Erleben,
was verbindet.

Public Cloud
im öffentlichen Sektor

Open
Telekom
Cloud

VORWORT

Die öffentliche Verwaltung modernisiert und digitalisiert derzeit umfassend ihre Angebote und Prozesse. Public-Cloud-Lösungen bilden einen wichtigen Baustein, um die eigenen Kapazitäten zu einer flexiblen IT-Infrastruktur zu ergänzen. Aufgrund seiner besonderen Stellung sowie aus Sicherheits- und Datenschutzgründen kann der Sektor die Angebote jedoch nur eingeschränkt und unter spezifischen Voraussetzungen nutzen.

Dieses Whitepaper bietet eine Orientierung bezüglich der Anforderungen, die Public-Cloud-Services und -Provider für den Einsatz bei Bund, Ländern und Kommunen erfüllen müssen. Die Deutsche Telekom AG (kurz „Telekom“) bringt dabei ihre langjährige Erfahrung in der Zusammenarbeit mit dem Sektor sowie bei der Umsetzung von IT-Projekten im öffentlichen Bereich ein. Dennoch kann dieses Papier das Thema Public-Cloud-Lösungen im öffentlichen Sektor nur in einem begrenzten Umfang abbilden. Es behandelt dieses also keineswegs abschließend und bildet insbesondere nur die Situation zum Zeitpunkt des Erscheinungstermins (Januar 2022) ab. Es ersetzt keine sicherheitstechnische, datenschutzrechtliche oder darüberhinausgehende juristische Beratung im Einzelfall. Trotz größter Sorgfalt bei der Erstellung übernehmen die Herausgeber keine Haftung.

Inhalt

1. Zusammenfassung

Um Angestellten und Bürgern in Zukunft bessere Services zu bieten, modernisiert die öffentliche Verwaltung derzeit mit umfangreichen Maßnahmen ihre Prozesse und Angebote. Um in diesem Zuge schnell auf neue Bedürfnisse reagieren zu können, ist eine flexible IT-Infrastruktur unerlässlich. Public-Cloud-Lösungen bieten viele Vorteile und Möglichkeiten, um die eigenen Kapazitäten unkompliziert zu ergänzen. Aufgrund ihrer besonderen Stellung kann die öffentliche Verwaltung aber nur sehr eingeschränkt Public-Cloud-Angebote wahrnehmen. So kommen beispielsweise schon aus Sicherheits- und Datenschutzgründen viele Provider gar nicht erst in Frage. Weil Bund, Länder und Kommunen ihre Aufträge regelmäßig neu ausschreiben müssen, dürfen sie sich zudem nicht fest an einen Anbieter binden. Da viele Cloud-Anbieter aber proprietäre Schnittstellen und Dateiformate betreiben, die einen Transfer der Daten im Falle eines Provider-Wechsels erschweren, können öffentliche Auftraggeber einen Vendor-Lock-In in vielen Fällen nicht ausschließen.

Behörden sind daher auf ein möglichst offenes Public-Cloud-Angebot angewiesen, das ausschließlich europäischem Recht unterliegt und alle Anforderungen der DSGVO erfüllt. Leistungen wie dezidierte Ressourcen und fortschrittliche Verschlüsselungsmethoden erhöhen das Sicherheitsniveau. Idealerweise können Betreiber das mit aussagekräftigen Zertifikaten nachweisen. Wie Bund, Länder und Kommunen von den flexiblen Leistungen einer sicheren Public Cloud profitieren, zeigen beispielsweise die zahlreichen Projekte der Open Telekom Cloud. Von der Infrastruktur für Bürger-Apps über die Digitalisierung von Verwaltungsleistungen bis hin zu geballter Rechenpower für die Forschung hat sich die Lösung in vielfältigen Szenarien des öffentlichen Sektors bewährt.

2. Einleitung:
Mit flexiblen IT-Infrastrukturen die Digitalisierung voranbringen

Die Digitalisierung im öffentlichen Sektor nimmt Fahrt auf: Mit dem Onlinezugangsgesetz (OZG) werden Bund, Länder und Kommunen ihre Verwaltungsdienstleistungen spätestens bis Ende 2022 auch digital anbieten. Bürger sollen dann die Möglichkeit haben, Dokumente wie den Personalausweis, Reisepass oder die Geburtsurkunde komplett online zu beantragen. Mehr als 500 Dienstleistungen werden die Verwaltungen im Zuge der Umsetzung digital zugänglich machen, darunter beispielsweise auch Vorgänge wie KFZ-Zulassungen oder Umzugsmeldungen. Darüber hinaus sieht das Gesetz vor, dass die bisher voneinander unabhängigen Portale von Ländern und Kommunen zu einem einheitlichen Portalverbund zusammengeschlossen werden.

Damit die Digitalisierungsmaßnahmen eine stabile Grundlage bekommen, modernisieren die Behörden auch verstärkt die Prozesse hinter der Antragsstellung. Auf Grundlage des im Frühjahr 2021 vom Bundesrat verabschiedeten Registermodernisierungsgesetzes bauen die öffentlichen Einrichtungen beispielsweise redundante Datenverarbeitung ab und schaffen eine einheitliche Identifikationsmöglichkeit für die OZG-Leistungen. So brauchen Bürger bei ihren (digitalen) Behördengängen in Zukunft nur noch ihre Steueridentifikationsnummer, statt im Kontakt mit den verschiedenen staatlichen Registern ihre Daten immer wieder aufs Neue angeben zu müssen.

Neue Technologien verbessern den Arbeitsalltag

Von der Digitalisierung in der öffentlichen Verwaltung profitieren nicht nur die Bürger, sondern auch die Mitarbeiter im öffentlichen Sektor: Moderne IT-Lösungen entlasten die Verwaltung von lästigen Routineaufgaben, machen papierbasierte Prozesse überflüssig und ermöglichen mit cloudbasierten Technologien ein flexibleres und ortsunabhängiges Arbeiten. In öffentlichen Einrichtungen mit einem hohen Digitalisierungs- und Automatisierungsgrad haben Beamte und Angestellte mehr Zeit für den Bürger: Denn sie arbeiten Bewilligungsprozesse schneller ab, haben wichtige Informationen schneller zur Hand und sind besser erreichbar.

Dass sich die Digitalisierung positiv auf die tägliche Arbeit der Mitarbeiter auswirkt, zeigen auch die aktuellen Untersuchungen zum Thema: Laut Price Waterhouse Coopers (PwC) sind 64 Prozent der Arbeitnehmer in deutschen Unternehmen davon überzeugt, dass neue Technologien ihren Arbeitsalltag verbessern[1]. Eine Umfrage der Deutsche Angestellten Krankenkasse (DAK) verdeutlicht indes, wie stark sich die Corona-Pandemie auf die positive Einstellung gegenüber der Digitalisierung am Arbeitsplatz ausgewirkt hat. Demnach ist der Anteil der Arbeitnehmer, die neue Technologien als Entlastung empfinden, während der Pandemie um 39 Prozent gestiegen[2].

Flexible IT-Infrastrukturen helfen öffentlichen Einrichtungen dabei, schnell auf die Bedürfnisse der Beschäftigten und Bürger zu reagieren. Dabei eröffnet vor allem die Public Cloud den Planern und Verantwortlichen als Ergänzung zu ihren eigenen Rechenzentren viele Chancen. Sei es die unkomplizierte Skalierung von Anwendungen für hybride Arbeitsmodelle, die schnelle Bereitstellung neuer Services oder die Erschließung innovativer Technologien auf Basis von KI – die Vorteile liegen auf der Hand. Weil die öffentliche Verwaltung aber besonders kritisch auf Aspekte wie Sicherheit und Datenschutz schauen muss, kommen Public-Cloud-Lösungen für die Behörden nur unter bestimmten Voraussetzungen in Frage.

Die folgenden Kapitel zeigen, wie Behörden die verschiedenen Anforderungen der Digitalisierung mit der richtigen Cloud-Technologie erfüllen und auf dieser Basis innovative Lösungen entwickeln, die allen Verwaltungsmitarbeitern und Bürgern einen echten Mehrwert bieten.

Nachhaltige Digitalisierung

Um eine nachhaltige Digitalisierung zu fördern, müssen öffentliche Einrichtungen an ihren IT-Infrastrukturen ansetzen. Dreh- und Angelpunkt dieser Betrachtung: der Stromverbrauch in den Rechenzentren. Denn mit dem global wachsenden Datenverkehr steigt auch der Energiebedarf konstant. Laut Untersuchungen des Uptime Institutes waren Rechenzentren im Jahr 2018 für 0,8 bis 2 Prozent des globalen Stromverbrauches verantwortlich[3]. Wer seine Ressourcen aus der Cloud bezieht, statt ein eigenes Rechenzentrum zu betreiben, profitiert von der deutlich effizienteren Auslastung, Kühlung und Energieverteilung der großen Cloud-Rechenzentren. Der Effekt: Ein kleinerer CO_2-Fußabdruck. Laut dem Eco Verband können Unternehmen ihren Energiebedarf auf diese Weise um bis zu 84 Prozent reduzieren[4].

3. Cloud im öffentlichen Sektor: Hürden und Herausforderungen

Damit Cloud-Lösungen im öffentlichen Sektor ihr volles Potenzial entfalten, ist es wichtig, die Grenzen für etwaige Projekte abzustecken. Diese werden durch eine Reihe von Vorgaben, Richtlinien und Gesetzen definiert, auf die öffentliche Organisationen verpflichtet sind. Die Strategie für einen nachhaltigen und wertschöpfenden Einsatz der Technologie muss innerhalb dieser gesetzten Koordinaten funktionieren. Um den daraus resultierenden Rahmen besser zu verstehen, blicken wir an dieser Stelle auf drei wesentliche Eckpfeiler für eine funktionierende Cloud-Strategie: Datenschutz, Vergaberecht und Anbieterunabhängkeit.

3.1 Datenschutz: DSGVO, Schrems II, Cloud Act

Der Datenschutz stellt für öffentliche Auftraggeber eine wesentliche Herausforderung bei der Nutzung von Public-Cloud-Lösungen dar. Die Organisationen verarbeiten in der Regel ein hohes Maß an personenbezogenen Informationen und müssen sich bei der Übermittlung dieser Daten im Sinne der Auftragsdatenverarbeitung an strenge Vorschriften halten. Sie sind demnach dazu verpflichtet, alle datenschutzrechtlichen Aspekte einer potenziellen Cloud-Lösung eigenverantwortlich zu kontrollieren und bleiben während der gesamten Dauer des Geschäftsverhältnisses für die Einhaltung der Anforderungen verantwortlich.

Wenn Bund, Länder oder Kommunen einen Public-Cloud-Anbieter unter diesen Gesichtspunkten beurteilen müssen, sind der Ort der Datenverarbeitung sowie der Ort des Firmensitzes des Anbieters entscheidende Faktoren. Es stellt sich zunächst die Frage, wo die Server des Cloud-Dienstleisters stehen, auf denen die Daten verarbeitet werden. Gemäß Art. 45 der DSGVO dürfen Organisationen personenbezogene Daten nur dann an ein Drittland übermitteln, wenn diese dort einem im Wesentlichen gleichwertigen Schutz unterliegen. Mit dem Urteil des Europäischen Gerichtshofes, welches das EU-US Privacy Shield für nichtig erklärte (sog. Schrems-II-Urteil), wurde klargestellt, dass in den USA diese Bedingungen nicht erfüllt sind.[5]

58 %

der Unternehmen haben ihre Cloud-Strategie infolge des Schrems-II-Urteils angepasst.[6]

Um die Folgen des Urteils aufzufangen, diskutierten viele US-Cloud-Anbieter darüber, Daten von europäischen Kunden nur noch in der EU zu speichern. Doch selbst dann wären öffentliche Institutionen einem großen Risiko ausgesetzt, könnten die US-Behörden doch auf Basis des Cloud Act Zugriff auf die Daten erwirken, sofern der Cloud-Dienstleister seinen Unternehmenssitz in den USA hat. Die öffentliche Verwaltung sollte sich daher neben einer Datenspeicherung in Deutschland auf rein europäische Provider konzentrieren.

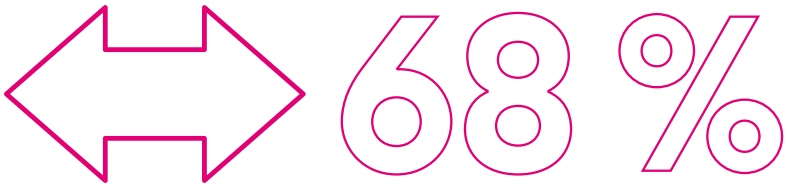
3.2. Auftragsausschreibung und Vergabeverfahren: Mehr Flexibilität gefragt

Weil sich Wirtschaft und Gesellschaft mit einem immer höheren Tempo verändern, wird die langfristige Planungssicherheit für sämtliche Akteure in Zukunft deutlich kleiner. Unvorhersehbare Ereignisse werden von der Ausnahme zur Regel. Aus diesem Grund müssen sich auch die IT-Verantwortlichen in der öffentlichen Verwaltung immer schneller auf neue Bedürfnisse und Anforderungen einstellen. Weil die Beschaffung von IT-Lösungen aber an strenge Ausschreibungs- und Vergabeverfahren gekoppelt ist, stoßen sie bei der kurzfristigen Bereitstellung von zusätzlichen Ressourcen oder neuen Diensten schnell an ihre Grenzen. So kann es beispielsweise passieren, dass es in Phasen einer unerwartet hohen IT-Auslastung zu Engpässen kommt.

Werden solche Lastspitzen nicht durch zusätzliche Kapazitäten abgefangen, kann die Leistungsfähigkeit von Anwendungen, Netzwerken und Datenbanken spürbar leiden. Das schränkt schließlich auch die Belegschaft bei ihrer Arbeit ein, so dass ganze Prozessketten ins Stocken geraten. Um ihren Geschwindigkeitsnachteil bei der Aufstockung von IT-Ressourcen wettzumachen, können Ministerien und Behörden auf Cloud-Lösungen setzen, deren Leistungen spontan und flexibel skalierbar sind. Um dafür eine entsprechende Vertragsgestaltung auf den Weg zu bringen, sollten die Verantwortlichen den Rahmen für solche Nutzungsszenarien schon in der Ausschreibungsphase setzen. So wird zum Beispiel ein kurzfristiger Leistungsabruf über speziell ausgestaltete Rahmenverträge möglich. Damit können IT-Verantwortliche die Kapazitäten in anspruchsvollen Situationen rasch hochfahren und bei Bedarf wieder runterskalieren. Langwierige Ausschreibungsverfahren für neue Server im eigenen Rechenzentrum werden für solche Szenarien überflüssig. Investitionsrisiken lassen sich so ebenfalls minimieren.

3.3. Abhängigkeit von einzelnen Lieferanten durch fehlende Portabilität

Experten debattieren immer wieder über die Gefahren der Anbieterabhängigkeit in Public-Cloud-Umgebungen, auch Vendor Lock-In genannt. Eine pauschale Aussage bezüglich des Risikos lässt sich in der Regel nicht treffen, da der Effekt unmittelbar mit der Art und Weise der Nutzung der Ressourcen zu tun hat. Wenn Ministerien und Behörden beispielsweise eigene Anwendung in der Cloud entwickeln und bereitstellen, entsteht bei vielen proprietären Cloud-Plattformen ein Lock-In-Effekt.



der CIOs sind wegen eines möglichen Vendor-Lock-Ins in der Public Cloud besorgt.[7]

Einige Public-Cloud-Anbieter arbeiten mit eigenen Standards, die einen Transfer der Anwendungen und Daten im Falle eines Provider-Wechsels massiv erschweren. Das gilt in bestimmten Fällen auch, wenn Nutzer virtuelle Maschinen migrieren möchten. Ministerien und Behörden stehen daher in jedem Fall vor der Herausforderung, diese Aspekte in ihrer Cloud-Strategie zu berücksichtigen.

4. Lösungsansätze
für den Weg in die Public Cloud

Um Cloud-Projekte gesetzeskonform und sicher innerhalb des vorgegebenen Rahmens umzusetzen, können öffentliche Auftraggeber spezielle Betriebsmodelle und Funktionalitäten kombinieren. Aufeinander abgestimmte Konstellationen aus dezidierten Ressourcen, effektiven Sicherheits- und Verschlüsselungstechnologien sowie offenen Standards auf Open-Source-Basis ermöglichen Ministerien und Behörden vielfältige Anwendungsszenarien.

4.1 Virtual Private Cloud: Schutz vor fremdem Zugriff

Um auch in der Public Cloud den hohen Anforderungen an Datenschutz und Sicherheit gerecht zu werden, müssen öffentliche Organisationen eine Virtual Private Cloud (VPC) einsetzen. VPCs isolieren Netzwerke innerhalb und zwischen Mandanten mit eigenen IP-Adressen. Sie stellen sicher, dass kein unbefugter Zugriff auf fremde Ressourcen erfolgt. Mit dieser Netzwerk-Isolierung erhält jeder Kunde seinen eigenen IP-Adressbereich. VPCs können sich über ein oder mehrere Rechenzentren (Verfügbarkeitszonen) erstrecken. Unterhalb eines VPC können weitere Subnetze aufgebaut werden.
Bei der Einrichtung der VPCs können die IT-Fachkräfte über Firewalls und Sicherheitsgruppen Zugriffskontrollen vergeben. Später wird entschieden, über welche Ports welche Ressourcen für welche Nutzergruppen zugänglich gemacht werden. Über IP-VPN lässt sich beispielsweise eine sichere Tunnel-Verbindung zu eigenen IT-Ressourcen im Rechenzentrum einrichten.

4.2 Dezidierte Ressourcen: Dedicated Host und Bare Metal Server

Organisationen aus dem öffentlichen Sektor können für sensible Anwendungen oder Workloads sogenannte Dedicated Hosts nutzen. In diesem Fall steht die Server-Hardware ausschließlich für einen Kunden bereit. Die sonst übliche Aufteilung der virtuellen Maschinen für verschiedene Kunden entfällt. Im Gegensatz zu diesen Shared Hosts geht der Nutzer auf diese Weise sicher, dass auf der eingesetzten Hardware keine leistungsintensiven Anwendungen von Dritten betrieben werden, die die eigenen Dienste negativ beeinflussen. IT-Fachkräfte konfigurieren und betreiben ausschließlich ihre eigenen virtuellen Maschinen auf diesen Dedicated Hosts.

Bei spezielleren Anforderungen können Organisationen über die Public Cloud auch Bare Metal Server ohne Virtualisierung buchen, um die Hardware frei nach ihren Vorstellungen und Bedürfnissen zu konfigurieren. Ideal geeignet ist dieser Servertyp bei Applikationen, die nicht virtualisierbar sind oder spezielle Lizenzbedingungen mitbringen.

4.3 Verschlüsselung: Zuverlässige Absicherung des Datenverkehrs

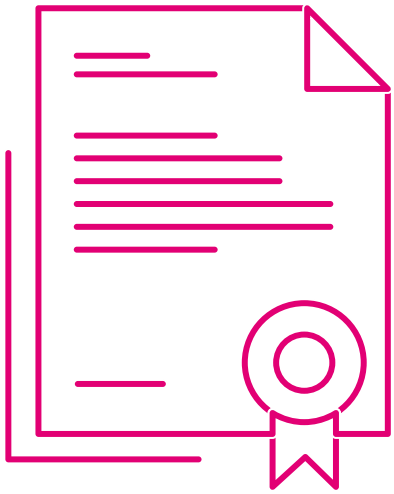
Bei der Wahl eines Cloud-Providers ist die Verschlüsselung aller Daten im Entscheidungsprozess ein wichtiger Faktor. Geht es um personenbezogene Daten, schreibt die DSGVO dem Auftragsverarbeiter vor, geeignete technische und organisatorische Maßnahmen zum Schutz dieser Daten zu ergreifen. Die Verschlüsselung ist dabei nicht nur ein naheliegendes Mittel, sondern wird in Artikel 32 der DSGVO auch explizit erwähnt. Werden personenbezogene Daten in die Cloud übertragen, fordern die Aufsichtsbehörden eine Ende-zu-Ende-Verschlüsselung. Ein angemessenes Sicherheitsniveau ist beispielsweise gegeben, wenn der Cloud-Provider Verschlüsselung für Block und Object Storage auf Basis des AES-256-Standards zur Verfügung stellt, um Datenbestände bestmöglich zu schützen.

4.4 Zertifikate: Aussagekräftige Nachweise erkennen

Um einen umfassenden Eindruck von den Sicherheitskompetenzen eines Public-Cloud-Providers zu bekommen, sollten Entscheider und IT-Fachleute aus dem öffentlichen Dienst eine Reihe von Zertifikaten als Orientierungshilfe heranziehen. Da es inzwischen eine Vielzahl von Nachweisen gibt, lohnt sich ein genauerer Blick. Verpflichtend ist zunächst die Erfüllung des Kriterienkatalogs C5 (Cloud Computing Compliance Criteria Catalogue) des Bundesamts für Sicherheit in der Informationstechnik (BSI). Dieser formuliert strenge Mindestanforderungen an sichere Cloud-Lösungen und richtet sich direkt an professionelle Cloud-Anbieter, deren Prüfer und Kunden. Cloud-Anbieter beauftragen eigenständig Prüfer, um die Erfüllung der Kriterien gegenüber Kunden nachzuweisen.

Ein weiterer Indikator für ein hohes Maß an Sicherheit ist die DIN ISO 27001. Mit dem Zertifikat belegen Dienstleister, dass sie alle Anforderungen an die Umsetzung, Optimierung und den Betreib eines dokumentierten Informationssicherheits-Managementsystems erfüllen. Auftraggeber erkennen an diesem Nachweis ein hohes Maß an IT-Sicherheit und Datenschutz. Weitere aussagekräftige Cloud-Zertifizierungen wie ISO 27017, ISO 27018, TCDP 1.0 (Trusted Cloud Data Profile), CSA Star Level sowie die SOC-Berichte und der BSI C5-Kriterienkatalog haben sich ebenfalls als Marktstandard durchgesetzt. Außerdem bietet die Listung als Trusted Cloud vom Bundesministerium für Wirtschaft und Energie eine gute Orientierung für einen sicheren Cloud-Einsatz im öffentlichen Sektor.

Darüber hinaus benötigen Ämter und Behörden je nach Einsatzbereich der Cloud-Lösung ergänzende Sicherheiten wie zum Beispiel die Verpflichtung zum Geheimnisschutz im Sinne des § 203 StGB. Auf Basis dessen darf ein Cloud Provider auch die besonders zu schützenden Daten von Berufsgeheimnisträgern verarbeiten. Sozialleistungsträger und deren Dienstleister sind zudem auf eine Verpflichtung des Sozialgeheimnisses nach § 35 SGB I angewiesen, wenn sie Daten in der Cloud hosten möchten, die unter das Sozialgeheimnis fallen.



4.5 Open Source: Mehr Möglichkeiten durch offene Standards

Um zu starke Abhängigkeiten gegenüber einzelnen Cloud-Providern zu vermeiden, sollten sich Organisationen aus dem öffentlichen Sektor an Public-Cloud-Lösungen auf Open-Source-Basis halten. Mit ihren offenen und anerkannten Standards gewährleisten solche Angebote eine größtmögliche Unabhängigkeit. Nutzer wählen dabei für ihre jeweiligen Bedürfnisse verschiedene Anbieter, ohne der Produktpolitik eines einzelnen Providers ausgesetzt zu sein. Entwickler haben zudem die Möglichkeit, sich an der Weiterentwicklung der Software zu beteiligen und selbstständig Änderungen am Code vorzunehmen. Das schafft maximale Freiheit.

Obwohl populäre Open-Source-Frameworks herstellerunabhängig funktionieren, profitieren die Nutzer von der Erfahrung großer IT-Unternehmen. So beteiligen sich an der OpenStack-Initiative beispielsweise Unternehmen wie HP, IBM, SAP oder die Deutsche Telekom. Auch andere Industriesektoren wie zum Beispiel die deutschen Automobilhersteller treiben das Thema voran.

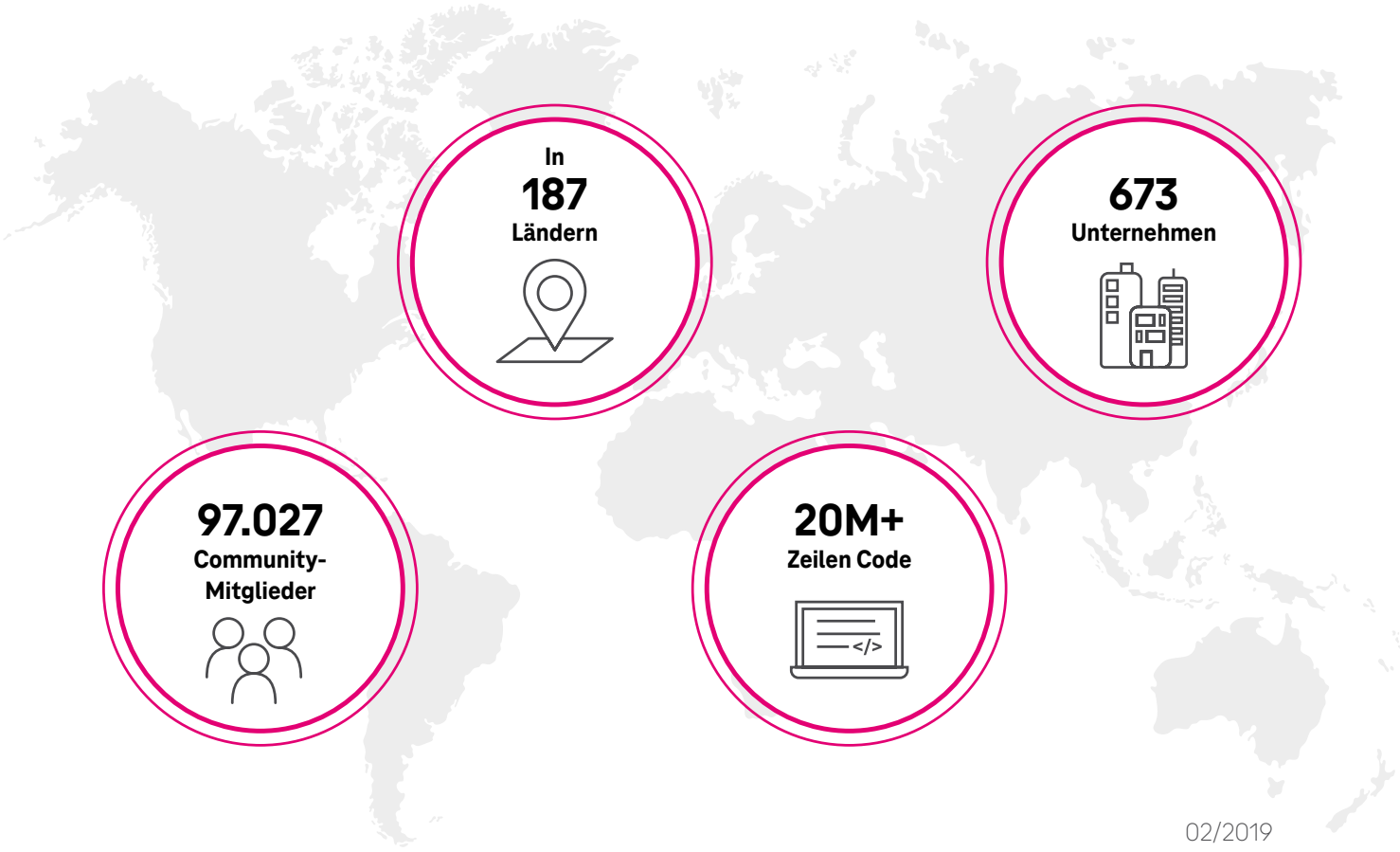


Abbildung: Eine große Community treibt die Entwicklung des Cloud-Betriebssystems OpenStack kontinuierlich voran.

4.6 Datenschutzkonforme Open-Source-Lösung aus europäischen Rechenzentren

Die Open Telekom Cloud hat sich in der Vergangenheit immer wieder als passendes Angebot für Projekte aus dem öffentlichen Sektor bewährt. Sowohl Bund, Länder und Kommunen als auch Bildungs- und Forschungseinrichtungen vertrauen auf die Lösung. Die Telekom stellt die Cloud über zwei hochverfügbare, miteinander vernetzte Rechenzentren (Twin Core) mit Standorten in Magdeburg und Biere (Distanz rund 25 Kilometer) bereit. Optional besteht die Möglichkeit eines Betriebs in Amsterdam mit den gleichen technischen Möglichkeiten. Auch dieser Standort ist DSGVO-konform. Zudem ist eine Kopplung aller Standorte möglich, um „echte“ Georedundanz zu erreichen.

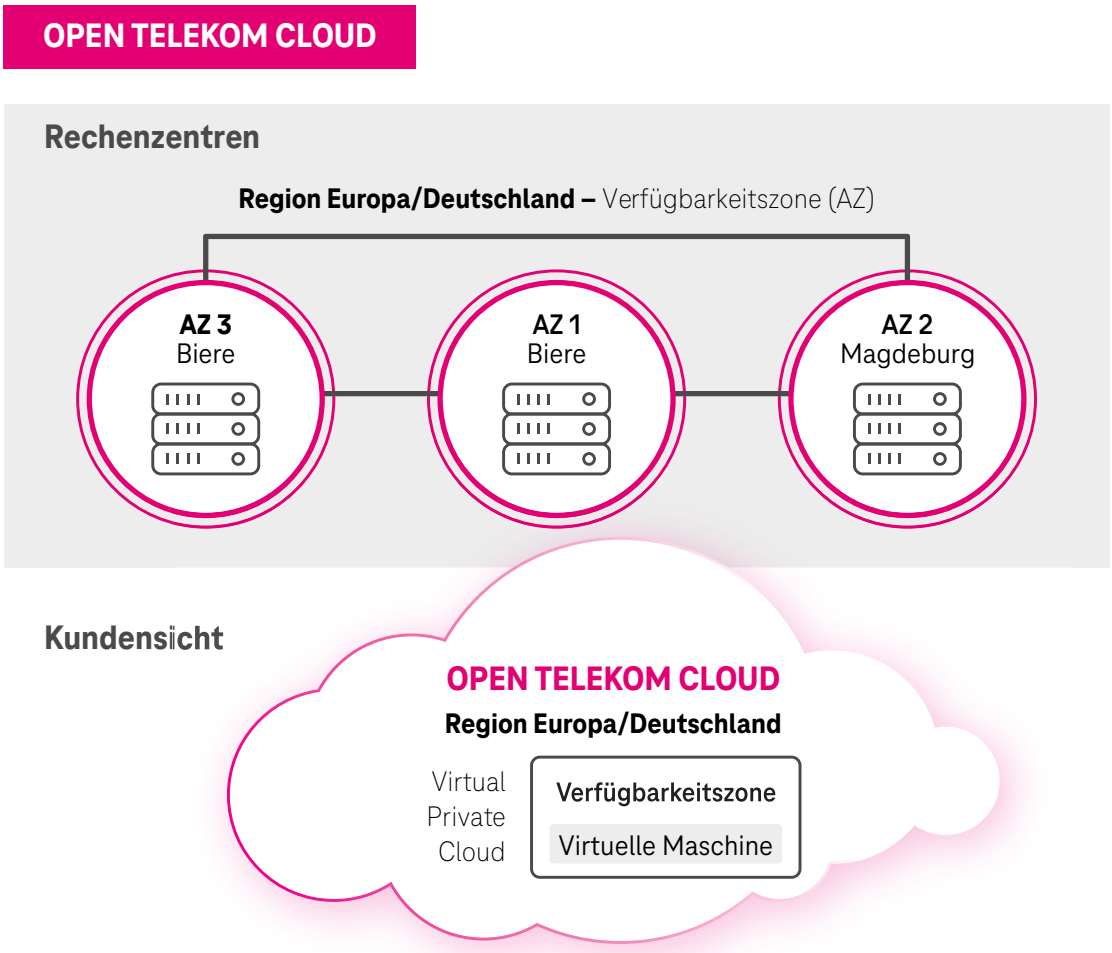


Abbildung: Die Telekom stellt die Cloud über zwei hochverfügbare, miteinander vernetzte Rechenzentren mit Standorten in Magdeburg und Biere.

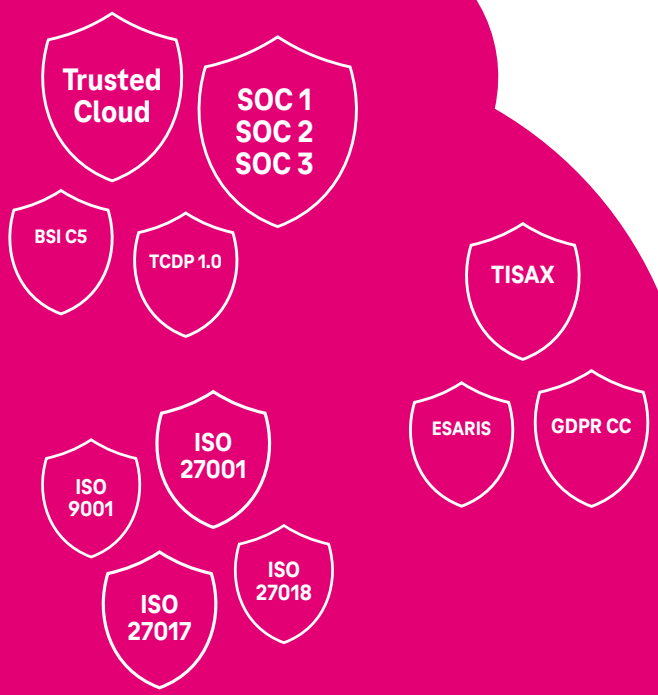
Weil viele IT-Anwender keine reinen Public- oder Private-Cloud-Szenarien umsetzen können, stehen sie vor der Herausforderung, beide Welten schlüssig zusammenzuführen. Kombinieren Unternehmen beide Modelle, kann das große Vorteile schaffen, zugleich aber auch gewisse Hürden mit sich bringen. Daher ist es von zentraler Bedeutung, dass an den Schnittstellen keine Brüche entstehen und die IT-Anwender alle Instanzen homogen verwalten können. Dafür wurde in Ergänzung zur Open Telekom Cloud die Open Telekom Cloud Hybrid entwickelt, die auch als Private Cloud einsetzbar ist.

Die Private- und Public-Variante der Open Telekom Cloud beruhen auf der gleichen technischen Basis. Migrationen von IT-Systemen und deren Daten zwischen beiden Modellen sind dadurch mit minimalem Aufwand möglich. Dem Angebot liegt zudem der OpenStack-Standard zugrunde und gewährleistet als Open-Source-Lösung maximale Unabhängigkeit. Damit ist die Lösung schon jetzt Teil der GAIA-X-Initiative, die an einer souveränen europäischen Dateninfrastruktur arbeitet.

Mit der Open Telekom Cloud sind Organisationen aus dem öffentlichen Sektor in der Lage, Server- und Speicherkapazitäten innerhalb von Minuten zu vergrößern und bei Bedarf auch wieder zu verkleinern. Das erlaubt es den Einrichtungen, ihre IT-Kapazitäten bei erhöhter Auslastung flexibel zu erweitern. Ebenso kurzfristig können Nutzer Massenspeicher in verschiedenen Geschwindigkeitsklassen umdisponieren.

Durch die Eigentumsverhältnisse der Deutschen Telekom AG unterliegt die Open Telekom Cloud nicht dem Cloud-Act der Vereinigten Staaten von Amerika. Alle Prozesse und Technologien sind zu 100 Prozent DSGVO-konform und auf maximalen Datenschutz ausgerichtet. Das Belegen zahlreiche Nachweise: Sie bietet die gängigen ISO-Zertifikate wie ISO 27001 und ISO 27017, spezifische Datenschutzzertifikate wie ISO 27018 und TCDP 1.0 sowie eine Reihe weiterer Zertifikate und Berichte wie SOC 1, SOC 2, SOC 3 und BSI C5. Außerdem wird sie vom Bundesministerium für Wirtschaft und Energie als Trusted Cloud gelistet und erfüllt branchenspezifische Bestimmungen für das sichere Verarbeiten von Daten von Berufsgeheimnisträgern (im Sinne des § 203 StGB) und von Trägern von Sozialleistungen (nach § 35 SGB I). Die Public Cloud der Telekom ist auf höchstmögliche Sicherheit ausgelegt und bietet eine Reihe von Features, die einen optimalen Schutz der Infrastrukturen gewährleisten. Damit sind die Ressourcen der Nutzer zu jeder Zeit gegen unbefugten Zugriff abgesichert. Kunden vergeben über ein modernes Zugangsmanagement individuelle Rechte und Rollen an ihre Angestellten, so dass jeder nur auf die Anwendungsbereiche zugreifen kann, die für ihn vorgesehen sind. Zusätzliche Verschlüsselungs- und Überwachungsdienste sowie effektive Abwehrlösungen garantieren einen sorgenfreien Betrieb der Cloud.

Hybrid-Cloud
Um den vollen Nutzen aus einer hybriden Cloud-Umgebung zu ziehen, müssen Unternehmen ihre Workloads und Anwendungen unkompliziert zwischen Public- und Private-Cloud verschieben können. Dabei helfen unter anderem einheitliche APIs und Management-Tools, mit denen IT-Anwender alle Instanzen übergreifend verwalten. Für Ministerien und Behörden eignet sich dieses Modell beispielsweise, um die Ressourcen der Public Cloud für die Entwicklung zu nutzen und die fertigen Applikationen schließlich datenschutzkonform in der Private Cloud zu betreiben. Bei entsprechender Vertragsgestaltung können die Einrichtungen zudem unkompliziert zusätzliche Ressourcen aus der Public Cloud nutzen.



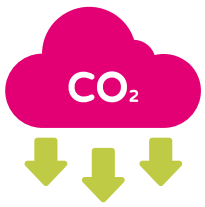
- **Made in Germany**
- **DSGVO konform**
- **Wahrung des Berufgeheimnisses** i.S.d. § 203 StGB
- **Wahrung des Sozialgeheimnisses** nach § 35 SGB I

5. Der nachhaltige Weg in die digitale Souveränität für Deutschland

Wer in einem hohen Maße von digitalen Lösungen profitieren möchte, wird früher oder später vor der Frage stehen, wie er diese möglichst nachhaltig und zukunftsfähig gestalten kann. Für Ministerien und Behörden eröffnet sich an diesem Punkt die Chance, eine wichtige Vorbildrolle einzunehmen und den öffentlichen Diskurs um eine klimafreundliche Digitalisierung voranzubringen. Die Public Cloud kann dafür ein aktiver Beitrag sein: Wenn Einrichtungen aus der öffentlichen Verwaltung ihre Anwendungen in der Open Telekom Cloud betreiben, teilen sie sich die stromintensiven Ressourcen in den Rechenzentren nämlich mit vielen anderen Parteien.

Weil die Telekom kontinuierlich an einem energieeffizienten Zusammenspiel sämtlicher Komponenten in ihren Rechenzentren arbeitet, verbraucht sie dort sogar 30 Prozent weniger Energie als in vergleichbaren Rechenzentren. Der Strom für die Rechenleistung kommt dabei zu 100 Prozent aus erneuerbaren Energiequellen. Um die Klimabilanz ihrer Infrastrukturen in Zukunft weiter zu verbessern, arbeitet die Telekom gemeinsam mit dem Fraunhofer IFF an Technologien für ein noch effizienteres Zusammenspiel aus regenerativer Erzeugung, Speicherung und flexiblen Verbraucherkomponenten. Das langfristige Ziel: ein Rechenzentrum, das sich selbst versorgt.

59 Mio.



Tonnen an CO_2-Emissionen könnten Migrationen in die Public Cloud pro Jahr einsparen.[8]

5.1 Smart City: Grüne Lebensräume mit der Cloud gestalten

Mit der Open Telekom Cloud verringern Bund, Länder und Kommunen nicht nur den CO_2-Fußabdruck ihrer IT-Infrastrukturen, sondern können auch über Smart-City-Projekte eine nachhaltigere Zukunft fördern. Intelligente Verkehrsleitsysteme, moderne E-Mobilitätskonzepte oder smarte Beleuchtungslösungen für den öffentlichen Raum steigern durch ihre emissionsreduzierenden Effekte schon jetzt die Nachhaltigkeit und erhöhen die Lebensqualität vieler Bürger. Der Trend zur Vernetzung des öffentlichen Raumes ist bereits da, wird künftig erheblich an Bedeutung gewinnen und so Schritt für Schritt das Konzept des „Digitalen Zwillings" (Digital Twin) einer Stadt mit Leben füllen. Die Verantwortlichen in den öffentlichen Einrichtungen stehen aufgrund dieser Dynamik permanent vor der immensen Herausforderung, ihre IT-Infrastrukturen jeweils kurzfristig an die Anforderungen anzugleichen. Bedarfsorientierte und schnell skalierbare Ressourcen aus der Public Cloud sind aus diesem Grund die passende Wahl für die Umsetzung von Smart-City-Projekten.

84 %

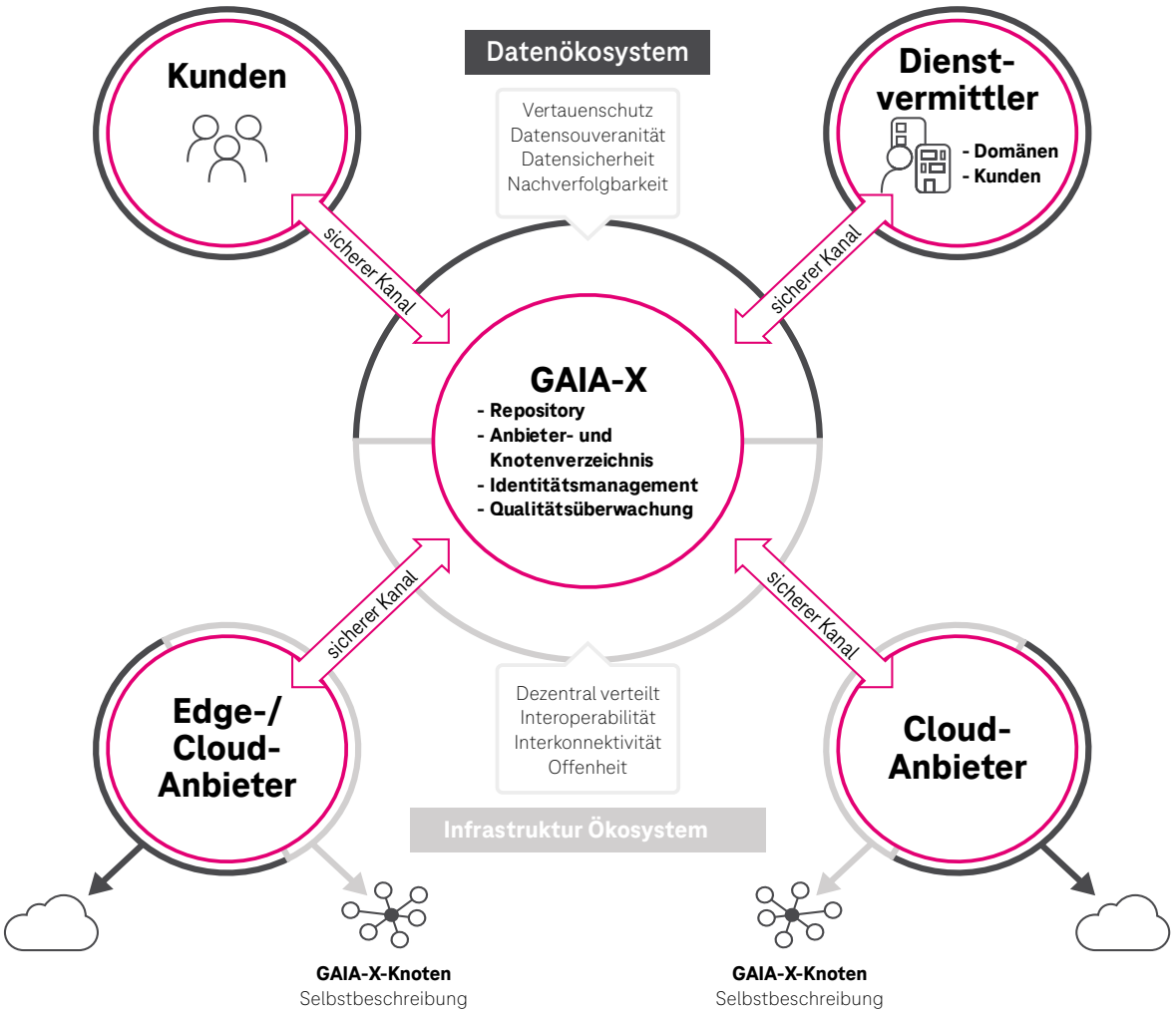
aller IoT-Anwendungen tragen schon jetzt zum Erreichen der Nachhaltigkeitsziele bei oder bringen das Potenzial dafür mit.[9]

Weil die intelligente Vernetzung öffentlicher Räume zu weiten Teilen auf dem Internet of Things (IoT) fußt, ist der Umgang auch mit diesen Daten ein zentraler Erfolgsfaktor für die digitale Stadt. Erst wenn die verantwortlichen Planer alle Informationen der öffentlichen IoT-Infrastruktur zentral zusammenführen, analysieren und auswerten, können sie die Vernetzung in einem größeren Zusammenhang betrachten und effizient steuern – es entsteht ein Digital Twin der Stadt. Für diese Anforderungen steht Nutzern der Open Telekom Cloud eine sogenannte Urban Data Platform zur Verfügung. In ihr laufen alle Informationen der digitalen Stadt zusammen. Erst mit dieser SaaS-Lösung machen Städte und Regionen die gesamten Daten über eine sichere Ende-zu-Ende-Plattform nutzbar – von der Aggregation über die Harmonisierung und Analyse bis hin zur Erstellung von digitalen Services für die Bürger. Kurz: Die Lösung bildet das Rückgrat der Smart-City-Infrastruktur. Ein weiterer Vorteil: Kommunen können auf diese Weise zum Beispiel die Erfüllung von Nachhaltigkeitszielen, etwa im Sinne der Sustainable Development Goals (SDG) der Vereinten Nationen, erfassen und per Dashboard für die Öffentlichkeit sichtbar machen. Damit erfüllen Regionen nicht nur eine Vorbildfunktion, sondern stärken auch ihre Attraktivität.

5.2 GAIA-X: Grundlage für zukunftssichere Investitionen

Für Unternehmen und öffentliche Auftraggeber ist die Nachhaltigkeit einer Cloud-Lösung nicht nur in ökologischer, sondern auch in strategischer Hinsicht wichtig. Kunden müssen neue IT-Infrastrukturen häufig auf viele kleinteilige Prozesse abstimmen und möchten daher möglichst langfristig von ihren Investitionen in die Public Cloud profitieren, sobald die passende Konfiguration einmal steht. Wer diesen Aspekt in seiner Strategie nicht berücksichtigt, muss mit Störfaktoren wie wechselnden Geschäftsbedingungen, problematischen Abhängigkeiten oder rechtlichen Unklarheiten rechnen. Faktoren, die im schlimmsten Fall statt einer langfristig geplanten Investition eine kurzfristige Neuausschreibung bedeuten – nachhaltige Planung sieht anders aus.

Als Gründungsmitglied der GAIA-X-Initiative erfüllt die Telekom mit der Open Telekom Cloud schon jetzt alle Voraussetzungen für die Bereitstellung einer langfristig gedachten, unabhängigen und sicheren Cloud-Infrastruktur, die zu 100 Prozent dem europäischen Datenschutz entspricht. Ziel der Initiative ist es, die digitale Souveränität der EU mit einer eigenen Dateninfrastruktur zu stärken. Damit gehen verbindliche Standards und Prinzipien einher, an denen die Deutsche Telekom aktiv mitwirkt – und die jetzt schon für die Open Telekom Cloud gelten. Wer sich einmal für die Lösung entscheidet, kann sich daher sicher sein, in eine nachhaltige und zukunftssichere Infrastruktur zu investieren.



GAIA-X-AUFGABEN

Rahmenbedingungen schaffen

- **Architektur**
- **Schnittstellen**
- **Datenklassifikation**
- **Prozesse zwischen Akteuren**
- **Interoperabilität und Interkonnektivität**

Gouvernanceregeln

- **Teilnahmebedingungen**
- **Teilnehmerliste**
- **Regeln und „Datenverträge“**
- **Zertifizierung**

Betrieb koordinieren

- **Notwendige zentrale Dienstleistung**

Abbildung: Funktionsprinzip der GAIA-X-Initiative

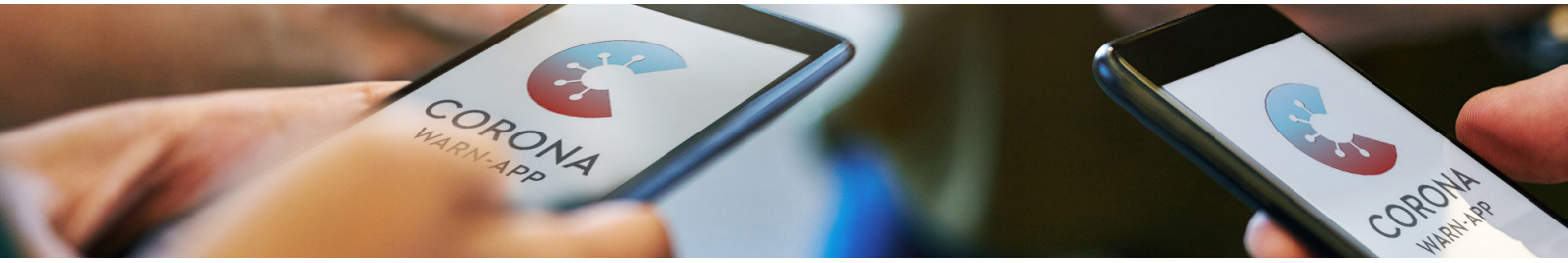
Quelle:iBMW

6. Referenzen: Open Telekom Cloud in der Praxis

Haben öffentliche Institutionen einmal ihr individuelles Cloud-Set-Up definiert und im Einsatz, sind die Möglichkeiten enorm. Digitale Verwaltungsdienstleistungen, automatisierte Prozesse oder auch die schnelle Bereitstellung von neuen Anwendungen – in der Praxis gleicht kaum ein Anwendungsszenario dem anderen. Grund genug, an dieser Stelle noch einmal auf einige ausgewählte Erfolgsgeschichten zu blicken.

6.1 Corona-Warn-App für Deutschland und Europa

Um die Kontaktpersonennachverfolgung im Kampf gegen die Corona-Pandemie zu unterstützen, hat das Bundesgesundheitsministerium im vergangenen Jahr die Corona-Warn-App in Auftrag gegeben. T-Systems hat in Zusammenarbeit mit SAP sowie verschiedenen Institutionen und Arbeitsgruppen eine DSGVO-konforme Lösung erarbeitet. Für das Bundesgesundheitsministerium als Auftraggeber und das Robert Koch-Institut als Betreiber der Corona-Warn-App hatten der Schutz personenbezogener Daten und die Einhaltung der Datenschutzgrundverordnung (DSGVO) höchste Priorität.
Doch auch der übrige Anforderungskatalog war anspruchsvoll. Die wichtigsten Vorgaben: Die verwendete Technologie musste auf offenen Standards basieren, die Rechenzentren in Deutschland sein und wichtige Sicherheitszertifizierungen aufweisen. Damit fiel die Wahl für die technische Infrastruktur schnell auf die Open Telekom Cloud, die Public-Cloud-Lösung des App-Entwicklungspartners Telekom. Bereitgestellt aus hochsicheren Rechenzentren in Magdeburg und Biere, basiert die Open Telekom Cloud auf dem offenen Standard OpenStack. Außerdem erfüllt sie den Anforderungskatalog C5 vom Bundesamt für Sicherheit in der Informationstechnik (BSI), der Cloud-Anbietern ein Höchstmaß an Sicherheit bescheinigt.



6.2 Corona-Soforthilfe Bayern

Damit Selbstständige, Landwirte und Unternehmen die Corona-Soforthilfe einfacher und schneller beantragen können, implementierte das bayerische Wirtschaftsministerium eine spezielle Online-Antragslösung. Sie ersetzt das Antragsverfahren über PDF-Dokumente, die teils handschriftlich ausgefüllt, eingescannt und per E-Mail an die Antragsstellen zugeschickt wurden. Mit dem neuen Online-Formular im Internet liegen sämtliche Daten ab Beginn der Antragsstellung digital vor und fließen so in den Prüf- und Freigabeprozess der Verwaltung. Das bayerische Wirtschaftsministerium entwickelte die Antrags- und Prozessplattform zur Corona-Soforthilfe gemeinsam mit Pegasystems und konnte sie zusammen mit T-Systems in nur fünf Tagen fertigstellen. Sie läuft auf der hochkonfigurierbaren Low-Code- Plattform von Pegasystems und wird von T-Systems auf einer sicheren, hochverfügbaren und skalierbaren Infrastruktur in eigenen Rechenzentren in Deutschland betrieben. Das neue Online-Verfahren wird von den bayerischen Betrieben bereits äußerst rege genutzt. Schon kurze Zeit nach seiner Inbetriebnahme stellten mehr als 108.500 von ihnen Anträge auf Soforthilfe.

Gemäß der Kieler Beschlüsse kann die Lösung auch für die Nutzung in weiteren Bundesländern, Kommunen und dem Bund zur Verfügung gestellt werden – gewissermaßen als Blaupause für spezifische Erfordernisse, Verwaltungsprozesse und Infrastrukturen der jeweiligen Stellen.

6.3 Digitale Bürgerkarte: Digitale Verwaltungsleistungen aus der Cloud

Für eine deutsche Kommune hat T-Systems die Implementierung und den Betrieb für eine digitale Bürgerkarte mit umfangreichen Verwaltungsleistungen (Bibliotheksdienste, Nachrichten und Veranstaltungen, kostenloser ÖPNV) umgesetzt. Die Lösung, welche u. a. personenbezogene Daten verarbeitet, wird auf der Open Telekom Cloud betrieben.

Die verschiedenen Services der Cloud-nativen-Architektur (Microservice-Architektur) sind als Docker-Container realisiert, die in einer hochverfügbaren Zielumgebung in der Open Telekom Cloud laufen. Für die Verwaltung der Container kommt eine Container-Orchestrierung zum Einsatz. Aus der Open Telekom Cloud werden weitere Cloud-Dienste wie Server-Infrastruktur, Loadbalancing, Anti-DDoS und Datenbank-Dienste in das System integriert. Für die Entwicklung wurde der auf der Open Telekom Cloud betriebene DevOps-as-a-Service eingesetzt, mit dem ein Ende-zu-Ende CI/CD-Prozess mit integrierten und automatisierten Tests und Security-Checks ausgeführt wurde. Auf dieser Basis konnten die wesentlichen DevOps-Prinzipien wie schnelle Lieferung, hohe Qualität und Nachvollziehbarkeit umgesetzt werden.

6.4 Mundi Web Services: Skalierbare Rechenleistung für anspruchsvolle Analysen

Mit dem Copernicus-Programm erfüllt die European Space Agency (ESA) den Auftrag der Europäischen Union, die Erde aus dem Weltall zu beobachten. Zu diesem Zweck funken eine Serie von Sentinel-Erdbeobachtungssatelliten tagtäglich etwa 20 Terabyte an Bildern zur Erde. Mittlerweile haben die verfügbaren Satelliten mehrere 100 Petabytes an Daten für Nutzern innerhalb und außerhalb der EU bereitgestellt, die neue Blicke auf Umwelt und Klimaänderungen ermöglichen. Über Mundi Web Services werden diese Daten cloud-basiert zugänglich gemacht. Ziel davon ist es, neue geobasierte Geschäftsmodelle zu fördern.

Mit Mundi Web Services wurde eine Plattform realisiert, auf der Nutzer direkt vorkonfigurierte Geoservices nutzen können. Sie bietet aber auch neuen Geoservice-Anbietern die Option, ihren Service am Markt anzubieten. Die große Stärke von Mundi Web Services: Alle notwendigen Komponenten, um neue geo-basierte Business-Ideen zu realisieren, sind bereits integriert. Dies betreffen ständig aktualisierte Daten der Sentinel-Satelliten sowie historische Daten des amerikanischen Landsat-Programms, Geoservice-Applikationen und flexibel einsetzbare IT-Ressourcen aus der Open Telekom Cloud. Da die Rechenkapazitäten für die Auswertungen und die Daten auf derselben technischen Plattform liegen, entfallen langwierige Kopiervorgänge. Zudem erlaubt Mundi die spezifische Auswahl der für die jeweilige Analyse relevanten Daten.

Mit der Open Telekom Cloud hat Mundi das passende Infrastruktur-Fundament: Die Ressourcen aus der Cloud sind optimal für temporäre Hochlastberechnungen und passen sich an den gewünschten Bedarf der Nutzer an. Wünscht er schnellere Ergebnisse, kann er die Auswertung mit zusätzlichen Kapazitäten beschleunigen. Je nach Geschwindigkeit - immer gilt: Es fallen nur Kosten für tatsächlich genutzte Ressourcen an.

Bei welchem Projekt können wir Sie unterstützen?

Sie wollen Ihre IT-Infrastruktur um leistungsfähige Ressourcen ergänzen oder eigene Anwendungen und Dienste über die Cloud bereitstellen, ohne schwerwiegende Hardware-Investitionen zu tätigen? Dann sprechen Sie uns gerne an. Wir erarbeiten für Ihr individuelles Anwendungsszenario praxiserprobte Lösungen auf Basis der Open Telekom Cloud. Dank unserer umfangreichen Erfahrungen mit Projekten im öffentlichen Sektor kennen wir die Bedürfnisse und Hürden der Branche aus erster Hand. Aus diesem Grund haben Datenschutz, IT-Sicherheit und Compliance bei uns höchste Priorität.

Mit der Open Telekom Cloud realisieren Sie Ihre Digitalisierungsprojekte auf einer hochmodernen Infrastruktur, die ausschließlich in europäischen Rechenzentren betrieben wird.

Wir beantworten Ihre Fragen zu Testmöglichkeiten, Buchung und Nutzung – kostenfrei und individuell. Wir sind 24 Stunden am Tag, 7 Tage die Woche für Sie da.
Probieren Sie es jetzt aus!
0800 33 04477

Quellenverzeichnis

1 PwC: Upskilling hopes and fears 2021
2 DAK: Digitalisierung und Homeoffice in der Corona-Pandemie
3 Uptime Institute: Renewable energy for data centers
4 Eco-Studie: Rechenzentren sind Garant für nachhaltige Digitalisierung in Europa
5 EuGH: Rechtssache C-311/18
6 KPMG/Bitkom: Cloud Monitor 2021
7 The Flexera 2020 CIO Priorities Report
8 IDC: Cloud Computing Could Eliminate a Billion Metric Tons of CO_2 Emission Over the Next Four Years
9 WEF: Internet of Things Guidelines for Sustainability

Kontakt:
open-telekom-cloud.com/de/kontakt

Internet:
open-telekom-cloud.de

Herausgeber:
T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Deutschland

Erleben, was verbindet.