

Version	Datum	Autor:in	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

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-koordinierungsstelle@fitko.de

Stand

Februar 2025

Nachdruck, auch auszugsweise, ist genehmigungspflichtig.

Inhaltsverzeichnis

Präambel.....	5
1 Einführung.....	7
1.1 Zielsetzung und Aufbau des Dokumentes.....	9
1.2 Geltungsbereich und Zielgruppe des Dokuments.....	10
1.3 Weiterentwicklung des Dokumentes.....	10
2 Rahmenbedingungen der Deutschen Verwaltungscloud.....	12
2.1 Nahestehende Vorhaben.....	12
2.2 Relevante Vorgaben und Richtlinien der Öffentlichen Verwaltung.....	15
2.3 Datenklassifizierung in der Öffentlichen Verwaltung.....	17
3 Geschäftsarchitektur der Deutschen Verwaltungscloud.....	19
3.1 Zusammenarbeitsmodell.....	19
3.2 Rollen und Akteure in der Deutschen Verwaltungscloud.....	21
3.2.1 Rollen auf der Kundenseite.....	21
3.2.2 Rollen auf der Anbieterseite.....	22
3.2.3 Prinzip der geteilten Verantwortung.....	23
3.3 CSP-Ökosystem.....	25
3.4 Vertragsmodalitäten.....	26
3.5 Einbindung von verwaltungsexternen Anbietern.....	29
4 Technische Architektur der Deutschen Verwaltungscloud.....	30
4.1 Reduktion von Abhängigkeiten.....	32
4.2 Steigerung der Effizienz und Effektivität in Entwicklung, Inbetriebnahme und Betrieb.....	33
4.2.1 Entwicklung und Inbetriebnahme.....	33
4.2.2 Betrieb.....	34
4.2.3 Angebot von Cloud-Services.....	35
4.3 Sicherstellung und Stärkung von Datenschutz und Informationssicherheit.....	37
4.4 Optimierung von Datenaustausch, -speicherung und -nutzung zwischen Bund, Ländern und Kommunen.....	40
5 Reifegradmodell der Deutschen Verwaltungscloud.....	41
6 Weiterführende Informationen.....	44

Präambel

Mit der Deutschen Verwaltungscloud (DVC) wird das Ziel verfolgt, die Digitalisierung der öffentlichen Verwaltung voranzutreiben und somit 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.

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 wird ein neuer digitaler Marktplatz – das Cloud-Service-Portal – aufgebaut, auf dem Cloud-Service-Angebote von öffentlichen IT-Dienstleistern und perspektivisch auch von verwaltungsexternen Anbietern gemäß DVC-Mindestanforderungen angeboten werden¹. Diese Dienste stehen den Verwaltungen und ihren IT-Dienstleistern auf Bundes-, Landes- und Kommunalebene über einheitliche Vertragsmodelle für eine rechtskonforme Beschaffung zur Verfügung.

Die DVC soll als zentraler Marktplatz für Cloud-Service-Angebote ein neues föderales IT-Zusammenarbeitsmodell schaffen. 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.

¹ Marktplatz der Zukunft (19.06.2024): IT-Planungsrat, Link zu Beschluss IT-PLR 2024/23. Neben der DVC existieren in der Domäne des IT-Planungsrats diverse Marktplätze, die unterschiedliche Ziele verfolgen. In seiner 44. Sitzung hat der IT-Planungsrat die FITKO damit beauftragt, ein Konzept für den konsolidierten „Marktplatz der Zukunft“ unter Einschluss der DVC zu erstellen.

Die Schaffung eines einheitlichen rechtlichen, organisatorischen und technischen Rahmens mit der DVC – einem föderalen Cloud-Ökosystem – soll dazu führen, 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.

1 Einführung

Die Stärkung der Digitalen Souveränität² für die IT der Öffentlichen Verwaltung ist ein gemeinsames Ziel von Bund, Ländern und Kommunen in Deutschland. Die IT der öffentlichen Verwaltung steht als kritische Infrastruktur in unmittelbarem Zusammenhang mit der Handlungsfähigkeit des Staates. 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 Rahmen der Strategie zur Stärkung der Digitalen Souveränität hat der IT-Planungsrat (IT-PLR) die „Deutsche Verwaltungscloud-Strategie“ (DVS) verabschiedet⁴ 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. In die DVC sollen zunächst bereits existierende Cloud-Services der oben genannten Anbieter eingebunden werden, soweit sie die DVC-Mindestanforde-

2 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“.

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 zum Dokument "Strategie zur Stärkung der Digitalen Souveränität", S. 6.

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

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

rungen des Reifegradmodells erfüllen (siehe Kap. 5 Reifegradmodell der Deutschen Verwaltungscld). Durch die Schaffung einheitlicher DVC-Mindestanforderungen und der auf diese Weise erhöhten Kompatibilität der bestehenden Services können vorhandene Kapazitäten optimal genutzt und Synergien gehoben werden.

- **Allgemeine Verfügbarkeit von Cloud-Services:** Angebotene Cloud-Services in XaaS-Servicemodellen (z. B. IaaS, PaaS, SaaS) 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 durch die Cloud-Service-Kunden nachgenutzt werden können.
- **Einsatz von OS-Software (OSS):** OSS⁶ wird für den Aufbau der DVC priorisiert⁷. Innerhalb der DVC betriebene Cloud-Services müssen nicht auf OSS basieren, Lock-in-Effekte⁸ 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 im 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.
- **Gemeinsame Weiterentwicklung:** Zur Kooperation an öffentlichen Entwicklungsprojekten und zur Weiterentwicklung wesentlicher Softwarekomponenten (z. B. Standard-Images

6 Open Source Initiative: <https://opensource.org/>.

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 sonstigen Wechselbarrieren erschwert, das Produkt, den Service oder den Anbieter zu wechseln.

oder Policies⁹ für den Betrieb von Containern¹⁰) soll die OS-Plattform der Öffentlichen Verwaltung „Open CoDE“¹¹ genutzt werden, auf der Repositories für (OS-)Softwareprojekte angelegt und gepflegt werden können.

1.1 Zielsetzung und Aufbau des Dokumentes

Ziel des vorliegenden Dokumentes „Rahmenwerk der Zielarchitektur“ ist es, die Deutsche Verwaltungswolke (DVC) 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-¹² und Strategiepapier¹³ 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 Konzeptes, 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 Rollenmodell, das Cloud-Service-Portal-Ökosystem, die Vertragsmodalitäten sowie Aspekte der Einbindung von verwaltungsexternen Anbietern.

9 Ergebnisbericht – Deutsche Verwaltungswolke-Strategie – Proof-of-Concept, in: IT-Planungsrat, 22.04.2022, https://www.it-planungsrat.de/fileadmin/it-planungsrat/foederale-zusammenarbeit/Gremien/AG_Cloud/220420_PoC-Ergebnisdokument_Langfassung_AG_Cloud_vf.pdf.

10 IG BVC, in: Software, https://wikis.opencode.de/de/Organisationen/IG_BvC.

11 Open CoDE: <https://www.opencode.de/>.

12 Beschluss 2020/19 – Stärkung der Digitalen Souveränität der öffentlichen Verwaltung – Eckpunkte – Ziel und Handlungsfelder, in: IT-Planungsrat, 04.05.2020, https://www.it-planungsrat.de/fileadmin/beschluesse/2020/Beschluss2020-19_Entscheidungsniederschrift_Umlaufverfahren_Eckpunktepapier.pdf.

13 Beschluss 2021/09 – Strategie zur Stärkung der Digitalen Souveränität für die IT der Öffentlichen Verwaltung – 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, https://www.it-planungsrat.de/fileadmin/beschluesse/2021/Beschluss2021-09_Strategie_zur_Staerkung_der_digitalen_Souveraenitaet.pdf.

- **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.
- **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 Verwaltungswolke (DVC) 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 Verwaltungswolke ist die Umsetzung der Minimalkriterien des DVC-Reifegradmodells (siehe Kapitel 0) 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 das CSP einheitliche Vertragsbedingungen (CSP-AGB)¹⁴.

1.3 Weiterentwicklung des Dokumentes

Das Dokument „Rahmenwerk der Zielarchitektur“ wird anlassbezogen und iterativ weiterentwickelt und mit einem Beschluss im Rahmen der Governance der Deutschen Verwaltungswolke (DVC) 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 Reifegradmodell¹⁵, 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

14 Es gilt die jeweils gültige Fassung auf der Website: <https://deutsche-verwaltungswolke.de/>.

15 Es gilt die jeweils gültige Fassung auf der Website: <https://deutsche-verwaltungswolke.de/>.

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 (DVC) 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:

- **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 oder Justizcloud) im Einsatz oder befinden sich in der Entwicklung.
- **Cloud-Lösungen verwaltungsexterner Anbieter:** In Reaktion auf die Souveränitätsanforderungen der Öffentlichen Verwaltung werden neue verwaltungsexterne Cloud-Lösungen für die Nutzung durch die Öffentliche Verwaltung entwickelt (z. B. Delos Cloud oder vergleichbare „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.
- **Cloud-Broker:** Organisationen der Öffentlichen Verwaltung nutzen Cloud-Broker-Modelle (z. B. gd.Cloud-Broker oder zukünftig Multicloud-Broker der Bundesanstalt für Arbeit, der DRV Bund und der Deutschen Gesetzlichen Unfallversicherung (DGUV)) 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.

- **OZG-Umsetzung**¹⁶: 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 (OZGÄndG) baut auf diesen Grundlagen auf und zielt darauf ab, die weitere Digitalisierung der Verwaltung voranzutreiben 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).¹⁷
- **BundID / DeutschlandID**¹⁸: Das OZG-Änderungsgesetz sieht vor, die Nutzerkonten für die Bürger:innen (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:innen 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“**¹⁹: 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**²⁰: Das Vorhaben zielt darauf ab, eine deutschland- und die EU-weite Nachweisübermittlung aus bestehenden Registern zu ermöglichen. Durch Vernetzung der Register wird das Once-Only-Prinzip²¹ umgesetzt und damit auch eine medienbruchfreie Bearbeitung und Bereitstellung von Verwaltungsleistungen ermöglicht. Die Registermodernisierung steht in engem Zusammenhang mit der OZG-Umsetzung.

16 Onlinezugangsgesetz: Wohnzimmer statt Wartezimmer – Umsetzung des Onlinezugangsgesetzes, in: Bundesministerium des Innern und für Heimat, <https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/onlinezugangsgesetz-node.html?sessionid=41DA8FAA9922FD8F1B666E74509CA7CA.live861>.

17 Das „EFA“-Prinzip bedeutet, dass einmal entwickelte Lösungen eines Landes in anderen Ländern nachgenutzt werden können, um arbeitsteilig und zeitsparend bei der Digitalisierung vorzugehen.

18 OZG-Änderungsgesetz, in: Bundesministerium des Innern und für Heimat, <https://www.digitale-verwaltung.de/Webs/DV/DE/onlinezugangsgesetz/das-gesetz/ozg-aenderungsgesetz/ozg-aenderungsgesetz-node.html>.

19 Mein Unternehmenskonto, <https://info.mein-unternehmenskonto.de/>.

20 Registermodernisierung, in: Bundesministerium des Innern und für Heimat, <https://www.digitale-verwaltung.de/Webs/DV/DE/registermodernisierung/registermodernisierung-node.html>.

21 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.

Perspektivisch sollen OZG, Registermodernisierung und Deutsche Verwaltungscloud (DVC) ineinandergreifen. Die OZG-Umsetzung und die Registermodernisierung sind nicht abhängig vom Aufbau der DVC und werden als parallele Handlungsstränge betrachtet. 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.

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 (DVC) 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:

- **IT-Grundschutz²²**: Der IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) 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.
- **Kriterienkatalog Cloud Computing des BSI (kurz: C5)²³**: Der Katalog spezifiziert Mindestanforderungen an die Informationssicherheit für Cloud-Services. 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 Informationssicherheit („Shared Responsibility“) betrachtet.
- **Architekturrichtlinie für die IT des Bundes²⁴**: Mit der Architekturrichtlinie für die IT des Bundes wird ein aktives Architekturmanagement für die IT der Bundesverwaltung verfolgt. Die von der IT-Konsolidierung Bund²⁵ betroffenen Bereiche sollen durch konkrete strategische Architekturvorgaben aktiv bei **Entscheidungsprozessen** unterstützt werden und die Vorgaben für die Weiterentwicklung der IT des Bundes einhalten. Außerdem unterstützen

22 BSI-IT-Grundschutz: in: Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html.

23 Kriterienkatalog C5, in: Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html.

24 IT-Architektur Bund, in: Der Beauftragte der Bundesregierung für Informationstechnik, https://www.cio.bund.de/Webs/CIO/DE/digitaler-wandel/Achitekturen_und_Standards/IT_Architektur_Bund/IT_Architektur_Bund-node.html?sessionId=A016330E93E1A66FB01C8EABF5C030DC.live892.

25 IT-Konsolidierung Bund, in: Bundesministerium des Innern und für Heimat, <https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/it-konsolidierung/it-konsolidierung-node.html>.

die Vorgaben eine Ausrichtung der laufenden IT-Projekte an den strategischen Anforderungen und politischen Aufgaben.

- **Weitere Architekturrichtlinien/-vorgaben bzw. Mindestanforderungen für die IT:** Neben den Architekturrichtlinien des Bundes existieren weitere bundes- sowie länderspezifische Architekturvorgaben und Mindestanforderungen für die durch die Öffentliche Verwaltung eingesetzte IT. Dazu zählen die Datenschutz-Grundverordnung (DSGVO) sowie weitere Anforderungen des BSI, darunter beispielsweise die Mindeststandards des BSI für die Sicherheit der Informationstechnik des Bundes.²⁶
- **Föderale IT-Architekturrichtlinien²⁷:** Um eine möglichst einheitliche beziehungsweise interoperable Architektur über alle föderalen Ebenen hinweg sicherzustellen und aktiv zu steuern, werden vom Föderalen IT-Architekturboard föderale IT-Architekturrichtlinien definiert und weiterentwickelt. Die Richtlinien gelten für alle laufenden und neuen Projekte und Vorhaben, die Einfluss auf die föderale IT-Landschaft haben.
- **Anforderungen an Technologieanbieter und -lösungen zur Stärkung der Digitalen Souveränität²⁸:** 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.

26 Mindeststandards des BSI gemäß § 8 Abs. 1 Satz 1 BSIG, in: Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Mindeststandards_node.html.

27 Föderale IT-Architekturrichtlinien: Dokumentation zur Föderalen IT-Architektur, in: Föderales Entwicklungsportal, <https://docs.fitko.de/arc/policies/foederale-it-architekturrichtlinien/>.

28 Anforderungen an Technologieanbieter und -lösungen zur Stärkung der Digitalen Souveränität, in: Der Beauftragte der Bundesregierung für Informationstechnik, https://www.cio.bund.de/SharedDocs/downloads/Webs/CIO/DE/cio-bund/steuerung-it-bund/beschluesse_cio-board/2024_01_Beschluss_CIO_Board_Technologieanbieter_Anlage.pdf?__blob=publication-File&v=2.

2.3 Datenklassifizierung in der Öffentlichen Verwaltung

Um einen Rahmen für die Datenklassifizierung zu etablieren, orientiert sich die Deutsche Verwaltungswolke (DVC) 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,
- Datenschutzgrundverordnung (DSGVO), Bundesdatenschutzgesetz (BDSG) und entsprechende Ländervorschriften sowie
- IT-Grundschutz und der Kriterienkatalog C5

Geheimschutz²⁹: 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 in der Verantwortung des Cloud-Service-Kunden.

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 Datenschutzfolgenabschätzung ist gemäß DSGVO Artikel 35 bei hohen Risiken für die Rechte und Freiheiten natürlicher Personen durchzuführen. Eventuell ist auch ein Vertrag über die Auftragsdatenverarbeitung erforderlich. Die Beurteilung,

29 Geheimschutz, in: Bundesamt für Sicherheit in der Informationstechnik, <https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Geheimschutz/geheimschutz.html>.

ob ein Cloud-Service der DSGVO oder weiteren datenschutzrechtlichen Regularien unterliegt, liegt in der Verantwortung des Cloud-Service-Kunden.

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, 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 Kriterienkatalog 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 Zusammenarbeitsmodell

Im Zusammenarbeitsmodell der Deutschen VerwaltungscLOUD (DVC) agieren folgende zentrale Rollen und Akteure:

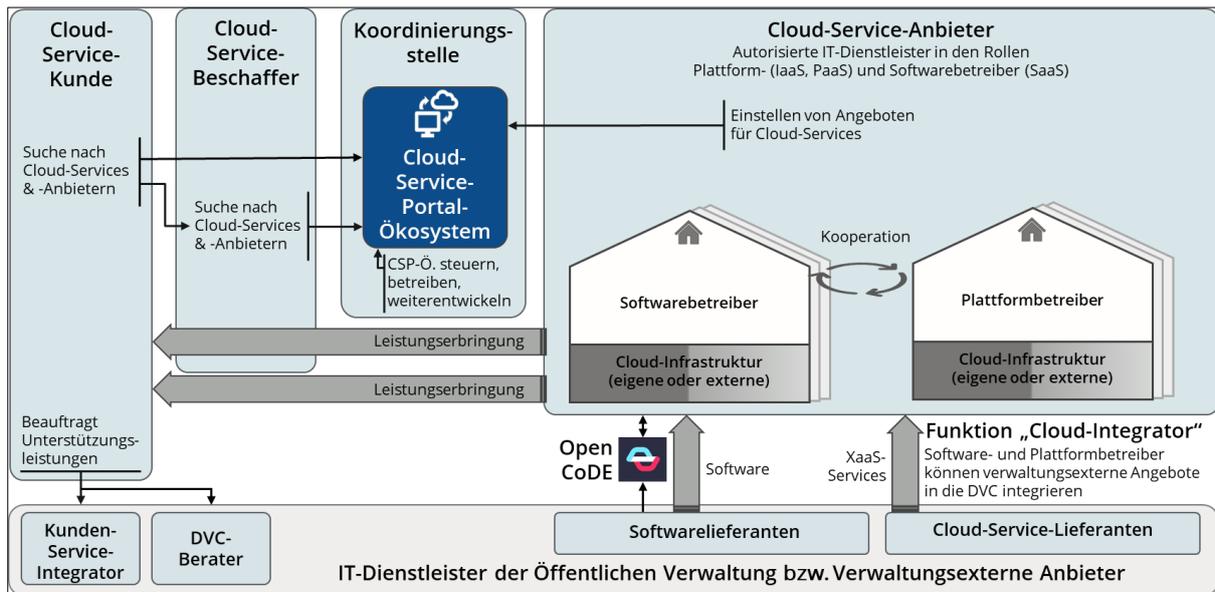


Abbildung 1: Zentrale Rollen und Akteure in der Deutschen VerwaltungscLOUD (illustrative Darstellung)

Die **Koordinierungsstelle** ist das zentrale Entwicklungs- und Steuerungselement für die Weiterentwicklung der DVC und des Cloud-Service-Portal-Ökosystems (CSP-Ökosystem). Das CSP-Ökosystem umfasst insbesondere das Cloud-Service-Portal (CSP) als zentrale E-Commerce-Plattform sowie IAM-Funktionalitäten und das Management der Anbieterinstanzen³⁰.

Die Koordinierungsstelle beauftragt den technischen CSP-Betreiber mit dem Betrieb und der Weiterentwicklung des CSP-Ökosystems (CSP und seine Umsysteme, inkl. Netzübergänge) und übernimmt die Steuerung des CSP-Betreibers.

Darüber hinaus übernimmt die Koordinierungsstelle weitere Aufgaben, wie die Moderation der Teilnahme an der DVC, das Management der Vertragsbedingungen (u. a. AGB des Cloud-Service-Portals), das Stakeholder-Management, die Kommunikation und Information. Im Rahmen der Moderation der Teilnahme überprüft die Koordinierungsstelle auf Grundlage des aktuell

³⁰ Eine technische Instanziierung, die der Cloud-Service-Anbieter dem Cloud-Service-Kunden bereitstellt.

geltenden Autorisierungsprozesses die **Konformität** der Cloud-Service-Anbieter und ihrer Cloud-Services mit den geltenden Minimal Kriterien der DVC (siehe Kapitel 5).

Das **Cloud-Service-Portal** ist der zentrale Einstiegspunkt für die Verwaltungen in Bund, Ländern und Kommunen und deren IT-Dienstleister in einem Marktplatz-Kontext. Über das Cloud-Service-Portal haben Cloud-Service-Kunden Zugriff auf einen Cloud-Service-Katalog mit DVC-konformen Cloud-Services und können diese über verschiedene Beschaffungsmodelle beziehen. Die Auswahl von Cloud-Services im Cloud-Service-Portal erfolgt im zentralen Cloud-Service-Katalog mit einheitlich definierten Service-Kategorien.

Die **OS-Plattform der Öffentlichen Verwaltung Open CoDE** ist Teil der Umsetzung der Deutschen VerwaltungscLOUD-Strategie³¹ und wird gegenwärtig vom Zentrum für Digitale Souveränität der Öffentlichen Verwaltung (ZenDiS)³² bereitgestellt. Softwarebetreiber und Softwarelieferanten der DVC haben die Möglichkeit, Open CoDE als gemeinsame Plattform für den Austausch von Open-Source-Software zu nutzen.

Open CoDE umfasst ein zentrales Verzeichnis der verwaltungsrelevanten und verfügbaren OS-Software-Projekte/-Lösungen, eine Webanwendung zur Versionsverwaltung und zur Ablage von offenem Quellcode beziehungsweise zur Beteiligung an Projekten (Code Repository) sowie ein Diskussionsforum.

31 Open CoDE ist kein direkter Bestandteil der DVC.

32 ZENDIS | Zentrum Digitale Souveränität: <https://zendis.de/>.

3.2 Rollen und Akteure in der Deutschen Verwaltungscld

Die Deutsche Verwaltungscld (DVC) verfügt über ein Rollenmodell, das sich 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.

3.2.1 Rollen auf der Kundenseite

Cloud-Service-Kunde

Cloud-Service-Kunden beziehen Cloud-Services über das Cloud-Service-Portal. 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 und Kunden des Cloud-Service-Beschaffers 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 der § 108 Absatz 1 oder Absatz 4 GWB vorliegen.

Cloud-Service-Beschaffer (bisher bezeichnet als Cloud-Service-Vermittler)

Cloud-Service-Beschaffer sind Cloud-Service-Kunden, die Cloud-Services über das Cloud-Service-Portal beziehen, um diese ihrerseits durch ihre Kunden (Kunden des Cloud-Service-Beschaffers) nutzen zu lassen.³³

Intermediär³⁴

Vertragspartner des Cloud-Service-Anbieters und (spiegelbildlich) des Cloud-Service-Kunden im Umklappvertragsmodell (vgl. Kapitel 3.4, Abbildung 4).

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

34 Die Rolle des Intermediärs wird derzeit durch die govdigital eG ausgeübt.

Kunden-Service-Integrator

Kunden-Service-Integratoren sind von Cloud-Service-Kunden Beauftragte. Sie unterstützen die Integration von über das Cloud-Service-Portal bezogenen Cloud-Services in die Umgebung des Cloud-Service-Kunden.

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

DVC-Berater

Der DVC-Berater berät den Cloud-Service-Kunden zu den technisch-fachlichen Möglichkeiten der DVC-Nutzung. 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.

3.2.2 Rollen auf der Anbieterseite

Cloud-Service-Anbieter

Cloud-Service-Anbieter bieten als Plattformbetreiber und/oder Softwarebetreiber Cloud-Services auf dem Cloud-Service-Portal an und verantworten die Leistungserbringung. Cloud-Service-Anbieter können dabei auch Services eines Cloud-Service-Lieferanten in der Funktion des „Cloud-Integrators“ einbinden.

Cloud-Service-Anbieter von Cloud-Services im Cloud-Service-Portal 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 Cloud-Services im IaaS- oder PaaS-Modell bereitstellen.

Softwarebetreiber

Softwarebetreiber sind Cloud-Service-Anbieter, die Cloud-Services im SaaS-Modell bereitstellen.

Cloud-Service-Lieferanten

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 und stellen diese dem Softwarebetreiber bereit. Softwarelieferanten übernehmen gegebenenfalls die Wartung und Pflege der Software und sind in dieser Rolle Unterauftragnehmer der Softwarebetreiber.

Softwarelieferanten können sowohl Akteure der Öffentlichen Verwaltung als auch verwaltungsexterne Anbieter sein.

3.2.3 Prinzip der geteilten Verantwortung

Das Prinzip der geteilten 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 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.

3.3 CSP-Ökosystem

Das Cloud-Service-Portal (CSP) ist der zentrale Cloud-Service-Marktplatz der DVC. Das Ökosystem des Cloud-Service-Portals (CSP-Ökosystem) soll im Rahmen der DVC aktuell insbesondere folgende Aufgaben erfüllen:

1. Bereitstellung einer E-Commerce-Plattform und Abbildung der E-Commerce-Prozesse als Self-Service. Dies beschreibt den heutigen CSP-Marktplatz und auch weitere zukünftige Funktionen, wie beispielsweise ITSM-Funktionalitäten sowie Billing/Reporting.
2. Bereitstellung der IAM-Funktionalitäten, inklusive Zuordnung von Rollen und Berechtigungen
3. Management der Anbieterinstanzen
4. Schaffung von Voraussetzungen für zukünftige Automation und Weiterentwicklung der Plattform

Im Rahmen der Weiterentwicklung der Deutschen Verwaltungscloud (DVC) können über die vorgenannten Aufgaben hinaus bei Bedarf weitere zentrale Dienste für die DVC in das CSP-Ökosystem integriert werden.

Aktuell dient ein zentrales API-Gateway als Vermittler zwischen den Bausteinen des CSP und ermöglicht so eine reibungslose Kommunikation sowohl innerhalb des Systems als auch mit externen Schnittstellen. Die Kapselung der Komponenten durch das Gateway gewährleistet die Modularität der Architektur und unterstützt die flexible Erweiterung der Funktionalität.

Die Funktionen des CSP sind die Bereitstellung³⁵ von Cloud-Service-Angeboten und die Beschaffung sowie Änderung von Cloud-Services, die mit einem Webshop-System realisiert werden. Das CSP soll sowohl die über das CSP gebuchten Anbieterinstanzen als auch weitere Statusinformationen anzeigen sowie Änderungen und Kündigungen ermöglichen.

Auf der Seite des CSP-Betreibers sind einschlägige Systeme für die Dokumentation der Verträge sowie die Leistungserbringung und Abrechnung notwendig, um die angebotenen Cloud-Services entsprechend den Vertragsmodalitäten abzuwickeln.

Im Rahmen der DVC sollen eine benutzerfreundliche und gleichzeitig sichere Authentisierung und Autorisierung, wenn möglich sogar ein Single Sign-on (SSO) mit bestehenden Identitäten

³⁵ Bereitstellung bezieht sich aktuell darauf, dem Cloud-Service-Kunden Informationen in einem einheitlichen Format zur Verfügung zu stellen, um die Beschaffung zu ermöglichen und in der Folge den Cloud-Service zur Nutzung bereitzustellen.

der Öffentlichen Verwaltung, ermöglicht werden. Die Authentisierung (Identitäten) und Autorisierung (Rollen) aller Cloud-Services der DVC soll durch die Organisation der Cloud-Service-Kunden bzw. -Anbieter in ihren bestehenden Systemen erfolgen.

Der Zugang zum CSP-Ökosystem erfolgt perspektivisch über Verwaltungsnetze. Teile des CSP-Ökosystems und Endkundenaufrufe für Verfahren können dabei auch über das Internet adressiert werden. Ein entsprechendes Sicherheitskonzept für die Absicherung des Internet Traffic ist noch zu entwickeln.

3.4 Vertragsmodalitäten

Ziel bei der Gestaltung der Vertragsmodalitäten ist eine einheitliche Vertragsgestaltung für alle Akteure im Cloud-Service-Portal (CSP). 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 über das CSP Cloud-Services bestellen zu können:

- das Direktvertragsmodell und
- das sogenannte Umklappvertragsmodell,

die nachfolgend erläutert werden. Darüber hinaus sind Vertragsketten über einen Cloud-Service-Beschaffer möglich.

Welche der Modelle für einen Cloud-Service angeboten werden, legt der Cloud-Service-Anbieter in seinem Service Offering im CSP für jeden einzelnen Cloud-Service fest. Der Cloud-Service-Kunde (oder ggf. der Cloud-Service-Beschaffer) entscheidet mit der Bestellung über das CSP, in welchem Vertragsmodell er den Cloud-Service beziehen möchte.

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. 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.

Falls Cloud-Services von Cloud-Service-Kunden über Cloud-Service-Beschaffer bezogen werden, entsteht folgende Vertragskette: Der Cloud-Service-Beschaffer schließt den Vertrag über

3.5 Einbindung von verwaltungsexternen Anbietern

Verwaltungsexterne Angebote können bereits im bestehenden Rollenmodell der Deutschen Verwaltungscloud (DVC, vgl. Abschnitt 3.2) eingebunden werden. Verwaltungsexterne Anbieter agieren als DVC-externe Cloud-Service-Lieferanten oder Softwarelieferanten. Cloud-Service-Anbieter (Softwarebetreiber oder Plattformbetreiber) können diese Cloud-Services in ihrer Funktion als Cloud-Integrator für die Kunden der DVC nutzbar machen.

Ein direktes Angebot verwaltungsexterner Cloud-Services kann perspektivisch ein wichtiger Baustein der DVC sein. Die rechtlichen, technischen und organisatorischen Voraussetzungen, wie verwaltungsexterne Cloud-Services (u. a. auch Angebote der Public-Cloud-Anbieter) DVC-konform angeboten werden können, werden im DVC-Umsetzungsprojekt geklärt und verifiziert. Im Rahmen des Projekts wird ein entsprechender Bericht zu den Rahmenbedingungen für die Integration verwaltungsexterner Angebote vorgelegt. Eine Entscheidung zur Aufnahme verwaltungsexterner Angebote und zu den diesbezüglichen Voraussetzungen wird abschließend durch den IT-Planungsrat getroffen.

der Prinzipien der Technischen Architektur umfasst das Cloud-Service-Portal-Ökosystem (CSP-Ökosystem) sowie die angebotenen Cloud-Services der autorisierten Cloud-Service-Anbieter. Die im Rahmenwerk formulierten Prinzipien der Technischen Architektur sollen an den aktuellen Stand der Technik³⁷ 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.

37 „Stand der Technik“ umsetzen, in: Bundesamt für Sicherheit in der Informationstechnik, https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/Stand-der-Technik-umsetzen/stand-der-technik-umsetzen_node.html.

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	Entkoppelung 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 so gewählt, dass diese am Markt etabliert, stabil und selbsttragend sind. Der Einsatz von Containertechnologien (z. B. Kubernetes) erfüllt diese Prinzipien.
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.
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 Open CoDE Repository hinterlegt. Der Quellcode (oder die Quellcodes) aus der Realisierung digitaler Angebote der Verwaltung (Eigenentwicklung) wird als Open Source ³⁸ , das heißt in nachnutzbarer Form, eine Veränderung gestattender Lizenzierung, zur Verfügung gestellt.

Tabelle 1: Reduktion von Abhängigkeiten

38 Open Source Initiative, <https://opensource.org/>.

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. Die Build-Pipeline ist bei Open-Source-Software auf der Plattform Open CoDE konfiguriert. Anwendungscode, der unter einer Closed-Source-Lizenz verwendet wird, bzw. Konfigurationen für den lokalen Betrieb werden in lokalen Versionsverwaltungssystemen vorgehalten.
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 Open CoDE 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.
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 Wechselbarkeit 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.
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).
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 (Multi-Cloud-Fähigkeit). Die Cloud-Service-Anbieter unterstützen gemäß dem Stand der Technik gängige Virtualisierungs- und Orchestrierungstechniken ³⁹ und arbeiten auf einen hohen Automatisierungsgrad in ihren Organisationen und Abläufen hin. Die zukünftige Verwendung von IPv6 stellt einen ausreichend großen Adressraum sicher.
SE-07	Mandanten-trennung	Die Daten und Ressourcen der Mandanten sind nach aktuellem Stand der Technik sicher getrennt.
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

39 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	Es ist ein Self-Service-Portal für Cloud-Services 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	Barrierefreiheit	Für alle berechtigten Endanwender von Cloud-Services sind Cloud-Services zugänglich und nutzbar gestaltet, unabhängig von deren Fähigkeiten oder Einschränkungen. Die rechtlichen Vorgaben zu Barrierefreiheit werden erfüllt.
SE-12	Elastische und skalierbare Cloud-Services	Es ist ein konstantes Antwortzeitverhalten des Cloud-Service bei unterschiedlichen Last-Aufkommen sichergestellt. Voraussetzung hierfür ist eine einfache, kurzfristige und automatisierbare Anpassungsmöglichkeit der Ressourcen bei veränderten Bedarfen (z. B. saisonale Schwankungen oder neue Vorhaben). Den Cloud-Kunden wird über ein professionelles Verfügbarkeitsmonitoring kontinuierlich Einblick geben, sodass unmittelbar eine Störung des konstanten Antwortzeitverhalten festgestellt und nachgesteuert werden kann.

ID	Prinzip	Inhalt
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.
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 Service vereinbart.
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 Öffentliche 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 ⁴⁰	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.
SI-02	Präferenz für Zero Trust	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 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.

40 Einzelheiten regeln die nachgelagerten regulatorischen Dokumente der DVC, insbesondere Reifegradmodell und Detailstandards.

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 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.
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 DevOps, ergänzt um Bausteine zur Sicherheit (z. B. DevSecOps, Clean Code, Secure Coding, Penetrationstests, Dynamische Sicherheitstests). Die Lieferkette der Software-Artefakte ist unter Sicherheitsaspekten verifiziert und dokumentiert.
SI-06	Sichere Betriebsüberführung 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 gehört 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).

ID	Prinzip	Inhalt
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.
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.
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 während der gesamten Übertragung verschlüsselt bleiben, ohne dass der Cloud-Anbieter Zugang zu unverschlüsselten Daten erhält.
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.
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-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 im Rahmen einer Serviceklasse sofern möglich interoperabel zu konzipieren, d. h., sie ermöglichen einen standardisierten Datenaustausch über definierte Schnittstellenvereinbarungen. ⁴¹ 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. ⁴² Hier soll eine strikte Trennung von Nutzdaten (kundenspezifischen Inhaltsdaten eines Services), Transaktionsdaten (z. B. Abrechnungsdaten) und Metadaten (servicespezifischen Konfigurationsdaten eines Serviceerfolgen).
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

41 Dies gilt insbesondere für Verfahren, für die die föderalen IT-Standards des „Föderalen Standardisierungsboards“ gelten.

42 Regelungen der Registermodernisierung bleiben davon unberührt.

5 Reifegradmodell der Deutschen Verwaltungscloud

Mit der Deutschen Verwaltungscloud (DVC) sollen verbindliche Mindestanforderungen für alle teilnehmenden Cloud-Service-Anbieter eingeführt werden⁴³, die in einem Reifegradmodell abgebildet sind.

Durch die Anwendung des Reifegradmodells⁴⁴ soll sichergestellt werden, dass die eingereichten Cloud-Service-Kandidaten den Minimalkriterien der DVC entsprechen, sodass sie über das Cloud-Service-Portal angeboten werden können.⁴⁵

Darüber hinaus sollen die durch die Anwendung des Reifegradmodells erhobenen Informationen dem Cloud-Service-Kunden die Möglichkeit geben, 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 Cloud-Service-Portal 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.

43 Im Rahmenwerk Zielarchitektur 2.0 vom 10.10.2022 wurden Bedingungen (in Form obligatorischer und optionaler Standards) für die Teilnahme an der DVC definiert. Im Rahmen des MVP-Projekts 2022/23 wurde festgestellt, dass die im Rahmenwerk 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. Daher wurde das Prinzip eines Reifegradmodells entwickelt und in ersten Ansätzen im Rahmenwerk Zielarchitektur 2.5.4 vom 03.11.2023 sowie im Konzept zum Aufbau und Betrieb der Koordinierungsstelle der DVC (MVP-Ergebnis) beschrieben. Auf dieser Basis wurden erste Vorschläge für Reifegradkriterien von der UAG Technik & Betrieb erstellt, im Januar 2024 an das DVC-Umsetzungsprojekt übergeben und dort weiterentwickelt und operationalisiert.

44 Es gilt die jeweils gültige Fassung auf der Website: <https://deutsche-verwaltungscloud.de/>.

45 Werden diese Minimalkriterien nicht erfüllt, kann der Cloud-Service nicht angeboten werden.

- **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 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 an 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.

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. ⁴⁷
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	Beschaffung von Software als Abonnement, d. h. als fortlaufende Vereinbarung zur regelmäßigen Nutzung eines Cloud-Services für einen bestimmten Zeitraum.
Cloud-Service-Anbieter	Cloud-Service-Anbieter bieten als Plattformbetreiber und/oder Softwarebetreiber Cloud-Services über das Cloud-Service-Portal an und verantworten die Leistungserbringung.
Cloud-Service-Beschaffer	Cloud-Service-Beschaffer sind Cloud-Service-Kunden, die Cloud-Services auf dem Cloud-Service-Portal 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-Offering.

47 Cloud Computing Grundlagen, in: Bundesamt für Sicherheit in der Informationstechnik, <https://www.bsi.bund.de/dok/6622124>

Begriff	Erläuterung
Cloud-Service-Kunde	Cloud-Service-Kunden beziehen Cloud-Services eines Cloud-Service-Anbieters über das Cloud-Service-Portal.
Cloud-Service-Lieferanten	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 Cloud-Service-Portal im Sinne einer Leistungs- bzw. Produktbeschreibung des Cloud-Services.
Cloud-Service-Portal (CSP)	Zentraler Anlaufpunkt für die Öffentliche Verwaltung und deren IT-Dienstleister zur Beschaffung und Verwaltung von Cloud-Services. Es soll seinen Nutzenden ermöglichen, Cloud-Services zu bestellen, zu kündigen und Informationen über bereitgestellte Cloud-Services zu erhalten. Das Cloud-Service-Portal besteht aus mehreren technischen Komponenten (wie z. B. IAM), die gemeinsam das CSP-Ökosystem bilden.
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.
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.
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

Begriff	Erläuterung
	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.
CSP-AGB	Allgemeine Geschäftsbedingungen des Cloud-Service-Portals.
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.
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.

Begriff	Erläuterung
Intermediär	Vertragspartner des Cloud-Service-Anbieters und (spiegelbildlich) des Cloud-Service-Kunden im Umklappvertragsmodell.
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 Rechner-Verbund, der für den Betrieb von containerisierten Softwarelösungen zuständig ist.
Kunden-Service-Integratoren	Kunden-Service-Integratoren unterstützen bei der Integration von über das Cloud-Service-Portal bezogenen Cloud-Services in die Umgebung des Cloud-Service-Kunden.
Multi-Cloud	Die Nutzung mehrerer Cloud-Services verschiedener Cloud-Service-Anbieter in einer einzigen heterogenen Architektur durch einen Cloud-Service-Kunden.
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	Open Source und Open-Source-Software sind Lösungen, die Lizenzen für eine i. d. R. unentgeltliche Nutzung, Anpassung und Weitergabe nutzen und den Quelltext der jeweiligen Software offenlegen.
OS-Plattform der Öffentlichen Verwaltung „Open CoDE“	(Internet-)Plattform der öffentlichen Verwaltung, die aus einem zentralen und durchsuchbaren Verzeichnis an 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.

Begriff	Erläuterung
Pipeline	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 den Menschen lesbarer, in einer Programmiersprache verfasster Beschreibungstext einer Software. Dieser Text beschreibt die Software exakt und vollständig, sodass dieser vollständig automatisch von einem Computer in Maschinensprache übersetzt werden kann.
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.
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.

Begriff	Erläuterung
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)⁴⁸ mit der Erarbeitung der Zielarchitektur der Deutschen Verwaltungscloud (DVC) beauftragt. Seit der initialen Beauftragung wurde das Rahmenwerk der Zielarchitektur kontinuierlich fortgeschrieben. Die vorliegende Version 3.0 wurde im Rahmen des Umsetzungsprojekts DVC erarbeitet.⁴⁹ 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.⁵⁰

6.2.2 Anmerkungen zur ersten Fortschreibung (Version 2.0)

Mit der ersten Fortschreibung des Rahmenwerks zur Version 2.0 wurden substantielle 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.

48 AG Cloud Computing und Digitale Souveränität: <https://www.it-planungsrat.de/foederale-zusammenarbeit/gremien/ag-cloud-computing-und-digitale-souveraenitaet>.

49 Beschluss 2023/19 – Umsetzungsprojekt Deutsche Verwaltungscloud-Strategie, in: IT-Planungsrat, 04.07.2023, <https://www.it-planungsrat.de/beschluss/beschluss-2023-19>.

50 Beschluss 2021/46 – Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur, in: IT-Planungsrat, 29.10.2021, <https://www.it-planungsrat.de/beschluss/beschluss-2021-46>.

- **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 Open CoDE⁵¹ ein wichtiger Baustein in der Systematik der DVC integriert.

Das Rahmenwerk der Zielarchitektur wurde in der Version 2.0 in der 39. Sitzung des IT-Planungsrats beschlossen.⁵²

6.2.3 Anmerkungen zur zweiten Fortschreibung (Version 2.5)

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

- **Ergebnisübersicht des Minimum Viable Product (MVP):** Das MVP-Projekt wurde im Februar 2023 erfolgreich abgeschlossen. Im Projekt wurden 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.

51 Open CoDE: <https://opencode.de/de>.

52 Beschluss 2022/47 – Deutsche Verwaltungscloud-Strategie: Rahmenwerk der Zielarchitektur, in: IT-Planungsrat, 10.11.2022, <https://www.it-planungsrat.de/beschluss/beschluss-2022-47>.

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)

Das vorliegende Rahmenwerk der Zielarchitektur in der 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, 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 wesentlichen Eckpunkte der DVC-Vertragsmodalitäten beschrieben.

- Einbindung verwaltungsexterner Anbieter: Im neuen Unterkapitel werden zukünftig Rahmenbedingungen für die Integration verwaltungsexterner Angebote detaillierter beschrieben.

Abbildungsverzeichnis

Abbildung 1:	Zentrale Rollen und Akteure in der Deutschen Verwaltungscloud (illustrative Darstellung).....	19
Abbildung 2:	Direktvertragsmodell	27
Abbildung 3:	Direktvertragsmodell mit Cloud-Service-Beschaffer	27
Abbildung 4:	Umklappvertragsmodell.....	28
Abbildung 5:	Umklappvertragsmodell mit Cloud-Service-Beschaffer	28
Abbildung 6:	Säulen der DVC-Architektur.....	30
Abbildung 7:	Kontext des Reifegradmodells	42

Tabellenverzeichnis

Tabelle 1:	Reduktion von Abhängigkeiten.....	32
Tabelle 2:	Entwicklung und Inbetriebnahme.....	33
Tabelle 3:	Betrieb	34
Tabelle 4:	Angebot von Cloud-Services	36
Tabelle 5:	Sicherstellung und Stärkung von Datenschutz und Informationssicherheit.....	39
Tabelle 6:	Optimierung von Datenaustausch, -speicherung und -nutzung.....	40
Tabelle 7:	Glossar.....	49