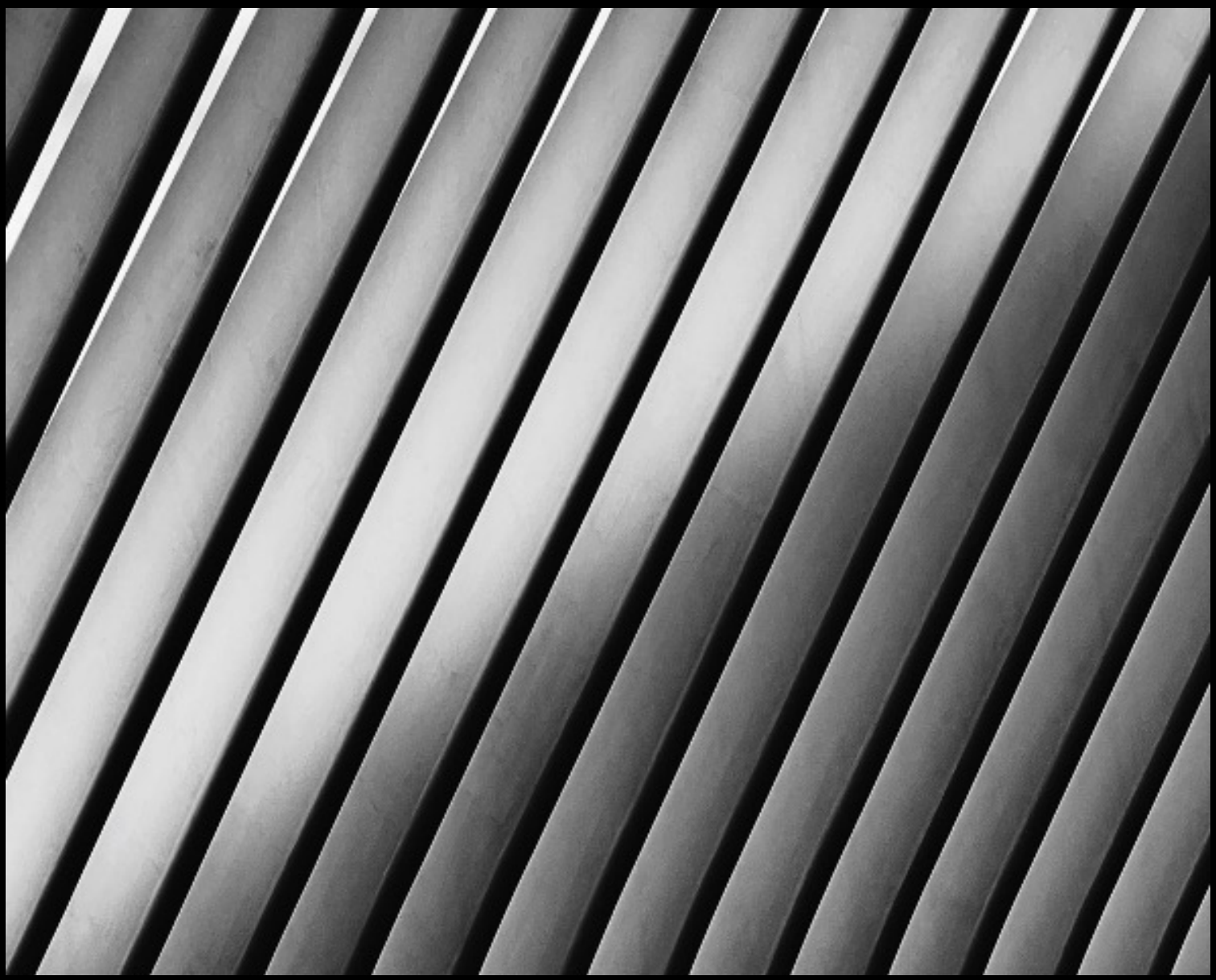
Cloud Reallabor
Sichere Verarbeitung in der Cloud

GovTech Campus Deutschland

FAQ zu Chancen und Risiken der „Cloud“



„Die Verwaltung in Deutschland muss handlungs- und steuerungs- fähig bleiben.“

Harald Joos
Projektleiter Cloud-Reallabor

Liebe Leserinnen und Leser,

die Diskussionen unserer Zeit sind geprägt von einer Vielzahl von Perspektiven. Ein einzelnes Argument mag isoliert betrachtet schlüssig erscheinen, im Kontext anderer Argumente kann sich seine Bedeutung jedoch schnell relativieren. Ich erlebe täglich, dass es unterschiedliche Antworten gibt, je nachdem wer gefragt wird und welche Interessen und Herausforderungen gerade im Vordergrund stehen.

Dabei besteht dringender Handlungsbedarf angesichts des prognostizierten Personalabgangs von über 30 Prozent bis 2030. Innovative IT-Lösungen, die Nutzung Künstlicher Intelligenz und stärkere Automatisierung sind für die Verwaltung unverzichtbar, um handlungsfähig zu bleiben. Die „Cloud“ spielt dabei eine entscheidende Rolle und ist eine wesentliche Grundlage, um zeitgemäße Dienstleistungen anbieten zu können. Welche Möglichkeiten die „Cloud“ bietet, konnten wir zum Beispiel bei der Nutzung von Videokonferenz-Lösungen während der Corona-Pandemie erfahren, wo wir innerhalb kürzester Zeit auch mobil arbeitsfähig waren.

Wichtige Entscheidungen müssen jetzt schneller getroffen werden. Dazu müssen wir weg von einem Schwarz-Weiß-Denken. Es geht nicht mehr um ein Entweder-oder, sondern um ein flexibles Sowohl-als-auch. In der Verwaltung betreiben wir eigene Rechenzentren und können Cloud-Lösungen ergänzend nutzen – so haben wir viele Optionen.

Unser Projekt „Cloud-Reallabor: Sichere Verarbeitung in der Cloud“ bringt die öffentliche Verwaltung und Privatwirtschaft auf dem GovTech Campus zusammen, um Blaupausen für den sicheren Einsatz von Public-Cloud-Lösungen zu entwickeln. Projektmitglieder sind Cloud-Anbieter aus den USA, Deutschland und Europa und Bedarfsträger der öffentlichen Verwaltung, die bereits Cloud-Lösungen nutzen oder auf dem Weg dorthin sind. Von zentraler Bedeutung sind das Bundesamt für Sicherheit in der Informationstechnik (BSI) und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI), die ebenfalls im Projekt mitwirken.

Ein Grundverständnis zu den Chancen und Risiken der „Cloud“ ist eine wichtige Voraussetzung, um Entscheidungen zu treffen. Die von uns vorgelegten Fragen und Antworten sollen eine erste Orientierung für Entscheidungsträger bieten – auch außerhalb der IT.

Harald Joos
Projektleiter Cloud-Reallabor

Warum beschäftigen wir uns mit der „Cloud“?

Potenziale der „Cloud“ (Auswahl)

- Moderne, zeitgemäße Arbeitsplätze, die die Attraktivität des Arbeitgebers erhöhen
- Energieeffizienz und Nachhaltigkeit, um den CO_2-Fußabdruck zu reduzieren
- Verbrauchsabhängiger Bezug von Leistungen
- Schnellere Bereitstellung innovativer Lösungen

Die „Cloud“ wird schon heute in vielen Organisationen eingesetzt, da immer mehr Lösungen von den Anbietern vorrangig oder ausschließlich als „Cloud-Lösung“ angeboten werden. Zudem müssen wir schneller mit der Verwaltungsdigitalisierung vorankommen – die „Cloud“ bietet uns zusätzliche Möglichkeiten, dieses Ziel zu erreichen.

Hinzu kommt der Fachkräftemangel in der IT, der uns dazu zwingt, auch über zusätzliche Optionen neben dem eigenen Betrieb eines eigenen Rechenzentrums nachzudenken. Wir müssen uns daher stärker mit der „Cloud“ beschäftigen, um die Vorteile zu nutzen, ohne die Risiken außer Acht zu lassen.

Spannungsfeld „Digitale Souveränität“ vs. Digitalisierung?

Obwohl die „Cloud“ heute schon genutzt wird und man um eine weitere Nutzung in der Zukunft nicht herumkommt, führen wir Grundsatzdiskussionen, ob und von welchen Anbietern Cloud-Lösungen in der Verwaltung genutzt werden dürfen. Diese Diskussion wird häufig unter dem Stichwort „Digitale Souveränität“ geführt.

Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023

„Der Begriff „Digitale Souveränität“ wird (dabei) in der öffentlichen Debatte mit unterschiedlichen Bedeutungen verwendet. Je nach Sichtweise – etwa aus dem Blickwinkel der Ökonomie, der Forschung, der Innovationskraft, der inneren und äußeren Sicherheit sowie der IT-Sicherheit – werden unterschiedliche Schwerpunkte der technologischen Unabhängigkeit betont.“

Es gibt weitere prominente Beispiele für unterschiedliche Sichtweisen auf „Digitale Souveränität“, wie die Debatte über den Einsatz chinesischer Technologien in Kommunikationsnetzen (z. B. „Huawei“) und die Förderung ausländischer Firmen zur Chipherstellung in Deutschland.

Eines ist unstrittig: Wir wollen und brauchen mehr „Digitale Souveränität“. Doch lässt sich diese überhaupt herstellen? Falls ja, in welchen Bereichen und in welcher Zeit ist das möglich?

Wir müssen unsere Abhängigkeiten Stück für Stück reduzieren, ohne dabei auf innovative Lösungen Dritter zu verzichten, denn dazu sind die Herausforderungen zu groß.

Was ist die „Cloud“?

Abkürzungen
Cloud-Dienste werden häufig als Service angeboten. In diesem Zusammenhang gibt es einige Abkürzungen, deren wichtigste Bedeutungen hier beispielhaft aufgeführt werden.

- IaaS: Infrastructure as a Service (z. B. Speicher, Rechenkapazitäten)
- PaaS: Platform as a Service (z. B. ERP-Systeme)
- SaaS: Software as a Service (z. B. Office-Lösungen)
- XaaS: Everything as a Service

Vereinfacht gesagt kann die „Cloud“ wie ein großes industriell betriebenes, geografisch verteiltes Rechenzentrum verstanden werden. Dies erlaubt, Daten und Programme online zu speichern, auszuführen und grundsätzlich von überall darauf zuzugreifen, anstatt sie lokal auf einem eigenen Gerät vorzuhalten. Im Wesentlichen handelt es sich dabei um Leistungen, die aus einem Rechenzentrum eines Drittanbieters bezogen werden. Typische Angebote sind Speicher, Server, ganze Plattformen und Softwarelösungen (z. B. Videokonferenzlösungen während der Corona-Pandemie).

Was bedeutet die „Cloud“ für das eigene Rechenzentrum?

Das eigene Rechenzentrum kann auch in Zukunft eine wichtige Rolle spielen. So kann es zum Beispiel geschäftskritische Daten geben, die den Hoheitsbereich der eigenen Organisation nicht verlassen sollen.

Auch kann es wirtschaftlicher sein, Anwendungen weiterhin im eigenen Rechenzentrum zu betreiben. Ein Dienst, der die eigene Infrastruktur kontinuierlich auslastet, kann im eigenen Rechenzentrum kostengünstiger betrieben werden. Umgekehrt gibt es Anwendungen, die nur temporär hohe Lastspitzen bewältigen müssen. Ein Beispiel hierfür ist der morgendliche Anmeldeprozess aller Schülerinnen und Schüler in einer Schul-Cloud. Das Vorhalten dauerhaft hoher Kapazitäten im eigenen Rechenzentrum für solche punktuellen Anforderungen vorzuhalten, wäre wirtschaftlich unvorteilhaft. Diese Kapazitäten würden den Rest des Tages weitgehend ungenutzt bleiben, jedoch trotzdem Kosten verursachen, zudem Energie verbrauchen und unnötig zu CO_2-Emissionen beitragen.

Neben wirtschaftlichen Überlegungen gibt es zahlreiche weitere Faktoren, die für den Betrieb im eigenen Rechenzentrum oder in der Cloud sprechen können. Dazu zählen die Energieeffizienz, die Verbesserung der Informationssicherheit, der Schutz vor Cyberangriffen und die allgemeine Erhöhung der Resilienz. Zudem ist immer zu berücksichtigen, dass ausreichend Fachkräfte für den Betrieb eines Rechenzentrums vorhanden sein müssen.

Weitere Aspekte können auch technologischer Natur sein, etwa die Frage, ob der Betrieb und die Weiterentwicklung neuer Technologien vollumfänglich im eigenen Rechenzentrum gewährleistet werden können. Bei der Verarbeitung großer Datenmengen, wie zum Beispiel beim Einsatz Künstlicher Intelligenz, sind Cloud-Lösungen meist erforderlich.

Es ist daher sinnvoll, die Möglichkeit zu haben, von Fall zu Fall auf Lösungen außerhalb des eigenen Rechenzentrums zuzugreifen, dies aber nicht zwangsläufig zu müssen.

Wie sicher ist die „Cloud“?

Für **Cloud-Anbieter** ist die Sicherheit (Vertraulichkeit und Verfügbarkeit) ihrer Angebote überlebensnotwendig und ist dementsprechend hoch priorisiert. Damit werden den Kunden laufend neue Sicherheitslösungen angeboten.

Das Bundesamt für Sicherheit in der Informationstechnik **(BSI)** hat in den letzten Jahren einen umfassenden Katalog mit Sicherheitsanforderungen an Cloud-Dienste etabliert, der europaweit auf große Zustimmung stößt. Durch den Nachweis der Einhaltung dieser Anforderungen gewährleistet der Cloud-Anbieter die effektive Einhaltung von IT-Sicherheitsstandards. Weiter unterliegen Cloud-Anbieter in bestimmten Fällen besonderen gesetzlichen Vorgaben und damit auch dem BSI-Gesetz (dazu zählen zum Beispiel die „KRITIS-Verordnung“ und die kommende „NIS2-Richtlinie“). Alle zwei Jahre muss durch unabhängige Prüfer nachgewiesen werden, dass wirksame Sicherheitsmaßnahmen, auch gegen Cyber-Angriffe, umgesetzt wurden.

Gleichwohl befreit dies den **Cloud-Nutzer** nicht von der Verantwortung, eigene Sicherheitsmaßnahmen zu ergreifen. Es werden unter anderem technische Lösungen angeboten, die Daten während der Speicherung, Übertragung und Verarbeitung verschlüsseln und somit vor unberechtigtem Zugriff schützen. Befinden sich die Schlüssel im **alleinigen** Besitz des Kunden, kann der Cloud-Anbieter die gespeicherten Informationen nicht lesen (dies umfasst auch Informationsanfragen aus Drittstaaten).

Es ist daher auch möglich, Daten „sicher“ in der Cloud zu verarbeiten. Letztlich bleibt es eine risikobasierte Einzelentscheidung, ob eine Verarbeitung im eigenen Rechenzentrum oder in der Cloud sicherer ist.

BSI C5

Das BSI hat den „**C**loud **C**omputing **C**ompliance **C**riteria **C**atalogue“ (Kriterien-katalog Cloud Computing C5) entwickelt und schreibt diesen kontinuierlich fort. Der Nachweis der Einhaltung der Kriterien erfolgt nach den bewährten Prüfungsstandards für Wirtschaftsprüfer. Seitens der öffentlichen Verwaltung ist ein C5-Testat eine der Mindestanforderungen, die ein Cloud-Anbieter nachweisen muss. Durch regelmäßig zu wiederholende Testierung wird sichergestellt, dass ein Cloud-Anbieter das Sicherheitsniveau des C5 erreicht hat.

Sind Cloud Angebote nachhaltiger als ein eigener Rechenzentrumsbetrieb?

Die Infrastruktur der Cloud-Anbieter entspricht in der Regel dem neuesten Stand der Technik und erfüllt bereits heute hohe Anforderungen an Energieeffizienz und Nachhaltigkeit. Die kontinuierliche Verbesserung dieser Infrastrukturen wird nicht nur aus ökologischen, sondern auch aus ökonomischen Gründen vorangetrieben, sodass von einer weiteren positiven Entwicklung auszugehen ist.

Parallel dazu ist auch die Verwaltung bestrebt, die Nachhaltigkeit und Energieeffizienz ihrer eigenen Rechenzentren im Rahmen der technischen Möglichkeiten und baulichen Gegebenheiten zu verbessern. Dabei spielen Faktoren wie Alter und Standort des Rechenzentrums eine entscheidende Rolle. Auch wenn in eigenen Rechenzentren Fortschritte erzielt werden, bieten Cloud-Lösungen aufgrund von Skaleneffekten und Spezialisierung oft erweiterte Möglichkeiten, die Energieeffizienz und Nachhaltigkeit der IT zu steigern.

Wissenschaftliche Dienste Deutscher Bundestag, Aktenzeichen WD 8 – 3000 – 070/21

Energieeffizienz

Die Energieeffizienz eines Rechenzentrums wird häufig mit dem Power Usage Efficiency-Wert (PuE) angegeben. Er gibt an, wie viel Energie insgesamt aufgewendet werden muss, um eine Einheit Nutzenergie für die IT-Infrastruktur bereitzustellen. Ein PuE-Wert von 1,5 bedeutet zum Beispiel, dass 1,5 Kilowatt aufgewendet werden müssen, um 1 Kilowatt Energie zu nutzen, wobei 0,5 kWh verloren gehen.

Eine Studie des Deutschen Bundestages zum Energieverbrauch deutscher Rechenzentren im Jahr 2023 zeigt, dass der durchschnittliche PuE-Wert in Deutschland von 1,98 im Jahr 2010 auf 1,63 im Jahr 2020 gesunken ist. Man kann davon ausgehen, dass dieser Wert in der Zwischenzeit weiter gesunken ist. Große Cloud-Rechenzentren erreichen vergleichsweise PuE-Werte von 1,1 oder sogar darunter.

Können die Daten ausschließlich in Rechenzentren in Deutschland, der EU gespeichert werden?

Alle großen Cloud-Anbieter – ob aus Deutschland, der EU oder den USA – bieten ihre Dienste in Rechenzentren an, die auf Standorte weltweit verteilt sein können. Dabei erlauben sie ihren Kunden in der Regel ausdrücklich zu bestimmen, ob deren Daten ausschließlich im Rechtsraum der EU verarbeitet werden sollen. Der Kunde entscheidet, wo seine Daten gespeichert und weiterverarbeitet werden. Dies sichern die Cloud-Anbieter auch vertraglich zu. Es gibt jedoch Ausnahmen, bei denen es notwendig sein kann, auf Experten außerhalb Europas zurückzugreifen. Dies ist zum Beispiel in besonderen Supportfällen oder bei speziell vereinbarten Services der Fall.

Trotz der Option, die Daten ausschließlich innerhalb der EU zu speichern, können bestimmte Daten, z. B. Metadaten zu Abrechnungszwecken oder zur Gewährleistung der Servicequalität, den Rechtsraum der EU verlassen. Da kein direkter Personenbezug hergestellt werden kann, sind diese Daten aus Sicht der Cloud-Anbieter nicht personenbezogen. Kunden sollten jedoch genau prüfen, ob die Übermittlung solcher Daten, die indirekt einen Personenbezug aufweisen können, tatsächlich erforderlich ist.

US-CLOUD ACT

Das Gesetz verpflichtet Internet-Firmen und IT-Dienstleister, die in den USA Dienste erbringen, US-Behörden Zugriff auf gespeicherte Daten zu gewährleisten, auch wenn diese außerhalb der USA gespeichert sind. Die konkrete Durchsetzbarkeit dieses Gesetzes in Bezug auf Daten souveräner Staaten wie Deutschland bleibt fraglich. Vertraglich sind Cloud-Anbieter zu verpflichten, durch rechtliche Schritte sicherzustellen, dass nur rechtmäßige Anfragen von US-Bundesgerichten beantwortet und unberechtigte Anfragen abgewiesen werden.

Ein dabei oft übersehener, aber entscheidender Aspekt ist die technische Absicherung der Daten. Daten, die z. B. durch Verschlüsselungstechniken geschützt sind, bleiben unabhängig von Gesetzesänderungen oder Herausgabeverlangen verschlüsselt. Wenn der Schlüssel ausschließlich beim Kunden liegt, ist ein Zugriff auf die Daten im Klartext ohne Zustimmung nicht möglich.

Machen wir uns durch den Einsatz von Cloud-Angeboten zu abhängig von den Anbietern?

Die Nutzung von Cloud-Diensten birgt das Risiko der Abhängigkeit von bestimmten Anbietern – ein Effekt, der als „Vendor-Lock-in“ bezeichnet wird. Um diese Gefahr zu minimieren, sollten Anwendungen so entwickelt werden, dass sie plattformunabhängig und damit unabhängig von den Cloud-Anbietern ablauffähig sind. Optimal sind Anwendungen, die sowohl im eigenen Rechenzentrum als auch auf mindestens einer weiteren Cloud-Plattform betrieben werden können. Dies reduziert nicht nur das Risiko eines Vendor-Lock-ins, sondern erhöht auch die Resilienz. Angesichts der jüngsten Cyber-Angriffe auf verschiedene Institutionen wie Krankenhäuser, Universitäten und Kommunalverwaltungen ist dies von immer wichtigerer Bedeutung, falls ein Rechenzentrum aufgrund eines schwerwiegenden Vorfalls einmal längerfristig ausfallen sollte.

Es müssen grundsätzlich Vorkehrungen getroffen werden, damit ein Wechsel zwischen Cloud-Anbietern möglich ist, nicht zuletzt, um auch auf veränderte Anforderungen und Marktbedingungen reagieren zu können.

Trotz der möglichen Nachteile eines Vendor-Lock-ins können sich Organisationen auch bewusst für diesen entscheiden. Dies kann zum Beispiel der Fall sein, wenn die Vorteile der Lösung die Produktivität so stark erhöhen, dass die möglichen Risiken in Kauf genommen werden.

Impressum

Herausgeber
GovTech Campus Deutschland e.V.
Max-Urich-Straße 3
D-13355 Berlin

Ansprechpartner
Harald Joos
Projektleiter Cloud-Reallabor & Cloudbeauftragter der DRV Bund

Cloud-Reallabor
Sichere Verarbeitung in der Cloud

Das Projekt „Cloud-Reallabor: Sichere Verarbeitung in der Cloud“ bringt öffentliche Verwaltung und Privatwirtschaft auf dem GovTech Campus zusammen, um Blaupausen für den sicheren Einsatz von Public-Cloud-Lösungen zu entwickeln. Auf Basis einer Evaluierung verschiedener Public-Cloud-Angebote aus Deutschland, der EU und den USA wird deren Nutzbarkeit für die öffentliche Verwaltung untersucht. Ein besonderer Fokus liegt dabei auf der Konsolidierung einschlägiger Proof of Concepts und deren Übertragbarkeit, um entsprechende Handlungsempfehlungen abzuleiten. Die Ergebnisse des Projekts werden öffentlich zugänglich gemacht, um einen Mehrwert für die gesamte öffentliche Verwaltung und einen sachlichen Beitrag zur Diskussion zu schaffen, für die sichere Nutzung von Public-Cloud-Lösungen.

Stand
April 2024

Genderhinweis
Um die Lesbarkeit zu verbessern, wird in diesem Dokument das generische Maskulinum verwendet.
Die verwendeten Personenbezeichnungen schließen – wenn nicht anders angegeben – alle Geschlechter ein.

Bildquellen
Titelseite: Jean-Remy Bena / Pexels.com
Vorwort: DRV Bund