrat Beschluss B-2026/03-IT, Link

DRV Bund und der Deutschen Gesetzlichen Unfallversicherung) für den direkten Zugriff auf Cloud-Services verwaltungsexterner Anbieter. Der Cloud-Broker-Ansatz ermöglicht den jeweiligen Kunden den Bezug von Cloud-Services verschiedener Cloud-Anbieter „aus einer Hand" sowie typischerweise eine zentrale Verwaltung von Zugängen und Abrechnungsdaten.

- **ZenDiS/openCode**: Die Open-Source-Plattform der Öffentlichen Verwaltung openCode ist Teil der Umsetzung der Deutschen Verwaltungscloud-Strategie und wird vom Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS) bereitgestellt. Teilnehmer der DVC haben die Möglichkeit, openCode als gemeinsame Plattform für den Austausch von Open-Source-Software untereinander, mit der weiteren Öffentlichen Verwaltung und Zivilgesellschaft zu nutzen. openCode umfasst aktuell ein zentrales Verzeichnis der verwaltungsrelevanten und verfügbaren Open-Source-Software-Projekte/-Lösungen, eine Webanwendung zur Versionsverwaltung und zur Ablage von offenem Quellcode beziehungsweise zur Beteiligung an Projekten (Code Repository) sowie ein Diskussionsforum und Begleitlösungen, zum Beispiel für IT-Sicherheit in Softwareprojekten oder Konsentierungen. Außerdem ist ein System von „Badges" etabliert, welches verschiedene Aspekte von Qualität der hinterlegten Projekte, zum Beispiel für die Qualitätsmessung einer Auftragsentwicklung, messbar machen hilft. Über die Plattformfunktionen hinaus stellt das ZenDiS Bausteine für eine sichere Software-Lieferkette bereit, unter anderem gehärtete Container-Images sowie Werkzeuge zur Schwachstellen- und Compliance-Prüfung von Software-Repositories. Diese Bausteine sind für die Realisierung und den Betrieb von Cloud-Services der DVC nachnutzbar. openCode spielt eine gesetzte Rolle im Kontext der Errichtung des Deutschland-Stacks. In diesem Kontext ist es für die DVC ein relevantes Schnittstellensystem, dessen Bedeutung tendenziell wächst. Dies betrifft Felder wie „Sichere Softwarelieferketten", „Sichere Containerimages" oder auch der Aufbau von Entwicklungsplattformen im DevSecOps Kontext.
- **OZG-Umsetzung**[18]: Das Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG) verpflichtet Bund und Länder (und damit auch die Kommunen) dazu, ihre Verwaltungsleistungen (auch) digital anzubieten. Das Gesetz zur Änderung des Onlinezugangsgesetzes (OZG-Änderungsgesetz) baut auf diesen Grundlagen auf und zielt darauf ab, die weitere Digitalisierung der Verwaltung voranzutreiben

[18] Onlinezugangsgesetz: Wohnzimmer statt Wartezimmer – Umsetzung des Onlinezugangsgesetzes, in: Bundesministerium des Innern und für Heimat, Link

sowie zentrale Voraussetzungen für nutzerfreundliche und vollständig digitale Verfahren zu schaffen. Ein zentraler Grundsatz bei der OZG-Umsetzung ist das „Einer für Alle"-Prinzip (EfA).[19]

- **BundID / DeutschlandID**[20]: Das OZG-Änderungsgesetz sieht vor, die Nutzerkonten für die Bürger (BundID) an die IT-Infrastruktur von Bund, Ländern und Kommunen anzubinden. Vor dem Inkrafttreten des OZG-Änderungsgesetzes war eine zentrale Bereitstellung des Nutzerkontos für die Bürger gesetzlich nicht vorgegeben und mehrere Bundesländer etablierten parallel zum bestehenden Nutzerkonto BundID bereits eigene ID-Konten. Mit dem OZG-Änderungsgesetz übernimmt der Bund diese Aufgabe zentral. Perspektivisch soll die BundID so zu einer DeutschlandID ausgebaut werden.
- **„Mein Unternehmenskonto"**[21]: Das Unternehmenskonto ist das bundesweit einheitliche Nutzerkonto für Unternehmen und darauf ausgelegt, dass es für alle Bereiche im Umfeld der Öffentlichen Verwaltung genutzt werden kann. Es ist ein zentraler Authentifizierungs- und Identifizierungsdienst.
- **Registermodernisierung/NOOTS**[22]: Das Vorhaben zielt darauf ab, eine Deutschland- und EU-weite Nachweisübermittlung aus bestehenden Registern zu ermöglichen. Durch Vernetzung der Register wird das Once-Only-Prinzip[23] umgesetzt und damit auch eine medienbruchfreie Bearbeitung und Bereitstellung von Verwaltungsleistungen ermöglicht. Die Registermodernisierung steht in engem Zusammenhang mit der OZG-Umsetzung.
- **FIT-Connect**: FIT-Connect unterstützt Hersteller von Online-Antragsdiensten bei der Umsetzung einer einfachen, maschinenlesbaren und verschlüsselten Kommunikation zwischen Antragstellern und den zuständigen Fachbehörden. Dazu verknüpft FIT-Connect Online-Verwaltungsdienste mit den Systemen zur Antragsbearbeitung in Bund, Ländern und Kommunen. FIT-Connect ist eine durch den IT-Planungsrat festgelegte Basis-Komponente im Aufbau des Deutschland-Stacks.
- **Föderale API-Autorisierungsinfrastruktur:** Das Vorhaben ist ein konkreter Beitrag zum Zielbild des Schwerpunktthemas Digitale Transformation des IT-Planungsrats.24 Dieses

---

19 Das „EfA"-Prinzip bedeutet, dass einmal entwickelte Lösungen eines Landes in anderen Ländern nachgenutzt werden können, um arbeitsteilig und zeitsparend bei der Digitalisierung vorzugehen, Link.

20 OZG-Änderungsgesetz, in: Bundesministerium des Innern und für Heimat, Link.

21 Mein Unternehmenskonto: Das Unternehmenskonto auf Basis von ELSTER, Link.

22 Registermodernisierung, in: Bundesministerium des Innern und für Heimat, Link.

23 Das Once-Only-Prinzip verfolgt das Ziel, dass Bürgerinnen und Bürger sowie Unternehmen notwendige Angaben nur noch ein einziges Mal an die Verwaltung übermitteln müssen. Mit dem Einverständnis der Nutzerinnen und Nutzer dürfen diese Daten für andere Anliegen später wiederverwendet werden, wenn dies notwendig ist.

24 Föderale API-Autorisierungsinfrastruktur, Link

Zielbild sieht vor, verbindliche Standards für die Verwaltungsdigitalisierung zu schaffen, um die interföderale Zusammenarbeit zu vereinfachen und skalierbare Lösungen sicherzustellen. Mit einheitlichen Sicherheitsstandards und Architekturvorgaben für die API-Absicherung setzt das Vorhaben hier an.

- **„Zero-Trust-Transformation des Bundes"**: Mit den ‚Eckpunkten einer Zero-Trust-IT-Sicherheitsarchitektur des Bundes' (Version 1.0, August 2025) und der Weiterentwicklung des IT-Grundschutzes hin zu maschinenlesbaren Anforderungsprofilen (IT-Grundschutz++) entsteht ein verbindliches Zielbild für die Sicherheitsarchitektur der Bundesverwaltung. Die DVC richtet ihre Sicherheitsprinzipien und Reifegradkriterien an dieser Entwicklung aus, um für Bundesbedarfe anschlussfähig zu bleiben, sofern im föderalen Verbund möglich.

Perspektivisch sollen OZG, Registermodernisierung und Deutsche Verwaltungscloud ineinandergreifen. Die OZG-Umsetzung und die Registermodernisierung sind nicht direkt abhängig vom Aufbau der DVC und werden als parallele Handlungsstränge betrachtet. Alle Vorhaben sollen aber im Kontext der Deutschland-Architektur und bei der Errichtung des Deutschland-Stacks zusammenspielen. Für diese Errichtung bedarf es des perspektivischen Zugriffs auf ein gemeinsames und sicheres Verbindungsnetz der Teilnehmer (NV-DE). Während das OZG die Digitalisierung von Verwaltungsleistungen betrifft und die Registermodernisierung die Grundlagen für eine Ende-zu-Ende-Digitalisierung schafft, soll die DVC die IT-Infrastruktur der Öffentlichen Verwaltung zukunftsfähig ausrichten und damit eine wesentliche unterstützende Wirkung entfalten. Die DVC im Sinne einer Multi-Cloud-Infrastruktur ist dabei als "Zentrale Plattform" im Deutschland-Stack verankert und kann auf den angeschlossenen Betriebsplattformen wesentliche Teile des Plattformkerns des Deutschland-Stacks beherbergen.

2.2 Relevante Vorgaben und Richtlinien der Öffentlichen Verwaltung

Die folgenden Vorgaben und Richtlinien der Öffentlichen Verwaltung wurden bei der Weiterentwicklung der Zielarchitektur der Deutschen Verwaltungscloud grundsätzlich mitbetrachtet. Die Mitbetrachtung der Vorgaben und Richtlinien der Öffentlichen Verwaltung entbindet weder den Cloud-Service-Kunden noch den Cloud-Service-Anbieter von der Verpflichtung zur Einhaltung dieser Vorgaben und Richtlinien, die in ihrem jeweiligen konkreten Fall gelten. Diese Vorgaben und Richtlinien sind die Grundlage für die technische Spezifikation der DVC, die außerhalb des Rahmenwerks durchgeführt wird:

- **BSI-Vorgaben:** Die DVC als Cloud-Infrastruktur des Deutschland-Stacks orientiert sich an den Veröffentlichungen des BSI. Diese Veröffentlichungen des BSI (Vorgaben, Richtlinien,

Standards, Mindeststandards des BSI, Empfehlungen etc.) werden, sofern anwendbar, in den Detailstandards der Deutschen Verwaltungscloud verankert. Für alle Cloud-Services und damit auch für die Services der DVC spezifiziert der Kriterienkatalog Cloud Computing des BSI (kurz: C5)[25] Mindestanforderungen an die Informationssicherheit, die nicht unterschritten werden sollten. Dabei steht die Umsetzung der Kriterien im Vordergrund, eine Testierung nach C5 kann in weiteren Ausbaustufen erfolgen. Ziel ist die transparente Darstellung der Erfüllung von Kriterien an die Informationssicherheit eines Cloud-Services auf Basis einer standardisierten Prüfung. Im C5 werden auch explizit die Pflichten von Cloud-Anbietern und Cloud-Kunden hinsichtlich der geteilten Verantwortung („Shared Responsibility“) betrachtet. Das Portfolio der DVC orientiert sich vorrangig an den Anforderungen des IT-Grundschutzes. Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik führt Methoden, Anleitungen und Empfehlungen auf, um das Niveau der Informationssicherheit in einer Institution aufrechtzuerhalten und anzuheben. Es wird dabei ein ganzheitlicher Ansatz verfolgt: Neben technischen Aspekten werden auch infrastrukturelle, organisatorische und personelle Themen betrachtet. Dabei fällt der Ausgestaltung des IT-Grundschutzes entlang der Rollen der DVC eine zentrale Bedeutung zu.

- **Sicherheitsvorgaben des Bundes mit Bezug zur Cloud-Nutzung:** Über den Kriterienkatalog C5 hinaus sind für Bundesbedarfe insbesondere die ‚Eckpunkte einer Zero-Trust-IT-Sicherheitsarchitektur des Bundes‘, die Weiterentwicklung des IT-Grundschutzes (IT-Grundschutz++, maschinenlesbare Anforderungsprofile), die Bausteine APP.4.4 (Kubernetes) und SYS.1.6 (Containerisierung) des IT-Grundschutz-Kompendiums sowie die Technischen Richtlinien BSI TR-03183-2 (Software-Stückliste/SBOM) und BSI TR-03191 (maschinenlesbare Sicherheitsmeldungen, CSAF 2.0) relevant. Aus dem europäischen Rechtsrahmen sind zusätzlich die NIS-2-Richtlinie in ihrer nationalen Umsetzung sowie der Cyber Resilience Act (CRA) zu beachten.

[25] Kriterienkatalog C5, Link

- **Architekturvorgaben und Richtlinien:** Es gibt in Deutschland auf verschiedenen Ebenen diverse Architekturrichtlinien, die sich aus der Nationalen Architekturrichtlinie ableiten. Für die DVC als interföderales Vorhaben ist daher nur die „Föderale IT-Architekturrichtlinie" als Bestandteil der Deutschland-Architektur relevant. Diese dient sowohl als Orientierungsmarke für Angebote durch Cloud-Service-Anbieter in der DVC als auch für Cloud-Service-Kunden bei der Beschaffung von DVC-Cloud-Services. Weiterführende lokalisierte Architekturrichtlinien wie die „Architekturrichtlinie für die IT des Bundes" oder landesspezifische Architekturrichtlinien sowie weitere Architekturrichtlinien dürfen in einem gemeinsamen Vorhaben keine spezifische Relevanz für die Bereitstellung von inter-föderal nutzbaren und nachgenutzten Cloud-Services spielen.
- **Anforderungen an Technologieanbieter und -lösungen zur Stärkung der Digitalen Souveränität in der Beschaffung**[26]: Die Arbeitsgruppe Cloud Computing und Digitale Souveränität (kurz AG Cloud) sowie deren Unterarbeitsgruppe Beschaffung (kurz UAG Beschaffung) definieren übergreifende Empfehlungen an IT-Leistungen und die Auswahl der Anbieter für die Beschaffung von Informations- und Kommunikationstechnik durch beziehungsweise für die Öffentliche Verwaltung und deren bedarfs- und risikogerechte Anwendung. Dies konkretisiert die Vorgaben des Deutschland-Stacks zu seinen Standards für „Managed Services und Cloud" bzgl. „Ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen (EVB-IT bzw. EVB-IT Cloud)".
- **Digitale Barrierefreiheit:** Die DVC berücksichtigt die rechtlichen Vorgaben zur digitalen Barrierefreiheit, insbesondere die Barrierefreie-Informationstechnik-Verordnung (BITV 2.0). Maßgeblicher technischer Standard ist die harmonisierte europäische Norm EN 301 549 in ihrer jeweils gültigen Fassung, die unter anderem Anforderungen an Webanwendungen, mobile Anwendungen, Software und elektronische Dokumente definiert.

2.3 Digitale Souveränität für die DVC

Die EU hat das „Cloud Sovereignty Framework" in einer Version 1.2.1 im Oktober 2025 veröffentlicht und damit erstmals messbare Kriterien für „Digitale Souveränität" auf europäischer Ebene formuliert. Das BSI hat in Ergänzung dazu den C3A-Kriterienkatalog („Criteria enabling Cloud Computing Autonomy") veröffentlicht.[27] Dieser nimmt Bezug auf die im EU Cloud Sovereignty Framework eingeführten acht „Souveränitätsdimensionen" („Sovereignty

[26] Anforderungen an Technologieanbieter und -lösungen zur Stärkung der Digitalen Souveränität, in: Der Beauftragte der Bundesregierung für Informationstechnik, Link.

[27] C3A - Criteria enabling Cloud Computing Autonomy, Link

Objectives“), von denen eine („SOV-8 Environmental Sustainability“) aus Gründen mangelnder Zuständigkeit des BSI nicht betrachtet wurde und eine weitere Dimension („SOV-7 Security & Compliance Sovereignty“) bereits im Kriterienkatalog C5 behandelt wird. Die anderen sechs „Souveränitätsdimensionen“ wurden analog übernommen.
Diese Sicht dient der DVC bis auf Weiteres als Orientierungsgrundlage für die Ausgestaltung von Kriterien im Bereich der Digitalen Souveränität. Der C3A-Kriterienkatalog des BSI ist bislang keine verbindliche Richtlinie für die Öffentliche Verwaltung.
Mit dem am 3. Juni 2026 von der Europäischen Kommission vorgelegten Verordnungsvorschlag COM (2026) 502 zum Cloud and AI Development Act (CADA) liegt inzwischen zusätzlich ein europäischer regulatorischer Rahmenentwurf vor. Dieser sieht im Bereich „Autonomy“ insbesondere einen einheitlichen EU-weiten Bewertungsrahmen für die Souveränität von Cloud- und KI-Angeboten sowie einen Mechanismus zur Anwendung im öffentlichen Sektor vor.
Da sich CADA zum Zeitpunkt der Erstellung dieses Rahmenwerks noch im europäischen Gesetzgebungsverfahren befindet, ergeben sich daraus noch keine unmittelbar verbindlichen Anforderungen für die DVC. Die DVC wird jedoch die Weiterentwicklung des CADA sowie die daraus resultierenden europäischen Konkretisierungen berücksichtigen und die bestehenden Souveränitätskriterien, insbesondere ihre Ableitung aus dem EU Cloud Sovereignty Framework und dem C3A des BSI regelmäßig auf Konsistenz und Anpassungsbedarf überprüfen.
Werden daraus Änderungen der DVC-Kriterien erforderlich, sind diese versioniert in das Reifegradmodell beziehungsweise die zugehörigen Detailstandards zu überführen. Details und Handlungserfordernisse werden nach Vorliegen der verbindlichen CADA-Regelungen für die DVC konkretisiert, bspw. die Übergangsfristen und Regelungen für bereits autorisierte Cloud-Service-Anbieter und Cloud-Services.

2.4 Datenklassifizierung in der Öffentlichen Verwaltung

Um einen Rahmen für die Datenklassifizierung zu etablieren, orientiert sich die Deutsche Verwaltungscloud an den für den Bereich der Öffentlichen Verwaltung geltenden Regelwerken. Die Verantwortung für die Prüfung und Festlegung des Schutzbedarfes der zu verarbeitenden Daten und daraus folgende Maßnahmen liegt bei den Cloud-Service-Kunden.
Die Sicherstellung einer Verarbeitung gemäß den anwendbaren gesetzlichen und vertraglichen Regelwerken innerhalb der Cloud-Services obliegt den Cloud-Anbietern.

Für die DVC sind hinsichtlich der Datensicherheit und des Datenschutzes insbesondere die folgenden Regelwerke relevant:

- **Geheimschutz**[28]: Der staatliche Geheimschutz umfasst alle Maßnahmen zur Geheimhaltung von Informationen, die durch staatliche Stellen als Verschlusssachen (VS) eingestuft sind. Im Rahmen der DVC wird die Schaffung von Voraussetzungen für deren Verarbeitung bis zum Grad „VS-Nur für den Dienstgebrauch" (VS-NfD) angestrebt. Die Beurteilung, ob ein spezifischer Cloud-Service die Anforderungen des Grades VS-NfD erfüllt, liegt im Einzelfall immer in der Verantwortung des Cloud-Service-Kunden. Der Cloud-Service-Kunde stellt den Schutzbedarf fest und entscheidet über den konkreten Einsatz eines Cloud-Services. Der Cloud-Service-Anbieter weist die hierfür erforderliche Eignung nach und stellt die zugehörige Dokumentation bereit; für die Verarbeitung von Verschlusssachen können darüber hinaus formale Zulassungs- und Betriebsanforderungen gelten. Eine Verarbeitung oberhalb von VS-NfD ist derzeit nicht Gegenstand der DVC.
- **Datenschutzgrundverordnung (DSGVO)**: Die DSGVO dient dem Schutz personenbezogener Daten innerhalb der Europäischen Union (EU) und verpflichtet Daten verarbeitende Stellen insbesondere zur Rechtmäßigkeit der Verarbeitung, Transparenz, Sicherheit und Rechenschaftspflicht, wobei sie den Betroffenen weitreichende Rechte zur Kontrolle ihrer Daten einräumt.

  Für die Cloud-Service-Kunden der DVC ist die Feststellung des Schutzbedarfs vor der Beauftragung eines Cloud-Services relevant. Eine Datenschutzfolgeabschätzung ist gemäß DSGVO Artikel 35 bei hohen Risiken für die Rechte und Freiheiten natürlicher Personen durchzuführen. Eventuell ist auch ein Vertrag über die Auftragsverarbeitung (Art. 28 DSGVO) erforderlich. Die Beurteilung, ob ein Cloud-Service der DSGVO oder weiteren datenschutzrechtlichen Regularien unterliegt, liegt in der Verantwortung des Cloud-Service-Kunden. Die für die Beurteilung notwendige Dokumentation ist durch den Cloud-Service-Anbieter bereitzustellen.

  Im Rahmen der DVC wird auch die Möglichkeit angestrebt, personenbezogene Daten der „besonderen Kategorien" gemäß Artikel 9 DSGVO zu verarbeiten, insoweit sind gegebenenfalls auch die einschlägigen Vorschriften des BDSG und der Landesdatenschutzgesetze zu beachten. Unter Umständen können auch Fachgesetze, wie z. B. das Sozialgesetzbuch,

[28] Geheimschutz, in: Bundesamt für Sicherheit in der Informationstechnik, Link.

relevant sein. Die Beurteilung, ob ein spezifischer Cloud-Service die Anforderungen der DSGVO erfüllt, liegt im Einzelfall in der Verantwortung des Cloud-Service-Kunden.

- **IT-Grundschutz:** Ziel des IT-Grundschutzes ist es, das Niveau der Informationssicherheit in einer Institution anzuheben und aufrechtzuerhalten. Die Schutzbedarfsfeststellung im IT-Grundschutz dient dazu, den spezifischen Schutzbedarf systematisch zu ermitteln. Für die Cloud-Service-Kunden der DVC ist die Aufstellung einer Schutzbedarfsfeststellung vor der Beauftragung eines Cloud-Services relevant. Die Basiskriterien des Kriterienkatalogs C5 (Cloud Computing Compliance Criteria Catalogue) spiegeln aus Sicht des BSI das Niveau an Informationssicherheit wider, das ein Cloud-Dienst mindestens bieten muss, wenn Cloud-Kunden mit diesem Informationen verarbeiten, die einen normalen Schutzbedarf haben. Der C5 richtet sich an Cloud-Anbieter, deren Prüfer und Kunden. Er bildet die Grundlage, um ein kundeneigenes Risikomanagement durchführen zu können. Die Zusatzkriterien des C5 können einen Ausgangs- bzw. Ansatzpunkt darstellen, um eine Bewertung für Informationen vorzunehmen, die einen höheren Schutzbedarf haben.

3 Geschäftsarchitektur der Deutschen Verwaltungscloud

3.1 Produktmanagement-Modell der FITKO

Das Produkt Deutsche Verwaltungscloud wird gemäß Beschluss (IT-PLR 2024/51) nach dem Produktmanagement-Modell für Produkte des IT-PLR gesteuert[29]. Das DVC-Produktboard ist auf der strategischen Ebene angeordnet und definiert entsprechend den strategischen Rahmen für die Produktentwicklung. Es entscheidet über die größeren, strategisch bedeutsamen Änderungsvorhaben der DVC. Das DVC-Produktteam ist auf der koordinierenden Ebene das zentrale Team, das sich fortwährend mit der Weiterentwicklung des Produkts und dem laufenden fachlichen und technischen Betrieb beschäftigt. Es verknüpft die strategische Ebene mit der nachfolgenden umsetzenden Ebene. Zu seinen Aufgaben zählen die Strategieentwicklung (mit dem Produktboard), das Stakeholder-Management, die Umsetzung sowie die Verwaltung des Produkts.

Das DVC-Produktmanagement der FITKO beauftragt einen Betreiber mit dem Betrieb und der Weiterentwicklung der beauftragten Komponenten der DVC und übernimmt die Steuerung des Betreibers. Darüber hinaus übernimmt das DVC-Produktmanagement weitere Aufgaben, wie den Abbau von Nutzungshürden, die Moderation der Teilnahme an der DVC, das Stakeholder-Management, die Kommunikation und Information. Im Rahmen der Moderation der Teilnahme hat das DVC-Produktmanagement das Recht, die Eigenerklärungen der Cloud-Service-Anbieter zu ihren Cloud-Services zu plausibilisieren und im Detail zu prüfen und zu verifizieren; es ist dazu jedoch nicht verpflichtet.

[29] Produktmanagement-Modell FITKO: Link.

3.2 Zusammenarbeitsmodell

Die Teilnehmer der Deutschen Verwaltungscloud verfolgen einen arbeitsteiligen Kooperationsansatz. Die öffentlichen IT-Dienstleister erbringen die Cloud-Services der DVC als verteilt arbeitendes, bundesweit orchestriertes Ökosystem auf Basis cloud-nativer Entwicklungsprinzipien. Die Cloud-Service-Kunden in Bund, Ländern und Kommunen nutzen diese Services flächendeckend und effizient. Im Zusammenarbeitsmodell agieren die Teilnehmer in folgenden zentralen Rollen:

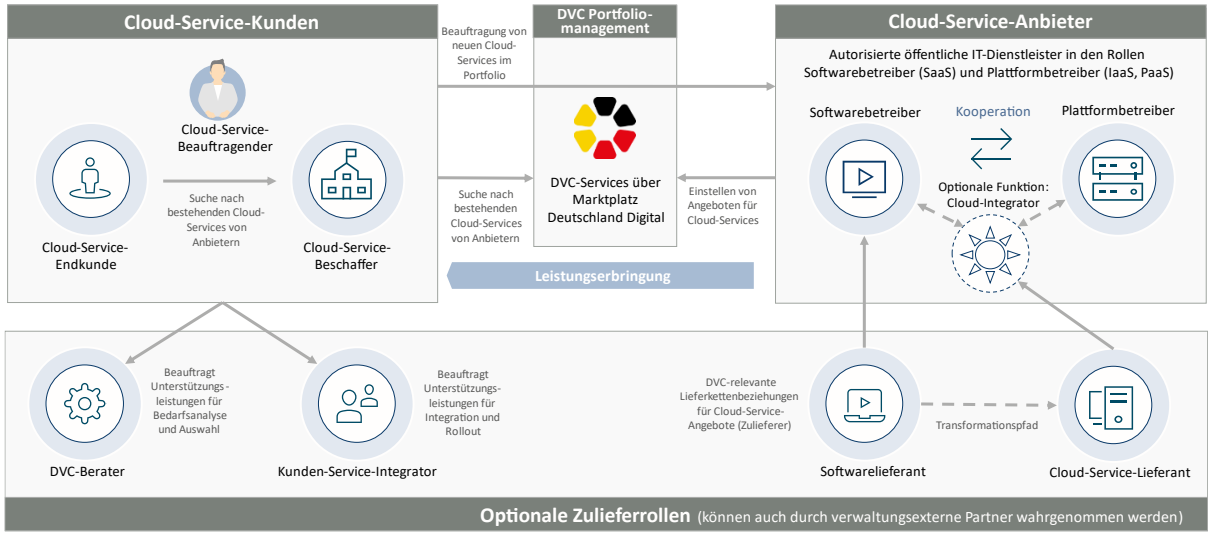

Abbildung 2: Zentrale Rollen und Akteure in der Deutschen Verwaltungscloud

Über den Marktplatz Deutschland Digital haben Cloud-Service-Kunden u.a. Zugriff auf einen Cloud-Service-Katalog mit DVC-konformen Cloud-Services und können diese über verschiedene Beschaffungsmodelle beziehen. Die Auswahl von Cloud-Services im MDD erfolgt nach einheitlich definierten Service-Kategorien. Die weiteren Rollen des Zusammenarbeitsmodells werden in den nachfolgenden Kapiteln beschrieben.

3.3 Rollen und Akteure in der Deutschen Verwaltungscloud

Das Rollenmodell der Deutschen Verwaltungscloud wurde entwickelt, um die klassischen Verantwortungen für Herstellung, Bezug und Betrieb von IT-Services in ein modernes Cloud-basiertes Modell der geteilten Verantwortungen zu überführen. Dieses Modell wird im Zuge des Ausbaus der DVC kontinuierlich weiterentwickelt. Die nachfolgend spezifizierten Rollen dienen der Orientierung und beschreiben insbesondere fachlich-technische Aspekte. Organisationen können mehrere Rollen einnehmen. Die daraus entstehenden Vertragsbeziehungen sind im Kapitel 3.5 „Vertragsmodelle“ behandelt.

Das Rollenmodell beschreibt die Verantwortungen, die aus der Vertragsbeziehung zwischen Cloud-Service-Anbieter und Cloud-Service-Kunde entstehen. Verantwortungen für gemeinsam genutzte Bausteine des Deutschland-Stacks – etwa für querschnittliche Sicherheitswerkzeuge – werden nicht im DVC-Rollenmodell geregelt, sondern in der Produkt- und Architektur-Governance des Deutschland-Stacks. Die Schnittstelle zwischen beiden Modellen einschließlich der Entscheidungs- und Eskalationswege wird gemeinsam beschrieben.

3.3.1 Rollen auf der Kundenseite

- **Cloud-Service-Kunden:** Cloud-Service-Kunden beziehen als Cloud-Service-Endkunden oder Cloud-Service-Beschaffer DVC-Cloud-Services über den Marktplatz Deutschland Digital (MDD) aus dem DVC-Portfolio. Cloud-Service-Kunden nutzen die Cloud-Services selbst und/oder beziehen diese als Cloud-Service-Beschaffer (bisher Cloud-Service-Vermittler), um sie ihrerseits durch ihre Kunden (Kunden des Cloud-Service-Beschaffers) nutzen zu lassen.

  Cloud-Service-Kunden können sein:

  - öffentliche Stellen im Sinne von § 1 Absatz 1 OZG,
  - Rechtsträger von Behörden im Sinne von § 2 Absatz 9 OZG,
  - öffentliche Auftraggeber im Sinne des § 99 Nummer 1 bis 3 Gesetz gegen Wettbewerbsbeschränkungen (GWB) und
  - juristische Personen des öffentlichen oder privaten Rechts, hinsichtlich derer die Voraussetzungen des § 108 Absatz 1 oder Absatz 4 GWB vorliegen.

- **Cloud-Service-Endkunde:** Cloud-Service-Endkunden beziehen DVC-Cloud-Services direkt über den Marktplatz Deutschland Digital für sich selbst oder beschaffen diese Services über einen Cloud-Service-Beschaffer.
- **Cloud-Service-Beschaffer:** Cloud-Service-Beschaffer sind Cloud-Service-Kunden, die Cloud-Services über den Marktplatz Deutschland Digital (MDD) aus dem DVC-Portfolio beziehen, um diese ihrerseits durch ihre Kunden (Cloud-Service-Endkunden) nutzen zu lassen.[30]
- **Cloud-Service-Beauftragender:** Cloud-Service-Beauftragende veranlassen die Erstellung neuer Cloud-Services oder die Modernisierung bestehender Services. Laut MPK-Beschluss vom 06.11.2023 „sollten IT-Lösungen der Öffentlichen Verwaltung entsprechend der Deutschen Verwaltungscloud-Strategie (DVS) cloudfähig hergestellt werden, damit sie einfach auf allen föderalen Ebenen nutzbar sind".31 Damit fällt den Cloud-Service-Beauftragenden im Kontext der DVC die besondere Verantwortung zu, eine IT-Lösung DVC-konform zu beauftragen und zu prüfen, ob dieser Service in der Deutschen Verwaltungscloud (über den Marktplatz Deutschland Digital im DVC-Portfolio) zur Nachnutzung angeboten werden kann. Im Falle der Nachnutzung in der DVC beauftragen sie einen Cloud-Service-Anbieter, den Service in der DVC anzubieten. Dazu bedarf es eines gemeinsam getragenen Beauftragungsprozesses für Cloud-Services, der in eine gemeinsame Nachnutzung münden muss.

Auf der Kundenseite gibt es neben den direkt im Kontext des DVC-Portfolios agierenden drei vorgestellten Rollen zwei weitere ergänzende Rollen, auf die der Cloud-Service-Kunde optional zugreifen kann, um DVC-Cloud-Services in seiner jeweiligen lokalen Umgebung im Verbund mit der dort vorhandenen spezifischen IT-Landschaft erfolgreich zu nutzen. Diese Rollen können auch aus dem bestehenden Partner-Umfeld des Cloud-Service-Kunden besetzt werden.

- **DVC-Berater:** Der DVC-Berater berät den Cloud-Service-Kunden zu den technisch-fachlichen Möglichkeiten der DVC-Nutzung und kann bei der Auswahl geeigneter DVC-Cloud-Services unterstützen. Diese Rolle können sowohl Akteure der Öffentlichen Verwaltung als auch verwaltungsexterne Anbieter (z. B. Softwarelieferanten) wahrnehmen. DVC-Berater sollen perspektivisch bei der DVC akkreditiert werden.

---

30 Beispiel: Ein öffentlicher IT-Dienstleister bezieht Cloud-Services über den MDD, um diese den Behörden seiner Träger zur Verfügung stellen zu können.

31 Besprechung des Bundeskanzlers mit den Regierungschefinnen und Regierungschefs der Länder am 6. November 2023, Link

- **Kunden-Service-Integrator:** Kunden-Service-Integratoren sind von Cloud-Service-Kunden Beauftragte. Sie unterstützen die Integration von DVC-Cloud-Services in die Umgebung des Cloud-Service-Kunden.

Kunden-Service-Integratoren können sowohl Akteure der Öffentlichen Verwaltung als auch verwaltungsexterne Anbieter sein.

3.3.2 Rollen auf der Anbieterseite

- **Cloud-Service-Anbieter:** Cloud-Service-Anbieter bieten als Plattformbetreiber und/oder Softwarebetreiber DVC-Cloud-Services über den Marktplatz Deutschland Digital (MDD) im Rahmen des DVC-Portfolios an und verantworten die Leistungserbringung. Die Unterscheidung von Softwarebetreibern und Plattformbetreibern ist im Sinne der Spezialisierung in einem auf verteilter Verantwortung beruhenden Zusammenarbeitsmodell zu sehen. Cloud-Service-Anbieter können dabei auch verwaltungsexterne Services eines Cloud-Service-Lieferanten in der Funktion des „Cloud-Integrators" einbinden.

  Cloud-Service-Anbieter von DVC-Cloud-Services im MDD können ausschließlich sein:

  - öffentliche Stellen im Sinne von § 1 Absatz 1 OZG,
  - Rechtsträger von Behörden im Sinne von § 2 Absatz 9 OZG,
  - öffentliche Auftraggeber im Sinne des § 99 Nummer 1 bis 3 GWB und
  - juristische Personen des öffentlichen oder privaten Rechts, hinsichtlich derer die Voraussetzungen des § 108 Absatz 1 oder 4 GWB vorliegen.

  Cloud-Service-Anbieter kann nicht sein, wer 20 Prozent oder mehr seiner Tätigkeiten am offenen Markt erbringt (vgl. § 108 Abs. 1 Nr. 2, Abs. 4 Nr. 2 bzw. Abs. 6 Nr. 3 GWB).
- **Plattformbetreiber:** Plattformbetreiber sind Cloud-Service-Anbieter, die DVC-Cloud-Services im IaaS- oder PaaS-Modell - vorzugsweise über Betriebsplattformen – bereitstellen. Eine Betriebsplattform setzt auf IaaS oder PaaS auf und schafft einen standardisierten, automatisierten Rahmen, in dem diese Ressourcen als konsumierbare Services bereitgestellt und im Betrieb geführt werden (inkl. Monitoring, Security, Standards, Automatisierung, Self-Service). Plattformbetreiber können verwaltungsexterne Cloud-Services in ihrer Funktion als Cloud-Integrator in ihre Services integrieren.
  Im Rahmen der DVC liegt ein besonderer Fokus auf standardisierten Kubernetes-basierten Plattformservices. „Namespace-as-a-Service" und „Cluster-as-a-Service" bezeichnen dabei DVC-spezifische Serviceausprägungen innerhalb einer Betriebsplattform und stellen keine

eigenständigen Cloud-Service-Modelle neben IaaS, PaaS und SaaS dar. Sie sollen Softwarebetreibern eine standardisierte, automatisiert bereitstellbare und möglichst wechselfähige Containerorchestrierungsumgebung zur Verfügung stellen.

Beim „Namespace-as-a-Service" stellt der Plattformbetreiber einen logisch abgegrenzten Mandantenbereich innerhalb einer gemeinsam betriebenen Kubernetes-Plattform bereit. Er verantwortet insbesondere die sichere technische Mandantentrennung auf Plattformebene sowie die hierfür erforderlichen Mechanismen für Netzwerksegmentierung, Storage, Secrets-Management, Ressourcenquoten und Plattform-Policies. Der Softwarebetreiber verantwortet die innerhalb dieses Bereichs betriebenen Workloads, deren Anwendungskonfiguration sowie den Lifecycle der darauf bereitgestellten Cloud-Services.

Beim „Cluster-as-a-Service" wird dem Softwarebetreiber demgegenüber eine stärker isolierte Kubernetes-Umgebung mit einer entsprechend erweiterten Verantwortungsgrenze bereitgestellt. Die konkrete Ausgestaltung der Isolation, Berechtigungen, Sicherheitsmechanismen und Verantwortungsübergänge wird in den nachgelagerten Detailstandards und im jeweiligen Shared-Responsibility-Modell des Cloud-Services spezifiziert.

Die konkrete Ausgestaltung der Mandantentrennung, Isolation, Berechtigungen, Ressourcenquoten und Plattform-Policies sowie der Verantwortungsübergang zwischen Plattform- und Softwarebetreiber werden in den nachgelagerten Detailstandards und im jeweiligen Shared-Responsibility-Modell spezifiziert.

- **Softwarebetreiber:** Softwarebetreiber sind Cloud-Service-Anbieter, die DVC-Cloud-Services im SaaS-Modell bereitstellen. Sie verantworten den Betrieb konsumierbarer Services im Full Lifecycle Management. Sie müssen dabei keinen eigenen RZ-Betrieb ausbilden, sondern können auf dem Fundament der als DVC-Cloud-Services bereitgestellten Betriebsplattformen der Plattformbetreiber aufsetzen. Softwarebetreiber können Softwarelieferanten für Entwicklungs- und Wartungsleistungen für Softwarekomponenten ihres Services einbinden und verwaltungsexterne Cloud-Services in ihrer Funktion als Cloud-Integrator in ihre Services integrieren.

Auf der Anbieterseite gibt es neben den direkt im Kontext des DVC-Portfolios agierenden zwei vorgestellten Rollen zwei weitere ergänzende Rollen, die mit Cloud-Service-Anbietern interagieren können und somit helfen, den Anbieterkreis über die Grenzen von IT-Dienstleistern der Öffentlichen Verwaltung zu erweitern:

- **Cloud-Service-Lieferant:** Cloud-Service-Lieferanten stellen Leistungen als Unterauftragnehmer eines Plattformbetreibers oder Softwarebetreibers bereit. Plattform- beziehungsweise Softwarebetreiber können Leistungen von Cloud-Service-Lieferanten beziehen, diese DVC-konform ausgestalten und als Teil ihres Cloud-Service-Portfolios anbieten.
  Cloud-Service-Lieferanten können sowohl Akteure der Öffentlichen Verwaltung als auch verwaltungsexterne Anbieter sein.
- **Softwarelieferant:** Softwarelieferanten entwickeln Softwareanwendungen als Unterauftragnehmer eines Softwarebetreibers und stellen diese dem Softwarebetreiber im Rahmen von durch den Softwarebetreiber definierten Schnittstellen bereit. Softwarelieferanten übernehmen gegebenenfalls die Wartung und Pflege der Software. Softwarelieferanten können sowohl Akteure der Öffentlichen Verwaltung als auch verwaltungsexterne Anbieter sein. Ihr Arbeitsergebnis ist dabei aber stets Entwicklung und Pflege von Software. Softwarelieferanten, die als Ergebnis eines Transformationsprozesses selbst als Endprodukt Services erzeugen wollen, sind in der Rolle des Cloud-Service-Lieferanten oder des Softwarebetreibers in der DVC aktiv.

3.3.3 Prinzip der geteilten Verantwortung

Das Prinzip der geteilten Verantwortung (inkl. der datenschutzrechtlichen Verantwortung), bekannt als „Shared Responsibility“, ist ein zentrales Konzept im Bereich der Bereitstellung und des Betriebs von Cloud-Services. Es beschreibt die Aufteilung der Sicherheits- und Compliance-Verantwortlichkeiten zwischen dem Cloud-Service-Anbieter und dem Cloud-Service-Kunden. Nicht alle Sicherheitsaspekte eines Cloud-Services liegen allein in der Verantwortung des Cloud-Service-Anbieters. Stattdessen müssen Cloud-Service-Kunden bestimmte Sicherheitsmaßnahmen selbst übernehmen. Die geteilte Verantwortung umfasst neben Sicherheits- und Compliance-Verantwortlichkeiten auch die betrieblichen Service-Management-Verantwortlichkeiten. Für jeden Cloud-Service sind Zuständigkeiten, Übergabepunkte und Eskalationswege für den operativen Betrieb über die vollständige Bereitstellungskette transparent und verbindlich zu regeln.

Die spezifische Aufteilung der Verantwortlichkeiten hängt unter anderem vom jeweiligen Cloud-Service-Modell ab. Daher ist für jeden Cloud-Service gesondert die Aufgabenverteilung zwischen den beteiligten Akteuren (Cloud-Service-Kunde, Cloud-Service-Anbieter) zum Schutz der Cloud-Umgebung transparent und verbindlich über die vollständige Bereitstellungskette zu regeln. Um dieses Modell besser im Kontext der DVC als Zusammenarbeitsmodell handhabbar zu machen, sind die erweiterten Rollendefinitionen in Kapitel 3.3 entstanden. Die Aufgabenverteilung wird je Cloud-Service in einer strukturierten Verantwortungsmatrix dokumentiert, die Bestandteil der Leistungsbeschreibung ist. Sie weist mindestens aus, welche Sicherheitsmaßnahmen der Cloud-Service-Anbieter erbringt, welche der Cloud-Service-Kunde zu erbringen hat und welche gemeinsam erbracht werden.

3.3.4 DevSecOps in der DVC und der Öffentlichen Verwaltung

DevOps (Development und Operations) ist eine Unternehmenskultur und Methodik, die Softwareentwicklung und IT-Betrieb über den gesamten Lebenszyklus eines Cloud-Services integriert. Für die Deutsche Verwaltungscloud wird dieser Ansatz im Sinne von DevSecOps erweitert: Informationssicherheit und Compliance werden nicht als nachgelagerte Prüfungen verstanden, sondern als gleichberechtigte und kontinuierlich zu berücksichtigende Dimensionen neben Entwicklung und Betrieb. Ziel ist es, durch Automatisierung, enge Zusammenarbeit und kontinuierliche Verbesserung die Qualität, Sicherheit und Regelkonformität der Cloud-Services zu erhöhen, Entwicklungs- und Bereitstellungszyklen zu verkürzen sowie Deployments sicher und zuverlässig durchzuführen.

DevSecOps lässt sich weder unmittelbar im Rollenmodell der DVC abbilden noch allein durch die Einführung technischer Werkzeuge und Plattformen erreichen. Es handelt sich vielmehr um ein organisations- und prozessübergreifendes Arbeitsmodell, in dem Entwicklung, Betrieb, Informationssicherheit und Compliance gemeinsam Verantwortung für den gesamten Lebenszyklus eines Cloud-Services übernehmen. Sicherheits- und Compliance-Anforderungen sollen dabei möglichst frühzeitig („Shift Left“) berücksichtigt und durch automatisierte Prüfungen in Entwicklungs-, Build-, Test-, Bereitstellungs- und Betriebsprozesse integriert werden. Die Umsetzung erfordert einen kontinuierlichen organisatorischen und technischen Reifeprozess.

Auf der Anbieterseite der DVC-Cloud-Services kommt der Rolle des Softwarebetreibers eine zentrale Bedeutung zu. Nur in dieser Rolle fallen Entwicklungs- und Betriebsverantwortung für einen konsumierbaren Service zusammen.
Der Softwarebetreiber ist daher ein zentraler Katalysator für eine DevSecOps-Kultur bei Cloud-Service-Angeboten und trägt gemeinsam mit den beteiligten Plattform-, Sicherheits- und Governance-Funktionen dazu bei, Entwicklungs-, Betriebs-, Sicherheits- und Compliance-Anforderungen durchgängig miteinander zu verzahnen.

Voraussetzung für den Erfolg eines solchen Modells ist jedoch eine grundlegende Veränderung der Beschaffungsprozesse in der Öffentlichen Verwaltung. Die bisherige Praxis, Software zu beschaffen und diese selbst in eigenen Umgebungen zu betreiben, muss zugunsten eines Bezugs fertiger, konsumierbarer Cloud-Services aus einem gemeinsamen Ökosystem aufgegeben werden.

3.4 DVC-Ökosystem

Das DVC-Ökosystem umfasst alle Elemente, die für die standardisierte Bereitstellung, Beschaffung und den Betrieb von Cloud-Services der Deutschen Verwaltungscloud zusammenwirken:

- **Gemeinsamer Rahmen der DVC:** Der gemeinsame Rahmen schafft die verbindliche Standardisierungsgrundlage der DVC. Er umfasst das vorliegende Rahmenwerk der Zielarchitektur, die Detailstandards, das Reifegradmodell mit seinen Minimalkriterien, die einheitlichen Allgemeinen Geschäftsbedingungen sowie die Leitfäden und Blaupausen. Gemeinsam sichern sie Interoperabilität, Wechselfähigkeit sowie ein einheitliches Sicherheits- und Qualitätsniveau der in der DVC angebotenen Cloud-Services.
- **Föderales Zusammenarbeitsmodell.** Im föderalen Zusammenarbeitsmodell (vgl. Abschnitt 3.2) kooperieren die Cloud-Service-Anbieter in ihren Rollen als Softwarebetreiber und Plattformbetreiber (ggf. in der zusätzlichen Funktion eines Cloud-Integrators) und bringen ihre Cloud-Services nach den Vorgaben der DVC ein. Die so entstehenden DVC-konformen Cloud-Services werden heute über den Marktplatz Deutschland Digital (MDD) angeboten und beschafft. Die marktplatz- und beschaffungsbezogenen Funktionen (E-Commerce, Vertragsabwicklung) liegen damit im Verantwortungsbereich des MDD. Die DVC verantwortet den gemeinsamen Rahmen, die Anforderungen für die Weiterentwicklung des DVC-Ökosystems, die Entwicklung des Serviceportfolios der DVC-konformen Cloud-Services sowie die nachfolgend beschriebenen Cloud-Infrastruktur-Komponenten.
- **DVC-Cloud-Infrastruktur-Komponenten (im Aufbau).** Mit den Cloud-Infrastruktur-Komponenten verbessert die DVC die technische Grundlage für den Betrieb DVC-konformer Cloud-Services. Hierzu zählen insbesondere die im Aufbau befindlichen DVC-Cloud-Betriebsplattformen (Fokus zunächst auf Public Cloud), auf denen Plattformbetreiber standardisierte Plattformdienste bereitstellen. Zur sprachlichen Unterscheidung werden die Betriebsplattformen, die möglichst direkt auf den Cloud-Services externer Cloud-Service-Lieferanten aufbauen **DVC-Betriebsplattform (public)** und die Betriebsplattformen, die auf den privaten Clouds der öffentlichen IT-Dienstleister (DVC-Plattformbetreiber) aufbauen **DVC-Betriebsplattform (private)** genannt. Dabei können auch die privaten Clouds der IT-Dienstleister Services von externen Cloud-Service-Lieferanten enthalten.

Auf Basis dieser IaaS/PaaS Betriebsplattformen kann perspektivisch eine DVC „Multi-Cloud Management Plattform" (MCMP) entstehen, die die Orchestrierung der Cloud-Services der Betriebsplattformen und die Verrechnung der genutzten Cloud-Services regelt und durch

vereinheitlichte Cloud-Management Prozesse einen Cloudbetrieb unabhängig von den darunterliegenden Betriebsplattformen gewährleistet.
Zudem wird die Föderierte Authentifizierungskomponente (FöAk) entwickelt, die eine einheitliche, sichere Authentisierung über die Akteure und Services der DVC hinweg ermöglicht. Die DVC benennt Anforderungen für die Weiterentwicklung der Verwaltungsnetze und schlägt Umsetzungsoptionen vor.

3.5 Vertragsmodelle

Grundlage für die Gestaltung der Vertragsmodelle sind die allgemeinen Vertragsbedingungen für Cloud-Services im Marktplatz Deutschland Digital (CS-AGB).
Die Vertragsgestaltung soll sich möglichst nah an marktüblichen Grundlagen für Cloud-Services orientieren und die Belange der Öffentlichen Verwaltung berücksichtigen.
Grundsätzlich bestehen zwei Vertragsmodelle, um Cloud-Services über den Marktplatz Deutschland Digital (MDD) beziehen zu können:

- das Direktvertragsmodell und
- das Umklappvertragsmodell,

die nachfolgend erläutert werden. Darüber hinaus sind Vertragsketten über einen Cloud-Service-Beschaffer möglich.
Im **Direktvertragsmodell** (siehe nachfolgende Abbildung Szenario 1) geht der Kunde nach der Bestellung einen Vertrag direkt mit dem Anbieter ein. Dies ist insbesondere dann möglich, wenn der Kunde eine Inhouse-Beziehung gemäß § 108 GWB zur Anbieterin / zum Anbieter hat. Darüber hinaus ist ein Direktvertrag bei unentgeltlichen Services sowie bei Unterschreiten bestimmter vergaberechtlicher Wertgrenzen („Bagatellgrenzen") möglich.
Ein **Umklappvertragsmodell** (siehe nachfolgende Abbildung Szenario 2) ist möglich, wenn sowohl Anbieter als auch Kunde jeweils eine Inhouse-Beziehung gemäß § 108 GWB zum Intermediär haben. Die Inhouse-Beziehung kann dabei auch mittelbar in Form einer „Inhouse-Kette" bestehen, z.B. vermittelt über einen öffentlichen IT-Dienstleister. Im Umklappvertragsmodell besteht pro Cloud-Service-Abonnement ein Vertragspaar: einerseits ein Vertrag zwischen dem Cloud-Service-Anbieter und einem Intermediär sowie andererseits ein Vertrag zwischen dem Intermediär und dem Cloud-Service-Kunden. Der Intermediär ist Vertragspartner des Cloud-Service-Anbieters und (spiegelbildlich) des Cloud-Service-Kunden im Umklappvertragsmodell. Welche der Modelle für einen Cloud-Service angeboten werden, legt der Cloud-Service-Anbieter in seinem Service Offering im MDD für jeden einzelnen Cloud-Service fest. Der Cloud-

Service-Kunde (oder ggf. der Cloud-Service-Beschaffer) entscheidet mit der Bestellung über den MDD, in welchem Vertragsmodell er den Cloud-Service beziehen möchte.

Falls Cloud-Services von Cloud-Service-Kunden über Cloud-Service-Beschaffer bezogen werden, entsteht folgende Vertragskette: Der Cloud-Service-Beschaffer schließt den Vertrag über ein Cloud-Service-Abonnement mit dem Cloud-Service-Anbieter. Darüber hinaus schließt er Verträge mit seinen Cloud-Service-Kunden. Gegebenenfalls wird der Intermediär in die Vertragskette einbezogen.
Im Zuge des Ausbaus der Deutschen Verwaltungscloud können auch weitere Ausgestaltungen und Modelle entwickelt werden.
Zur Verdeutlichung der Interaktionen der zuvor definierten Rollen sind im Folgenden typische Szenarien innerhalb der DVC beispielhaft dargestellt:

Szenario 1: Beschaffung im Direktvertragsmodell

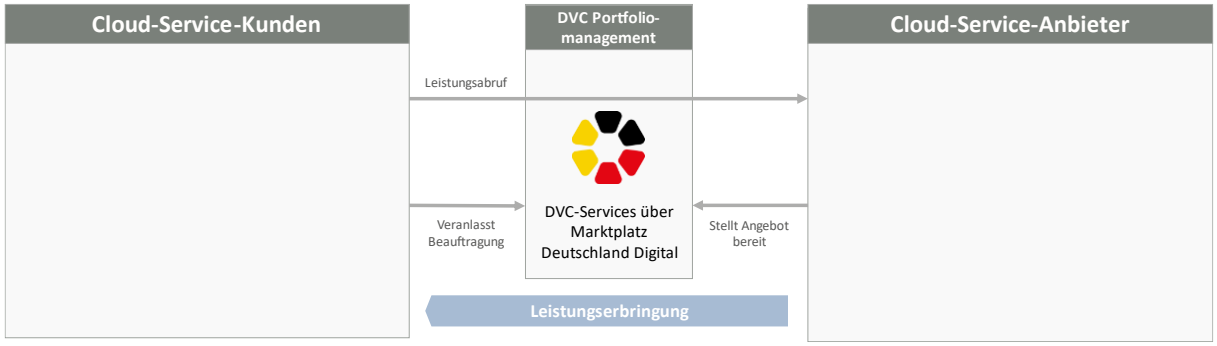

Abbildung 3: Direktvertragsmodell

Alternativ kann ein Cloud-Service-Kunde einen Cloud-Service-Beschaffer mit der Beschaffung beauftragen:

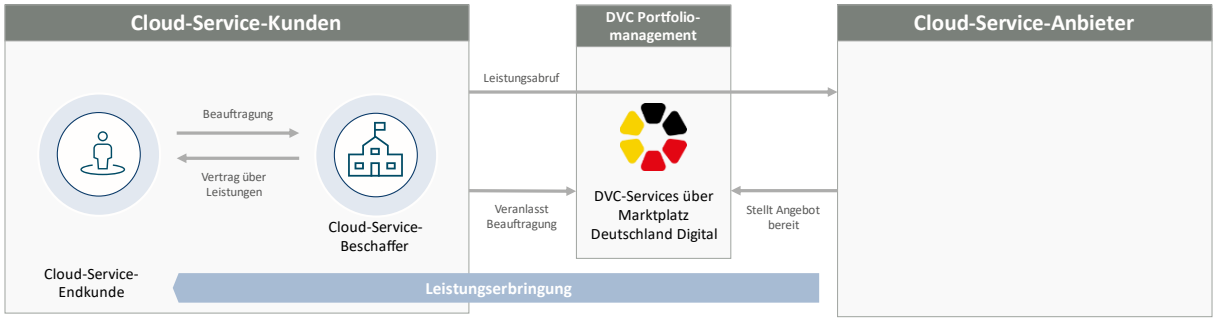

Abbildung 4: Direktvertragsmodell mit Cloud-Service-Beschaffer

Szenario 2: Umklappvertragsmodell

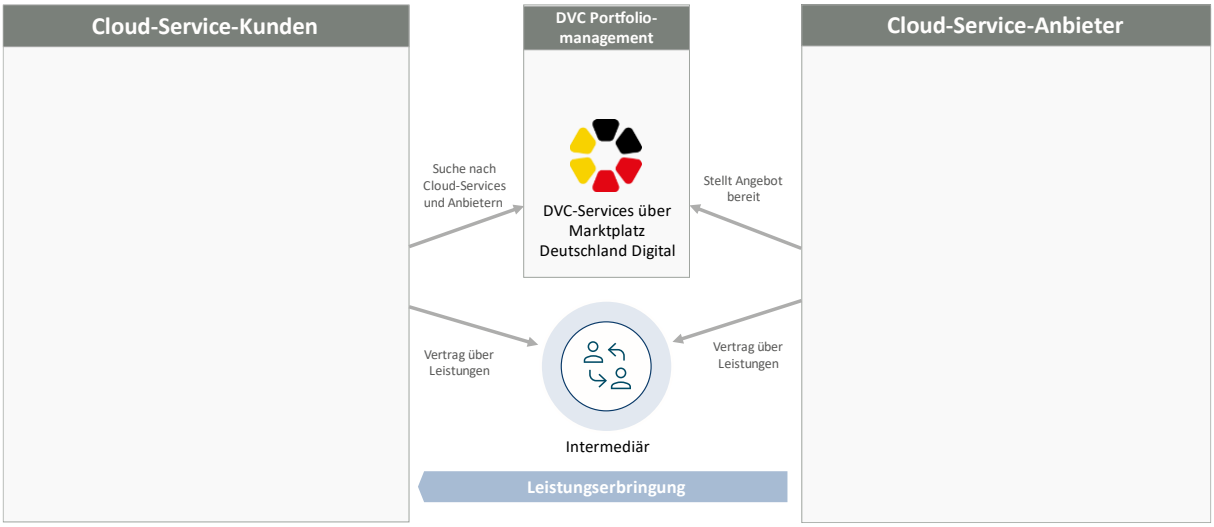

Abbildung 5: Umklappvertragsmodell

Alternativ kann ein Cloud-Service-Beschaffer eingeschaltet werden:

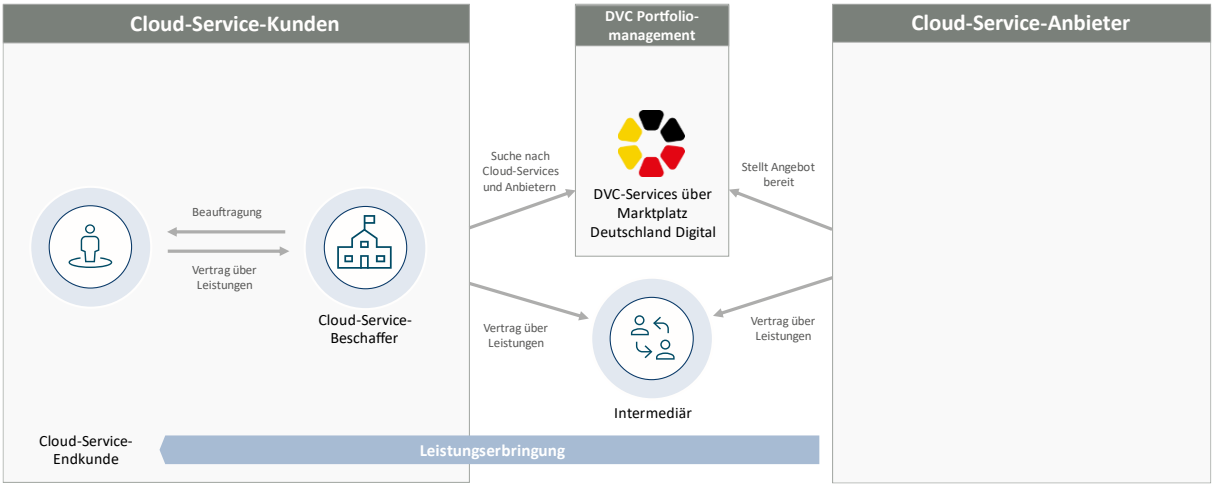

Abbildung 6: Umklappvertragsmodell mit Cloud-Service-Beschaffer

Die Vertragsbeziehung zwischen Cloud-Service-Endkunden und Cloud-Service-Beschaffer ist zum Redaktionszeitpunkt des Rahmenwerks nicht durch die CS-AGB des MDDs geregelt. Eine Anwendung der CS-AGB wird empfohlen.

3.6 Einbindung von verwaltungsexternen Anbietern

Verwaltungsexterne Anbieter können sich indirekt in den Rollen Softwarelieferant und Cloud-Service-Lieferant in die Deutsche Verwaltungscloud einbringen.

- **Softwarelieferanten:** können Vertragsbeziehungen zu einem oder mehreren Softwarebetreibern aufbauen. Diese Softwarebetreiber erzeugen DVC-konforme Cloud-Services auf Basis der Software des Softwarelieferanten und übernehmen den Betrieb. Der Softwarebetreiber wird in der Regel eine Markterkundung und eine Ausschreibung durchführen, um eine Software und ggf. den Support für die Software vergabekonform zu beziehen. Der Softwarebetreiber stellt den Service im MDD bereit und hält die Vertragsbeziehungen zu den Cloud-Service-Kunden. Details zur Herstellung DVC-konformer Software und zu den Möglichkeiten Software über einen Softwarebetreiber in der DVC als Cloud-Service anzubieten werden im Leitfaden Softwarelieferant.[32]
- **Cloud-Service-Lieferanten** können Vertragsbeziehungen zu einem oder mehreren Cloud-Service-Anbietern aufbauen. Diese Cloud-Service-Anbieter (Softwarebetreiber oder Plattformbetreiber) können dann die Cloud-Services der Cloud-Service-Lieferanten in ihrer Funktion als Cloud-Integrator für die Kunden der Deutschen Verwaltungscloud DVC-konform nutzbar machen. Der Cloud-Service-Anbieter wird in der Regel eine Markterkundung und eine Ausschreibung durchführen, um die externen Cloud-Services und ggf. den Support für die externen Cloud-Services vergabekonform zu beziehen. Der Cloud-Service-Anbieter stellt den Service im MDD bereit und hält die Vertragsbeziehungen zu den Cloud-Service-Kunden.

In der DVC als Multi-Cloud können so vollständig neue IaaS/PaaS Betriebsplattformen auf Basis der Cloud-Services von externen Cloud-Service-Lieferanten aufgebaut werden, um diese dann den Softwarebetreibern der DVC für den Betrieb ihrer Services zur Verfügung zu stellen.

[32] Leitfaden Softwarelieferant | Dokumentation zur Deutschen Verwaltungscloud (DVC): Link

4 Technische Architektur der Deutschen Verwaltungscloud

Zur Stärkung der Digitalen Souveränität der Öffentlichen Verwaltung benennt die Deutsche Verwaltungscloud-Strategie vier eigene strategische Ziele:

- Reduktion von Abhängigkeiten,
- Steigerung der Effizienz und Effektivität in Entwicklung, Inbetriebnahme und Betrieb,
- Sicherstellung und Stärkung von Datenschutz und Informationssicherheit,
- Optimierung von Datenaustausch, -speicherung und -nutzung zwischen Bund, Ländern und Kommunen.[33]

Sie charakterisieren den durch die Umsetzung der Deutschen Verwaltungscloud zu erreichenden Zielzustand:

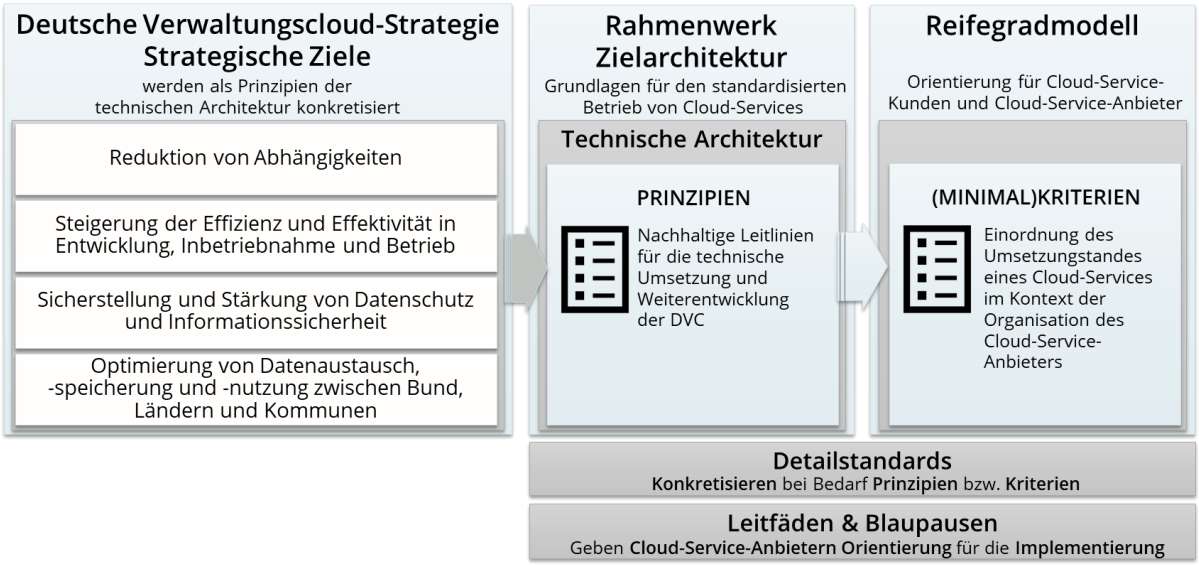

Abbildung 7: Säulen der DVC-Architektur

Diese Ziele werden in diesem Kapitel durch Prinzipien operationalisiert und konkretisiert. Sie dienen als nachhaltige Leitlinien für die Gestaltung der technischen Architektur und der Umsetzung der DVC sowie der in der DVC angebotenen Cloud-Services. Der Anwendungsbereich der Prinzipien der Technischen Architektur umfasst das DVC-Ökosystem sowie die angebundenen Cloud-Services der autorisierten Cloud-Service-Anbieter.

[33] Deutsche Verwaltungscloud-Strategie: Föderaler Ansatz, in: IT-Planungsrat, 17.11.2020, Link zur Strategie, S. 7.

Die im Rahmenwerk formulierten Prinzipien der Technischen Architektur sollen an den aktuellen Stand der Technik[34] angepasst werden, können also mit jeder Fortschreibung des Rahmenwerks verändert werden. Die Entscheidung, wann, wie und mit welchem Verbindlichkeitsgrad die Prinzipien der Technischen Architektur im Reifegradmodell der DVC oder in den Detailstandards verankert werden, wird im Rahmen der Governance der DVC-Architektur getroffen.
Das Reifegradmodell setzt die Prinzipien der Technischen Architektur in konkrete prüfbare Kriterien um. Bei Änderungen des Reifegradmodells sind die Auswirkungen auf die Detailstandards zu prüfen.

Leitfäden und Blaupausen bieten potenziellen Cloud-Anbietern Orientierung, indem sie als Leitfaden für verschiedene Rollen dienen und auf zu implementierende Spezifikationen oder beispielhafte Referenzimplementierungen verweisen.
In der Summe stellen alle vorgenannten Stufen eine Standardisierungsgrundlage für die technische Umsetzung der DVC dar.

[34] „Stand der Technik" umsetzen, in: Bundesamt für Sicherheit in der Informationstechnik, Link.

4.1 Reduktion von Abhängigkeiten

Die Öffentliche Verwaltung muss im Bereich der Informations- und Kommunikationstechnologien selbstständig, selbstbestimmt und unabhängig von einzelnen Herstellern agieren können. Dies wird durch die Umsetzung der folgenden Prinzipien der Technischen Architektur erreicht:

ID	Prinzip	Inhalt
RA-01	Unterstützung von Betreiberwechsel	Jeder Cloud-Service-Anbieter stellt dem Cloud-Service-Kunden geeignete Möglichkeiten für einen Betreiberwechsel innerhalb der Deutschen Verwaltungscloud zur Verfügung. Gespeicherte Daten sowie auch Konfigurationen sind exportierbar und werden dem Cloud-Service-Kunden so bereitgestellt, dass ein Import oder eine Wiederherstellung bei einem anderen Cloud-Service-Anbieter umsetzbar ist.
RA-02	Entkopplung von Hard- und Software	Die angebotenen Cloud-Services stellen definierte Anforderungen an die Leistungsfähigkeit der Hardware und sind auf jede Hardware-Plattform, die diese Anforderungen erfüllt, portierbar. Die Schnittstellen sind sowohl auf der Hardware- als auch auf der Software-Seite offen und klar definiert. Die eingesetzten Technologien sind offen spezifiziert, versioniert und werden durch ein tragfähiges Ökosystem oder eine aktive Community gepflegt. Die Schnittstellen liegen als offene, versionierte Verträge vor. Werden Container- und Orchestrierungstechnologien eingesetzt, sind diese konformitätsgeprüft; für Kubernetes-Distributionen ist ein anerkannter Konformitätsnachweis (CNCF-Conformance) zu erbringen. Auch die Identitäten der Workloads sind zwischen Plattformen portierbar zu gestalten.
RA-03	Uneingeschränkte Konformität mit deutschem Recht	Die Verträge für Bezug und Nutzung von Cloud-Services unterliegen deutschem Recht und stehen nicht unter dem Einfluss widersprechender Rechtsnormen.
RA-04	Verbindlicher Leistungsort	Die Speicherung und sonstige Verarbeitung von Daten der Cloud-Service-Kunden (einschließlich Metadaten) erfolgen ausschließlich im Gebiet des EWR und der Schweiz.

ID	Prinzip	Inhalt
RA-05	Präferenz für Open-Source-Software (OSS)	Bei der Realisierung von Cloud-Services wird der Einsatz von Open-Source-Komponenten auf der Applikationsebene sowie bei wesentlichen Infrastrukturkomponenten (Datenbanken, Betriebssysteme, Plattformen etc.) präferiert. Dies gilt insbesondere für Neuentwicklungen im Kontext der DVC. Der Code der Open-Source-Komponenten ist im openCode-Repository hinterlegt. Der Quellcode (oder die Quellcodes) aus der Realisierung digitaler Angebote der Verwaltung (Eigenentwicklung) wird als Open Source[35] zur Verfügung gestellt, das heißt in nachnutzbarer Form und unter einer Veränderungen gestattenden Lizenzierung. Für die Veröffentlichung auf openCode gelten die dort etablierten Qualitäts- und Sicherheitsmechanismen, insbesondere signierte Commits, geschützte Hauptzweige, verpflichtende Code-Reviews und die automatisierte Suche nach versehentlich veröffentlichten Geheimnissen. Bei der Auswahl von Open-Source-Komponenten wird zusätzlich die Qualität und Wartbarkeit des Upstream-Projekts bewertet; hierfür können etablierte Bewertungsverfahren und das Badge-Programm von openCode herangezogen werden. Quelloffenheit allein ersetzt keinen Nachweis über Lieferkette und Wartbarkeit.

Tabelle 1: Reduktion von Abhängigkeiten

[35] Open Source Initiative, Link.

4.2 Steigerung der Effizienz und Effektivität in Entwicklung, Inbetriebnahme und Betrieb

Im strategischen Ziel „Steigerung der Effizienz und Effektivität in Entwicklung, Inbetriebnahme und Betrieb" ist Automatisierung ein Schlüsselprinzip, um Effizienz und Skalierbarkeit zu erreichen. Durch Automatisierung können repetitive Aufgaben reduziert werden, was zu einer verbesserten Produktivität und zu geringeren Fehlerraten führt.

4.2.1 Entwicklung und Inbetriebnahme

Eine vollständige Automatisierung der Entwicklungs- und Inbetriebnahmeprozesse ist anzustreben (dies gilt für IaaS-, PaaS-, SaaS-Komponenten). Dadurch wird in der Regel die Qualität der Software und damit auch die Qualität der Inbetriebnahme deutlich erhöht. Zusätzlich reduziert sich der Zeit- und Aufwandsbedarf für wiederkehrende Aufgaben. Dies wird durch die Umsetzung der folgenden Prinzipien der Technischen Architektur erreicht:

ID	Prinzip	Inhalt
SE-01	Automatisierung in Entwicklung und Inbetriebnahme	In der Entwicklung ist ein CI/CD-Prozess etabliert, der die Software vollautomatisch baut und testet. Konfigurationen werden als Code hinterlegt. Anwendungscode, Infrastrukturdefinitionen und Sicherheitspatches werden ausschließlich über diesen einen Bereitstellungspfad – Versionsverwaltung, automatisierter Bau und Test, automatisierte Bereitstellung – in die Zielumgebungen überführt. Manuelle Änderungen an produktiven Umgebungen unter Umgehung dieses Pfades sind ausgeschlossen. In den Bereitstellungspfad sind Sicherheitsprüfungen fest eingebunden, mindestens die statische Analyse des Quellcodes, die Prüfung der eingebundenen Abhängigkeiten sowie die Prüfung von Container-Images und Infrastrukturdefinitionen. Bei kritischen Funden wird die Bereitstellung automatisiert unterbrochen. Die Build-Pipeline ist bei Open-Source-Software auf der Plattform openCode konfiguriert. Anwendungscode, der unter einer Closed-Source-Lizenz verwendet wird, bzw. Konfigurationen für den lokalen Betrieb werden in lokalen Versionsverwaltungssystemen vorgehalten.

ID	Prinzip	Inhalt
SE-02	Sicherstellung der Transparenz und Reproduzierbarkeit von Software	Für Open-Source-Anwendungen sind der Quellcode der Cloud-Services, die Stücklisten (SBOM) und die Bauanleitungen öffentlich zugänglich auf der Plattform openCode hinterlegt. Für alle nicht quelloffenen Anwendungen sind die Stückliste (SBOM) und die Bauanleitung in einem eigenen Versionsverwaltungssystem hinterlegt. Für die betrieblichen Konfigurationen der Cloud-Services werden eigene Repositories vorgehalten. Die Stückliste wird automatisiert im Bauprozess erzeugt, umfasst auch transitive Abhängigkeiten und liegt in einem etablierten, maschinenlesbaren Format gemäß den einschlägigen Technischen Richtlinien des BSI vor (SPDX oder CycloneDX, vgl. BSI TR-03183-2). Abhängigkeiten und Basis-Images werden eindeutig referenziert (Festlegung über kryptografische Prüfsummen statt über veränderliche Versionskennzeichen). Bau-Ergebnisse werden signiert und mit einem nachprüfbaren Herkunftsnachweis (Provenance) versehen.
SE-03	Automatische Provisionierung	Automatisierte Provisionierungsprozesse sind zu bevorzugen, da auf diese Weise der Aufwand für wiederkehrende Aufgaben reduziert werden kann.

Tabelle 2: Entwicklung und Inbetriebnahme

4.2.2 Betrieb

Es wird ein verteilter Betrieb der Cloud-Services der DVC in Rechenzentren von Bund, Ländern und Kommunen angestrebt. Dies gilt insbesondere auch für die daraus entstehende Wechselfähigkeit der Cloud-Services.

Zusätzlich bietet der verteilte Betrieb eine höhere Resilienz im Schadensfall. Dabei ist eine möglichst vollständige Automatisierung der Betriebs- und Bereitstellungsprozesse anzustreben. Dies wird durch die Umsetzung der folgenden Prinzipien der Technischen Architektur erreicht:

ID	Prinzip	Inhalt
SE-04	Automatisierung der Betriebsprozesse	Der Betrieb präferiert automatisierte Betriebsprozesse. Dies gilt insbesondere für wiederkehrende Bereitstellungsprozesse im Betrieb (Continuous Deployment), Datensicherung und Wiederherstellung, Logging, Monitoring, Alarmierung, Netzwerkkonfiguration und Zertifikatsmanagement. Der Soll-Zustand der Zielumgebungen wird versioniert in einem Repository geführt. Änderungen erfolgen ausschließlich über nachvollziehbare, geprüfte Änderungsanträge und werden durch einen Abgleichsmechanismus automatisiert angewendet, der Abweichungen vom Soll-Zustand erkennt und zurücksetzt (GitOps). Dieses Vorgehen stellt neben der Automatisierung die Auditierbarkeit und die Rücksetzbarkeit von Änderungen sicher. Ergänzender Hinweis: Als Härtungsmaßstab für Kubernetes-Umgebungen ist der Baustein APP.4.4 des IT-Grundschutz-Kompendiums heranzuziehen; die Einhaltung ist automatisiert prüfbar.
SE-05	Bereitstellung notwendiger Dokumentationen	Alle betrieblichen Akteure stellen die für den Betrieb der bereitgestellten Cloud-Services im Kontext der jeweiligen Umgebungen notwendigen Dokumentationen zur Verfügung (z. B. Benutzerhandbücher für Kunden, Betriebshandbücher sowie Systemdokumentationen für IT-Dienstleister).

ID	Prinzip	Inhalt
SE-06	Unterstützung eines verteilten IT-Betriebs in der DVC	Alle technischen Elemente eines Cloud-Services, die innerhalb der Deutschen Verwaltungscloud betrieben werden, können ohne größeren Aufwand den Plattformbetreiber oder die Cloud-Standorte wechseln (Interoperabilität). Die Cloud-Service-Anbieter unterstützen gemäß dem Stand der Technik gängige Virtualisierungs- und Orchestrierungstechniken[36] und arbeiten auf einen hohen Automatisierungsgrad in ihren Organisationen und Abläufen hin. Die zukünftige Verwendung von IPv6 stellt einen ausreichend großen Adressraum sicher.
SE-06a	Gesicherte Netzanbindung der Cloud-Standorte	Die Cloud-Standorte der DVC werden über das gemeinsame Verbindungsnetz der Öffentlichen Verwaltung (NV-DE) angebunden. Der Datenverkehr zwischen Cloud-Standorten sowie zwischen Cloud-Standorten und Cloud-Service-Kunden der Öffentlichen Verwaltung erfolgt nicht über das öffentliche Internet. Übergänge zwischen Cloud-Standorten, Netzen und externen Anbietern werden als kontrollierte Übergabepunkte ausgestaltet, an denen Zugriffsrichtlinien durchgesetzt werden; erforderliche Internet-Übergänge sind definiert, abgesichert und dokumentiert.
SE-07	Mandantentrennung	Die Daten und Ressourcen der Mandanten sind nach aktuellem Stand der Technik sicher getrennt. Die Tiefe der Trennung richtet sich nach dem Schutzbedarf und ist je Serviceklasse definiert – von der logischen Trennung innerhalb einer gemeinsam genutzten Umgebung über dedizierte Cluster bis hin zu dedizierter Hardware. Die Trennung umfasst die Netz-, Speicher- und Schlüsselebene und wird technisch durchgesetzt und nachgewiesen.
SE-08	Ausfallsicherheit durch Redundanz	Cloud-Standorte können die Funktion eines Ausweichrechenzentrums für den Betrieb von Cloud-Services mit besonderen Anforderungen (beispielsweise mit dem Ziel der Georedundanz) übernehmen.

Tabelle 3: Betrieb

[36] Für den verteilten IT-Betrieb von Cloud-Services fokussiert die DVC eine containerbasierte Software- und Verfahrensentwicklung, die betriebsseitig auf Kubernetes-Orchestrierungstechnik lauffähig ist.

4.2.3 Angebot von Cloud-Services

Die angebotenen Cloud-Services innerhalb der DVC sollen für Organisationen der Öffentlichen Verwaltung aus Bund, Ländern und Kommunen nutzbar sein. Entstehende Erweiterungen und Anpassungen eines Services bei einem Teilnehmenden der DVC sollen grundsätzlich an anderen Cloud-Standorten nachgenutzt werden können. Dies wird durch die Umsetzung der folgenden Prinzipien der Technischen Architektur erreicht:

ID	Prinzip	Inhalt
SE-09	Angebot von Cloud-Services als Self-Service-Angebot	Über den Marktplatz Deutschland Digital ist ein Self-Service-Angebot für die Öffentliche Verwaltung eingerichtet, über das sich Cloud-Services unterschiedlicher Cloud-Service-Anbieter in verschiedenen Servicemodellen (z. B. IaaS, PaaS, SaaS) auswählen und konfigurieren lassen (z. B. bestellen, erweitern, kündigen). Für jeden Cloud-Service ist der Leistungsumfang dokumentiert (technische und Benutzerdokumentation) und sind Service Level Agreements (SLA) definiert. Die geteilte Verantwortung zwischen Cloud-Service-Anbietern und Cloud-Service-Kunden ist klar dokumentiert.
SE-10	Bereitstellung von Cloud-Services	Rechtskräftig bestellte Cloud-Services werden innerhalb definierter Zeiträume möglichst automatisiert bereitgestellt.
SE-11	Digitale Barrierefreiheit	Für alle berechtigten Endanwender von Cloud-Services sind Cloud-Services zugänglich und nutzbar gestaltet, unabhängig von deren Fähigkeiten oder Einschränkungen. Die Umsetzung orientiert sich an der europäischen Norm EN 301 549 in ihrer jeweils gültigen Fassung sowie an den einschlägigen rechtlichen Vorgaben zur digitalen Barrierefreiheit, insbesondere BITV 2.0. Dies umfasst insbesondere die barrierefreie Gestaltung von Nutzeroberflächen (z. B. Marktplatz Deutschland Digital, Administrationsoberflächen), von Benutzer- und Systemdokumentationen sowie von bereitgestellten elektronischen Dokumenten (z. B. PDF/UA-Konformität). Cloud-Service-Anbieter weisen den Umsetzungsstand der digitalen Barrierefreiheit transparent aus, etwa durch eine Erklärung zur Barrierefreiheit vergleichbar den Vorgaben nach BITV 2.0.

ID	Prinzip	Inhalt
SE-12	Elastische und skalierbare Cloud-Services	Es ist ein konstantes Antwortzeitverhalten des Cloud-Service bei unterschiedlichem Lastaufkommen sichergestellt. Voraussetzung hierfür ist eine einfache, kurzfristige und automatisierbare Anpassungsmöglichkeit der Ressourcen bei veränderten Bedarfen (z. B. saisonale Schwankungen oder neue Vorhaben). Den Cloud-Service-Kunden wird über ein professionelles Verfügbarkeitsmonitoring kontinuierlich Einblick gegeben, sodass unmittelbar eine Störung des konstanten Antwortzeitverhaltens festgestellt und nachgesteuert werden kann.
SE-13	Bereitstellung neuester Programmstände	Durch regelmäßige Updates werden Cloud-Services auf dem neuesten Stand gehalten, um von den neuesten Funktionen, Sicherheitsverbesserungen und Fehlerbehebungen zu profitieren. Updates werden im Voraus angekündigt und beeinträchtigen den laufenden Betrieb möglichst nicht. Falls in Einzelfällen ein Update nicht on the fly möglich ist, ist dies im SLA mit Rahmenbedingungen für Downtimes (Zeitfenster, Dauer, ggf. gestuft nach Kritikalität der Updates) definiert. Sicherheitsrelevante Aktualisierungen werden von funktionalen Versionswechseln unterschieden. Sie werden risikobasiert priorisiert – insbesondere anhand des Schweregrads, der Exponiertheit des betroffenen Systems und der Kenntnis über eine aktive Ausnutzung – und innerhalb definierter Fristen bereitgestellt, die im Service Level Agreement beziehungsweise im Reifegradmodell verbindlich festgelegt sind. Auch beschleunigte Bereitstellungen durchlaufen den regulären Bereitstellungspfad; ein Umgehen der Prüfschritte ist nicht zulässig.
SE-14	Verbindliche Servicezeiten des Supports	Im Service Level Agreement sind Zeitfenster definiert, innerhalb derer der Cloud-Service-Kunde Anspruch auf Störungs- bzw. Mangelbehebung durch den Cloud-Service-Anbieter hat.
SE-15	Angemessener Umgang mit Störungen, Vereinbarung von Reaktions- und Entstörungszeiten	Der Cloud-Service-Anbieter stellt dedizierte Kanäle für die strukturierte Meldung und Bearbeitung von Störungen zur Verfügung. Cloud-Service-Kunden können den Status ihrer Meldungen transparent verfolgen und meldungsübergreifend analysieren. Es werden Reaktions- und Entstörungszeiten zur Wiederherstellung des Services vereinbart.

ID	Prinzip	Inhalt
SE-16	Verbindliche Verfügbarkeit, Verbrauchsmonitoring & Reporting	Der Cloud-Service-Anbieter definiert verbindlich die Verfügbarkeit des Cloud-Services, d. h. den Anteil innerhalb eines Zeitraums, in dem der Cloud-Service aktiv und zugänglich ist sowie ordnungsgemäß funktioniert. Die Nutzung von Cloud-Service-Ressourcen (z. B. Rechenleistung, Datenspeicher) wird zeitnah dokumentiert und ausgewertet. Diese Information ist Grundlage für die Abrechnung der Cloud-Services.
SE-17	Erreichung von nutzungsbasierten Abrechnungsmodellen	Der Cloud-Service-Anbieter setzt Cloud-Services nach einem nutzungsbasierten Modell um. Der Cloud-Service-Anbieter ist für die ordnungsgemäße Erfassung der Nutzung (Monitoring) und deren Abrechnung verantwortlich. Dies schließt auch Reklamationsprozesse ein. Angestrebt werden ein „Pay-as-you-go"-Abrechnungsmodell sowie periodische Abrechnungen.

Tabelle 4: Angebot von Cloud-Services

4.3 Sicherstellung und Stärkung von Datenschutz und Informationssicherheit

Datenschutz und Informationssicherheit sind von entscheidender Bedeutung für den Schutz der Informationen von Einzelpersonen, Unternehmen und Organisationen. Gerade im Bereich der Öffentlichen Verwaltung werden häufig sensible Daten verarbeitet.

Auch das Vertrauen der Bürgerinnen und Bürger in die Digitalisierung der Öffentlichen Verwaltung soll gestärkt werden. Daher müssen die sichere Erhebung, Verarbeitung, Speicherung, Löschung und Übertragung von Daten gewährleistet werden.

Dies wird durch die Umsetzung der folgenden Prinzipien der Technischen Architektur erreicht:

ID	Prinzip	Inhalt
SI-01	Besondere Verpflichtung zur Informationssicherheit und zum Datenschutz[37]	Die Informationssicherheit und der Datenschutz, insbesondere im Sinne der für die Öffentliche Verwaltung geltenden Rechtsvorschriften und Normen (z. B. DSGVO, IT-Grundschutz, geltende Verwaltungsvorschriften zur Handhabung von Verschlusssachen), sind zu jedem Zeitpunkt durch angemessene technische und organisatorische Maßnahmen für jeden Cloud-Service in Entwicklung, Inbetriebnahme und Betrieb sichergestellt und dokumentiert. Die Weiterentwicklung des IT-Grundschutzes hin zu maschinenlesbaren Anforderungsprofilen und einer kontinuierlichen statt punktuellen Bewertung (IT-Grundschutz++) wird als Zielbild berücksichtigt. Die DVC strebt an, ihre Kriterien und die zugehörigen Nachweise perspektivisch maschinenlesbar bereitzustellen und automatisiert prüfbar zu machen.

[37] Einzelheiten regeln die nachgelagerten regulatorischen Dokumente der DVC, insbesondere Reifegradmodell und Detailstandards.

ID	Prinzip	Inhalt
SI-02	Zero Trust als Zielarchitektur	Die Sicherheitsarchitektur der Cloud-Services der DVC folgt dem Zero-Trust-Ansatz. Maßgeblich sind die technische Leitlinie Zero Trust des BSI sowie die Eckpunkte einer Zero-Trust-IT-Sicherheitsarchitektur des Bundes. Die Umsetzung einer Zero-Trust-Network-Access-Architektur, die der technischen Leitlinie Zero Trust des BSI entspricht, wird präferiert. Dies umfasst Maßnahmen zur Authentifizierung und Autorisierung, Signierung von Code und Konfigurationen, Verschlüsselung von Zugangscodes mit minimalen Zugangsrechten und Privilegien. Cloud-Services stellen ein flexibles Authentisierungsverfahren bereit, das die Integration mit externen Identity Providern (IdP) mittels Standard-Protokollen ermöglicht. Die Zugriffskontrolle endet nicht mit der Anmeldung. Der Cloud-Service unterstützt eine kontinuierliche und risikoadaptive Prüfung: mehrstufige Authentisierung auch im laufenden Zugriff, attributbasierte Autorisierung mit bedarfsgerechter und zeitlich befristeter Rechtevergabe, Zugriffstoken mit begrenzter Gültigkeit und Kontextbezug (z. B. Gerätezustand, Herkunft, Risikobewertung) sowie den Entzug von Zugriffsrechten bei veränderter Sicherheitslage. Die Kommunikation zwischen Diensten erfolgt gegenseitig authentisiert auf Basis eigener Dienst-Identitäten. Die Standard-Protokolle sind in das IAM der DVC eingebunden. Der Cloud-Service stellt ein Autorisierungsverfahren bereit, das sowohl die Zuweisung von Standardrollen als auch eine feingranulare Berechtigungsvergabe ermöglicht und in das IAM der DVC integriert ist. Zero Trust wird über die Dimensionen Identitäten, Endgeräte, Netze, Anwendungen und Daten ausgestaltet und folgt den Leitprinzipien ‚Assume Breach', ‚Never Trust, Always Verify', ‚Least Privilege' und ‚Continuous Monitoring'; ergänzend sind Sichtbarkeit sowie Automatisierung und Governance zu gewährleisten. Für jeden Cloud-Service ist zu benennen, wo die Zugriffsentscheidung getroffen (Policy Decision Point), wo sie durchgesetzt (Policy Enforcement Point), woher die Entscheidungsgrundlagen stammen (Policy Information Point) und wo die Richtlinien verwaltet werden (Policy Administration Point). Der Umsetzungsstand wird über einen Reifegradpfad abgebildet.

ID	Prinzip	Inhalt
SI-03	Transparenter Einsatz von KI	Für den Cloud-Service-Kunden ist jederzeit eindeutig ersichtlich, ob ein beauftragter Cloud-Service KI-Komponenten (inkl. Nennung der eingesetzten KI-Modelle) im Sinne der KI-Verordnung der EU enthält bzw. ob und unter welchen Bedingungen die Daten eines beauftragten Cloud-Services als Trainingsdaten für KI-Modelle verwendet werden könnten. Es ist sichergestellt, dass die Anforderungen der KI-Verordnung der EU erfüllt werden. Dabei sollten Entscheidungen und Verantwortlichkeit ultimativ der menschlichen Kontrolle unterliegen.
SI-04	Durchgängige Datenklassifizierung und semantische Beschreibung für Cloud-Services	Die Dokumentation der Cloud-Services unterstützt die Datenklassifizierung sowie die semantische Beschreibung der Daten und damit die Erstellung von Sicherheitskonzepten durch den Cloud-Service-Kunden. Es ist durchgängig ersichtlich, welche Sicherheitsmaßnahmen für welche Schutzstufen von Daten gemäß mindestens der drei wichtigsten Schutzziele (Vertraulichkeit, Integrität und Verfügbarkeit) über den Lebenszyklus der Daten (Transport, Speicherung, Verarbeitung) umgesetzt sind.
SI-05	Sicherheit bereits in der Design- und Entwicklungsphase	In der Entwicklung von Cloud-Services werden bewährte Sicherheitspraktiken in den Softwareentwicklungs- und -bereitstellungsprozess integriert („Security by Design"). Dazu zählt beispielsweise DevSecOps, ergänzt um Bausteine zur Sicherheit (z. B. Clean Code, Secure Coding, Penetrationstests, dynamische Sicherheitstests). Die Lieferkette der Software-Artefakte ist unter Sicherheitsaspekten verifiziert und dokumentiert. Die Sicherheitsprüfungen sind verbindlicher Bestandteil des Bereitstellungspfades und wirken bei kritischen Funden blockierend. Um das Risiko einer einzelnen fehlerhaften oder kompromittierten Prüfkomponente zu begrenzen, werden für sicherheitskritische Prüfungen mehrere unabhängige Werkzeuge eingesetzt. Die Werkzeugkette selbst ist Schutzobjekt: Bau- und Prüfumgebungen sind gehärtet und in ihrem ausgehenden Datenverkehr beschränkt, Manipulationen werden erkannt. Langlebige Zugangsdaten werden vermieden; Zugriffe erfolgen über kurzlebige, an die Bau-Identität gebundene Berechtigungen. Geheimnisse werden in einem dedizierten Verwaltungsdienst gehalten und nach Sicherheitsvorfällen unverzüglich gewechselt.

ID	Prinzip	Inhalt
SI-06	Sichere Betriebs-überführung von Software-Artefakten	Software-Artefakte werden sicher in den Betrieb überführt. Dies beinhaltet die unveränderte Übernahme und die Überprüfung der während der Entwicklung erstellten Signaturen mit den öffentlichen Schlüsseln der jeweiligen Distributoren.
SI-07	Absicherung aller Konfigurationen	Alle Konfigurationen im Betrieb sind abgesichert. Dies zielt auf die Erstellung und Wiederherstellung sowie Veränderung von Konfigurationen der Umgebungen („Stages“) aus einem versionierten Repository ab. Dazu gehören auch der Aufbau und die Änderung von Test-Umgebungen und die Durchführung von automatisierten Tests in einer betriebsnahen Konfiguration. Der Aufbau und die Änderung der Betriebsumgebung werden ebenfalls aus einem Repository konfiguriert und sind ohne Einwirkung von Betriebspersonal möglich (Zero Admin oder Zero Privileges).
SI-08	Prozessgestaltung zum schnellen Erkennen, Testen und Handeln bei Sicherheitslücken	Alle Betriebsprozesse sind darauf ausgelegt, Sicherheitslücken so schnell wie möglich durch Schwachstellenmanagement, Analyse der Monitoring-Daten, Prüfungen der Konfigurationen und eingesetzten Artefakte zu erkennen bzw. durch eigene Tests zu finden (z. B. Penetrationstests). Ziel ist es, die Lücken schneller zu schließen, als sie in Angriffen ausgenutzt werden. Dazu trägt insbesondere eine durchgängige Automatisierung bei. Grundlage des Schwachstellenmanagements ist eine aktuelle Inventur der eingesetzten Komponenten auf Basis der Software-Stücklisten. Diese wird automatisiert gegen maschinenlesbare Sicherheitsmeldungen abgeglichen (CSAF 2.0, vgl. BSI TR-03191) und durch authentifizierte Schwachstellenscans der Systeme ergänzt. Die Behebung wird risikobasiert priorisiert – anhand des Schweregrads, der Exponiertheit und der Kenntnis über eine aktive Ausnutzung – und erfolgt innerhalb verbindlich festgelegter Fristen.
SI-09	Automatisiertes Backup und Recovery	Der Cloud-Service ermöglicht eine regelmäßige und integritätsgeprüfte Sicherung und Wiederherstellung von Kundendaten. Die zugehörigen Betriebsprozesse sollen automatisiert werden. Cloud-Service-Kunden können bei Bedarf einzelne Datenpunkte oder Dateien wiederherstellen lassen. Eine kontinuierliche Überwachung und Benachrichtigung bei Backup-Fehlern, ist eingerichtet. Backup und Recovery müssen explizit für jeden Cloud-Service in der Leistungsbeschreibung geregelt sein (inkl. der Möglichkeit, dies explizit begründet auszuschließen).

ID	Prinzip	Inhalt
SI-10	Definierte Inhalts-Verschlüsselung	Kunden-Daten und deren Backups können gemäß aktuellem Stand der Technik verschlüsselt abgespeichert werden.
SI-11	Durchgängige Transport-Verschlüsselung	Der Cloud-Service bietet eine hohe Datensicherheit durch Transportverschlüsselung gemäß dem aktuellen Stand der Technik. Es ist sichergestellt, dass Daten auf der gesamten Übertragungsstrecke verschlüsselt sind, ohne dass auf dem Übertragungsweg durch Dritte Klartextdaten ausgelesen werden können.
SI-12	Dokumentationspflicht von Zugriffen und Änderungen	Im laufenden Betrieb werden die privilegierten Zugriffe und Änderungen der Cloud-Services dokumentiert. Die Auditlogs werden in einem separaten System revisionssicher gespeichert. Sicherheitsrelevante Ereignisdaten werden darüber hinaus über standardisierte Schnittstellen an die zentrale Detektions- und Reaktionsfähigkeit der Öffentlichen Verwaltung übergeben. Erkenntnisse aus der Detektion fließen als Entscheidungsgrundlage in die Zugriffsentscheidung zurück, sodass Berechtigungen bei veränderter Sicherheitslage eingeschränkt oder entzogen werden können. Ergänzender Hinweis: Für die Zeitspanne zwischen Erkennung und Durchsetzung einer Maßnahme ist ein Service Level festzulegen.
SI-13	Übernahme von neuen oder verbesserten Sicherheitstechnologien	Neue Sicherheitstechnologien, wie beispielsweise Confidential Computing (Verschlüsselung des Server-Speichers), sollten in der Weiterentwicklung der DVC berücksichtigt und übernommen werden.
SI-13a	Kryptoagilität und Schlüsselhoheit	Die eingesetzten kryptografischen Verfahren sind so gekapselt, dass sie ohne Änderung der Architektur ausgetauscht werden können (Kryptoagilität). Dies gilt für die Transport- ebenso wie für die Ruhedatenverschlüsselung. Die Migration zu post-quantensicheren Verfahren ist vorzusehen und in der Planung des Cloud-Service-Anbieters zu dokumentieren. Der Cloud-Service-Anbieter beschreibt den eingesetzten Schlüsselverwaltungsdienst sowie die dem Cloud-Service-Kunden angebotenen Möglichkeiten der Schlüsselhoheit – insbesondere die Nutzung kundeneigener Schlüssel und die Verwahrung von Schlüsselmaterial außerhalb des Cloud-Services.

ID	Prinzip	Inhalt
SI-14	Bewertung von IT-Sicherheit und Datenschutz durch Audits und Tests	Cloud-Service-Anbieter veranlassen regelmäßige Auditierungen und Prüfungen des erreichten Datenschutz- und IT-Sicherheitsniveaus ihrer Organisation und der angebotenen Cloud-Services, um Schwachstellen und Verbesserungspotenziale zu erkennen.

Tabelle 5: Sicherstellung und Stärkung von Datenschutz und Informationssicherheit

4.4 Optimierung von Datenaustausch, -speicherung und -nutzung zwischen Bund, Ländern und Kommunen

Die Optimierung von Datenaustausch, -speicherung und -nutzung ist ein zentraler Aspekt für die Öffentliche Verwaltung, um effizienter arbeiten und wertvolle Ressourcen sparen zu können. Die Automatisierung von Datenaustauschprozessen spielt dabei eine wichtige Rolle. Standardisierte Application Programming Interfaces (APIs) ermöglichen die nahtlose Kommunikation zwischen unterschiedlichen Systemen. Dies wird durch die Umsetzung der folgenden Prinzipien der Technischen Architektur erreicht:

ID	Prinzip	Inhalt
DA-01	Durchgängige Interoperabilität durch definierte Schnittstellen	Die Cloud-Services sind, sofern möglich, interoperabel zu konzipieren, d. h., sie ermöglichen einen standardisierten Datenaustausch über definierte Schnittstellenvereinbarungen.[38] Werden Schnittstellenvereinbarungen durch die anzubindenden Systeme des Cloud-Service-Kunden nicht unterstützt, so liegt es im Verantwortungsbereich des Cloud-Service-Kunden, diese zu ertüchtigen.
DA-02	Steuerung der Datenströme	Die Steuerung der durch die Nutzung von Cloud-Services entstehenden Datenströme (Routing, Zugriffskontrolle, Authentifizierung und Autorisierung, Limitierung von Datenmengen, Versionierung, Gruppierung in Namensräume) erfolgt präferiert über API-Gateways. Dabei ist zu berücksichtigen, dass es eine fachliche und eine technische Steuerung von Datenströmen gibt. Die DVC fokussiert hier auf die technische Steuerung von Datenströmen.[39] Hier soll eine strikte Trennung von Nutzdaten (kundenspezifischen Inhaltsdaten eines Services), Transaktionsdaten (z. B. Abrechnungsdaten und Metadaten) und servicespezifischen Konfigurationsdaten eines Services erfolgen.

[38] Dies gilt insbesondere für Verfahren, für die die föderalen IT-Standards des „Föderalen Standardisierungsboards“ gelten.
[39] Regelungen der Registermodernisierung bleiben davon unberührt.

ID	Prinzip	Inhalt
DA-03	Datenübertragung im REST-Architekturstil	Die Datenübertragung wird präferiert im REST-Architekturstil realisiert (Zustandslosigkeit, HTTP-Caching, Einheitlichkeit der Schnittstellen, Adressierbarkeit von Ressourcen, Repräsentation zur Veränderung von Ressourcen, selbstbeschreibende Nachrichten).

Tabelle 6: Optimierung von Datenaustausch, -speicherung und -nutzung

5 Reifegradmodell der Deutschen Verwaltungscloud

Mit der Deutschen Verwaltungscloud wurden verbindliche Mindestanforderungen für alle teilnehmenden Cloud-Service-Anbieter eingeführt, die in einem Reifegradmodell abgebildet sind. Durch die Anwendung des Reifegradmodells[40] wird sichergestellt, dass die eingereichten Cloud-Service-Kandidaten den Minimalkriterien der DVC entsprechen, sodass sie über den Marktplatz Deutschland Digital als Cloud-Services angeboten werden können.[41]

Darüber hinaus geben die durch die Anwendung des Reifegradmodells erhobenen Informationen dem Cloud-Service-Kunden die Möglichkeit, die angebotenen Cloud-Services zu vergleichen und zu bewerten, ob ein bestimmter Cloud-Service für den geplanten Einsatzzweck geeignet ist. Die Entscheidung, ob für bestimmte Einsatzzwecke (z. B. im Sicherheitsbereich) bei einzelnen Kriterien höhere Stufen als Mindestanforderung angesetzt werden sollen beziehungsweise müssen, obliegt dabei ausschließlich dem jeweiligen Cloud-Service-Kunden.
Das Reifegradmodell wird den Cloud-Service-Anbietern in seiner jeweils aktuellen Version durch die DVC zur Verfügung gestellt. Die von den Cloud-Service-Anbietern bereitgestellten Informationen zum erreichten Reifegrad eines Cloud-Services werden im Marktplatz Deutschland Digital veröffentlicht.

Das Reifegradmodell gibt Kunden und Anbietern eine Orientierung zum Stand der Umsetzung des jeweiligen Cloud-Services im Kontext der Organisation des Cloud-Service-Anbieters.

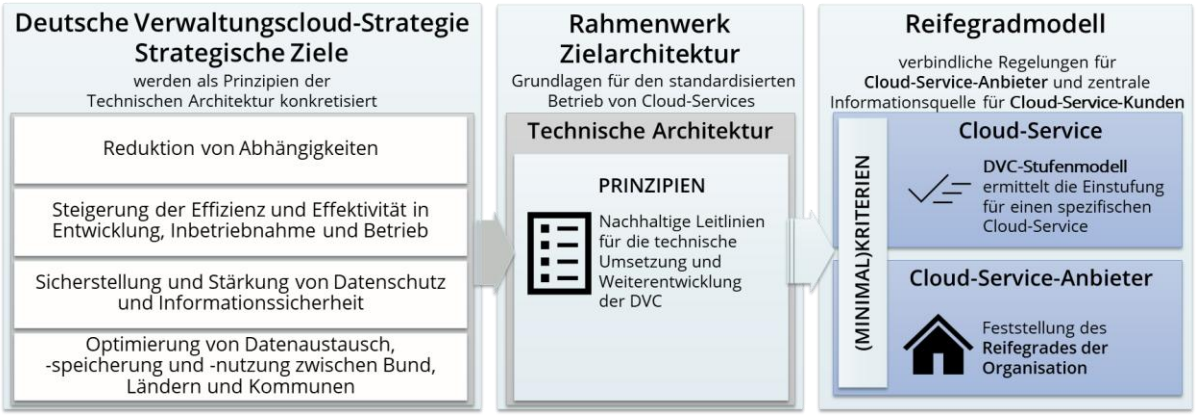

Abbildung 8: Kontext des Reifegradmodells

[40] Es gilt die jeweils gültige Fassung, Link.
[41] Werden diese Minimalkriterien nicht erfüllt, kann der Cloud-Service nicht angeboten werden.

Das Reifegradmodell setzt die Prinzipien der Technischen Architektur in konkrete prüfbare Kriterien um. Dabei werden die Eigenschaften spezifischer Cloud-Services unter Anwendung des DVC-Stufenmodells eingeordnet sowie das Informationssicherheitsniveau der Organisation des Cloud-Service-Anbieters festgestellt. Die Erhebung der Informationen erfolgt als Selbsteinschätzung des Cloud-Service-Anbieters. Diese Informationen werden anschließend plausibilisiert[42].

Die Erhebung als Selbsteinschätzung mit anschließender Plausibilisierung ist die Ausgangsstufe der Nachweisführung. Mittelfristig werden Nachweise, soweit verfügbar, maschinenlesbar erbracht und kontinuierlich statt punktuell ausgewertet – insbesondere Software-Stücklisten, der automatisierte Abgleich gegen Sicherheitsmeldungen sowie maschinenlesbare Anforderungsprofile. Die Ausgestaltung dieses Entwicklungspfades einschließlich Zeithorizont und Verantwortlichkeiten erfolgt im Rahmen des Reifegradmodells 2.0 durch das Produkt DVC gemeinsam mit dem DVC-Architekturboard.

Das DVC-Stufenmodell schafft damit eine transparente Grundlage zur Bestimmung der Qualität der angebotenen Cloud-Services und bildet in Kombination mit Kriterien zur Feststellung des Reifegrads der Organisation des Cloud-Service-Anbieters das DVC-Reifegradmodell.
Bei Bedarf konkretisieren Detailstandards die Auslegung von Prinzipien der Technischen Architektur oder der Kriterien des Reifegradmodells.
Bei der Entwicklung der Reifegradkriterien und des DVC-Stufenmodells sowie für die spätere Plausibilisierung wurden folgende Leitlinien festgelegt, die in der Handhabung der Prüfung fest verankert sind:

- **Transparenz**: Reifegrade und Kriterienstufen sind für Kunden vollständig einsehbar und nachvollziehbar.
- **Fairness**: Die Reifegradprüfung erfolgt fair, das heißt, Anbieter werden aufgrund individueller Lösungsansätze nicht benachteiligt. Die Selbsteinschätzung der Anbieter wird nach einem identischen, öffentlich zugänglichen Schema plausibilisiert.
- **Effizienz**: Eine erneute Feststellung des Reifegrads der Organisation des Cloud-Service-Anbieters ist nur dann notwendig, wenn sich beim Cloud-Service-Anbieter wesentliche

[42] Die operativen Vorgehensweisen zur Plausibilisierung werden außerhalb des Rahmenwerks im Rahmen der Prozesse zur Autorisierung von Cloud-Service-Anbietern durch das Produkt DVC detailliert.

Änderungen (z. B. betriebliche Reorganisation, neue Standorte, Veränderungen im Betriebsmodell) ergeben oder neue Informationen aufkommen, die Einfluss auf das Ergebnis der Selbsteinschätzung haben könnten (z. B. ein Sicherheitsvorfall).

- **Aktualität**: Das Stufenmodell ist modular aufgebaut und wird kontinuierlich gemäß dem aktuellen Stand der Technik sowie regulatorischen Anforderungen angepasst.

Das Reifegradmodell berücksichtigt auch in zukünftigen Versionen den zu erwartenden technologischen Wandel sowie die Anforderungen und Vorgaben von und an den öffentlichen Sektor für eine sichere Nutzung von Cloud-Services. Die festgelegten Abstufungen werden sich also zukünftig verschieben. Je nach Fähigkeiten der Organisationen können so zusätzliche Kriterien definiert werden oder auch höhere Stufen auf niedrigere Stufen reduziert werden.

Ausblick: Reifegradmodell 2.0

Das Reifegradmodell 2.0 soll auf der bestehenden Struktur aufbauen und sie um **Reifegradkriterien** erweitern, die eng mit den **DVC-Detailstandards** verknüpft sind. Dadurch sollen die Detailstandards (z. B. zu Cloud-Standorten, Netzen, Kubernetes, Deployment, IAM- und MDD-Schnittstellen, Handling von Sicherheitsvorfällen, digitaler Barrierefreiheit und Informationssicherheit) verbindlich in das Stufenmodell integriert werden.
Ziel des Reifegradmodells 2.0 ist es, die Detailstandards als zentrales Steuerungsinstrument für Qualität und Konformität im DVC-Ökosystem verbindlich zu verankern. So kann langfristig die DVC-Konformität von Cloud-Services transparent ausgewiesen und als Grundlage für verbesserte Filter- und Recherchemöglichkeiten für Cloud-Service-Kunden genutzt werden.

6 Weiterführende Informationen

6.1 Glossar

Begriff	Erläuterung
Anbieterinstanz	Eine technische Instanziierung, die der Cloud-Service-Anbieter dem Cloud-Service-Kunden bereitstellt.
Audit	Ein Audit untersucht, ob Prozesse, Anforderungen und Richtlinien die geforderten Standards erfüllen. Ein Audit-System stellt die möglichst automatisierte Durchführung von Audits sicher.
Change	Modifizieren oder Aktualisieren einer IT-Lösung.
Cloud Computing	Paradigma, einen netzwerkbasierten Zugang auf ein skalierbares und elastisches Reservoir gemeinsam nutzbarer physischer oder virtueller Ressourcen nach dem Selbstbedienungsprinzip und bedarfsgerechter Administration zu ermöglichen. Als Beispiele für Ressourcen werden "Server, Betriebssysteme, Netzwerke, Software, Anwendungen und Speichergeräte" genannt. "Selbstbedienungsprinzip" bezieht sich in diesem Kontext auf die Bereitstellung von Ressourcen für Cloud-Dienste, die von Cloud-Kunden mit Hilfe automatisierter Mittel vorgenommen werden.[43]
Cloud-Service	Ein Cloud-Service ist eine im Rahmen von Cloud Computing angebotene Dienstleistung der Informationstechnik. Ein Cloud-Service ist ein netzwerkbasierter Dienst in den Servicemodellen Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) oder Software-as-a-Service (SaaS).
Cloud-Service-Abonnement	Fortlaufende vertragliche Vereinbarung über den Bezug und die Nutzung eines Cloud-Services für einen bestimmten Zeitraum. Ein Cloud-Service-Abonnement kann sich auf Cloud-Services der Servicemodelle Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) oder Software-as-a-Service (SaaS) beziehen.
Cloud-Service-Anbieter	Cloud-Service-Anbieter bieten als Plattformbetreiber und/oder Softwarebetreiber Cloud-Services über den Marktplatz Deutschland Digital an und verantworten die Leistungserbringung.
Cloud-Service-Beschaffer	Cloud-Service-Beschaffer sind Cloud-Service-Kunden, die Cloud-Services über den Marktplatz Deutschland Digital beziehen, um diese ihrerseits durch ihre Kunden (Kunden des Cloud-Service-Beschaffers) nutzen zu lassen.
Cloud-Service-Instanz	Eine – in einem oder mehreren Cloud-Standorten – betriebene Instanz eines gebuchten Cloud-Service-Offerings.

[43] Cloud Computing Grundlagen, in: Bundesamt für Sicherheit in der Informationstechnik, Link.

Begriff	Erläuterung
Cloud-Service-Kunde	Cloud-Service-Kunden beziehen Cloud-Services eines Cloud-Service-Anbieters über den Marktplatz Deutschland Digital.
Cloud-Service-Lieferant	Cloud-Service-Lieferanten stellen Leistungen als Unterauftragnehmer eines Plattformbetreibers oder Softwarebetreibers bereit. Plattform- bzw. Softwarebetreiber können Leistungen von Cloud-Service-Lieferanten beziehen, diese DVC-konform ausgestalten und als Teil ihres Cloud-Service-Portfolios anbieten. Cloud-Service-Lieferanten können sowohl Akteure der Öffentlichen Verwaltung als auch verwaltungsexterne Anbieter sein.
Cloud-Service-Offering, auch: Cloud-Service-Angebot	Repräsentanz des Cloud-Services im Marktplatz Deutschland Digital im Sinne einer Leistungs- bzw. Produktbeschreibung des Cloud-Services.
Cloud-Service-Portal (CSP)	Historisches Bestellportal der DVC. Das Cloud-Service-Portal wurde mit Beschluss 2025/08 des IT-Planungsrats in den Marktplatz Deutschland Digital überführt. Bestellung, Kündigung und Information zu Cloud-Services erfolgen über den MDD.
Cloud-Standort	Bei einem Cloud-Standort handelt es sich um einen (physikalischen/virtuellen) Rechenzentrumsstandort, der für das Hosting von Angeboten aus den Bereichen IaaS, PaaS und/oder SaaS und von einem Cloud-Service-Anbieter als Plattform für seine anzubietenden Services genutzt werden kann.
Cluster-as-a-Service	DVC-spezifischer Kubernetes-basierter Plattformservice, bei dem einem Softwarebetreiber eine dedizierte oder entsprechend isolierte Kubernetes-Cluster-Umgebung als standardisierte Betriebsumgebung bereitgestellt wird. Umfang und Verantwortungsgrenzen zwischen Plattform- und Softwarebetreiber werden im jeweiligen Service- und Shared-Responsibility-Modell festgelegt.
Code Repository	Zentrale Verwaltungsumgebung in der Softwareentwicklung zur Versionierung von Quellcode, inklusive Dokumentationsfunktion.
Compliance	Compliance bezeichnet die Gewährleistung von regelkonformem Handeln in Bezug auf die Einhaltung von Gesetzen und Richtlinien.
Containerisierung	Verpacken von Softwarecode in Pakete, die alle erforderlichen Komponenten, wie Libraries, Frameworks und andere Abhängigkeiten enthalten und in ihrem eigenen Container isoliert sind.

Begriff	Erläuterung
Containerumgebung	Technische Plattform zum Betrieb und zur Verwaltung von Kubernetes-Clustern (Beispiele entsprechender Technologien sind OpenShift und Rancher). Die in diesem Kontext betrachteten Containerumgebungen basieren auf dem Kubernetes-Standard.
Continuous Deployment	Ansatz in der Softwareentwicklung, bei dem Änderungen an der Software automatisiert und nach festen Kriterien in die aktuelle Software bzw. in die Produktion überführt werden. Auf diese Weise wird eine kontinuierliche Auslieferung der Software ermöglicht.
Continuous Integration	Ansatz in der Softwareentwicklung, bei dem neue Programmteile sofort getestet und zusammengeführt werden, anstatt dies beispielsweise nur einmal täglich zu tun.
CS-AGB	Allgemeine Geschäftsbedingungen für Cloud-Services im Marktplatz Deutschland Digital.
Digitale Barrierefreiheit	Digitale Barrierefreiheit bezeichnet die Eigenschaft von IT-Angeboten, für Menschen (mit Behinderungen) in der allgemein üblichen Weise, ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe auffindbar, zugänglich und nutzbar zu sein. Für die öffentliche Verwaltung wird dies insbesondere durch die BITV 2.0 konkretisiert.
Digitale Souveränität	Die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(-n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können (Definition gemäß ÖFIT).
Direktvertragsmodell	Im Direktvertragsmodell besteht pro Cloud-Service-Abonnement ein Vertrag zwischen dem Cloud-Service-Anbieter eines Cloud-Services und dem Cloud-Service-Kunden eines Cloud-Services.
DVC-Berater	Der DVC-Berater berät den Cloud-Service-Kunden zu den technisch-fachlichen Möglichkeiten der DVC-Nutzung.
DVC-Produktteam/-board	Das Produktteam der Deutschen Verwaltungscloud wird von der Föderalen IT-Kooperation geleitet. Die FITKO verantwortet im Auftrag des IT-Planungsrats das strategische Produktmanagement, die technische Umsetzung und die Koordination der beteiligten Partner.

Begriff	Erläuterung
Hyperscaler	Ein Hyperscaler ist ein Anbieter von Cloud-Infrastruktur, der eine hochgradig skalierbare und automatisierte IT-Infrastruktur bereitstellt. Diese ermöglicht es, große Datenmengen effizient zu verarbeiten und flexibel Rechenressourcen je nach Bedarf zu nutzen. Ein Hyperscaler zeichnet sich durch globale Netzwerke, große Rechenzentren und die Fähigkeit aus, sehr große Workloads zu bewältigen.
Identity and Access Management (IAM)	Identity and Access Management ist ein System, das in Organisationen verwendet wird, um die Identitäten von Benutzern zu verwalten und ihren Zugriff auf verschiedene Ressourcen zu steuern. Es umfasst Prozesse und Technologien, die sicherstellen, dass nur autorisierte Benutzer auf bestimmte Daten, Anwendungen und Systeme zugreifen können.
Identity Provider (IdP)	Ein Identity Provider ist ein Dienst, der digitale Identitäten verwaltet und die Authentifizierung von Benutzern übernimmt. Der Identity Provider speichert die Identitätsinformationen der Benutzer und stellt sicher, dass nur autorisierte Benutzer auf bestimmte Anwendungen und Dienste zugreifen können.
Incident	Sicherheitsvorfall oder eine Betriebsstörung einer IT-Lösung.
Infrastructure-as-a-Service (IaaS)	Infrastructure-as-a-Service ist ein Cloud-Service-Modell, das bedarfsgerechte IT-Infrastrukturressourcen, wie Rechenleistung, Speicher und Netzwerkdienste, bereitstellt.
Intermediär	Vertragspartner im Umklappvertragsmodell. Pro Cloud-Service-Abonnement schließt der Intermediär jeweils einen Vertrag mit dem Cloud-Service-Anbieter und mit dem Cloud-Service-Kunden. Voraussetzung ist eine – auch mittelbare – Inhouse-Beziehung gemäß § 108 GWB. Der Intermediär erbringt den Cloud-Service nicht selbst.
IT-Dienstleister der Öffentlichen Verwaltung	IT-Dienstleister der Öffentlichen Verwaltung sind Unternehmen, Organisationen oder sonstige juristische Personen, die IT-Dienstleistungen für Institutionen, Behörden oder Regierungsorganisationen bereitstellen und dabei von der Öffentlichen Verwaltung kontrolliert werden. Dies wird entweder durch staatliche Beteiligungen oder behördliche Aufsicht gewährleistet.
Kubernetes-Cluster	Cluster in Kubernetes sind ein Rechnerverbund, der für den Betrieb von containerisierten Softwarelösungen zuständig ist.
Kunden-Service-Integrator	Kunden-Service-Integratoren unterstützen bei der Integration von über den Marktplatz Deutschland Digital bezogenen Cloud-Services in die Umgebung des Cloud-Service-Kunden.

Begriff	Erläuterung
Marktplatz Deutschland Digital (MDD)	Der Marktplatz Deutschland Digital ist der zentrale Anlaufpunkt für die einfache, transparente und rechtssichere Bereitstellung und Beschaffung digitaler Produkte für öffentliche Organisationen.
Multi-Cloud	Die Nutzung mehrerer Cloud-Services verschiedener Cloud-Service-Anbieter in einer einzigen heterogenen Architektur durch einen Cloud-Service-Kunden.
Namespace-as-a-Service	DVC-spezifischer, Kubernetes-basierter Plattformservice, bei dem einem Softwarebetreiber ein logisch abgegrenzter Namespace innerhalb einer gemeinsam betriebenen Containerorchestrierungsplattform bereitgestellt wird. Der Namespace stellt einen definierten Mandanten- und Verantwortungsbereich für Anwendungen und zugehörige Ressourcen dar. Die erforderliche Isolation insbesondere hinsichtlich Netzwerk, Storage, Secrets, Berechtigungen, Ressourcenquoten und Policies wird durch die Betriebsplattform bereitgestellt und in den zugehörigen Detailstandards konkretisiert.
Native-Cloud-Service	Native-Cloud-Services bezeichnen Anwendungen und Dienste, die speziell für den Einsatz in Cloud-Umgebungen entwickelt wurden.
Normal Changes	Normal Changes sind alle Änderungen, die keine Standard-Changes oder Notfall-Changes darstellen (Definition gemäß ITIL).
Notfall-Changes (Emergency Changes)	Notfall-Changes sind Änderungen, die sofort implementiert werden müssen, zum Beispiel um einen Major Incident zu beheben (Definition gemäß ITIL).
Open Source und Open-Source-Software (OS, OSS)	Open-Source-Software ist Software, deren Quellcode zugänglich ist und die unter einer Open-Source-Lizenz bereitgestellt wird. Diese Lizenz erlaubt nach Maßgabe ihrer jeweiligen Lizenzbedingungen insbesondere die Nutzung, freie Weitergabe sowie Veränderung der Software und die Erstellung und Weitergabe abgeleiteter Werke, ohne bestimmte Personen, Gruppen oder Anwendungsbereiche zu diskriminieren. Open Source beschreibt die eingeräumten Nutzungs- und Weiterentwicklungsrechte und ist unabhängig von der Preisgestaltung; Open-Source-Software kann daher sowohl unentgeltlich als auch entgeltlich angeboten oder als kostenpflichtiger Service betrieben werden.

Begriff	Erläuterung
OS-Plattform der Öffentlichen Verwaltung „openCode (ZenDiS)“	(Internet-)Plattform der Öffentlichen Verwaltung, die aus einem zentralen und durchsuchbaren Verzeichnis von verwaltungsrelevanten Open-Source-Projekten, einem Code Repository zur Ablage von offenen Quellcodes bzw. einer Beteiligung an Projekten sowie einem Diskussionsforum besteht. Das Code Repository ist ein Standardisierungsbereich der DVC und soll die zentrale Ablage bzw. Spiegelung sowie Wiederverwendung von Quellcodes mit deren Dokumentation ermöglichen.
Pay-as-you-go	Das „Pay-as-you-go“-Modell ist ein Bezahlverfahren, bei dem Nutzer nur für die tatsächlich in Anspruch genommenen Dienstleistungen oder Ressourcen bezahlen.
Pipeline	Eine CI/CD-Pipeline dient zur Ausführung von Automatisierungsschritten für die Bereitstellung von neuen Softwareversionen.
Platform-as-a-Service (PaaS)	Platform-as-a-Service ist ein Cloud-Service-Modell, das eine virtuelle Plattform zur Verfügung stellt, auf der Kunden Webanwendungen entwickeln, testen und bereitstellen können.
Plattformbetreiber	Plattformbetreiber sind Cloud-Service-Anbieter, die Cloud-Services im IaaS- oder PaaS-Modell bereitstellen.
Quellcode/Quelltext	Für Menschen lesbare, formale Darstellung eines Programms oder von Teilen eines Softwaresystems, die in einer Programmiersprache, Skriptsprache oder einer vergleichbaren formalen Sprache verfasst ist und typischerweise die bevorzugte Form für Änderung, Wartung und Weiterentwicklung darstellt. Quellcode wird abhängig von der verwendeten Technologie durch Build-, Übersetzungs-, Interpretations- oder Laufzeitprozesse in eine ausführbare Form beziehungsweise in ausführbares Verhalten überführt.
Serviceklasse	Zusammenfassung von gleichartigen Cloud-Services in Klassen, welche die gleichen Service-Templates zur Konfiguration verwenden.
Service-Level-Agreement (SLA)	Vereinbarung zwischen Anbieter und Kunde, die der Qualitätssicherung dient. In dieser Vereinbarung werden die genauen Leistungseigenschaften und Gütestufen (Service Levels) des Produktes bzw. der Dienstleistung festgelegt.
Service-Orchestrierung	Unter Orchestrierung versteht man die automatisierte Konfiguration, Verwaltung und Koordinierung von Computersystemen, Softwarelösungen und Services. In Verbindung mit Containerumgebungen bezeichnet Orchestrierung vor allem die Steuerung, wann Container starten und stoppen, die Gruppierung von Containern in Clustern und die Koordinierung aller Prozesse, aus denen sich eine Softwarelösung zusammensetzt.

Begriff	Erläuterung
Servicetemplate	Servicetemplate beschreibt eine Vorlage für Leistungsbeschreibungen von Cloud-Services im Rahmen des Einstellungsprozesses der Services in den Marktplatz Deutschland Digital, die sich verändern kann.
Single Sign-on (SSO)	Single Sign-on ist ein Authentifizierungsverfahren, bei dem sich ein Benutzer nur einmal anmelden muss, um auf mehrere Anwendungen und Dienste zugreifen zu können, ohne sich bei jeder einzelnen Anwendung erneut anmelden zu müssen.
Software-as-a-Service (SaaS)	Software-as-a-Service (SaaS) ist ein Cloud-Service-Modell der Softwarebereitstellung, bei dem Anwendungen als Dienstleistung zur Verfügung gestellt werden. Kunden nutzen die Software auf Abonnementbasis.
Softwarebetreiber	Softwarebetreiber sind Cloud-Service-Anbieter, die Cloud-Services im SaaS-Modell bereitstellen.
Softwarelieferant	Softwarelieferanten entwickeln Softwareanwendungen und stellen diese dem Softwarebetreiber bereit.
Softwarelösung	Eine Softwarelösung ist eine Anwendungssoftware für eine bestimmte, konkrete Aufgabenstellung, die also der Lösung eines konkreten Problems eines Auftraggebers dient.
Standard Images	In der Containerisierung sind dies vorgefertigte Container-Images, die als Basis für die Erstellung neuer Container verwendet werden. Diese Images enthalten oft ein Betriebssystem und eine grundlegende Software, die für die Ausführung von Anwendungen erforderlich sind.
Umklappvertragsmodell	Im Umklappvertragsmodell besteht pro Cloud-Service-Abonnement ein Vertragspaar: einerseits ein Vertrag zwischen dem Cloud-Service-Anbieter und einem Intermediär sowie andererseits ein Vertrag zwischen dem Intermediär und dem Cloud-Service-Kunden.

Tabelle 7: Glossar

6.2 Dokumentation der Fortschreibung

In der 33. Sitzung des IT-Planungsrats wurde die Arbeitsgruppe Cloud-Computing und Digitale Souveränität (kurz AG Cloud)[44] mit der Erarbeitung der Zielarchitektur der Deutschen Verwaltungscloud beauftragt. Seit der initialen Beauftragung wurde das Rahmenwerk der Zielarchitektur kontinuierlich fortgeschrieben. Die vorliegende Version 4.0 wurde vom Architekturboard der Deutschen Verwaltungscloud erarbeitet. Nachfolgend sind die Änderungen zwischen den Versionen aufgeführt.

6.2.1 Initiales Rahmenwerk der Zielarchitektur (Version 1.0)

Die AG Cloud hat auf Grundlage des Beschlusses 2020/54 des IT-Planungsrats die technische Konzeption und Operationalisierung an die Unterarbeitsgruppe Technik und Betrieb (kurz UAG Technik) übergeben. Im Rahmen der initialen Version wurde die erforderliche Systematik beziehungsweise der grundsätzliche Aufbau der DVC entwickelt und es wurden wesentliche Standards und die Zielarchitektur spezifiziert.
Das Rahmenwerk der Zielarchitektur wurde in der Version 1.0 in der 36. Sitzung des IT-Planungsrats beschlossen.[45]

6.2.2 Anmerkungen zur ersten Fortschreibung (Version 2.0)

Mit der ersten Fortschreibung des Rahmenwerks zur Version 2.0 wurden substanzielle Änderungen in den folgenden Punkten vorgenommen:

- **Wesentliche Standards**: Bestehende Standards wurden ergänzt (insbesondere Containerumgebung und Kubernetes-Cluster, Entwicklungsbereich) und neue Standards wurden aufgenommen (Netzanbindung, Kommunikation zwischen Cloud-Standorten, Softwarebetreiber und Cloud-Service-Portal).
- **Systematik der Deutschen Verwaltungscloud**: Die für die DVC spezifizierten Rollen wurden anhand möglicher Nutzungsszenarien weiter detailliert.
- **Weiteres Vorgehen und Operationalisierung der Deutschen Verwaltungscloud**: Dieser Abschnitt wurde gemäß der zum Zeitpunkt der Fortschreibung aktuellen Entwicklungen zur Koordinierungsstelle und zur Pilotierung der DVC umfassend aktualisiert.

Darüber hinaus wurde mit dem Start des produktiven Betriebs der OS-Plattform der Öffentlichen Verwaltung openCode ein wichtiger Baustein in der Systematik der DVC integriert.

---

44 AG Cloud Computing und Digitale Souveränität, Link.
45 Beschluss 2021/46 – Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur, in: IT-Planungsrat, 29.10.2021, Link zum Beschluss.

Das Rahmenwerk der Zielarchitektur wurde in der Version 2.0 in der 39. Sitzung des IT-Planungsrats beschlossen.[46]

6.2.3 Anmerkungen zur zweiten Fortschreibung (Version 2.5)

Die Fortschreibung des Rahmenwerks in der Version 2.5 enthielt substanzielle Änderungen in den folgenden Punkten:

- **Ergebnisübersicht des Minimum Viable Product (MVP)**: Das MVP-Projekt wurde im Februar 2023 erfolgreich abgeschlossen. Im Projekt wurde eine erste funktionsfähige Version des Cloud-Service-Portals sowie eine verteilte Identity- und Access-Management-Infrastruktur (IAM-Infrastruktur) aufgebaut. Beide Komponenten (CSP und IAM) wurden im Januar 2023 erfolgreich erprobt. Das Cloud-Service-Portal der DVC ist seitdem im Internet unter https://deutsche-verwaltungscloud.de/ erreichbar.
- **Vorstellung des DVC-Umsetzungsprojekts**
- **Motivation und Vorstellen des Reifegradmodells**: Während der Durchführung des MVP-Projekts wurde festgestellt, dass die im Rahmenwerk 2.0 festgelegten DVC-Standards für sich alleinstehend nicht ausreichend sind, um als „Leitplanken" zur Erstellung und für den Betrieb von Cloud-Services in der DVC verwendet werden zu können. Aus diesem Grund wurde das Cloud-Service-Reifegradmodell entwickelt.
- **Schärfung der Rolle des Cloud-Integrators**

Die Entscheidung, eine Version 2.5 anstatt 3.0 des Dokuments zu veröffentlichen, beruhte darauf, dass die Einführung des Reifegradmodells sowie die damit verbundene Ablösung der aktuellen DVC-Standards im Umsetzungsprojekt erprobt und optimiert werden soll.
Das Rahmenwerk der Zielarchitektur wurde in der Version 2.5 in der 42. Sitzung des IT-Planungsrats beschlossen.

6.2.4 Anmerkungen zur dritten Fortschreibung (Version 3.0)

Die Version 3.0 enthält neben der neu eingeführten Präambel und redaktionellen Anpassungen (Kapitelstruktur, Glossar) inhaltliche Fortschreibungen zu folgenden Punkten:

- **Technische Architektur:** Formulierung von Prinzipien der Technischen Architektur zur Beschreibung der Zielarchitektur. Diese dienen als nachhaltige Leitlinien für die Gestaltung,

[46] Beschluss 2022/47 – Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur, in: IT-Planungsrat, 10.11.2022, Link zum Beschluss.

technische Architektur und Umsetzung der DVC sowie der in der DVC angebotenen Cloud-Services.

- **Auslagerung der Detailstandards:** Die Detailstandards sind eine Präzisierung der Prinzipien der Technischen Architektur beziehungsweise der Reifegradkriterien, die durch das DVC-Architekturboard erstellt und weiterentwickelt werden. Sie werden außerhalb des Rahmenwerks dokumentiert.
- **Ablösung der DVC-Standards:** Die bisher im Rahmenwerk dokumentierten DVC-Standards werden nicht mehr weiterverwendet. Sie sind in den Minimalkriterien des Reifegradmodells berücksichtigt.
- **Cloud-Service-Portal-Ökosystem (CSP-Ökosystem):** Im neuen Unterkapitel werden die Zielsetzung und der grundsätzliche Aufbau des CSP-Ökosystems beschrieben. Zukünftig werden an dieser Stelle weitere Anforderungen an die Weiterentwicklung des CSP-Ökosystems aufgenommen.
- **Anpassungen Rollenmodell:** Es wurden bestehende Rollenbeschreibungen aktualisiert und neue Rollen (Intermediär, Kunden-Service-Integrator, DVC-Berater) ergänzt.
- **Reifegradmodell:** Das Reifegradmodell wurde durch das DVC-Umsetzungsprojekt operationalisiert. Die bisher im Rahmenwerk formulierten Ausführungen zum Reifegradmodell wurden aktualisiert und um die Zielsetzung, den Ansatz und die Methodik des Reifegradmodells erweitert.
- **Vertragsmodalitäten:** Im neuen Unterkapitel werden die wesentlichen Eckpunkte der DVC-Vertragsmodalitäten beschrieben.
- **Einbindung verwaltungsexterner Anbieter:** Im neuen Unterkapitel werden zukünftig Rahmenbedingungen für die Integration verwaltungsexterner Angebote detaillierter beschrieben.

6.2.5 Anmerkungen zur vierten Fortschreibung (Version 4.0)

Die Version 4.0 enthält neben redaktionellen Anpassungen (Kapitelstruktur, Abbildungen, Glossar) inhaltliche Fortschreibungen zu folgenden Punkten:

- **Präambel:** Anpassung an das aktuelle Produkt- und Architekturverständnis. Bereitstellungsort der DVC-konformen Cloud-Services ist der Marktplatz Deutschland Digital (MDD). Neu beschrieben wird die Einordnung der DVC als souveränes Cloud-Fundament des Deutschland-Stacks und als Bestandteil der Deutschland-Architektur.
- **Transformation der föderalen IT-Landschaft:** Neuer Abschnitt in der Einführung zum Übergang vom manufakturartigen IT-Betrieb zu standardisiert hergestellten, nachnutzbaren Cloud-Services und zu den Mehrwerten in Beschaffung, Herstellung, Integration und Betrieb.
- **Nahestehende Vorhaben:** Aufnahme von Deutschland-Architektur, Deutschland-Stack, Netzverbund Deutschland (NV-DE), ZenDiS/openCode, FIT-Connect, Föderaler API-Autorisierungsinfrastruktur und Zero-Trust-Transformation des Bundes.
- **Relevante Vorgaben und Richtlinien:** Schärfung der BSI-Vorgaben und der Föderalen IT-Architekturrichtlinie. Neu berücksichtigt werden die Eckpunkte einer Zero-Trust-IT-Sicherheitsarchitektur des Bundes, Grundschutz++, NIS-2, Cyber Resilience Act, einschlägige Technische Richtlinien des BSI, Souveränitätsanforderungen in der Beschaffung sowie die digitale Barrierefreiheit.
- **Digitale Souveränität für die DVC:** Neues Kapitel. EU Cloud Sovereignty Framework, C3A-Kriterienkatalog des BSI und der Verordnungsvorschlag zum Cloud and AI Development Act (CADA) dienen als Orientierungsgrundlage.
- **Produktmanagement-Modell der FITKO:** Neues Kapitel zur Steuerung des Produkts DVC über Produktboard und Produktteam sowie zur Beauftragung des Betreibers.
- **Rollenmodell:** Neue Rolle Cloud-Service-Beauftragender. Schärfung von Plattform- und Softwarebetreiber.
- **DevSecOps in der DVC und der Öffentlichen Verwaltung:** Neues Kapitel. Entwicklung, Betrieb, Informationssicherheit und Compliance werden als durchgängiges Arbeitsmodell beschrieben.
- **DVC-Ökosystem:** Neufassung des bisherigen CSP-Ökosystems. Der gemeinsame Rahmen und die Cloud-Infrastruktur-Komponenten verbleiben bei der DVC; marktplatz- und beschaffungsbezogene Funktionen liegen beim MDD. Die Aufgaben der bisherigen Koordinierungsstelle gehen auf das Produkt DVC über.

- **Einbindung verwaltungsexterner Anbieter:** Neufassung mit Fokus auf Softwarelieferant und Cloud-Service-Lieferant sowie auf DVC-Betriebsplattformen (public) und (private).
- **Prinzipien der Technischen Architektur:** Fortschreibung und Schärfung bestehender Prinzipien, insbesondere zu Lieferkette und openCode, einheitlichem Bereitstellungspfad, GitOps, Mandantentrennung, Barrierefreiheit, Zero Trust, Schwachstellenmanagement sowie Detektion und Reaktion. Neu aufgenommen wurden die gesicherte Netzanbindung der Cloud-Standorte sowie Kryptoagilität und Schlüsselhoheit.
- **Reifegradmodell:** Beschreibung des Entwicklungspfads von der Selbstauskunft zum maschinenlesbaren Nachweis. Neuer Absatz zum geplanten Reifegradmodell 2.0 mit verbindlicher Verankerung der Detailstandards.
- **Glossar:** Ergänzung unter anderem um DVC-Produktteam/-board, Marktplatz Deutschland Digital (MDD) und Namespace-as-a-Service.
- **Ausblick auf die Version 4.1:** Neues Kapitel. Es bündelt die aus der Kommentierung übernommenen Präzisierungsbedarfe und stellt klar, dass das Rahmenwerk Prinzipien und Leitplanken beschreibt, nicht den Prüfkatalog.

6.3 Ausblick auf die Version 4.1

Im Rahmen der Kommentierung des Rahmenwerks der Zielarchitektur in der Version 4.0 sind eine Vielzahl von Rückmeldungen eingegangen. Diese zielen auf eine höhere technische Konkretisierungstiefe, insbesondere auf die Verzahnung der Deutschen Verwaltungscloud mit der Deutschland-Architektur und dem Deutschland-Stack sowie auf die Prüfbarkeit der Prinzipien der Technischen Architektur. Diese Rückmeldungen sind fachlich valide. Ihre gemeinsame Befassung war im Zeitrahmen dieser Fortschreibung jedoch nicht mehr zu leisten. Die technischen Detailfragen werden daher gebündelt in das Backlog des Rahmenwerks überführt.

Für die Version 4.1 werden schwerpunktmäßig die folgenden technischen Präzisierungen erwartet:

- **Detailliertere Einordnung in die Deutschland-Architektur:** Zuordnung „DVC-Prinzip zu Funktionsbausteinen des Deutschland-Stacks zu Referenzarchitektur" einschließlich einer Regel, welches Artefakt bei abweichenden oder unterschiedlich versionierten Anforderungen führend ist.
- **Zero Trust:** Überführung der bisherigen Präferenz in ein verbindliches Zielbild mit den Architekturrollen Policy Decision Point (PDP), Policy Enforcement Point (PEP), Policy Information Point (PIP) und Policy Administration Point (PAP), kontextbasierter und kontinuierlicher Zugriffsentscheidung sowie gegenseitiger Authentisierung zwischen Diensten.
- **Sicherer Software-Lebenszyklus und Lieferkette:** Durchgängiger Bereitstellungspfad (Single Path to Production, GitOps), Software Bill of Materials (SBOM) in standardisierten Formaten, Signatur- und Provenienznachweise mit definiertem Durchsetzungspunkt vor dem Deployment sowie wirksame Prüf-Gates in der Pipeline.
- **Portabilität, Betreiberwechsel und Souveränität:** Prüfbare Mindestkriterien für den Wechsel (Exportformate und Schnittstellen, Konfigurationen, Identitäten und Schlüsselmaterial, maximale Exit-Zeit, Löschnachweise) sowie eine Präzisierung des Leistungsorts über Nutz-, Meta-, Log-, Backup- und Control-Plane-Daten hinweg.
- **Betrieb und Resilienz:** Messbare Service Level und eine standardisierte Verfügbarkeitsmessung anstelle qualitativer Zusagen, risikobasierte Patch-Fristen sowie Anforderungen an Trennungstiefe, Georedundanz und regelmäßige Wiederanlauftests.
- **Kryptografie und Schlüsselhoheit:** Verbindliche Verschlüsselungsanforderungen je Schutzbedarf, klare Abgrenzung von Transport- und Ende-zu-Ende-Verschlüsselung sowie Kryptoagilität mit Blick auf post-quantensichere Verfahren.

- **Netzanbindung und Fachanwendungen:** Anforderungen an die Anbindung der Cloud-Standorte (föderiertes Peering, kein Transit über das öffentliche Internet) im Kontext des Netzverbunds Deutschland (NV-DE) sowie an die in der DVC betriebenen Fachanwendungen.
- **Detektion, Reaktion und Nachweisführung:** Anbindung an zentrale Detektions- und Reaktionsfähigkeiten, maschinenlesbares Schwachstellen- und Advisory-Management sowie die Beschreibung des Entwicklungspfads von der Selbstauskunft zum kontinuierlichen, maschinell prüfbaren Nachweis.
- **Aktualisierung der regulatorischen Bezüge:** Fortschreibung der Bezüge unter anderem zu den Eckpunkten einer Zero-Trust-IT-Sicherheitsarchitektur des Bundes, Grundschutz++, NIS-2, Cyber Resilience Act, den einschlägigen Technischen Richtlinien des BSI sowie zur Rollen- und Risikosystematik der EU-KI-Verordnung.
- **Geschäftsarchitektur der DVC:** Klarstellungen und ggf. Aufnahme von Detaillierungen zu Vertragsbeziehungen und zum Rollenmodell. Die verschiedenen föderalen Perspektiven von Bund, Ländern und Kommunen für eine Nutzung von DVC und Deutschland-Stack sind zu reflektieren. DVC-Konformität und Deutschland-Stack-Konformität sind weitestgehend synonym auszugestalten.

Die Arbeitsteilung zwischen den Dokumenten bleibt dabei unverändert: Das Rahmenwerk beschreibt auch in der Version 4.1 Prinzipien und Leitplanken, es ist kein Prüfkatalog. Prüfbare Einzelanforderungen werden im Reifegradmodell (Version 2.0), in den Cloud-Service-AGB und in den Detailstandards verankert. Die Version 4.1 schafft hierfür die architektonische Grundlage und die eindeutige Zuordnung.
In diesem Sinne ist es möglich, dass die Befassung der oben genannten Themenfelder nicht zu einer detaillierten Verankerung im Rahmenwerk der Zielarchitektur selbst führt. Stattdessen kann eine angemessene Behandlung auf einer anderen Ebene erfolgen – insbesondere im Reifegradmodell (Version 2.0), in den Cloud-Service-AGB und in den Detailstandards – oder eine begründete Rückstellung in das Backlog späterer Versionen des Rahmenwerks.

Abbildungsverzeichnis

Abbildung 1: Transformation der föderalen IT-Landschaft durch die DVC 9
Abbildung 2: Zentrale Rollen und Akteure in der Deutschen Verwaltungscloud 24
Abbildung 3: Direktvertragsmodell 34
Abbildung 4: Direktvertragsmodell mit Cloud-Service-Beschaffer 34
Abbildung 5: Umklappvertragsmodell 35
Abbildung 6: Umklappvertragsmodell mit Cloud-Service-Beschaffer 35
Abbildung 7: Säulen der DVC-Architektur 37
Abbildung 8: Kontext des Reifegradmodells 55

Tabellenverzeichnis

Tabelle 1: Reduktion von Abhängigkeiten 40
Tabelle 2: Entwicklung und Inbetriebnahme 42
Tabelle 3: Betrieb 44
Tabelle 4: Angebot von Cloud-Services 47
Tabelle 5: Sicherstellung und Stärkung von Datenschutz und Informationssicherheit 53
Tabelle 6: Optimierung von Datenaustausch, -speicherung und -nutzung 54
Tabelle 7: Glossar 64