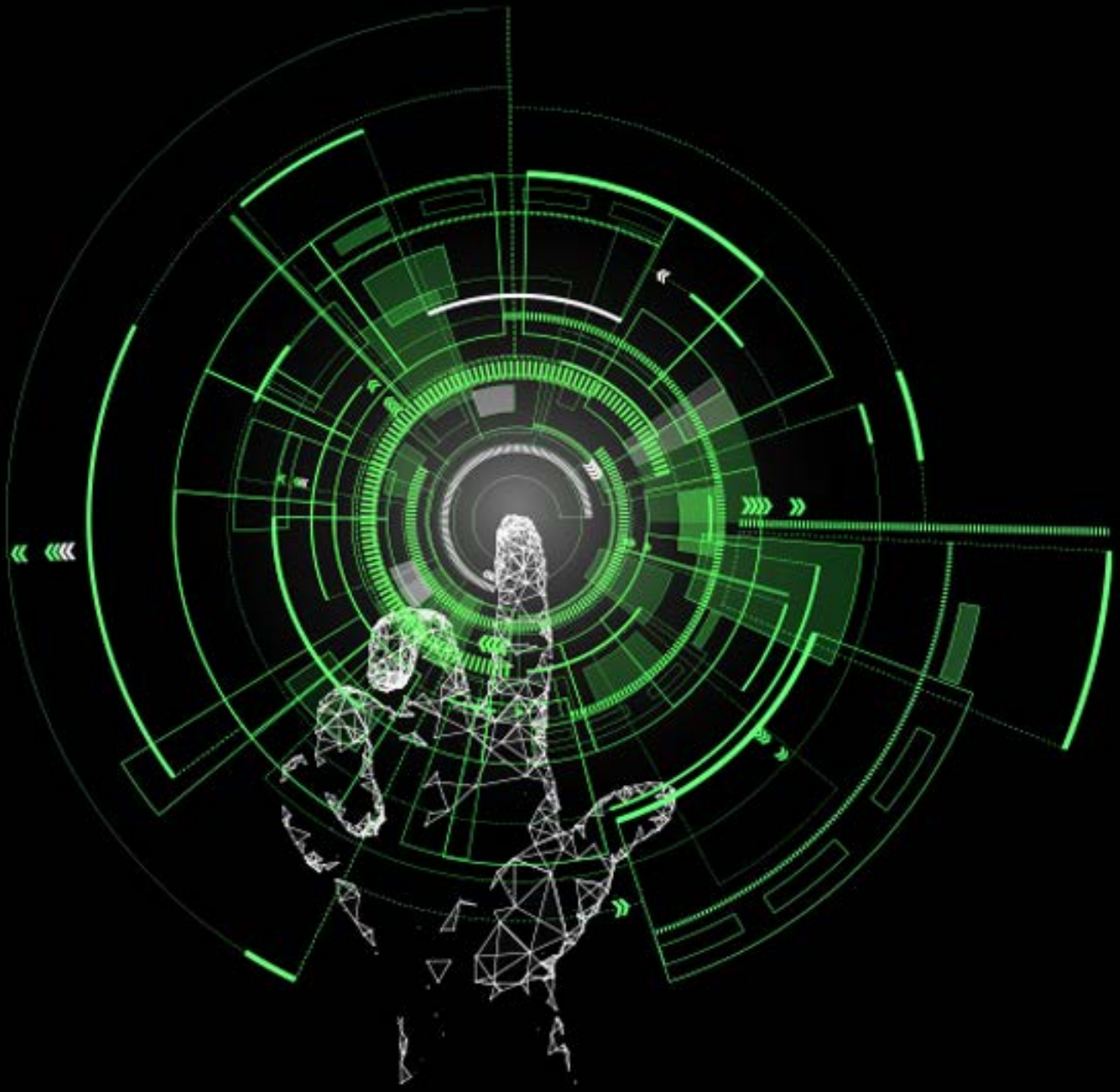
Deloitte.



Die Cloud in der öffentlichen Verwaltung möglich machen

MAKING AN IMPACT THAT MATTERS since 1845

Mit der Cloud den Digitalisierungsschub meistern

Der öffentlichen Verwaltung in Deutschland bietet sich derzeit die große Chance, in der digitalen Transformation einen deutlichen Sprung vorwärts zu machen. Die Pandemie hat die Defizite in der operativen Umsetzung der Digitalisierung im öffentlichen Sektor klar vor Augen geführt. Lockdown-bedingte Schließungen von beispielsweise Bürgerämtern haben sowohl Entscheidungsträger:innen in Politik und Verwaltung als auch der Bevölkerung die Dringlichkeit des Themas verdeutlicht. Die Erwartungen von Unternehmen und Bürger:innen an einen digital leistungsfähigen Staat sind höher denn je. Gleichzeitig startet das Onlinezugangsgesetz (OZG) in diesem Jahr in die entscheidende Umsetzungsphase. Zusätzlich werden die Digitalisierungsbemühungen der öffentlichen Verwaltung durch eine Milliardenförderung aus den Corona-Konjunkturpaketen des Bundes und der Europäischen Union (EU) beflügelt, die umfangreiche Fördermaßnahmen in den Bereichen Smart City, Smart Region und der Registermodernisierung vorsehen.

Allerdings stoßen die großzügigen Fördermittel und die zahlreich initiierten Digitalisierungsinitiativen in der Realität des öffentlichen Dienstes häufig auf nur begrenzt vorhandene personelle Ressourcen und teils technologisch veraltete Infrastrukturen. Für einen echten Digitalisierungsschub bedarf es also mehr als nur monetärer Förderung und guter Ideen: Führende Staaten in der Digitalisierung der öffentlichen Verwaltung, wie etwa Dänemark oder auch die Niederlande, adaptieren innovative Technologien besonders schnell und umfangreich.[1] Die öffentliche Verwaltung in Deutschland tut sich mit der Adaption neuer technologischer Möglichkeiten meist vergleichsweise schwerer, so insbesondere auch mit dem Einsatz von Cloud-Technologie. Dabei bietet besonders die Nutzung der Cloud ein großes Potenzial für die Digitalisierung und damit auch zur schnellen und flexiblen Skalierung von staatlichen Dienstleistungen.

Neben der Schaffung von grundlegenden E-Government-Angeboten gilt es auch bei Zukunftsthemen wie dem Einsatz von künstlicher Intelligenz oder Big Data, den Anschluss nicht zu verlieren. Dafür sind mehr Freiräume im operativen Betrieb und eine höhere Flexibilität in der Realisierung von IT-Lösungen erforderlich. Dabei ist der Einsatz neuer Technologien zwar bedachtsam abwägend, jedoch gleichzeitig auch Chancen nutzend zu betrachten. Der Normenkontrollrat mahnt in seinem fünften Monitor Digitale Verwaltung den Einsatz von industriellen Produktionsmustern an, zum Beispiel auf Basis von Low-Code-Plattformen, um somit „die Schnelligkeit von Softwareentwicklungen [zu] erhöhen". Gleichzeitig geht es nach Auffassung des Normenkontrollrates darum, die „Nachnutzung" dieser Lösungen zu „vereinfachen" sowie „Innovationskraft und Wettbewerb" aufrechtzuerhalten.[2]

Wenn es um das Thema staatliche Cloud-Nutzung geht, wird in diesem Zusammenhang in Brüssel und Berlin berechtigterweise auch intensiv über die digitale (Daten-)Souveränität Europas und des Staates und darüber diskutiert, wie man sie in der Cloud garantieren kann. In dieser Debatte bemängeln viele Akteure eine sich steigernde Abhängigkeit gegenüber den großen, meist amerikanischen oder chinesischen Cloud-Anbietern. Fakt ist jedoch auch, dass deutsche Unternehmen auf diesem Markt aktuell eine sehr untergeordnete Rolle spielen. Die Inanspruchnahme von Cloud-Angeboten nicht-deutscher bzw. außereuropäischer Anbieter scheint in einigen Anwendungsfeldern daher nahezu unvermeidlich. Insbesondere vor dem Hintergrund der Notwendigkeit zur Einhaltung des europäischen Datenschutzes (DS-GVO) und nationaler Datenschutzregeln wird dies

als problematisch angesehen. Dies gilt umso mehr seit der Außerkraftsetzung des Privacy-Shield-Abkommens sowie dem damit einhergehenden Fehlen eines entsprechenden, gültigen Rechtsrahmens in der Beziehung mit den USA.[3]

Auf der einen Seite steht also das Risiko eines möglicherweise weiteren Zurückfallens in der digitalen Transformation der öffentlichen Verwaltung, auf der anderen Seite droht eine potenziell hohe Abhängigkeit von den großen Cloud-Anbietern aus Übersee, ausgelöst durch sogenannte Lock-in-Effekte in der Cloud. Ein solcher Effekt tritt ein, wenn es den Cloud-Nutzer:innen nur schwer möglich ist, ihre Daten oder Anwendungen aus der einen Cloud heraus auf andere Infrastrukturtypen oder zwischen unterschiedlichen Cloud-Anbietern zu verschieben.

Wie lässt sich dieses Dilemma auflösen? Diese Publikation zeigt unterschiedliche Lösungsansätze zur Vermeidung des Lock-in-Effekts sowie Möglichkeiten zur Nutzung von Multi-Cloud-Architekturen auf, die ein Wechseln zwischen einzelnen Cloud-Anbietern erleichtern.

Neben der Schaffung von grundlegenden E-Government-Angeboten gilt es auch bei Zukunftsthemen wie dem Einsatz von künstlicher Intelligenz oder Big Data, den Anschluss nicht zu verlieren. Dafür sind mehr Freiräume im operativen Betrieb und eine höhere Flexibilität in der Realisierung von IT-Lösungen erforderlich. Dabei ist der Einsatz neuer Technologien zwar bedachtsam abwägend, jedoch gleichzeitig auch Chancen nutzend zu betrachten.

Grundlagen des Cloud-Computings

Das Cloud-Computing ist ein Outsourcing-Modell und besteht aus IT-Infrastrukturen, -Plattformen oder -Anwendungen, die als Dienst auf gemeinsam genutzten Betriebsmitteln bereitgestellt und nutzungsabhängig abgerechnet werden.

Große private Unternehmen, die Cloud-Lösungen anbieten und sich auf die „Bereitstellung von IT-Ressourcen (Provisioning), wie Rechenkapazität, Speicher und Kommunikationsnetze sowie grundlegender Dienste“[4] konzentrieren, werden Hyperscaler genannt. Zu den bekannten Hyperscalern zählen die US-amerikanischen Cloud-Anbieter Amazon, Google, Microsoft oder Alibaba aus China. In Europa fällt alleinig der französische Anbieter OVH in die Kategorie der Hyperscaler, der Abstand zur Konkurrenz aus den USA und China ist allerdings sehr groß. Allein die größten drei marktführenden amerikanischen Anbieter teilen mehr als die Hälfte des Gesamtmarkts unter sich auf.[5]

Funktional werden Cloud-Computing-Dienste in eine von drei Service-Kategorien eingeordnet:

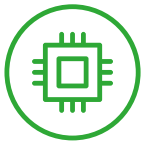
Abb. 1 – Servicekategorien des Cloud-Computings

Software als Dienstleistung
Software as a Service (SaaS)

Bereitstellung von Anwendungen als Dienstleistung über das Internet

IT-Infrastruktur als Service
Infrastructure as a Service (IaaS)

Bereitstellung von IT-Betriebsmitteln, z.B. Rechenleistung oder Speicherplatz, um Anwendungen zu betreiben und sie über das Internet verfügbar zu machen



Virtuelle IT-Plattform
Platform as a Service (PaaS)

Schließung der Lücke zwischen Applikations- (SaaS) und Infrastrukturangebot (IaaS) durch Bereitstellung von standardisierten Plattformen und Entwicklungsumgebungen, auf denen Kunden Anwendungen entwickeln, betreiben und auch anbieten können

Abb. 2 – Cloud-Typen

Öffentliche (Public) Cloud

Bezug von öffentlichen Cloud-Computing-Diensten, welche für zahlreiche Nutzer:innen auf einer gemeinsamen Infrastruktur erbracht werden. Der thematische Schwerpunkt dieser Publikation zielt in erster Linie auf die spezifischen Merkmale der Public Cloud ab.

Private Cloud

Betrieb einer eigenen Cloud-Umgebung/eigener Cloud-Computing-Dienste auf einer privaten Infrastruktur. Technologisch werden somit viele Eigenschaften einer Cloud umgesetzt, z.B. hohes Maß an Virtualisierung, Service-Orientierung, Standardisierung und Automatisierung. Durch die Nutzung dedizierter Infrastruktur ist jedoch die Skalierungsfähigkeit oft begrenzt und es entfallen die Effizienzvorteile gemeinsam genutzter Ressourcen.

Hybrid Cloud

Mischung aus den beiden genannten Betriebsmodellen für Cloud-Computing, z.B. eine Private Cloud, welche mit einem oder mehreren Public-Cloud-Services kombiniert wird.

Vorteile und Herausforderungen für den öffentlichen Sektor

Der öffentlichen Verwaltung bietet die Nutzung von Cloud-Technologie zahlreiche Vorteile. Dabei sind vor allem eine höhere Flexibilität, Effizienz, Produktivität und Skalierbarkeit ihrer (Verwaltungs-)Dienste und Vorgänge als auch geringere IT-Betriebskosten zu nennen.

- **Flexibilität**
  Die Cloud ermöglicht es, flexibel und kurzfristig Ressourcen zu beanspruchen oder abzugeben. Hierdurch wird den öffentlichen IT-Dienstleistern ein höheres Maß an bedarfsorientierter Servicebereitstellung ermöglicht. Auch die Chance zur stärkeren Fokussierung auf die eigentliche Kernaufgabe kann durch die gewonnene Flexibilität wahrgenommen werden.

- **Effizienz**
  Der Aufwand für Beschaffung, Installation, Konfiguration und Wartung von Hardware und Software wird durch Cloud-Dienste wesentlich reduziert. Dadurch werden IT-Dienstleister und Fachabteilungen der öffentlichen Verwaltung entlastet und können sich somit stärker auf den Kern ihrer Geschäftstätigkeit konzentrieren.

- **Produktivität**
  Die Nutzerfreundlichkeit vieler cloudbasierter Anwendungen ist höher, da die Prozesse in den Hintergrund verschoben werden, die nicht unmittelbar für den Zweck der Anwendung erforderlich sind.

- **Skalierbarkeit**
  Virtuelle IT-Ressourcen stehen in der Cloud jederzeit in beliebigem Umfang zur Verfügung – Speicherplatz, Prozessorleistung, Arbeitsspeicher oder Software-Lizenzen können hinzugefügt und auch wieder abgegeben werden. Hierdurch wird insbesondere ein kurzfristiges oder temporäres Hochfahren von IT-Systemen ermöglicht, wie es beispielswiese in Krisensituationen benötigt werden kann.

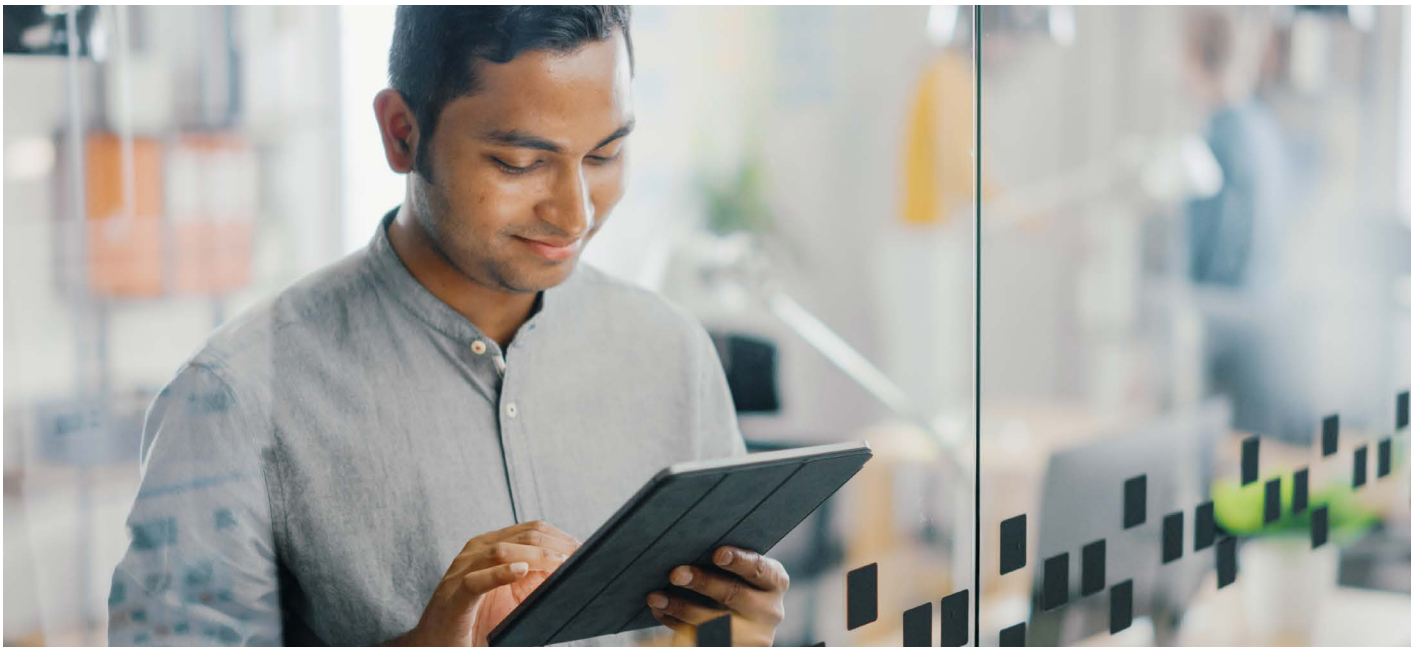
- **Wirtschaftlichkeit**
  Eine Reihe von Investitionen in IT-Infrastruktur, die sonst Investitionskapital binden würden, entfällt. Durch die Möglichkeit zur bedarfsgerechten und temporären Nutzung von IT-Ressourcen kann zudem ein Aufbau von überdimensionierten IT-Kapazitäten vermieden werden.

- **Nachhaltigkeit**
  Wird auf Dienstleister mit emmissionsarmen bzw. -freien Rechenzentren zurückgegriffen, trägt die Verwaltung ebenso zu einem nachhaltigen öffentlichen Sektor bei. Emissionsarme bzw. -freie Rechenzentren sind einfacher von dezentralen Anbietern zu betreiben.

Den zahlreichen Vorteilen stehen allerdings auch einige Herausforderungen gegenüber, die in besonderer Weise für das sensible Umfeld der öffentlichen Verwaltung gelten. Vor allem ein starker Datenschutz sowie Fragestellungen der digitalen Souveränität nehmen hier eine prominente Rolle ein.

- **Rechtssichere Beauftragung und Beschaffung**
  Die gängigen Vertragsarten der öffentlichen Beschaffung decken die üblichen Modalitäten von Cloud-Computing gegenwärtig nur unzureichend ab. Üblicherweise kommen hier die „ergänzenden Vertragsbedingungen für die Beschaffung von IT-Leistungen“ (EVB-IT) zum Einsatz. Die Standard-Nutzungsbedingungen von beispielsweise Hyperscalern sind hier jedoch noch nicht vorgesehen, EVB-IT für SAAS-Lösungen sind noch nicht vorhanden. Die Anpassung der EVB-IT an die Besonderheiten von Cloud-Diensten steht aufseiten des Bundes bisher noch aus.

- **Datenschutz und IT-Sicherheit**
  Anwendungen und Daten der öffentlichen Verwaltung unterliegen aus gutem Grund strengen Schutz- und Compliance-Anforderungen. So sind beispielsweise viele Daten ausfuhrbeschränkt oder Dienste als kritische Infrastruktur klassifiziert oder es werden gar im



Sinne des Geheimschutzhandbuchs als Verschlusssachen eingestufte Informationen verarbeitet. Es besteht also die Herausforderung, für Anwendungen und Daten der öffentlichen Verwaltung ein geeignetes Schutz- und Vertrauensniveau in der Cloud sicherzustellen.

- **IT-Strategie**
  Die bestehenden Lösungen großer Anbieter schaffen oftmals proprietäre Ökosysteme innerhalb der eigenen Plattform. Dies geht mit dem Risiko eines Lock-in-Effekts einher. Dadurch besteht die Herausforderung, kurzfristige Vorteile gegen langfristige strategische Risiken abzuwägen.

Deloitte-Projekt im Bereich Cloud im Public Sector

- Deloitte hat für die European Blood Alliance und die DG SANTE der Europäischen Kommission eine EU-weite Datenbank in einer Public Cloud entwickelt, welche die Organisation beim Kampf gegen die COVID-19-Pandemie unterstützt.
- Die Datenbank verfolgt rekonvaleszente Plasmaspenden und Transfusionen. Da Studien durchgeführt werden, um festzustellen, ob Rekonvaleszenzplasma von genesenen COVID-19-Patienten akut am Virus Erkrankten helfen kann, war das gesamte Spendenmodell zu berücksichtigen.
- Die Plattform umfasst daher den durchgängigen Prozess: die relevanten Details derjenigen, die ihr Plasma spenden (wie Geschlecht und Alter), die jeweilige Phase der klinischen Studien u.v.m. – unter Beachtung der DS-GVO und anderer Datenschutzbestimmungen durch Anonymisierung der Daten.
- Innerhalb von drei Wochen nach der Anfrage haben wir eine praktische Lösung entwickelt. Die erste Iteration fand in kleinerem Maßstab statt, wobei nur zwei bis drei Blutspendeeinrichtungen bedient wurden, nun sind es weit mehr als 100 Einrichtungen sowie Tausende registrierte Spender.
- Hier finden Sie das interaktive Dashboard der EU: https://www.euccp.dataplatform.tech.ec.europa.eu

Den Cloud-Einsatz in der öffentlichen Verwaltung aktiv gestalten

Cloud Bestrebungen der EU

Die EU hat sich das Ziel gesetzt, ihre digitale Souveränität im Bereich Cloud-Computing deutlich zu steigern. Zusätzlich bzw. viel mehr ergänzend zu den amerikanischen oder chinesischen Hyperscalern sollen alternative Cloud-Angebote geschaffen werden, die die Einhaltung europäischer Prinzipien und Datenschutzregeln in den Fokus rücken. Verschiedene europäische Akteure und Initiativen entwickeln hier unterschiedliche Ansätze mit besonderer Zielsetzung der Vermeidung von Lock-in-Effekten in der Cloud.

Die Datenstrategie[6] der Europäischen Kommission sieht vor, europäische Datenräume in der Cloud für neun Sektoren, u.a. auch für die öffentlichen Verwaltungen Europas, zu schaffen. Dieses Projekt wird sowohl legislativ mit Gesetzesvorschlägen (Data Governance Act[7] und Data Act[8]) als auch mit finanziellen Mitteln gestützt. Insgesamt sollen bis zum Jahr 2027 10 Milliarden Euro in eine europäische Cloud-Infrastruktur investiert werden – die geplanten Mittel stammen aus dem EU-Haushalt, dem EU-Konjunkturpaket „Next Generation EU", den Haushalten der Mitgliedsstaaten sowie Investitionen der Privatwirtschaft. Die Mitgliedsstaaten der EU haben mit der Gründung der „European Alliance on Industrial Data and Cloud" – einer Public Private Partnership – die Datenstrategie der EU-Kommission noch weiter untermauert. Kernpunkt dieser Allianz ist die gemeinsame Definition technischer Lösungen und Richtlinien bezüglich des Einsatzes von Cloud-Technologien.[9] Mit ihrem „2030 Digital Compass" ergänzt die EU-Kommission ihre Cloud-Vorhaben, indem sie hier einen starken Fokus auf die digitale Bildung der europäischen Bürger setzt, insbesondere im Bereich Datennutzung und Cloud.[10]

Jüngst wurde außerdem der EU Cloud Code of Conduct (CoC) offiziell genehmigt. Parallel hierzu wurde SCOPE Europe offiziell als Überwachungsstelle akkreditiert, die mit der Überwachung des Verhaltenskodex beauftragt ist.[11] Der CoC ist der erste länderübergreifende Kodex, der für alle Cloud-Angebote in der EU genehmigt wurde. Er wird es den Nutzern von Cloud-Diensten – insbesondere KMUs, öffentlichen Einrichtungen und Behörden – einfach machen, festzustellen, ob ein bestimmter Cloud-Dienst DS-GVO-konform und somit im Umgang mit personenbezogenen Daten nutzbar ist. Dies ist ein wichtiger Schritt für den Ausbau der Cloud-Nutzung in der öffentlichen Verwaltung, da durch den CoC nun das Vertrauen in solche Dienste gestärkt und das Niveau des Datenschutzes auf dem europäischen Cloud-Computing-Markt angehoben wird. Dies trägt dazu bei, die Einführung dieser Schlüsseltechnologie zu beschleunigen und die Vorteile des Cloud-Computings einem größeren Teil der europäischen Wirtschaft sowie der öffentlichen Verwaltung zugänglich zu machen.[12]

Das US-amerikanische Federal Risk and Authorization Management Program (FedRAMP) wurde 2011 ins Leben gerufen, um einen kosteneffizienten, standardisierten und risikobasierten Ansatz für die Sicherheitsbewertung, Einführung und Nutzung von Cloud-Diensten durch die amerikanischen Bundesbehörden zu schaffen. FedRAMP befähigt Behörden, moderne Cloud-Technologien zu nutzen, wobei der Schwerpunkt auf der Sicherheit und dem Schutz von Bundesinformationen liegt.[13]

Mit der europäischen Initiative GAIA-X sollen Unternehmen und die öffentliche Verwaltung durch die Schaffung von Wahlmöglichkeiten zwischen verschiedenen Anbietern auf Basis einheitlicher Datenaustauschstandards in die Lage versetzt werden, digitale Souveränität zu erlangen. Gleichzeitig werden mit GAIA-X auch industriepolitische Ziele verfolgt, die auf eine Stärkung des europäischen Industrie-4.0-Sektors abzielen.[14] Organisatorisch ist GAIA-X als internationale Non-Profit-Organisation mit Sitz in Brüssel registriert. Der politische Anstoß hierzu kam aus Frankreich und Deutschland, woher auch die ersten 22 Mitgliedsunternehmen kommen. Im Jahr 2021 sollen weitere, zunächst europäische Unternehmen hinzukommen. Die Tür steht jedoch auch für Unternehmen aus Drittstaaten offen – so zum Beispiel den genannten Cloud-Hyperscalern.

GAIA-X soll ein Infrastruktur- und Datenökosystem nach europäischen Werten und Standards bieten. Die Architektur von GAIA-X ist so erdacht, dass digitale Prozesse und Informationstechnologie eingesetzt werden, um eine Verbindung zwischen allen Akteuren der europäischen digitalen Wirtschaft herzustellen. Die oberste Prämisse ist dabei laut GAIA-X die Erreichung bzw. das Erhalten der europäischen Datensouveränität, welche die Organisation wie folgt definiert: „Daten-Souveränität ist die Ausführung der vollen Kontrolle und Steuerung durch einen Dateneigentümer über den Speicherort und die Verwendung der Daten." Basierend auf einem Open-Source-Prinzip vernetzt die GAIA-X-Infrastruktur dezentrale und zentrale Dateninfrastrukturen zu einem gemeinsamen System. Damit können sektorale Datenräume in der GAIA-X-Infrastruktur geschaffen werden, in denen die Nutzer:innen ihre Daten einspielen. Dies soll gemeinsame Big-Data-Projekte von unterschiedlichen Stakeholdern zur Effizienzgewinnung, beispielsweise bei der Steuerung des Verkehrs oder der Schaffung neuer Produkte oder Dienstleistungen ermöglichen.[15] Da es sich dabei um eine Dateninfrastruktur handelt, auf der verschiedenste Mitglieder ihre Cloud-Lösungen anbieten werden, wird GAIA-X in den nächsten Jahren voraussichtlich einen positiven Beitrag zur Vermeidung von Lock-in-Effekten in Europa leisten.

Lösungsansätze zur Vermeidung von Cloud-Lock-in-Effekten werden bei GAIA-X von Unternehmen entwickelt. Als ein vielversprechendes Beispiel ist hier das finnische Start-up Aiven zu nennen. Aiven will seinen Kunden Unabhängigkeit von einzelnen Hyperscalern ermöglichen und ihnen „per Klick" einen unkomplizierten Wechsel zwischen unterschiedlichen Cloud-Anbietern ermöglichen.[16] Mit der Entwicklung einer Art „unabhängigem Betriebssystem für die Cloud managt Aiven die Datenströme von Unternehmen mithilfe von Open-Source-Software und kann dafür die Rechenleistung beliebiger Cloudanbieter nutzen"[17]. Aiven möchte sich mit seiner Dienstleistung nicht gegen die bekannten Hyperscaler oder GAIA-X stellen, sondern viel mehr komplementär zu ihnen wirken. Dadurch sollen bei potenziellen Cloud-Nutzern Eintrittsbarrieren und Ängste bezüglich der Nutzung der Technologie abgebaut werden. Auch die Initiatoren von GAIA-X scheinen Lösungsansätze für hybride Cloud-Systeme, Beispiel Aiven, nicht als Konkurrenz zu GAIA-X zu bewerten, sondern äußern ganz gegenteilig, dass es zu begrüßen sei, „dass solche Anbieter Innovationen in den Markt bringen und sich aktiv an GAIA-X beteiligten"[18].

Vermeidung von Lock-in-Effekten in der Cloud

Cloud in Digital- und IT-Strategien

Die Digital-Strategie und die IT-Strategie sollten am Ausgangspunkt für die Bestimmung potenzieller Einsatzbereiche von Cloud-Technologie in der öffentlichen Verwaltung stehen. Darin sollten die strategischen Ziele der (IT-)Organisation sowie ein Plan zum Aufbau des Produkt- und Serviceportfolios enthalten sein. Diese sollten sich immer an den individuellen Geschäftsanforderungen sowie -risiken ausrichten und möglichst spezifisch auf die jeweilige Organisation bzw. Organisationseinheit zugeschnitten sein.

Die IT-Strategie sollte dabei auch Anforderungen und Rahmenbedingungen in Bezug auf den Einsatz bzw. die Nutzung von Cloud-Angeboten ableiten. Die Festlegung und Durchsetzung von einheitlichen Rahmenbedingungen für den Cloud-Einsatz von IT-Dienstleistern und Fachabteilungen der öffentlichen Verwaltung ist ein wesentlicher Erfolgsfaktor für den Einsatz von Cloud-Technologie. Oftmals berücksichtigen IT-Strategien in der öffentlichen Verwaltung den Umgang mit Cloud-Technologien noch nicht ausreichend oder sind nicht in dem erforderlichen Maße auf die spezifischen Anforderungen der jeweiligen Organisation angepasst. Dies sollte durch die Erweiterung bestehender Festlegungen oder die Formulierung einer spezifischen Cloud-Strategie nachgeholt werden.

Datenschutz und Datensicherheit

In der öffentlichen Verwaltung sollten ein effektiver Datenschutz und eine hohe Datensicherheit bereits frühzeitig Schwerpunkte in der Betrachtung von Cloud-Computing sein und entsprechende Leitlinien strategisch verankert werden. In der Operationalisierung des Cloud-Einsatzes in der öffentlichen Verwaltung sind besonders folgende Aspekte zu beachten.

- Datenschutz: Im Rahmen der Beauftragung und des Einsatzes von Cloud-Computing gilt es, die datenschutzrechtlichen Rollen der Beteiligten zu ermitteln und die Anforderungen durchgehend einzuhalten. Häufig wird insbesondere der Abschluss einer Vereinbarung zur Auftragsverarbeitung mit dem Anbieter gemäß Art. 28 DS-GVO erforderlich sein.

- Datensicherheit: Verschlüsselungen und Anonymisierungen sind übliche Maßnahmen zur Erhöhung der Sicherheit und sollten „by Design", also bereits bei der Konzipierung und Entwicklung von IT-Architekturen berücksichtigt werden.

- Drittstaatentransfer: Seit der Europäische Gerichtshof mit seinem Schrems-II-Urteil den EU-US Privacy Shield gekippt hat, wird insbesondere der Einsatz von Cloud-Lösungen mit Bezug zu den USA kritisch. Ein Datentransfer aus der EU kann insofern auch dann gegeben sein, wenn zwar die Daten in der EU gehostet und verarbeitet werden, aber z.B. zum Zwecke der Wartung oder des Supports auf diese Daten aus einem Drittland zugegriffen wird. Im Hinblick auf mögliche Drittstaatentransfers ist im Einzelfall zu prüfen, welche möglichen Garantien (z.B. sog. Standard Contract Clauses, technische-organisatorische Maßnahmen) hier implementiert werden können, um das Thema datenschutzrechtlich konform umzusetzen. In der öffentlichen Verwaltung ist jedenfalls eine Lokalisierung der Server in Deutschland oder mindestens in der EU stets zu empfehlen.

- Betriebssicherheit: Wie bei lokalen Infrastrukturen muss auch in der Cloud ein fortlaufender Betrieb sichergestellt werden. Entscheidend dafür sind robuste Komponenten in den Servern und Speichersystemen sowie Redundanzen der zentralen Infrastrukturbestandteile. Dies sollte bei der Planung bedacht und von Dienstanbietern nachgewiesen werden.

- Zertifizierung: Cloud-Anbieter können mithilfe geeigneter Zertifizierungen Qualität und Einhaltung von Standards in verschiedensten Bereichen nachweisen. Hier existiert eine Vielzahl an Zertifizierungen, darunter Nachweise über Datenschutz sowie Daten- und Betriebssicherheit. Durch die Vielfalt der möglichen Zertifizierungen sollten bei der Anbieterauswahl die Erfüllung der im Anwendungsfall relevanten Standards geprüft und Empfehlungen, insbesondere durch das Bundesamt für Sicherheit in der Informationstechnik (BSI), beachtet werden.

Klassifizierung von möglichen Cloud-Diensten

Vor dem Gang in die Cloud stellt sich die Frage, welche Dienste und Daten der IT-Landschaft sinnvollerweise in die Cloud migriert werden können bzw. sollten. Hier spielen verschiedene Faktoren eine Rolle. Beispielhaft zu nennen sind vor allem der Grad der Standardisierung eines Dienstes und die Anforderungen an den Datenschutz sowie die Sicherheit der Daten. Zur Schaffung von Kriterien zur Klassifizierung von Diensten und Daten sollte auf existierende Standards für die öffentliche Verwaltung zurückgegriffen werden, darunter insbesondere die „Mindeststandards des BSI zur Nutzung externer Cloud-Dienste" sowie „Vorgehensweise und Kriterien zu Inanspruchnahme und Beschaffung von Cloud-Diensten der IT-Wirtschaft" des IT-Planungsrats.

Die spezifische Klassifizierung ist auf Basis der individuellen Anforderungen der jeweiligen Organisation zu entwickeln, da eine übergreifende Standardisierung in Deutschland aktuell noch aussteht. Als Orientierung für eine solche Standardisierung kann beispielsweise das amerikanische FedRAMP (s. Infobox 4) dienen.

Multi-Cloud-Architektur

Um einem potenziellen Lock-in-Effekt entgegenzuwirken, ist die Architektur der IT-Landschaft einer Organisation entsprechend auszurichten. Eine geeignete Multi-Cloud-Architektur ist dabei oft der Schlüssel. Durch die Nutzung mehrerer Cloud-Dienste und die Verteilung von Daten und Diensten auf verschiedene Anbieter wird eine Abhängigkeit vermieden. Durch die geeignete Lieferantensteuerung und ein leistungsfähiges Architekturmanagement kann digitale Souveränität ermöglicht, nachhaltig gewahrt und in vielen Fällen sogar ausgebaut werden.

Für die Entwicklung einer Multi-Cloud-Architektur sind die Elemente der bestehenden IT-Landschaft auf Kompatibilität und Abhängigkeiten zu prüfen. Wenn Systeme für den Betrieb mit älteren Technologien ausgelegt sind, ist die Auswahl an Cloud-Plattformen und -Infrastrukturen üblicherweise begrenzt. Falls Dienste nur mit einer begrenzten Anzahl von Technologien kompatibel sind, sollte vor einer Cloud-Migration eine Überarbeitung der Dienst-Architektur in Betracht gezogen werden.

Dabei sollte insbesondere in der öffentlichen Verwaltung auf offene Standards gesetzt werden. Viele Cloud-Anbieter unterstützen die meisten offenen Standards verschiedener Branchen. Um eine verteilte Umgebung zu steuern, haben sich mittlerweile zahlreiche Hilfsmittel etabliert, darunter eine Reihe von Multi-Cloud-Management-Tools unterschiedlicher Hersteller wie BMC Software, Cisco, IBM, Microsoft und VMware. Daneben bieten einige Drittanbieter sowie Open-Source-Projekte anpassbare Speziallösungen an. Hierzu zählen beispielsweise Nagios, SolarWinds sowie Zabbix.

Durchführung der Migration

Das Vorgehen bei der Migration von Daten und Diensten in die Cloud muss im Einzelfall festgelegt werden, um die Brücke zwischen bestehender IT-Landschaft und Zielarchitektur zu schlagen. Nur so können die digitale Transformation beschleunigt und die in der IT-Strategie gesteckten Ziele über Cloud-Plattformen erreicht werden. Viele Cloud-Anbieter haben Migrations-Frameworks für ihr Angebot geschaffen, welche, basierend auf der zuvor definierten (Multi-)Cloud-Architektur, genutzt werden sollten.

Neben dem „Gang in die Cloud" sollte auch immer ein möglicher Gang bzw. Rückzug aus der Cloud geplant und in einer Ausstiegsstrategie festgelegt werden. Cloud-Anbieter sehen häufig in den vertraglichen Konditionen Klauseln für Änderungen ihres Geschäftsmodells vor, die ein Grund für die Entscheidung zu einem Anbieterwechsel sein können. Die rechtzeitige Festlegung einer eigenen Ausstiegs- und Migrationsstrategie und dahingehenden vertraglichen Vorsorge kann dieses Risiko maßgeblich reduzieren.

Rechtssichere Beauftragung und Beschaffung

Wie an vorheriger Stelle bereits herausgearbeitet, liegt derzeit kein EVB-IT-Vertrag vor, der speziell für den Cloud-Einsatz in der öffentlichen Verwaltung geeignet ist. Zwar gibt es bereits Bestrebungen, den juristischen Rahmen hier nachzuziehen und an die Nutzungsmöglichkeit dieser Technologie anzupassen, jedoch wird momentan der Cloud-Einsatz beschaffungstechnisch oftmals noch über Individualverträge oder eine Kombination verschiedener EVB-IT-Verträge gelöst. Eine rechtssichere und einheitliche juristische Regelung für die Beauftragung und Beschaffung im Bereich Cloud sollte für die öffentliche Verwaltung so schnell wie möglich erlassen und umgesetzt werden.

„Die Nutzung von Cloud-Technologie kann einen wichtigen Beitrag dazu leisten, die Digitalisierung der deutschen Verwaltung schneller voranzutreiben. Die gezielte Vermeidung von Lock-in-Effekten ist dabei ein geeignetes Instrument zur Herstellung von digitaler Souveränität.“

Felix Dinnessen, Partner

Fazit

Die Nutzung von Cloud-Technologie kann einen wichtigen Beitrag dazu leisten, die Digitalisierung der deutschen Verwaltung schneller voranzutreiben. Der Cloud-Einsatz und darauf aufsetzende Applikationen machen es möglich, den zum Teil bereits angestoßenen, ambitionierten Vorhaben und Projekten einen zusätzlichen Schub zu geben. Für eine effiziente wie umsichtige Nutzung der Cloud im öffentlichen Sektor sind die richtigen Rahmenbedingungen und Voraussetzungen, juristisch als auch technisch, von größter Bedeutung. Darüber hinaus ist es bedeutend, mit Blick auf die Wahrung der staatlichen (Daten-) Souveränität in Europa, sich nicht in nur schwer umzukehrende Abhängigkeiten von außereuropäischen Unternehmen zu begeben.

Hier gilt es für die öffentliche Verwaltung, sich aus organisationaler als auch technischer Ebene so aufzustellen, dass Lock-in-Effekte vermieden oder zumindest eingeschränkt werden. Wichtige Eckpunkte einer Strategie zur Vermeidung solcher Auswirkungen in der Cloud hat dieser Artikel aufgezeigt. Wird die Abhängigkeit gegenüber einem einzelnen Anbieter durch Anwendung dieser Strategie reduziert, kann die digitale Souveränität gewahrt bleiben. Der im weltweiten Vergleich streng ausgelegte europäische Datenschutz sollte beim Gang in die Cloud nicht als Hindernis, sondern viel mehr als europäisches Qualitätsmerkmal gesehen werden, der die digitale Souveränität der öffentlichen Behörden und Institutionen in Deutschland und somit auch der Unternehmen und Bürger sicherstellt und schützt.

In bestimmten Bereichen des öffentlichen Sektors gilt es noch einmal, besondere Herausforderungen im Bereich der digitalen Souveränität zu beachten, so zum Beispiel im Bereich der inneren Sicherheit, der Verteidigung oder der kritischen Infrastruktur. Die nächste Publikation dieser Serie wird einen Blick auf die spezifischen Rahmenbedingungen und Herausforderungen in sicherheitsrelevanten Anwendungsszenarien werfen.

Kontakte

Peter J. Wirnsperger
Partner | Public Sector
Tel: +49 40 32080 4675
pwirnsperger@deloitte.de

Felix Dinnessen
Partner | Public Sector
Tel: +49 221 9732 4128
fdinnessen@deloitte.de

Dr. Soentje Julia Hilberg
Director | Deloitte Legal
Tel: +49 30 2546 8225
shilberg@deloitte.de

Weiterer Ansprechpartner
Mosche Orth
Public Policy Manager | EU Policy Centre
Tel: +49 151 58071859
moorth@deloitte.de

Unter Mitwirkung von:
Stella Janzen und Bastian Kalytta,
Public Sector Consulting

01. Endspurt OZG, Behörden Spiegel Newsletter, Nr. 1.064, 30.04.2021.
02. Nationaler Normenkontrollrat, Monitor Digitale Verwaltung #5, Mai 2021, abgerufen am 28.05.2021.
03. Europäische Kommission, Commercial sector: EU-US Privacy Shield, Juli 2020, abgerufen am 31.05.2021.
04. Kompetenzzentrum Öffentliche IT, Cloud-Betrieb im öffentlichen Sektor: Selbstbedienung, Automatisiert, Februar 2021, abgerufen am 28.05.2021.
05. Statista, Cloud Infrastructure Market, Februar 2021, abgerufen am 04.06.2021.
06. Europäische Kommission, Europäische Datenstrategie, Februar 2020, abgerufen am 26.05.2021.
07. Europäische Kommission, Regulation of the European Parliament and of the Council, November 2020, abgerufen am 26.05.2021.
08. Europäische Kommission, Commission proposes measures to boost data sharing and support European data spaces, November 2020, abgerufen am 26.05.2021.
09. Europäische Kommission, Towards a next generation cloud for Europe, März 2021, abgerufen am 26.05.2021.
10. Europäische Kommission, Europas Digitale Dekade: digitale Ziele für 2030, März 2021, abgerufen am 26.05.2021.
11. EU Cloud CoC, The EU Cloud Code of Conduct becomes first GDPR code of conduct to receive green light from data protection authorities, Mai 2021, abgerufen am 26.05.2021.
12. EU Cloud CoC, The EU Cloud Code of Conduct becomes first GDPR code of conduct to receive green light from data protection authorities, Mai 2021, abgerufen am 26.05.2021.
13. Federal Risk and Authorization Management Program, abgerufen am 01.06.2021.
14. Siebel, Thomas, Gaia-X bietet neue Chancen für die Industrie 4.0, Industrie 4.0, Juli 2020, abgerufen am 28.05.2021.
15. GAIA-X, GAIA-X: Technical Architecture, Juni 2020, abgerufen am 27.05.2021.
16. Handelsblatt, Start-up Aiven verspricht einen einfachen Wechsel des Cloud Anbieters, abgerufen am 28.05.2021.
17. Handelsblatt, Start-up Aiven verspricht einen einfachen Wechsel des Cloud Anbieters, abgerufen am 28.05.2021.
18. Handelsblatt, Start-up Aiven verspricht einen einfachen Wechsel des Cloud Anbieters, abgerufen am 28.05.2021.

Deloitte.

Stand 07/2021