Cloud Computing
Positionspapier 2021

Ergänzend
CloudComp-Pos-2.1.0

Ergebnis der AG

Kurzbeschreibung:

Im Rahmen der BLSG existiert ein Orientierungspapier zum Thema Cloud Computing. Aufgrund der rasanten Entwicklung in diesem Bereich, der mit mobilen Geräten und verteilten Services in der Zwischenzeit eine zentrale Rolle gewonnen hat, war ein Überarbeiten notwendig, die durch einfachere Struktur auch im Einsatz in der Praxis verwendet werden kann. Dabei wurde ein Katalog von Fragen in das Zentrum gesetzt, die Anwendungen und Umsetzungen aus der jeweiligen Situation zu beantworten haben. Das vorliegende Positionspapier basiert auf dem seinerzeitigen Positionspapier und wurde aufgrund der nunmehrigen Gegebenheiten überarbeitet. Die Version 2.1.0 hat die Kapitel zu grundsätzlichen Erläuterungen und Überlegungen aus der letzten Version des Positionspapiers in Anhänge übernommen und dort Großteils noch keine Aktualisierung vorgenommen. Die Kapitel 2 und 3 dieses Positionspapiers versuchen eine mögliche Position der österreichischen Verwaltung zur Nutzung von Cloud Services für die Abstimmung im Rahmen der BLSG AG Cloud Computing zu skizzieren.

AutorInn(en): A-SIT/Posch, Research Institute AG & Co KG/Tschohl, BMF/Kasa, Amt der OÖ. Landesregierung, Amt der Salzburger Landesregierung, BKA, BMLV, BMLRT, BMDW, Stadt Wien

Weitere Arbeitsgruppenmitglieder: Hannes Baumgartner (BMLV), Rudolf Beier (BMLV), Stefan Dornauer (Tirol), Martin Ebner (BMLV), Patrick Einzinger (BMI), Susanne Fiedler (BMLV), Michael Füreder (OÖ), Martin Hackl (BMJ), Helmut Habermayer (BMLV), Franz Haider (BMK), Gerhard Hartmann (Wien), Michael Hauenschild (BRZ), Ronald Haupt (BRZ), Heide Havranek (BMDW), Info Hegny (BMK), Josef Heinschink (Bgld), Sanda Heissenberger (Wien), Alexander Hudec (BMLV), Markus Hinterseer (Salzburg), Thomas Hofmann (Dsb), Herbert Hüttenbrenner (Stmk), Rudolf Ivancsits (Bgld), Dominik Klauser (BMDW), Nicolas Knotzer (BMDW),Arnuf Kopeinig (BMLV), Ernst Koessl (BMK), Thomas Komada (BMLV), Roland Krenner (OÖ), Markus Krickl (BMLRT), Stephan Liebhart (BMF), Andrea Maierhofer (BMDW), Harald Marent (BMLV), Thomas Menzel (BMBWF), Gerhard Milletich (BMEIA), Joachim Minichshofer (OÖ), Alexander Miserka (NÖ), Kurt Mikula (BMLV), Clemens Möslinger (BKA), Lisbeth Mosnik (BMK), Renate Neumüller (OÖ), Jürgen Neustifter (Wien), Sigurd Oberhuber (Vorarlberg), Christian Panigl (Univie), Manfred Parzer (BMLV), Alexander Pfann (BRZ), Michael Pfister (BMLV), Raphaela Pöttinger (BKA), Wolfgang Prentner (Freie Berufe), Ferdinand Scheidbach (BMDW), Christian Schuller (Sozialversicherung), Martin Schwehla (BKA), Jochen Steiner (BRZ), Arno Siegel (BKA), Florian Silnusek (BMLV), Markus Steiner (BMF), Daniel Steinmetz (BMDW), Klaus Stromberger (BMLV), Norbert Weidinger (Wien) Michael Wiesmüller (BMK), Elke Wirthumer (OÖ), Hanna Wilhelmer (BKA), Martin Zöbl (Stmk), Alexander Rapolter (BMLV), Andreas Laschalt (BMBWF), Alfred Tanzer (BMBWF), Andreas Troll (BMLV), Christan Zec (BKA)

Projektteam/Arbeitsgruppe: AG-Cloud BLSG

Version / Datum: Cloud Comp-Pos-2.1.0

Doku-Stadium: Ergebnis der AG

Gültig seit: 20.04.2022

Nächste Überprüfung am: 20.04.2027

Inhaltsverzeichnis

1 Einleitung

Cloud Computing ist ein weiterer Schritt zur durchgängigen Virtualisierung[1] von IKT-Infrastruktur und -Services. Viele Innovationsprojekte und eine erfolgreiche Kooperation der letzten Jahre haben das österreichische E-Government in das europäische Spitzenfeld gebracht und zwischenzeitlich wieder ins Mittelfeld zurückfallen lassen. Die österreichische Verwaltung möchte das Ziel und den Weg für erfolgreiches E-Government der vergangenen Jahre in Zukunft weiterverfolgen - eine der möglichen Säulen dieses Weges kann das Potential von Cloud Computing sein. Mit der EU-Ratspräsidentschaft 2018 hat sich Österreich „Mobile First" auf die Fahnen geschrieben. Cloud Computing und „Mobile First" sind untrennbar verbunden und damit sind die Themen in diesem Umfeld, die Komfort, Interoperabilität, aber auch Sicherheit und Souveränität zentral berühren, jedenfalls neu zu sichten.

Cloud Computing ist eine Form der flexibel am Ressourcenbedarf orientierten Nutzung von IT-Leistungen und der Unabhängigkeit von konkreten Plattformen bei gleichzeitiger Abhängigkeit von Cloud-Betreibern, da Verarbeitungen entweder in der Cloud oder in einer sehr standardisierten Form erfolgen. Diese werden in Echtzeit als Service über das Internet bzw. Intranet bereitgestellt und meist nach Nutzung abgerechnet. Viele der Services erscheinen den Nutzern kostenfrei zu sein, sind jedoch eine Umschichtung des Kostenmodells und Risikomodells, welches oft einen genaueren Blick auf Datenschutzbestimmungen und Risiko- bzw. Resilienzfragen erfordert und daher vor allem für die Verwaltung sorgfältige Betrachtung bedingt. Cloud Computing ist keine grundsätzlich neue Technologie, sondern kombiniert vorhandene Technologien und Verfahren für eine standardisierte Bereitstellung und pro Provider standardisierten Schnittstellen von Diensten (Services) und ist daher eine Weiterentwicklung des Outsourcing Modells, um über größtmögliche Skaleneffekte verbesserte Flexibilität und Kostenvorteile zu erzielen. In diesem Zusammenhang ist der Aspekt der digitalen Souveränität eine wesentliche Komponente, die in einer getrennten Aktivität beleuchtet werden sollte, da sie nicht nur Cloud Services berührt.

Cloud Computing ist eine Chance, birgt aber auch Risiken. Die Plattform Digitales Österreich hat in einer gemeinsamen Arbeitsgruppe (AG Cloud) der Bund/Länder/Städte/Gemeinden-Kooperation (kurz Kooperation-BLSG) das vorliegende Positionspapier mit Stand Juni 2011 erstmals erstellt, welches die Möglichkeiten des Einsatzes von Cloud Computing in der österreichischen öffentlichen Verwaltung untersucht. Das Positionspapier wurde im März 2016 um die rechtliche Checkliste der AG Recht und Sicherheit (AG ReSi) ergänzt und mit September 2016 einer allgemeinen Aktualisierung unterzogen. Nach den Erfahrungen in der Praxis und aufgrund der Tatsache, dass Cloud nunmehr nicht nur eine Option ist, sondern in vielen Fällen technisch, aber vor allem lizenztechnisch von den Anbietern (Microsoft, Adobe, Google….) mit Nachdruck verfolgt wird, wurde das Papier 2020 nochmals überarbeitet und vereinfacht und hat nun den Schwerpunkt gemeinsamen Findens von Randbedingungen bei der Nutzung von Cloud Services. Das Positionspapier soll Grundlageninformationen für nötige strategische Entscheidungen bereit stellen bzw. wie man diese Entscheidungsgrundlagen erarbeitet und was man dabei beachten muss; es beinhaltet Begriffsdefinitionen, rechtliche/strukturelle/ wirtschaftliche/technische Aspekte (Geschäftsprozesse), Auswirkungen, Chancen und Risiken sowie potentielle Anwendungen für klassische Rechenzentren. Im Kontext der BLSG-Strukturen der Behörden der österreichischen Verwaltung geht es nicht nur um die

[1] Mit dem Portal-Verbund wurden bislang bereits erfolgreich Cloud-ähnliche Ziele verfolgt. Während allerdings der Portal-Verbund auf ein gemeinsam vereinbartes Vorgehen abstellt, ist das Wesen der Cloud die gemeinsame Nutzung von Ressourcen, ohne dass damit eine vertragliche Situation der Nutzer untereinander entsteht.

Betrachtung von Public Cloud Angeboten, sondern auch um den Einsatz der Konzepte des Cloud Computing in den eigenen Infrastrukturbereichen (sog. Private Cloud) sowie künftige E-Government Applikationen nach „Cloud-Prinzipien" zu designen. Dieser Aspekt tritt massiv in den Vordergrund, da die Mischung von on Premise Services und Cloud Services sowie das Angebot Dritter von Services auf Basis von Cloud Zugängen vor allem im mobilen Bereich deutlich zunimmt und damit die Verwaltung als Hüter der konsistenten und rechtskonformen Verarbeitung eine besondere Verantwortung hat. Gleichzeitig ist es eine besondere Herausforderung, das Know-how innerhalb der Verwaltung bei der Dynamik, die Cloud an den Tag legt, aufrecht zu erhalten und von den Behauptungen, die Marktplayer aus Konkurrenzgründen machen bzw. machen müssen, abzugrenzen.

Um bei geringstem Risiko den höchsten Mehrwert für Bürgerinnen und Bürger und Verwaltung durch Cloud Computing zu erreichen, wäre Cloud-Nutzung, welche auf die Notwendigkeit österreichischer Behörden abgestimmt ist, eine Option (Private Cloud oder Hybrid Clouds). Im mobilen Bereich ist dieser Ansatz bereits nahezu überholt, da sich die Frage der Kommunikation im Wege der Cloud nicht mehr stellt, sondern eine unvermeidbare Tatsache darstellt. Dennoch gibt es deutliche Unterschiede, wenn man die verschiedenen Plattformen ansieht. Während Android die Funktionalitäten den APPs relativ offen bereitstellt, ist bei iOS in vielen Fällen – besonders in systemnahen Bereichen und in Securitybereichen und oft auch in der APP-zu-APP-Kommunikation der dem Nutzer nicht bewusste „Umweg" über die Cloud eine Voraussetzung. Dennoch wäre die strategische Abhängigkeit von einem einzelnen Cloud Anbieter nach Möglichkeit zu vermeiden, wozu die Nutzung mittlerweile etablierter Cloud Standards (z.B. OpenStackArchitektur) beitragen kann und was bei der reinen Datenablage in der Cloud auch weitgehend gelingen kann. Dennoch ist diese strategische Abhängigkeit Teil des Geschäftsmodelles aller großen Cloud Anbieter. Es können und sollen Public Cloud Angebote genutzt werden, und dabei gilt es die Rahmenbedingungen und die Wirtschaftlichkeit sorgfältig abzuwägen, wozu dieses Dokument auch Hilfestellungen zu bieten versucht.

Die in diesem Zusammenhang zu betrachtenden Chancen und Risiken müssen in Bezug auf Rechtskonformität, Wirtschaftlichkeit, verbesserte Reaktionszeit bei wechselndem Ressourcenbedarf, strategischen Risiken „Wissens-/Skills Verlust" und strategische Abhängigkeit vom „Cloud Service Provider" (CSP), Verletzlichkeit der staatlichen Souveränität und durch Angriffe sowie Abhängigkeit von einer Netzinfrastruktur bewertet werden.

Die Frage der datenschutzrechtlichen Zulässigkeit der Nutzung von insbesondere Public Clouds, die von Providern zur Verfügung gestellt werden, die in den USA ihre Zentrale oder zumindest auch Niederlassungen, Sublieferanten oder Service-Partner haben, hat mit dem Fall des US-EU Privacy Shields neu an Aktualität und Komplexität gewonnen.

Einige „Private Cloud" - Lösungen sind mittlerweile in der österreichischen Verwaltung angekommen, auch öffentliche Cloud Ansätze werden oft ohne besondere Evaluierung einfach verwendet und man darf erwarten, dass durch die fortschreitende Digitalisierung Cloud Computing weiteren Auftrieb erhält.

Das Thema Cloud ist in allen Verwaltungen Europas zentral. Ebenso ist die Anforderung „Mobile First" spätestens seit der österreichischen EU-Ratspräsidentschaft 2018 massiv am Plan. Dennoch findet man in der Hoheitsverwaltung praktisch keine Cloud Only Lösungen, da hier der Aspekt der Souveränität der einzelnen Mitgliedsstaaten sowohl was die Datenhaltung aber auch - da die Prozesse in der Cloud letztlich von Provider bestimmt werden - was die Verarbeitung selbst betrifft, nicht als gelöst anzusehen ist. Zudem kommt die Befürchtung eines gewissen Willkürpotentials, das mit der Lizensierung „Per Use" entsteht und kaum so langfristig stabilisiert werden kann, dass eine Zwangslage vermeidbar wird und man Cloud bzw. die spezielle Cloud einfach wieder verlassen könnte. Die Förderung der Entwicklung von

europäischen Cloud Service Angeboten ist daher auch im Interesse der österreichischen Verwaltung.

Diese Einleitung zeigt, dass die Beantwortung der Frage nach der Sinnhaftigkeit und rechtlichen Zulässigkeit der Nutzung von Cloud Services, hier vor allem von öffentlichen und internationalen Cloud Services, eine Fülle von Kriterien zu berücksichtigen hat und von hoher Komplexität getragen ist. Dies nicht zuletzt durch die Tatsache, dass Cloud Service Provider unterschiedlichen und potentiell widersprüchlichen Rechtssystemen im Vergleich zum EU-Recht unterworfen sein können.

Gleichzeitig haben sich Cloud Services seit der letzten Version dieses Positionspapiers so weit etabliert, dass ein stark gestiegenes Verständnis bzgl. Terminologie und Charakteristika von Cloud Services auch in der öffentlichen Verwaltung besteht. Die Erläuterungen zur Natur der Cloud Services und zu grundsätzlich nötigen Überlegungen aus der letzten Version des Positionspapiers sind daher derzeit noch nicht aktualisiert (z.B. DSG 2000 statt DSGVO) in Anhänge als Referenz übergeführt worden. Die unmittelbar folgenden Kapitel des Positionspapiers versuchen eine mögliche Position der österreichischen Verwaltung zur Nutzung von Cloud Services zu skizzieren und im Rahmen der BLSG AG Cloud Computing abzustimmen.

In diesem Papier ist der Stand 2021 zusammengefasst, um den Institutionen in der Verwaltung aber auch den Stakeholdern, die für die Verwaltung agieren (BBG, BRZ GmbH, …) eine Grundlage bereitzustellen. Das Papier ist im Sinne der Lesbarkeit kurzgehalten. Folgeaktivitäten wie etwa Praxisbeispiele, der Nutzen und die Stellung von horizontalen und vertikalen Kooperationen bis hin zur Rolle der Ö-Cloud und damit auch des EU-Vorhabens GAIA-X werden bewusst als eine von diesem Papier getrennte Projektebene angesehen, mit der sich die österreichische Verwaltung koordiniert unter der Federführung des BMDW (vgl. Anlage zu § 2 Teil 2 lit. F Z 26 Bundesministeriengesetz)[2] auseinanderzusetzen haben wird.

2 Position der öffentlichen Verwaltung zur Nutzung von Cloud Services

Die vorgeschlagene Position der österreichischen Verwaltung zur Nutzung von Cloud Services im Rahmen der BLSG AG Cloud Computing dient dem Festmachen der notwendigen Randbedingungen zum Einsatz der von Cloud Computing in der öffentlichen Verwaltung. Die aufgelisteten Fragen und Kriterien sollen als Hilfestellung bei der grundsätzlichen Frage dienen, ob und unter welchen Randbedinungen Cloud Services in der öffentlichen Verwaltung zum Einsatz kommen können.

1) Das Interesse an der Nutzung von Cloud Services ist grundsätzlich gegeben
    a. Cloud Services haben sich weltweit als mittlerweile unverzichtbarer und beständig wachsender Teil der IT-Leistungen etabliert. Vor allem die (scheinbaren) potentiellen Kostenvorteile für hochskalierende und standardisierte IT-Services haben diesen bisher zum Durchbruch verholfen. Zunehmend stehen aber auch funktionale Alleinstellungsmerkmale, z.B. im Bereich der auf breite Datenbestände aufbauenden künstlichen Intelligenz, im Fokus des Interesses.

[2] Insbesondere die folgenden Angelegenheiten:
Koordination und zusammenfassende Behandlung in Angelegenheiten der Informationstechnologien.
Allgemeine Angelegenheiten einschließlich der Koordination, der Planung und des Einsatzes der automationsunterstützten Datenverarbeitung sowie der Beurteilung von Anwendungen der automationsunterstützten Datenverarbeitung unter Gesichtspunkten der Wirtschaftlichkeit, Zweckmäßigkeit und Sparsamkeit und des ressortübergreifenden Wirkungscontrollings sowie der Verwaltungsreform und des Datenschutzes.
Koordination in Angelegenheiten der elektronischen Informationsübermittlung.

b. Die österreichische öffentliche Verwaltung ist daher am Einsatz von Cloud Services in geeigneten Anwendungsbereichen zur Bereitstellung von kostengünstigen und zukunftssicheren IT-Anwendungen interessiert.

2) Nicht alle Cloud Services sind grundsätzlich bzw. in allen Anwendungsbereichen für die öffentliche Verwaltung geeignet. Ebenso wie teilweise bereits heute, wird es daher künftig eine Mischung aus unterschiedlichen Cloud Services („hybride" Cloud Services aus öffentlichen und privaten Cloud Services) und konventionellen IT-Services geben.
   a. Die Nutzbarkeit von Cloud Services ist – ebenso wie die Nutzbarkeit von konventionellen „as a Service" bezogenen IT-Dienstleistungen - im Einzelfall zu prüfen. Dabei sind insbesondere die folgenden Kriterien kumulativ zu prüfen. Nähere Ausführungen zu diesen Kriterien finden sich in den nachfolgenden Positionspunkten (ab 3); aus datenschutzrechtlicher Sicht können zudem die Empfehlungen und Leitlinien des Europäischen Datenschutzausschusses unterstützend herangezogen werden[3]):
      i. Ist der Datenschutz gemäß allgemeiner Rechtsvorschriften ausreichend gesichert?
         1. Betreibt der Cloud Service Provider eine Datenanwendung, die rechtmäßig und sicher ist und kann dies durch eine Datenschutzzertifizierung nachweisen?
         2. Existieren ausreichende privatrechtliche Zusicherungen und technische sowie betriebliche Vorkehrungen?
         3. Ist die Rechtssicherheit in den „Ursprungsländern" der Cloud Service Provider zur Durchsetzung aller Anforderungen gegeben?
      ii. Erlaubt die Kritikalität der Daten deren Auslagerung überhaupt bzw. an einen bestimmten Cloud Service Provider? Wird diese Beurteilung wiederkehrenden Prüfmechanismen unterworfen?
      iii. Ist die staatliche Souveränität durch eine ausreichend geringe Abhängigkeit vom betrachteten Cloud Service weitergegeben?
      iv. Ergibt eine umfassende wirtschaftliche Beurteilung klare Kostenvorteile der betrachteten Cloud Services zu vergleichbaren, durch die Verwaltung selbst betriebenen IT-Services?
      v. Risikobetrachtung der Cloud Services (z.B. welche Abläufe sind bei Data breach nach Art 35 DSGVO oder anderen Meldepflichten vorgesehen)?

3) Beurteilung des Datenschutzes gemäß allgemeiner Rechtsvorschriften
   a. Ausreichender Datenschutz muss für personenbezogene Daten gemäß DSGVO für das betrachtete Cloud Service gegeben sein. Die Letztbeurteilung obliegt dem jeweiligen datenschutzrechtlich Verantwortlichen[4] der Verwaltungsbehörde, die das Cloud Service nutzen würde. Dafür sind insbesondere erforderlich[5]

---

[3] EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten 2.0, angenommen am 18.06.2021, zuletzt abgerufen am 13.12.2021: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en;
EDSA, Leitlinien 2/2020 zu Artikel 46 Absatz 2 Buchstabe a und Absatz 3 Buchstabe b der Verordnung (EU) 2016/679 für die Übermittlung personenbezogener Daten zwischen Behörden und öffentlichen Stellen im EWR und Behörden und öffentlichen Stellen außerhalb des EWR 2.0, angenommen am 15.12.2020, zuletzt abgerufen am 13.12.2021: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22020-articles-46-2-and-46-3-b-regulation_en

[4] Als datenschutzrechtlich Verantwortlicher ist die jeweilige Verwaltungseinheit (Ministerium,…) zu sehen diese Rolle fällt nicht den Datenschutzbeauftragten zu.

[5] Vgl. dazu EDSA, Outcome of own-initiative investigation into EU institutions' use of Microsoft products and services, angenommen am 02.07.2020, zuletzt abgerufen am 13.12.2021: https://edps.europa.eu/data-protection/our-work/publications/investigations/outcome-own-initiative-investigation-eu_en;

i. klare Kommunikation und Vereinbarung der datenschutzrechtlichen Rollenverteilung.
ii. Vereinbarungen über den Einsatz von Sub-Auftragsverarbeitern und Konsequenzen der Ablehnung.
iii. wenngleich privatrechtliche Zusicherungen den Einfluss von Drittstaaten mittels Rechtsprechung nicht ausschließen können, sind gegebenenfalls zusätzliche vertragliche Maßnahmen im Sinne des Annex 2 der Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten 2.0 zu treffen; dies sollte auch schon bei allfälligen Vergabeverfahren berücksichtigt werden.[6]
iv. ausreichende privatrechtliche Zusicherungen für den Datenschutz in den Lieferverträgen mit dem jeweiligen Cloud Service Provider:
    1. In den Lizenz- und Nutzungsbedingungen eines Cloud Service Providers muss mittels verbindlicher Bestimmungen abgesichert sein, dass die Anforderungen der DSGVO erfüllt werden, der Standort / Speicherort der verarbeiteten Daten angegeben wird und die Daten in der EU gehostet werden. Dies gilt für Verträge mit Cloud Service Providern aus EU-Drittländern. Eine klare Leitlinie für geeignete Nutzungsbestimmungen findet sich in den EU-Standardvertragsklauseln.[7]
    2. Vorgaben hinsichtlich der Speicherbegrenzung bzw. des Nachweises einer rechtskonformen Löschung der Daten bzw. Vereinbarung der Herausgabe der Daten (Format, Prozedere) inkl. Sub-Auftragsverarbeitern.
    3. Sicherstellung, dass Teile der Vertragsbeziehung nicht einseitig abänderbar sind und durch Veröffentlichung im Internet bekanntgegeben werden (Vorgehen bei Vertragsänderungen und Erweiterungen wurde vereinbart).
    4. Kontrolle darüber, welche Daten von CSP von Nutzern erhoben werden oder was der CSP mit diesen Daten tun kann (Zweckbindung).
    5. Unabhängige Prüfungsrechte / Audits.

v. Geeignete technische und organisatorische Maßnahmen zur Absicherung des versprochenen Datenschutzes:
    1. Der Nachweis des tatsächlichen, nach DSGVO erforderlichen Schutzes der an den Cloud Service Provider exportierten Daten ist zu erbringen. Hier wird insbesondere auf eine Zertifizierung nach z.B.

EDSA, Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten 2.0, angenommen am 18.06.2021, zuletzt abgerufen am 13.12.2021: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.

[6] Etwa: Informationspflichten, wenn es zu Zugriffen und rechtlich bindenden Aufforderungen von Behörden zur Herausgabe von personenbezogenen Daten kommt, auch die betroffene Person (nicht nur der V muss informiert werden; Verpflichtung, dass CSP alle Rechtsmittel ausschöpfen muss und zuvor keine Daten herausgegeben werden; Sonderkündigungsrecht bei Zugriffen und Herausgabeanspruch; Schad- und Klagloshaltung.

[7] Durchführungsbeschluss (EU) 2021/915 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß Artikel 28 Absatz 7 der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates und Artikel 29 Absatz 7 der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32021D0915&from=DE

a. „Kriterienkatalog Cloud Computing C5: 2020" des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) oder
b. „ENISA Meta-Rahmen für Cloud-Zertifizierungsprogramme (Cloud Certification Schemes Metaframework, CCSM, mit der darin enthaltenen Liste bestehender Informationssicherheitszertifizierungsprogramme CCSL)"

als Nachweis verwiesen.

vi. Die Durchsetzbarkeit der privatrechtlichen Zusicherungen im „Ursprungsland" des betrachteten Cloud Service Providers:
    1. Neben den vertraglichen Zusicherungen und den geeigneten Schutzmaßnahmen des Cloud Service Providers selbst ist durch den datenschutzrechtlich Verantwortlichen aber auch die geeignete rechtliche Basis im Ursprungsland des Cloud Service Providers zu prüfen, z.B. ob (potentiell) Zugriffe/Herausgabeanordnungen von Behörden, Gerichten oder anderen staatlichen Institutionen fremder Jurisdiktionen (z.B. im Rahmen des U.S. Cloud Act) drohen.
    2. Dazu merkt beispielshaft die österreichische Finanzprokuratur im Hinblick auf die Zulässigkeit der Microsoft Cloud Services Office 365 im Herbst 2020 an:
        a. Es ist somit davon auszugehen, dass der Verantwortliche vor Übermittlung der Daten in ein Drittland auf Basis von Standardschutzklauseln verpflichtet ist, das Schutzniveau im jeweiligen Drittland zu prüfen und wenn erforderlich weitere Sicherungsmaßnahmen vorzukehren.
        b. Die Finanzprokuratur verweist dabei auf einen Beurteilungsbedarf mit Ermessensspielraum:
            i. Vor diesem Hintergrund ist davon auszugehen, dass eine Aussage, dass der Einsatz von MS-Cloudlösungen unter allen denkbaren Anwendungskonstellationen jedenfalls mit der DSGVO konformgeht, nicht möglich ist, zumal nicht bloß die konkreten Datenverarbeitungen vom jeweiligen Verantwortlichen individuell zu beurteilen sind, sondern auch keine konkrete Judikatur zur Frage vorliegt, wann das durch die DSGVO gewährleistete Schutzniveau entgegen Art 44 DSGVO untergraben würde.
    3. [8]Bei Cloud Service Providern innerhalb der EU entfällt die zusätzliche Komplexität der Prüfung eines angemessenen gesetzlichen Schutzniveaus, z.B. die derzeitigen Herausforderungen mit U.S.-basierten Cloud Service Providern aufgrund der unterschiedlichen Gesetzeslage zwischen den U.S. und der EU.

b. Für die Beurteilung kritischer Bereiche des ausreichenden Datenschutzes personenbezogener Daten insbesondere internationaler Cloud Services findet sich in Kapitel 3 ein geeigneter Fragebogen an einen Cloud Service Provider.

[8] Zu bedenken ist, dass diese Aussage (Cloud ServicCe Provider innerhalb der EU) nur unter der Maßgabe richtig ist, dass es sich bei den in der EU ansässigen Anbietern nicht um solche mit US-Kapitalbeteiligung handelt.

4) Erlaubt die Kritikalität der Daten deren Auslagerung generell bzw. an einen bestimmten Cloud Service Provider?
    a. Neben der DSGVO bestehen aus unterschiedlichen anderen fachlich fokussierten Gesetzen Verpflichtungen zur Absicherung der Vertraulichkeit der durch die jeweilige öffentliche Verwaltungsorganisation verarbeiteten Daten. Das dadurch auferlegte Schutzniveau kann eine Auslagerung der Daten an einen Auftragsverarbeiter außerhalb der öffentlichen Verwaltung generell oder an einen Auftragsverarbeiter auch im europäischen Ausland verhindern.
        i. In Bezug auf eine Datenverarbeitung im europäischen Ausland (z.B. in Deutschland) dürfte die Möglichkeit des richterlichen Zugriffs auf die Daten im jeweiligen Hoheitsgebiet bestehen, falls dies Daten einer öffentlichen Verwaltung betrifft, auch ohne Rechtshilfeersuchen. Negative Konsequenzen wie z.B. Verletzung der Verpflichtungen nach dem Informationssicherheitsgesetz für klassifizierte Informationen oder Amtshaftungsklagen sind dadurch nicht auszuschließen. Eine klare europaweite Regelung, dass auf Daten einer öffentlichen Verwaltung eines EU-Mitgliedslandes unabhängig von Standort der Datenverarbeitung innerhalb der EU nur im Zuge eines Rechtshilfeersuchens zugegriffen werden darf, würde die Nutzung von europäischen Cloudservices vereinfachen.
    b. Für die Beurteilung der Kritikalität und des Schutzbedarfs von Daten findet sich in Kapitel 3 ein Fragebogen inklusiver Fragen zu Souveränität, Betriebssicherheit und Vertraulichkeit an einen Cloud Service Provider sowie in Kapitel 4 die Empfehlung zur Erarbeitung eines Systems zur Erhebung des Schutzbedarfs von Daten in jeder öffentlichen Einrichtung, die Cloud Services einsetzt bzw. einsetzen möchte.

5) Ist die staatliche Souveränität durch eine ausreichend geringe Abhängigkeit vom betrachteten Cloud Service weitergegeben?
    a. Die Nutzung von Cloud Services darf die staatliche Souveränität nicht gefährden.
    b. Ist daher ein genutztes Cloud Service für die Erfüllung der gesetzlichen Aufgaben einer Verwaltungsorganisation als wesentlich zu betrachten, dann ist dafür Sorge zu tragen, dass die Verfügbarkeit der Daten und notwendigenfalls eine Migration der Daten zu einem anderen unabhängigen Cloud Service Provider mit einem äquivalenten Service oder in ein Rechenzentrum der öffentlichen Verwaltung zu vertretbaren Kosten und innerhalb vertretbarer Zeit möglich sein muss.

6) Für die Beurteilung der Kritikalität und des Schutzbedarfs von Daten findet sich in Kapitel 3 ein Fragebogen inklusiver Fragen zu Souveränität, Betriebssicherheit und Vertraulichkeit an einen Cloud Service Provider sowie in Kapitel 4 die Empfehlung zur Erarbeitung eines Systems zur Erhebung des Schutzbedarfs von Daten in jeder öffentlichen Einrichtung, die Cloud Services einsetzt bzw. einsetzen möchte.

7) Ergibt eine umfassende wirtschaftliche Beurteilung klare Kostenvorteile der betrachteten Cloud Services zu vergleichbaren, durch die Verwaltung selbst betriebenen IT-Services?
    a. Die Beurteilung der Kostenvorteile der Nutzung eines Cloud Services hat aus einer holistischen Perspektive über einen mehrjährigen Zeitraum zu erfolgen, z.B.: Cloud Services müssen hoch standardisiert sein und können damit nicht immer die spezifischen Anforderungen der öffentlichen Verwaltung optimal erfüllen. Damit sind in die Kostenbetrachtung auch Opportunitätskosten einzurechnen, die durch suboptimale Erfüllung der effektiven Unterstützung der Prozesse der Verwaltungsorganisation entstehen.

b. Das wirtschaftlich bewertete Risiko einer erforderlich werdenden Rückabwicklung des Cloud Services ist einzupreisen (vgl. die Punkte 2.2).a.iv. und 2.5).b. oben).

3 Fragebogen zur Beurteilung kritischer Bereiche insbesondere internationaler Cloud Services

Der in diesem Kapitel enthaltene Fragebogen dient der Vorlage an Cloud Services Anbieter und deckt neben datenschutzrechtlichen Fragen, die Themen Souveränität, Sicherheit sowie Vertraulichkeit ab.

Die datenschutzrechtlichen Fragen sollen jedem Cloud-Anbieter aus einem Nicht-EU-Staat bzw. der zu einem Konzern aus einem Nicht-EU-Staat gehört, insbesondere den U.S., vorgelegt werden, um kritische Bereiche des ausreichenden Datenschutzes personenbezogener Daten für Cloud Services Anbieter aus Nicht-EU-Staaten zu beurteilen.

Gleichzeitig wurde der Fragebogen um mögliche technische Mindestanforderungen für den Einsatz im staatlichen Bereich ergänzt. Damit sollen die Einhaltung von Souveränitätsvorgaben, Betriebssicherheit sowie Vertraulichkeit sichergestellt werden. Diese Mindestanforderungen sind jedenfalls im Bereich der hoheitlichen Verwaltungsaufgaben zu erfüllen.

Ein einheitlicher Fragebogen soll unnötige Mehrfachbelastungen für die betroffenen Dienstleister vermeiden. Der beantwortete Fragebogen kann in weiterer Folge als Inhalt des vertraglichen Verhältnisses zwischen der öffentlichen Einrichtung und dem Cloud Service Provider herangezogen werden. Aus dem EU-Bereich wird auch auf die Mindeststandards des BSI[9] zur Nutzung externer Cloud-Dienste verwiesen.

Hintergrund und Motivation zur datenschutzrechtlichen Fragestellung

Der Europäische Gerichtshof hat am 16. Juli 2020 mit dem Urteil EuGH C-311/18[10] das „EU-US-Privacy-Shield" für unwirksam erklärt. Das Urteil kennt dabei keine Übergangsfrist. In seinem Urteil prüfte das Gericht auch die Gültigkeit der Entscheidung 2010/87/EG der Europäischen Kommission über Standardvertragsklauseln (Standard Contractual Clauses, "SCC") und hielt diese für gültig. Allerdings weist der Gerichtshof insbesondere darauf hin, dass der Beschluss 2010/87/EG dem Datenexporteur und dem Empfänger der Daten (dem "Datenimporteur") die Verpflichtung auferlegt, vor jeder Übermittlung unter Berücksichtigung der Umstände der Übermittlung zu prüfen, ob dieses Schutzniveau in dem betreffenden Drittland eingehalten wird. Der EuGH hält auch fest, dass der Datenimporteur verpflichtet ist, den Datenexporteur über eine allfällige Unfähigkeit zu informieren sowie die Standarddatenschutzklauseln und erforderlichenfalls zusätzliche Maßnahmen zu den durch diese Klauseln gebotenen zu erfüllen. Der Datenexporteur ist dann seinerseits verpflichtet, die Datenübermittlung auszusetzen und/oder den Vertrag mit dem Datenimporteur zu kündigen.

Die Zulässigkeit der Übermittlung personenbezogener Daten in die USA auf der Basis von SCC hängt vom Ergebnis der Beurteilung im Einzelfall ab, wobei die Umstände der Übermittlung und zusätzliche Maßnahmen, die Verantwortliche oder Auftragsverarbeiter ergreifen könnten, zu berücksichtigen sind. Die ergänzenden Maßnahmen sowie die SCC müssen nach einer Einzelfallanalyse der Umstände der Übermittlung sicherstellen, dass das US-Recht das angemessene Schutzniveau, das zu garantieren ist, nicht beeinträchtigt. Das Urteil begründet

[9] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/Externe_Cloud-Dienste_node.html

[10] Volltext abrufbar unter http://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18 (02.10.2020).

jedenfalls eine Pflicht zur aktiven Prüfung im Hinblick auf jede Übermittlung personenbezogener Daten in die USA durch die Verantwortlichen.

Die Republik Österreich hat daher auf Bundesebene unverzüglich nach dem Urteil EuGH C-311/18 einen Prozess eingeleitet, um dieser Pflicht in der Rolle des Verantwortlichen für zahlreiche Verarbeitungstätigkeiten nachzukommen. Neben der inhaltlichen Analyse wurde in diesem Rahmen insbesondere ein Fragenkatalog ausgearbeitet, der jedem Cloud-Anbieter, der zu einem US-amerikanischen Konzern gehört, in weiterer Folge vorgelegt wird. Die Fragen wurden zwischen sämtlichen Bundesministerien der Republik Österreich abgestimmt, um unnötige Mehrfachbelastungen für die betroffenen Dienstleister (Auftragsverarbeiter) von vornherein zu vermeiden. In der Sache sind die Fragen auf das notwendige Ausmaß eingeschränkt. Zugleich sind die Fragen auch speziell im Hinblick auf die Datensicherheit iSd Art 32 DSGVO formuliert, wobei insbesondere der „Kriterienkatalog Cloud Computing C5: 2020"[11] des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Orientierung herangezogen wurde. Soweit dies eindeutig zuordenbar ist, wird dies in den Fragen nachstehend auch angemerkt. Eine analoge Abstimmung mit den österreichischen Bundesländern und Kommunen (auf Einladung und Initiative des Bundes im Rahmen des gesamtstaatlichen E-Governments) wäre zweckmäßig.

FRAGESTELLUNGEN AN CLOUD-ANBIETER

Anmerkung: Der Fragenkatalog wurde in *rot* um mögliche Mindestanforderungen für den Einsatz im staatlichen Bereich ergänzt, um Souveränität und nicht durch externe Faktoren störbare Betriebssicherheit sowie allenfalls erforderliche Vertraulichkeit sicherzustellen. Diese Mindestanforderungen sind jedenfalls im Bereich der hoheitlichen Verwaltungsaufgaben zu erfüllen. IT-Verfahren, die nicht hoheitliche Verwaltungsaufgaben unterstützen, z.B. nur Information für die Öffentlichkeit zur Verfügung stellen, soweit nicht ohnehin hoheitliche Aufgabe, und einfach von Provider zu Provider übertragbar sind, können evtl. geringeren Anforderungen unterliegen.

I. Hintergrund und Motivation zur Fragestellung

Anmerkung: Hier wird der obige Text eingefügt und wiederholt.

Der **Europäische Gerichtshof** hat am 16. Juli 2020 mit dem Urteil EuGH C-311/18[12] das **„EU-US-Privacy-Shield" für unwirksam erklärt**. Das Urteil kennt dabei keine Übergangsfrist. In seinem Urteil prüfte das Gericht auch die **Gültigkeit** der Entscheidung 2010/87/EG der Europäischen Kommission über Standardvertragsklauseln (**Standard Contractual Clauses, "SCC"**) und **hielt diese für gültig**. Allerdings weist der Gerichtshof insbesondere darauf hin, dass der Beschluss 2010/87/EG dem **Datenexporteur und** dem Empfänger der Daten (dem **"Datenimporteur"**) die **Verpflichtung auferlegt,** vor jeder Übermittlung unter Berücksichtigung der Umstände der Übermittlung **zu prüfen, ob dieses Schutzniveau in dem betreffenden Drittland eingehalten wird**. Der EuGH hält auch fest, dass der **Datenimporteur verpflichtet** ist, den Datenexporteur **über eine allfällige Unfähigkeit zu informieren sowie die Standarddatenschutzklauseln** und erforderlichenfalls zusätzliche Maßnahmen zu den durch diese Klauseln gebotenen **zu**

[11] Nachfolgend kurz mit „C5: 2020" referenziert.

[12] Volltext abrufbar unter http://curia.europa.eu/juris/liste.jsf?language=de&num=C-311/18 (02.10.2020).

erfüllen. Der Datenexporteur ist dann seinerseits verpflichtet, die Datenübermittlung auszusetzen und/oder den Vertrag mit dem Datenimporteur zu kündigen.

Die **Zulässigkeit der Übermittlung** personenbezogener Daten in die USA **auf der Basis von SCC hängt vom Ergebnis der Beurteilung im Einzelfall** ab, wobei die Umstände der Übermittlung und zusätzliche Maßnahmen, die Verantwortliche oder Auftragsverarbeiter ergreifen könnten, zu berücksichtigen sind. Die **ergänzenden Maßnahmen sowie die SCC** müssen nach einer Einzelfallanalyse der Umstände der Übermittlung sicherstellen, dass das US-Recht das angemessene Schutzniveau, das zu garantieren ist, nicht beeinträchtigt. Das **Urteil begründet jedenfalls eine Pflicht zur aktiven Prüfung** im Hinblick auf **jede Übermittlung personenbezogener Daten in die USA** durch die Verantwortlichen.

Die Republik Österreich hat daher auf Bundesebene unverzüglich nach dem Urteil EuGH C-311/18 einen Prozess eingeleitet, um dieser Pflicht in der Rolle des Verantwortlichen für zahlreiche Verarbeitungstätigkeiten nachzukommen. Neben der inhaltlichen Analyse wurde in diesem Rahmen insbesondere ein Fragenkatalog ausgearbeitet, der jedem Cloud-Anbieter, der zu einem US-amerikanischen Konzern gehört, in weiterer Folge vorgelegt wird. Die Fragen wurden zwischen sämtlichen Bundesministerien der Republik Österreich abgestimmt, um unnötige Mehrfachbelastungen für die betroffenen Dienstleister (Auftragsverarbeiter) von vornherein zu vermeiden. In der Sache sind die Fragen auf das notwendige Ausmaß eingeschränkt. Zugleich sind die Fragen auch speziell im Hinblick auf die Datensicherheit iSd Art 32 DSGVO formuliert, wobei insbesondere der „Kriterienkatalog Cloud Computing C5: 2020"[13] des deutschen Bundesamts für Sicherheit in der Informationstechnik (BSI) zur Orientierung herangezogen wurde. Soweit dies eindeutig zuordenbar ist, wird dies in den Fragen nachstehend auch angemerkt.

Vielen Dank im Voraus für die sorgfältige Beantwortung unserer Fragen!

II. Fragenkatalog an NON-EU-basierte Cloud-Dienste

(Bitte möglichst umfassend auflisten, soweit bekannt bzw. feststellbar, auch wenn Sie die Eventualfrage nicht vollständig beantworten können; bitte um Angabe, falls Sie gesetzlich verpflichtet sind, diese Frage nicht zu beantworten).

1. Wo erfolgt die Datenverarbeitung, Backup und Datenhaltung?
(vgl. C5:2020 BC-01)

a) ausschließlich in Rechenzentren innerhalb der EU/EWR
b) ausschließlich in Rechenzentren innerhalb der EU/EWR, aber mit firmenmäßiger Beteiligung
von US-Unternehmen (z.B. EU-Provider mit U.S.-Mutter als Sub-Auftragsverarbeiter) US-Beteiligung (siehe auch Fragen 11 und 13)
c) in den Vereinigten Staaten von Amerika
d) in folgenden sonstigen Drittländern oder internationalen Organisationen:

Zusatzfrage zu 1.c) und 1.d): Ist eine ausschließliche Verarbeitung in Rechenzentren innerhalb der EU/EWR möglich? (C5.2020 PSS-12 fordert die Bestimmbarkeit der Region, in der die Daten verarbeitet werden)

[13] Nachfolgend kurz mit „C5: 2020" referenziert.

ANFORDERUNG (AT): Der Betrieb muss aus der Cloud in die volle Kontrolle und in die Infrastruktur österreichischer Behörden, z.B. als private, autarke Cloud und ohne Abhängigkeiten von der Public Cloud, in vertretbarer Zeit und mit vertretbaren Kosten übertragbar sein.

Mit welchen Randeffekten (z.B. Updatedelays, Übermittlungen von Kundendaten bzw. Metadaten außerhalb der EU/EWR in speziellen Fällen, z.B. Lastausgleich, richterliche Anordnung) wird diese Anforderung umgesetzt?

In welchen Stufen wird diese Anforderung umgesetzt?

2. **Welche rechtlichen Instrumente iSv Art 45 - 49 DSGVO setzen Sie für Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen ein?**

Sofern die Übertragung auf SCCs (oder alternativ auf BCRs) basiert, ersuchen wir um Vorlage dieser in der aktuellen Fassung (Internetlink ausreichend).

3. **Bestehen spezifische (technische und/oder organisatorische) Zusicherungen Ihrerseits, die über die in den SCCs/BCRs enthaltenen Datenschutz-maßnahmen hinausgehen (zusätzliche Maßnahmen, um die Einhaltung des EU-Schutzniveaus zu gewährleisten, siehe EuGH C-311/18 Randnr. 132 ff)?**

Wenn ja: bitte um Vorlage;

Wenn nein: Sind Sie bereit, solche einzugehen, insbesondere solche, die (hinkünftig) vom Europäischen Datenschutzbeauftragten/EDPB und/oder nationalen Datenschutzbehörden vorgeschlagen werden?

ANFORDERUNG (AT): Welche Zeitlinien für die Umsetzung technischer/organisatorischer Maßnahmen können in dem Fall zugesichert werden?

Welche interimistischen Übergangslösungen zur gesicherten Einhaltung des EU-Schutzniveaus sind kurzfristig umsetzbar?

4. **Wie kommen Sie den Anforderungen an Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen gemäß Art 25 DSGVO nach („Privacy by Design and by Default"); Welche Prozesse bestehen bei der Entwicklung oder der Übernahme externer Komponenten zur Wahrung des Grundsatzes nach Art 25 DSGVO?**

ANFORDERUNG (AT): Diese technischen Maßnahmen müssen für österreichische Behörden auch im Anlassfall einsehbar sein. Welche Mittel des Einsehens/ Nachvollziehens sind Bestandteil des Vertrages (Dokumentation, Source Code Einschau)?

5. **Welche konkreten risikominimierenden technischen oder organisatorischen Maßnahmen gemäß Art 32 DSGVO setzen Sie server- und clientseitig ein (z.B. Transport- und Inhaltsverschlüsselung, Bring your own key (BYOK), Double key encryption etc.)?**

(vgl. C5: 2020 CRY-02 „data in transit", CRY-03 „data at rest" und CRY-04 "Schlüsselmanagement"). Verfügen Sie als Anbieter über die Verschlüsselungskeys des Kunden? Können vom Kunden Maßnahmen gesetzt werden, um eine Entschlüsselung durch Sie als Anbieter effektiv zu verhindern?

ANFORDERUNG (AT): Wie erfolgt der Nachweis für das Vorhandensein von Bring your own key (BYOK), Double key encryption etc.? Falls erforderlich sind Übergangslösungen zu solchen Maßnahmen kurzfristig möglich, sind die Übergangslösungen in eine private, autarke Zielplattform migrierbar?

6. Die niederländische Regierung (Strategisch Leveranciersmanagement Rijk) hat Datenschutz-Folgenabschätzungen zu verschieden IT-Produkten durchgeführt. Waren Sie oder ein Produkt/Service/Dienstleistung Ihres Unternehmens davon umfasst?

Wenn ja: Welche konkreten risikominimierenden Maßnahmen wurden vereinbart oder umgesetzt? Stehen diese Vereinbarungen/Zusagen über solche Maßnahmen auch anderen Vertragspartnern offen?

7. Der Europäische Datenschutzbeauftragte (EDPS) hat eine Untersuchung zu von EU-Institutionen eingesetzter Software vorgenommen. Waren Sie oder eine Konzerneinheit davon betroffen?

Wenn ja: Welche konkreten risikominimierenden Maßnahmen wurden bzw. werden implementiert oder zugesagt?

8. Über welche aufrechten Zertifikate bzgl. Datenschutz / Datensicherheit / Datenschutzmanagementsystem / IT-Sicherheit verfügen Sie bzw. Ihre angebotenen Produkte/Services (z.B. ISO 27001 und ISO 27701)?

9. Besteht zu Ihren Produkten/Leistungen/Services ein Testat bzw. ein Report im Hinblick auf den Kriterienkatalog Cloud Computing C5:2020 des BSI?

Wenn ja: Können entsprechende Dokumente zur Verfügung gestellt werden?

10: Findet durch Sie eine Weiterverarbeitung von personenbezogenen Daten (Nutzerdaten/Telemetriedaten) für eigene Zwecke statt?

Wenn ja: Welche Daten und für welche Zwecke und auf welcher Grundlage?

Wurde eine Datenschutz-Folgenabschätzung durchgeführt? (Bitte um Vorlage bzw. Begründung, warum nicht)

Kommt es aus Ihrer Sicht dadurch zu einer gemeinsamen Verantwortung nach Art 26 DSGVO?

11. Unterliegen unsere Datenbestände bei Ihnen oder bei von Ihnen herangezogenen Sub-Dienstleistern (potentiell) Zugriffen/ Herausgabeanordnungen von Behörden, Gerichten oder anderen staatlichen Institutionen fremder Jurisdiktionen (z.B. im Rahmen des U.S. Cloud Act, 50 U.S.C. § 1881a = FISA 702)?

Wenn ja: Unter welchen Voraussetzungen dürfen diese auf in Ihrem Einflussbereich verarbeitete Daten zugreifen?

Wenn ja: Sind Sie in der Lage, einen solchen Zugriff faktisch zu blockieren? Bitte geben Sie an, auf welchen rechtlichen und/oder technischen Schutz Sie sich berufen.

11.a. Sind Sie oder ein von Ihnen herangezogener Sub-Dienstleister

a) ein Telekommunikationsanbieter (47 U.S.C § 153)?
b) ein Anbieter elektronischer Kommunikationsdienste (18 U.S.C. § 2510)?
c) ein Anbieter eines Remote-Computing-Dienstes (18 U.S.C § 2711)?
d) ein anderer Kommunikationsdiensteanbieter, der Zugang zu drahtgebundener oder elektronischer Kommunikation hat, entweder während diese Kommunikation übertragen oder gespeichert werden?

ANFORDERUNG (AT): Im Sinne der staatlichen Souveränität darf ein Zugreifen nur durch österreichische Behörden erfolgen. Welche Prozesse sind vorhanden, die diese Umstände absichern?

Bestehen Möglichkeiten, Bring-your-own-key-Verschlüsselung auf Anordnung zu umgehen?

12. Wie erfolgt die interne Prüfung solcher Zugriffe/Herausgabeanordnungen? Gehen Sie als Cloud-Anbieter rechtlich dagegen vor?
(vgl. C5: 2020, INQ-01, INQ-02 und INQ-04 zur Darstellung der entsprechenden Prozesse)

13. Wie kommen Sie als Anbieter von Cloud-Diensten den Vorgaben des Art 48 DSGVO (Unzulässigkeit extraterritorialer Datenzugriffe von Drittstaaten) nach? Sind Sie als Anbieter technisch und rechtlich in der Lage, Art 48 DSGVO zu erfüllen?

14. Arbeiten Sie oder eine andere relevante US-Einheit als Verantwortlicher oder (Sub-) Auftragsverarbeiter für personenbezogene Daten in irgendeiner Hinsicht (freiwillig oder verpflichtend) mit den US-Behörden zusammen, die die Überwachung der Kommunikation beispielsweise gemäß Executive Order EO 12.333 durchführen?

14.a. Haben Sie für jeden Schritt der Verarbeitung geeignete technische und organisatorische Maßnahmen (siehe Art 32 DSGVO) ergriffen, mit denen sichergestellt wird, dass eine massenhafte und wahllose Verarbeitung personenbezogener Daten durch oder im Auftrag von U.S. Behörden im Transit (wie im Rahmen des "Upstream"-Programms in den USA) unmöglich gemacht wird (FISA 702 and EO 12.333)?

Wenn ja: Welche technischen und organisatorischen Maßnahmen (einschließlich Verschlüsselung) wurden getroffen, damit weder Inhalte noch Metadaten von ausgeklügelten staatlichen Akteuren mit direktem Zugang zum Internet-Backbone, zu Switches, Hubs, Kabeln und dergleichen verarbeitet werden können?

15. Unterliegen Sie oder eine andere relevante Unternehmenseinheit (für die Verarbeitung Verantwortlicher oder Auftragsverarbeiter) bzw. von Ihnen herangezogene Subdienstleister, die personenbezogene Daten des jeweiligen Kunden verarbeiten, anderen ausländischen Gesetzen bzw. sonstigen Regularien / Anordnungen, die als Minderung des Niveaus des Schutzes personenbezogener Daten gegenüber dem Schutzniveau der DSGVO (siehe insb. Art 44 DSGVO) angesehen werden könnten?

Bei Cloud-Lösungen, die Teil eines wesentlichen Dienstes lt. NISG sind, ist die Überprüfung der Umsetzbarkeit der Sicherheitsmaßnahmen laut Anlage 1 der Netz- und Informationssystemsicherheitsverordnung – NISV erforderlich. RIS Dokument (bka.gv.at)

16. Informieren Sie die Betroffenen über derartige Zugriffe/ Herausgabeanordnungen?

(vgl. C5:2020, INQ-02)

Wenn ja: Wie?

Wenn nein: Warum nicht?

17. Mit welchen technischen Mitteln können Sie garantieren, dass der Betrieb nicht durch Maßnahmen, die von außerhalb Österreich kommen – einschließlich vom Hersteller selbst, der allenfalls unter Anordnung handelt – unterbrochen oder unterbunden werden kann und die Souveränität des Staates dadurch nicht untergraben wird?

4 Aspekte der Kryptographie und der Sicherheit insbesondere auch bei großen Cloud-Anbietern

Dazu wurden im Herbst 2021 Amazon(AWS), Microsoft(AZURE)[14], Google und SAP befragt und die als verbindlich bezeichneten Antworten sind nachfolgend zusammengefasst:

- Die Cloud muss in der Lage sein, Daten so zu verschlüsseln, dass es ausschließlich dem Nutzer (und nicht dem Cloud-Provider) möglich ist, diese zu entschlüsseln.
    - **AWS (Amazon Web Services:** Cloud HSM FIPS 140-2 Level 3 zertifiziert (AWS Artifact) ist geeignet, aus technischer Hinsicht den Zugriff und die Schlüsselerzeugung auf den Kunden (österr. Verwaltung) einzuschränken. Physische Initialisierung vor Ort (z.B. in Frankfurt) ist technisch und organisatorisch möglich.
    - **AZURE:** Im Rahmen der Azure Information Protection Lösung kann ein Microsoft Cloud Kunde Verschlüsselungsschlüssel in FIPS 140 (bis zu Level 3) validierten Hardwaresicherheitsmodulen (HSMs) unter seiner ausschließlichen Kontrolle initialisieren und für den Schlüsselzugriff und die Schlüsselverwaltung den Schlüsselverwaltungsdienst Azure Key Vault nutzen. Damit hat Microsoft keine technische Möglichkeit eines Schlüsselzugriffs. Derzeit sind derartige Cloud-Dienste in mehreren Cloud Regionen in der EU verfügbar; bedarfsorientiert ist dies auch in Österreich denkbar.
    - **GOOGLE:** Google kann nach Common Criteria zertifizierte HSM einsetzen und diese können vom Kunden mit den vom Kunden vorgegebenen Sicherheitslevels initialisiert werden. Damit geraten die geheimen Schlüssel zu keinem Zeitpunkt in die Hände von Google. Eine derartige Verschlüsselung findet grundsätzlich zusätzlich zur Verschlüsselung des gesamten Cloud-Verkehrs nach den Standard Schemen von Google statt.
    - **SAP:** SAP verschlüsselt Daten am Speicherort (at-rest, z.B. AES 256-bit Verschlüsselung) und während der Übertragung (in-transit, HTTPS mit 256-bit AES Verschlüsselung, TLS 1.2). Schlüssel werden durch SAP sicher verwaltet. Durch Kunden selbst verwaltete Schlüssel (BYOK, Bring-Your-Own-Key) wird bislang, bis auf wenige Ausnahmen, nicht unterstützt. SAP klassifiziert in den Cloud Services verarbeitete Kundendaten als „Vertraulich" und gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit der personenbezogenen Daten im Cloud-Service vertraglich durch den Einsatz angemessener Technischer und Organisatorischer Maßnahmen (TOMs), darunter u.a. Datenzugriffskontrolle. Dies gilt gleichermaßen auch beim Einsatz von Hyperscalern als Sub-Auftragsverarbeiter für SAP Österreich (sofern relevant): Hyperscaler haben keinen Zugriff auf unverschlüsselte Kundendaten im Cloud Service.

- Der Cloud-Provider bietet Verträge an, die unter österreichischem Recht und mit Gerichtsstand Österreich abgeschlossen werden.
    - **AWS:** Grundsätzlich werden Verträge nach luxemburgischem Recht und mit Gerichtsstand Luxemburg geschlossen. Gesetzliche Anforderungen eines EU-Mitgliedstaates können umgesetzt werden.
    - **AZURE:** Verträge über Microsoft Produkte und Services werden zw. Microsoft und einem Volumenlizenzkunden in der EU grundsätzlich nach irischem Recht und teilweise mit Gerichtsstand Irland abgeschlossen (d.h. es gilt jener

[14] Die Angaben sind eine unverbindliche Zusammenfassung der Microsoft Österreich GmbH und dient dem Fragesteller nur zu Referenzzwecken. MICROSOFT GIBT KEINE GARANTIEN, WEDER AUSDRÜCKLICH NOCH STILLSCHWEIGEND.

Gerichtsstand wo die beklagte vertragsschließende Partei ihren Hauptsitz hat; Microsoft Irland ist Vertragspartei eines EU-Kunden).
    - **GOOGLE:** Google kann Verträge nach österreichischem Recht abschließen und eine Vereinbarung eines ordentlichen Gerichts in Österreich als Gerichtsstand ist möglich.
    - **SAP:** Cloud-Verträge mit SAP Österreich werden nach österreichischem Recht und mit Gerichtsstand in Österreich geschlossen.

- Der Cloud-Provider ist in der Lage für Management und Nutzung eIDAS (EU eID) zu verwenden ohne, dass Daten bzw. Services mit anderen Identifikationstechnologien zugänglich werden und Österreich damit in der Lage ist die Verantwortung zu übernehmen.
    - **AWS:** Auf der Nutzungsebene ist eIDAS voll umsetzbar und es existieren auch Referenzen, die unter NDA ansprechbar wären. Auf der Managementebene bietet AWS eigene Methoden (Nitro Hypervisor), die die Verantwortung seitens des Kunden nicht einschränken und sicherstellen, dass eIDAS Umsetzungen nicht kompromittiert werden können.
    - **AZURE:** Auf Nutzungsebene ist derzeit eine voll eIDAS konforme Einbindung schon möglich.
    - **GOOGLE:** Ein Einbinden von eIDAS als Identifikationsschema mit allen Sicherheitsmechanismen, die es dem Staat Österreich ermöglichen, die Haftungen, die eIDAS erfordert, auch wahrzunehmen, ist möglich. Entsprechende Erweiterungen von Chrome sind auch bereits in Belgien in Verwendung.
    - **SAP:** SAP Cloud Services erlauben Single Sign-On (SSO) durch die Möglichkeit der Anbindung ggf. bereits vorhandener Identity Authentication Services oder Active Directory Federated Services (ADFS), zum Beispiel mittels SAML 2.0 Protokoll – über die auch der Einsatz von Multi-Faktor Authentication (2FA, MFA) gesteuert werden kann. Alternativ ist die Verwendung des in der Miete enthaltenen SAP Identity Authentication Services (IAS) möglich. SAP IAS unterstützt ebenfalls den Einsatz von 2FA.

- Es existiert ein nachvollziehbarer Nachweis, dass Sicherheitslücken (Meltdown und ähnliche aus dieser Kategorie) geschlossen wurden.
    - **AWS:** Soweit es technisch möglich ist und im Einflussbereich AWS liegt, schließt AWS Sicherheitslücken zeitnah. Darüber hinaus betont AWS, dass Sicherheit in der Cloud eine geteilte Verantwortung zwischen dem Kunden und dem Cloud Service Provider darstellt ("Shared Responsibility"-Modell). Es gibt Patches, die zwingend vom Kunden eingespielt werden müssen: AWS hat technisch und organisatorisch keinen Zugriff auf die entsprechende Ausführungsebene der Kundeninstanz. AWS geht das Thema des "Vulnerability-Management" systematisch gemäß des eigens definierten "Information Security Management System" (ISMS) an: AWS zeichnet sich verantwortlich für die Sicherheit der Cloud, der Kunde für die Sicherheit in der Cloud: An den Stellen, wo nur AWS als Cloud-Service-Provider Sicherheit herstellen kann, ergreift AWS die entsprechenden Maßnahmen. Das Vorgehen ist und wird fortwährend im Zuge der ISO, SOC und C5 Audits durch unabhängige Dritte geprüft.
    - **AZURE:** Microsoft ergreift geeignete technische und organisatorische Maßnahmen, um Kundendaten, Professional Services-Daten und personenbezogene Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden, vor versehentlicher oder ungesetzlicher Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugriff zu

schützen. Diese Maßnahmen werden in einer Microsoft-Sicherheitsrichtlinie festgelegt. Microsoft stellt diese Richtlinie bei Bedarf dem Kunden zur Verfügung, zusammen mit anderen Informationen über die Sicherheitsverfahren und -richtlinien von Microsoft, die der Kunde angemessen anfordert. Darüber hinaus erfüllen diese Maßnahmen die Anforderungen von ISO 27001, ISO 27002 und ISO 27018.
    - **GOOGLE:** Die Schwachstellen Meltdown und der damit bekannten Derivate sind in den Systemen die Google einsetzt geschlossen. Google hat ein klares Commitment, auch in Hinkunft bekanntwerdende Schwachstellen rasch zu schließen.
    - **SAP:** SAP gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit personenbezogener Daten im Cloud Service vertraglich durch den Einsatz angemessener technischer und organisatorischer Maßnahmen (TOMs). Die entsprechende Umsetzung der TOMs wird regelmäßig durch unabhängige Dritte überprüft und in entsprechenden Prüfberichten (bspw. SOC-2 Typ II, BSI C5) dokumentiert. Prüfberichte stehen Kunden auf Nachfrage zur Verfügung. Identifizierte Sicherheitslücken werden risikobasiert gepatcht (Bewertung entsprechend CVSS-Standard). Der Einsatz von Hyperscalern als Sub-Auftragsverarbeiter verändert dieses Vorgehen der SAP nicht (sofern relevant).

- Sicherheitsüberprüftes vertrauenswürdiges Personal
    - **AWS:** AWS verfügt über einen klar definierten und strikten Prozess bei der Einstellung von Personal. Dieser kann je nach den vorhandenen landesspezifischen Gesetzen im Detail variieren.
    - **AZURE:** Microsoft Personal ist nach firmeninternen Standards sicherheitsüberprüft.
    - **GOOGLE**: Die Anforderung von sicherheitsüberprüftem Personal kann primär durch Verwenden von Personal aus dem EU-Raum (EU-BürgerInnen) abgedeckt werden.
    - **SAP:** SAP gewährleistet vertraglich, dass SAP und ihre Sub-Auftragsverarbeiter für die Verarbeitung von personenbezogenen Daten nur befugten Personen Zugriff gewährt, die sich zur Wahrung der Vertraulichkeit dieser Daten verpflichtet haben. SAP und ihre Sub-Auftragsverarbeiter schulen die befugten Personen, denen der Zugriff auf personenbezogene Daten gewährt wird, in regelmäßigen Abständen in Bezug auf die geltenden Datenschutz- und die zugehörigen Datensicherheitsmaßnahmen.

- Durchgängiges DNSSEC kann wesentliche Elemente einer „Man in the middle" Attacke vor allem bei Services für den Enduser bieten.
    - **AWS:** Betreibt das physische Netzwerk zwischen "Availability"-Zonen, Regionen und den "Point-of-Presence" Standorten wie unsere Edge-Standorte – auch in Wien – eigenständig, siehe https://aws.amazon.com/de/about-aws/global-infrastructure/ und https://aws.amazon.com/de/cloudfront/features/?whats-new-cloudfront.sort-by=item.additionalFields.postDateTime&whats-new-cloudfront.sort-order=desc Es findet an dieser Stelle kein "Public Internet Routing" statt.
    - **AZURE:** Ein Point-of-Presence in Österreich wird ab 1.HJ 2023 durch Microsoft umgesetzt sein. Bis dahin ist dies über Drittanbieter in Österreich auch heute schon möglich. DNSSEC Planungsstand und Verfügbarkeit wird in den Service Roadmaps angekündigt (z.B. siehe O365 Roadmap (SMTP) Microsoft 365-Roadmap | Microsoft 365).

- **GOOGLE:** Google besitzt im 21. Wiener Gemeindebezirk einen Point-of Presence zur Wahrung der Sicherheit (z.B. Abwehr von DNS basierten Attacken oder Umleitungen).
- **SAP:** Siehe auch Antwort zu Frage 1.: Man in the middle Attacken werden durch den Einsatz unterschiedlicher Maßnahmen verhindert, darunter die Verwendung einer globalen Zertifizierungsstelle (Certificate Authority: VeriSign), Netzwerk-Separierung und entsprechende Zugangskontrollmechanismen, ein zentrales Malware-Management System, Intrusion Prevention Systeme, u.v.m.. Dies gilt gleichermaßen auch beim Einsatz von Hyperscalern als Sub-Auftragsverarbeiter für SAP Österreich (sofern relevant).

5 Kritikalität und Schutzbedarf von Daten bestimmen

Bei der Nutzung von Cloud-Diensten bilden der Schutz und die Verfügbarkeit von Daten einen wichtigen Aspekt. Die Verwaltung ist grundsätzlich verpflichtet, Daten zu schützen und Geheimnishaltungspflichten zu gewährleisten. Die Entscheidungskompetenz, welche Anwendungen/Daten wo gespeichert werden, liegt bei den einzelnen Einrichtungen der öffentlichen Verwaltung. Bei der Haltung von Anwendungen und Daten durch Cloud Services, insbesondere in sogenannten Public Cloud, ist die Prüfung der Rechtskonformität sowie einer Risikobeurteilung im Vorfeld zu empfehlen.

Zur Bestimmung der Kritikalität von Daten wird daher jeder Einrichtung empfohlen, einen strukturierten Umgang mit potentiell betroffenen Daten durch ein internes Verfahren zu entwickeln. Im eigenen Wirkungsbereich – dort wo möglich auch Einrichtungs-übergreifend – empfiehlt es sich, ein System der Kategorisierung von Daten zu entwickeln, das die Kritikalität und den Schutzbedarf festlegt.

Daraus soll sich auf einfache Weise und unabhängig von weiteren technischen Fortschritten ableiten lassen, welche Anforderungen an Cloud Services bei der Verarbeitung zur berücksichtigen sind. Bereits vorhandene Standards und Regulativen, wie etwa Klassifizierungsstufen, sollten bei der Erarbeitung Berücksichtigung finden. Diese Kategorisierung geht dabei über die bloße Anwendung auf Cloud Computing hinaus; sie konkretisiert gleichzeitig Anforderungen der Informationssicherheit und macht diese für die betroffene Einrichtung im eigenen Wirkungsbereich anwendbar.

Um die größtmögliche Steuerungswirkung zum Zwecke eines sicheren und einheitlichen Umgangs mit Cloud Computing in der öffentlichen Verwaltung zu erreichen, wird auch ein Austausch zwischen den Verwaltungseinrichtungen zu diesem Thema empfohlen.

Anhang 1: Begriffsdefinition

Cloud Computing setzt sich aus zum Teil zwar altbekannten Architekturen und Konzepten zusammen, die aber Dank fortschreitender technischer Entwicklungen erstmals markttauglich umsetzbar sind. Einer der Schlüsselaspekte hinter dem breiten Interesse an Cloud Computing ist eine mögliche wirtschaftliche Effizienzsteigerung gegenüber traditionellen IT-Verfahren. Dazu ist aber anzumerken, dass es sich nach wie vor trotz der unbestritten hohen Skalenvorteile internationaler Clouds auch um strategische Preisbildung seitens der Anbieter handelt und damit die Stabilität des Preises vom Willen der Anbieter abhängt. Dem zur Seite stehen Begriffe wie Kunden/Nutzer/Auftraggeber/Anwender, Organisation, IT-Organisation, wobei im Zusammenhang mit Cloud Computing folgendes damit verstanden werden soll:

Cloud Computing[15] ist das Anbieten bzw. Nutzen von Ressourcen oder Diensten, die über Netzwerke zur Verfügung gestellt werden. Charakteristisch ist des Weiteren, dass Ressourcen oder Dienste nicht dediziert einem Kunden zugeordnet, sondern auch dynamisch zur Verfügung gestellt werden (shared services/resources).

[15] Das National Institute of Standards and Technology (NIST) kategorisiert Cloud Computing Dienste anhand von Charakteristiken, Servicemodellen sowie Einsatzvarianten.

Anhang 2: Rechtliche Aspekte

Die rechtliche Situation ist aufgrund der Tatsache, dass es unter den großen nur Anbieter aus Drittstaaten gibt, in besonderer Weise diffizil. Mit der Datenschutzgrundverordnung und den diversen Erkenntnissen (z.B. Schrems) wurde die Situation in einen klareren Rahmen gestellt. Dennoch ist allen Playern bewusst, dass eine Fülle von Aspekten noch offen ist und aufgrund der international deutlich unterschiedlichen und widersprüchlichen Rechtslage und Praxis auch zwiespältig bleiben muss. Daher wurde hier in der bestehenden Form der Ansatz gewählt, Teile der rechtlichen Aspekte im Anhang 1 in Form eines Fragenkataloges zusammenzufassen. Der Fragenkatalog ist damit abtrennbar und auch direkt verwendbar. Gleichzeitig stellt die Form des Fragenkataloges klar, dass es sich um keine abschließende Zusammenfassung handelt, sondern um eine Basis, die dem Nutzer bzw. Betreiber von Services auch einen Verantwortungs- und Entscheidungsspielraum offenlassen muss.

Öffentliche Daten – also Daten, die ohnehin öffentlich zugänglich sind – können grundsätzlich in jeder Cloud-Lösung verarbeitet werden (z.B. veröffentlichte Berichte, Webematerialien).[16]

Gerade bei Verantwortlichen des öffentlichen Bereichs fallen „spezielle" Daten an (systemkritische / staatstragende Daten, Amtsverschwiegenheit, personenbezogene Daten nach Art 9 und 10 DSGVO und dem 3. Hauptstück DSG etc.), deren „Outsourcing" und Verarbeitung speziellen Anforderungen unterliegt:

- Anforderungen an die Lokalität der Daten (Aufbewahrung in Österreich)
- rechtliche Anforderungen an den Anbieter (zwingende Anwendbarkeit österreichischen Rechts bzw. Kontrolle durch österreichische Einrichtungen)
- Offenbarungspflichten gegenüber dem Staat des CSP
- Sicherheit / Verfügbarkeit und Vertraulichkeit / Schutz vor unbefugter Preisgabe von Informationen / Integrität, Datensouveränität, Authentizität / Autorisierung
- spezielle Anforderungen (z.B. im Bereich der Sicherheit- oder Gesundheitsverwaltung)
- Interoperabilität[17]

Daher werden **bestimmte Daten (-verarbeitungen)** insb. aus Gründen des Daten- und Geheimnisschutzes, des Schutzes systemkritischer Institutionen und Informationen und der IT-Sicherheit aus derzeitiger Sicht **nicht „Cloud-geeignet"** sein. Hier kann z.B. auf das Informationssicherheitsgesetz (InfoSiG) i.V.m. der Informationssicherheitsverordnung zurückgegriffen werden: Demnach gibt es Daten, für die besondere Sicherheitsvorkehrungen (insb. betreffend Vertraulichkeit / Zugriffskontrolle, Integrität, Verfügbarkeit) zu treffen sind.[18]

[16] Leschanz/Ehrnberger, Interne Nutzung von Cloud-Dienstleistungen in Unternehmen, Dako 2015//45, 84 ff.
[17] Vgl. Hinterseer, Masterarbeit – Öffentliche Verwaltung in der Cloud, 90 f mwN.
[18] Vgl. Hinterseer, Masterarbeit – Öffentliche Verwaltung in der Cloud, 43 mwN.

Datenschutz

Werden personenbezogene Daten verarbeitet?

Werden keine personenbezogenen Daten verarbeitet, dann ist keine weitere datenschutzrechtliche Prüfung erforderlich.

Neben den in diesem Kapitel allgemein ausgeführten Überlegungen wird für die Leistungserbringung in einem Nicht-EU-Land bzw. durch einen Nicht-EU Cloud Service Provider insbesondere auch auf den Fragenkatalog in Anhang 1 verwiesen.

Wenn es sich hingegen um personenbezogene Daten handelt, dann sind bei der Wahl des Cloud Service Providers (CSP), welcher im Regelfall als Auftragsverarbeiter[19] im Sinne des Art. 4 Z 8 Datenschutz-Grundverordnung (DSGVO) (ggf. § 36 Abs. 2 Z 9 i.V.m. § 48 DSG) – zu dessen sorgfältiger Auswahl der Verantwortliche unter Berücksichtigung der IT-Sicherheit verpflichtet ist – anzusehen ist (wobei ja nach Ausgestaltung auch eine gemeinsame Verarbeitung mit dem Cloud-Anbieter vorliegen könnte, wenn der Cloud Anbieter personenbezogene Daten auch für eigene Zweck verwendet, wie z.B. Optimierung des Produkts und der Kundenfreundlichkeit; vgl. EuGH 05.06.2018, C-210/16 „Wirtschaftsakademie"; EuGH 29.07.2019, C-40/17 „Fashion ID"),, nachstehende Fragen zum Datenschutz zu prüfen. Alle Fragen sind vor der Auswahl eines Cloud Services stets mit „**Ja**" zu beantworten:

Verarbeitungs- bzw. Speicherort von Daten (Storage)

Bestimmte Datenschutzbestimmungen verbieten den Transfer von personenbezogenen Daten (Art 4 Z 1 DSGVO; § 36 Abs. 2 Z 1 DSG) in andere oder bestimmte Länder, oder es ist die explizite Zustimmung durch jene Person, auf die sich die Daten beziehen, erforderlich (wobei etwa betreffend Mitarbeiterdaten bei Einwilligung im Beschäftigungskontext im Hinblick auf die Freiwilligkeit strenge Maßstäbe angelegt werden bzw. die Personalvertretung zu beteiligen ist (jeweiliges Personalvertretungsgesetz „Planung und Einführung neuer Technologien"; Einbindung der Personalvertretung im Rahmen der Datenschutz-Folgenabschätzung nach Art 35 Abs. 9 DSGVO bzw. § 52 DSG)). Eine dynamische Umverteilung im Laufe der Zeit ist mit zu beachten.

Bestehende Regelungen, wonach Daten ausschließlich im Inland gespeichert werden dürfen (z.B. im Zusammenhang der umfassenden Landesverteidigung), schließen CSP außerhalb Österreichs aus!

- Werden die Daten ausschließlich im europäischen Wirtschaftsraum oder in Ländern, die im Angemessenheitsbeschluss der Europäischen Kommissionangeführt sind, verarbeitet? [20]

[19] Es wird angemerkt, dass der Auftraggeber (Verantwortlicher) bei der Auswahl seines Dienstleisters (Auftragsverarbeiters) die freie Wahl hat, jedoch muss dieser auch die Dienstleisterpflichten (Verpflichtungen nach Art 28 DSGVO) einhalten. Der Verantwortliche hat weiters seine Verantwortlichenpflichten einzuhalten bzw. sicherzustellen, dass sein Auftragsverarbeiter dies tut. Die Verantwortung für die Einhaltung dieser Verantwortlichen- und Auftragsverarbeiterpflichten verbleibt jedoch letztlich beim Verantwortlichen (ausgenommen Auftragsverarbeiterexzesse nach Art 28 Abs. 10 DSGVO). Im Einzelfall kann die Abgrenzung der Rolle des Verantwortlichen und des Auftragsverarbeiters schwierig sein. Im Zweifel ist jedoch anzunehmen, dass die Behörde als Verantwortlicher angesehen wird.

[20] Ein Angemessenheitsbeschluss ist ein Beschluss, der von der Europäischen Kommission gemäß Artikel 45 DSGVO angenommen wird und durch den festgelegt wird, dass ein Drittland (d. h. ein Land, das nicht an die DSGVO gebunden ist) oder eine internationale Organisation ein angemessenes Schutzniveau für personenbezogene Daten bietet. Im Rahmen dieses Beschlusses werden die innerstaatlichen Rechtsvorschriften des Landes, seine Aufsichtsbehörden und die von ihm eingegangenen internationalen Verpflichtungen berücksichtigt. Ein solcher Beschluss bedeutet, dass personenbezogene Daten von den EU-Mitgliedstaaten und den Mitgliedstaaten des Europäischen Wirtschaftsraums ohne weitere Anforderungen

- Wenn nein, liegt eine Genehmigung der Datenschutzbehörde oder liegen Standardvertragsklauseln[21] für die Übermittlung personenbezogener Daten in Drittländer (2001/497/EG geändert durch den Kommissionbeschluss (EU) 2016/2297 vom 16. Dezember 2016) vor?

Datensicherheitsmaßnahmen

- Stellt der Auftragsverarbeiter die Maßnahmen zur Datensicherheit gemäß Art. 5 Abs. 1 lit. f DSGVO sowie Art 28 Abs. 3, 4, 5 und 10 sicher?
- Trifft der Auftragsverarbeiter insbesondere Maßnahmen zum Schutz vor zufälliger und unrechtmäßiger Zerstörung?
- Trifft der Auftragsverarbeiter insbesondere Maßnahmen gegen den Verlust oder unbefugten Zugriff auf die Daten?
- Trifft der Auftragsverarbeiter insbesondere Maßnahmen zur Protokollierung der Zugriffe?
- Setzt der Auftragsverarbeiter Technologien ein, bei denen
  - Datenflüsse mit Transportverschlüsselung (TLS) abgesichert sind und
  - eine Ende-zu-Ende Verschlüsselung stattfindet.

Datenschutz-Folgenabschätzung

Die Cloud wird zwar sowohl in der DSGVO als auch im DSG nicht explizit als „neue oder neuartige" Technologie genannt, jedoch spricht sich die Lehre aktuell dafür aus, dass Cloud Services auf Grund ihrer relativen Neuartigkeit und den damit vorhandenen Risiken eine Pflicht zur Datenschutz-Folgenabschätzung begründen können. Dies insbesondere dann, wenn der Verantwortliche aufgrund der Organisation einen Kontrollverlust hinnimmt und im Zusammenhang mit einer vollständigen Beherrschbarkeit des Verfahrens Zweifel bestehen.

Informationspflichten und Betroffenenrechte (Recht auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertrag-barkeit, Widerruf und Widerspruch) gemäß Artikel 12 bis 23 DSGVO bzw. §§ 42 ff DSG

Zugriff auf Daten (Access): Die Person, auf die sich Daten beziehen (d.h. die betroffene Person im Sinne der DSGVO bzw. des DSG), kann sowohl Auskunft über als auch Korrektur oder das Löschen dieser Daten verlangen.

- Ist daher sowohl die Einsichtnahme als auch die Richtigstellung bzw. das Löschen der Daten der Betroffenen in der Cloud (Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerruf und Widerspruch) gemäß den rechtlichen Vorgaben gewährleistet und durchführbar?

---

an dieses Drittland übermittelt werden können. Die Europäische Kommission veröffentlicht eine Liste ihrer Angemessenheitsbeschlüsse auf ihrer Website.

Die Übermittlung an Empfänger innerhalb der EU/des EWR ist keinen weiteren (als den allgemeinen) Beschränkungen unterworfen. Das ergibt sich aus Artikel 3 DSGVO – Anwendungsbereich innerhalb der EU – und der Übernahme der DSGVO in das EWR-Abkommen. Die Übermittlung an Empfänger außerhalb der EU/des EWR ist auf Grundlage der Artikel 44 ff DSGVO zulässig, etwa aufgrund eines Angemessenheitsbeschlusses oder geeigneter Garantien.

Gemäß Artikel 44 Absatz 3 DSGVO können geeignete Garantien, vorbehaltlich der Genehmigung durch die Datenschutzbehörde, in Vertragsklauseln und Verwaltungsvereinbarungen bestehen.

21 Derzeit werden die Standardvertragsklauseln überarbeitet. Der EuGH erklärt sie in seinem Urteil „Schrems II" unter bestimmten Voraussetzungen weiterhin für zulässig, allerdings besteht eine Prüfpflicht auf Seiten des Verantwortlichen (Datenexporteurs) sowie des Datenimporteurs. Diese bezieht sich darauf, ob die Standardvertragsklauseln für die Übermittlung bereits hinreichende Garantien bieten oder ob zusätzliche Garantien geschaffen werden müssen.

- Gibt es ein Regelwerk, das das Verfahren zur Wahrung der Rechte betroffenen Person in bei gemeinsamer Verantwortung klar regelt?

Verbleib und Vernichtung von Daten (Retention/Destruction)

Am Ende der Haltezeit (Löschfrist) von Daten müssen diese geeignet gelöscht oder der (Langzeit-) Archivierung zugeführt werden.

- Gibt es ein Regelwerk zur Umsetzung der Skartierung von Daten (Retention-Policy)?
- Gibt es ein Regelwerk zur Skartierung von Protokolldaten einschließlich Verkehrs- und Metadaten?
- Werden die Daten tatsächlich gelöscht (und nicht nur die Zugriffsrechte entzogen)?
- Ist dabei sichergestellt, dass keine Kopien der Daten (z.B. Back-Up) erhalten bleiben?
- Gibt es ein Regelwerk, wonach die Zurückstellung / Übertragung (inkl. Löschung der Daten beim CSP) an den Verantwortlichen nach Beendigung des Vertragsverhältnisses erfolgt?

Datenschutzverletzungen (Privacy/Data Brauches)

Ist bei Datenschutzverletzungen ein Meldeprozess bei Verantwortlichen und Auftragsverarbeiter etabliert, damit der Verantwortliche seinen Verpflichtungen nach Art 33 f DSGVO und §§ 55 f DSG nachkommen kann?

Vertragsrecht

Sollte immer auf den Einzelfall abgestimmt sein. Folgende Punkte könnten jedoch Inhalt einer vertraglichen Regelung sein:

- Allgemeine Cloud-Computing Bedingungen inkl. Ausschluss abweichender AGB
- Nutzungsrechte an den eingebrachten Inhalten
- Zusicherung der Einhaltung der datenschutzrechtlichen Anforderungen
- Informationsverfahren bei datenschutzrechtlichen Verletzungen
- Gewährung eines Kontrollzugriffs durch den Verantwortlicher
- Auftragsverarbeitervereinbarungen (abhängig von der Anzahl der Auftragsverarbeiter bzw. Sub-Auftragsverarbeiter die in Anspruch genommen werden)
- Art der Leistung (Leihe, Miete, Werk- oder Dienstleistung)
- Leistungsstörungen, Schadenersatz, Haftung und Gewährleistungsansprüche Vertragsstrafen bei Verstößen;
- Technische Revision
- Haftung und Gewährleistungsansprüche
- Service-Level-Agreement (SLA) zu einem bestimmten Zeitpunkt fixieren;
- Verfügbarkeit des Service
- Sonstige Vereinbarungen und Vorlage eines Sicherheitskonzepts, wie regelmäßige Überprüfung des Auftragsverarbeiters (regelmäßige Audits), ggf durch Nachweis einer ISO Zertifizierung (z.B. ISO 27001, Informationssicherheitsmanagementsystem (ISMS))
- Einhaltung referenzierter Konvention (internationale Standards, BLSG-Konventionen)
- Migrierbarkeit der (Daten-)Standards im Fall des Betreiberwechsels, Unternehmensübergang oder im Insolvenzfall

- Gegebenenfalls können Auftragsverarbeiter bei der Erfüllung der Betroffenenrechte herangezogen werden
- Einspielen der neuesten Sicherheitspatches und Updates
- Häufigkeit von Sicherungen (Backups)
- Wo liegen die Backups – werden die Backups verschlüsselt
- Wie lange dauert ein Restore im Fehlerfall (Anforderungszeit – bis Umsetzung)
- Konzept für Disaster Receivers:
    - Wie lange darf ein Geschäftsprozess ausfallen
    - Wieviel Datenverlust kann in Kauf genommen werden
    - Unterbrechungsfreie Dienste
- Gerichtsstand
- Laufzeit und Folgen der Vertragsbeendigung
- Art und Weise der Datenrückgabe nach Art 28 Abs. 3 lit. g DSGVO (Zeitpunkt, Format etc.)
- Weisungsrecht des Verantwortlichen nach Art 29 DSGVO bzw. § 48 Abs. 6 DSG
- Kündigungsrechte (einseitige Kündigungen durch CSP)
- Abhängigkeitsprüfung
- Changemanagement durch den CSP
- Konventionalstrafen

Vergaberecht

Cloud Service Provider sind meist international tätig und stellen ihre Leistungen unter Standard-AGB zur Verfügung. Eine Anpassung der Standard-AGB an widersprüchliche Ausschreibungsbedingungen ist unwahrscheinlich. Daher sind die AGB geeigneter Cloud Service Provider Kandidaten auf Kompatibilität zu den rechtlichen Rahmenbedingungen für die öffentliche Hand in Österreich zu prüfen, bevor in Aufwände für eine Ausschreibung investiert wird.

Cloud Services bieten vielfach proprietäre Funktionen mit Monopolcharakter (z.B. im Bereich der Services für mobile Endgeräte oder im Bereich von Office-Produkten). Eine herkömmliche Ausschreibung ist daher oft nicht möglich. Ausschließlichkeitskriterien müssen evaluiert werden und bei Vorlage dieser nur eine Händlerausschreibung durchgeführt werden. Die Rechtskonformität abseits des Vergaberechts auch von monopolartigen Services ist natürlich trotzdem sicherzustellen.

Strafprozessrecht

Innerstaatliche Auskunftspflichten gegenüber österreichischen Strafverfolgungsbehörden sind zu beachten (z.B. Verkehrsdaten).

Auch Auskunftspflichten des Cloud Service Providers gegenüber Strafverfolgungsbehörden in den Ländern der Service-Erbringung sind zu berücksichtigen. Es ist sicherzustellen, dass ein Zugriff auf österreichische Verwaltungsdaten in einem ausländischen Cloud-Rechenzentrum im Rahmen der nationalen Strafverfolgung des Staates des Cloud-Rechenzentrums keine unzulässigen oder unerwünschten rechtlichen Konsequenzen erzeugt (z.B. Amtshaftung wg. unzureichenden Datenschutzes).

Anhang 3: Organisatorische Aspekte

Im folgenden Abschnitt werden Chancen und Risiken aus der organisatorischen Perspektive dargestellt und mögliche Auswirkungen von Cloud Computing auf die IT-Organisation der öffentlichen Verwaltung erläutert. Im Fokus der Betrachtungen steht dabei das Modell „Public Cloud", da sich hier die größten organisatorischen Änderungen in der IT-Struktur ergeben.

Wesentliche Teile der Überlegungen gelten jedoch auch für die Modelle „Private Cloud" und „Community Cloud".

Cloud Computing kann organisatorische Vorteile durch Standardisierung bieten. Organisatorische Nachteile und Risiken inkludieren eine erschwerte Steuerung des IT-Einsatzes, strukturelle Abhängigkeit aufgrund von Lock-in-Effekten gegenüber Cloud-Anbietern sowie die Notwendigkeit der Kontrolle der Einhaltung von Governance-Regeln [DSCC10]. Cloud Computing stellt die organisatorische Steuerung der IT in der öffentlichen Verwaltung vor zahlreiche Herausforderungen:

- **Standardisierung:** Prinzipiell bietet Standardisierung in der IT neben der Kostenreduktion auch mehrere mögliche organisatorische Vorteile (Vereinfachung von Prozessen, Integration externer Partner, Flexibilität und Agilität). Cloud Computing ist, sofern richtig eingesetzt, eine Möglichkeit, Standardisierung zu fördern und entsprechende Vorteile zu generieren. Falsch eingesetzt kann Cloud Computing jedoch auch zu gegenteiligen Ergebnissen führen. Bei den Standardisierungen im E-Government Umfeld soll Rücksicht genommen werden, dass Cloud nicht prinzipiell ausgeschlossen wird. Bislang sind die Tendenzen der großen Cloud-Anbieter noch immer proprietär und damit hemmen diese die Effekte des Marktes. Lediglich bei Open-Source Ansätzen kann man von einer kontrollierbaren, herstellerunabhängigen Situation ausgehen. Dies würde für die Verwaltung ein Konzentrieren auf derartige Open-Source Ansätze bedeuten aber gleichzeitig die Skaleneffekte der Großanbieter nicht mitnehmen. Der Ausweg aus der Situation könnte der GAIA-X Ansatz sein, der sich genau diesen Zielen verschreibt.

- **Organisatorische Aufspaltung:** Cloud Computing kann zu „Silo-Lösungen" führen, wenn die Zusammenhänge zwischen Anwendungen und Prozessen bei Entscheidungen nicht berücksichtigt werden. Dann kann sich der Datenaustausch zwischen Anwendungen (bei „Silo-Lösungen") als schwierig erweisen, was die Service-Qualität aus der Perspektive des Kunden reduziert. In diesem Aspekt haben „Mobile First" und „Cloud" relativ ähnliche Effekte. Damit werden mittel- und längerfristig Anwendungen und Prozesse angehalten sein, sich in kleine Schritte mit fest definierten Schnittstellen zu teilen und dann einzelne Schritte für den Massenbetrieb in Cloud-Prozesse auszulagern und für den Notbetrieb lokal als Backup-Situation und zum Sicherstellen der nachhaltigen Schnittstellen-kompatibilität parallel zu halten.

- **Strukturelle Abhängigkeit:** Durch zu starke Bindung an einen bestimmten CSP oder einen Service können Abhängigkeiten bis zu Lock-in-Effekten entstehen, die einen Wechsel zu einem anderen Dienstleister Auftragsverarbeiter oder einen internen Service erschweren. Das Vertragsende mit seinen massiven Auswirkungen, insbesondere im Hinblick auf potentielle Abhängigkeiten und Migrationskosten sollte deshalb bereits vor Vertragsschluss und dann laufend

berücksichtigt werden (entsprechende vertragliche Vorkehrungen und ausführliches Screening des CSP im Hinblick auf die Datenrückmigration).

- **Applikations- und Plattformvernetzung*:*** Bei modernen Anwendungen und vor allem bei mobilen Anwendungen ist es gängige Praxis, eine weit über die Anwendung hinausgehende Vernetzung zu akzeptieren. Push Mitteilungen, automatisierte Einbindung von Kommunikationsplattformen etc. sind Beispiele, was seitens der Nutzer erwartet wird und in der Praxis primär mit Großanbietern aus Drittstaaten ermöglicht wird. Eine besondere und aktuelle Herausforderung ist die Einbindung und Einbettung von Audio- und Videokonferenzsystemen.

- **Potentielle Steigerung des Verarbeitungsvolumens:** Bei einem Einsatz von Cloud Computing werden grundsätzlich sinkende Kosten erwartet. In der Praxis kann es aber aufgrund gesteigerter Nutzung entsprechender Services zu höheren Verbrauchsmengen und damit in weiterer Folge schnell zu unerwartet steigenden Kosten kommen. Cloud-Preise sind nach wie vor strategisch durch die Anbieter definierte und nicht auf Komponentenpreise aufbauende Situationen. Dieser Umstand verstärkt die Notwendigkeit, sich auf Standards von Services und offene Schnittstellen zu konzentrieren, um auch mittelfristig von den Skaleneffekten der Cloud profitieren zu können.

- **Fehlender Kostenvergleich:** In der öffentlichen Verwaltung sind die internen Kosten bei fehlender Kostenrechnung oft nicht exakt bekannt. Ein aussagekräftiger Vergleich der Kosten zwischen einer Cloud-Lösung und einer internen Lösung ist dann oftmals nicht oder nur schwierig möglich. (Anm.: Das ist ein generelles Thema, kein Cloud-spezifisches; könnte hier auch wieder gelöscht werden.)

- **Vereinbarungen:** Oftmals ist in einer traditionell strukturierten internen IT-Abteilung wenig Erfahrung mit Auftragsverarbeitern und entsprechenden Vereinbarungen vorhanden.

  Gerade sorgfältig ausgearbeitete Bestimmungen in den Auftragsverarbeiter sind für einen erfolgreichen Einsatz von Cloud Computing aber von großer Bedeutung. Zu berücksichtigende Aspekte beinhalten u.a. Service Level Agreements (SLA), Verfügbarkeit, Change-Management, Notfallmanagement, Qualitätssicherung. Auch die Kontrolle dieser Vereinbarungen muss organisatorisch berücksichtigt werden.

Um die Risiken des Cloud Computing zu minimieren bzw. die Potentiale bestmöglich auszuschöpfen, ist eine ausführliche Voranalyse über Ziele und Anforderungen erforderlich. Idealerweise wird dabei ein Vorgehensmodell zur Einführung von Cloud Computing eingesetzt [PCEC09].

Ein Beispiel dafür ist das fünfstufige Vorgehensmodell von Reeves und Santos [BSCA10].

1. Projektvorbereitung: Formierung eines Kernteams zur Entwicklung einer Cloud Strategie, Definition von Geschäftszielen und Darlegung der Migrationsgrundsätze, Entwicklung einer Migrations-Roadmap sowie Sicherstellen der Nachhaltigkeit von Schnittstellen und Gliederung in möglichst überschaubare und unabhängige Teilprozesse. Diese Schnittstellen und Teilprozesse sind jedenfalls im Sinne optimaler Re-Use-Situationen in einem gemeinsamen Katalog für alle Verwaltungen zusammenzustellen.

2. Analyse des Geschäftsfeldes sowie der bestehenden IT-Anwendungen:

   Identifizierung der Risiken und der Einflüsse im Falle eines Ausfalls der Cloud, Analyse der Anforderungen und Abhängigkeiten der IT-Anwendungen, Kostenvergleich Cloud vs. „interner" Betrieb der IT-Anwendungen, Analyse der Änderung der internen organisatorischen Abläufe sowie generelle Auswirkungen auf die Organisation, Erarbeitung von Richtlinien zur Bestimmung des passenden Cloud Modells (Software as a Service, Hardware as a Service, Infrastructure as a Service) bzw. der Ausprägung (Private, Public oder Hybrid).

3. Auswahl des Cloud-Anbieters: Analyse des Leistungsvermögens sowie des Risikopotenzials der Cloud-Anbieter anhand der ermittelten Anforderungen und den vorliegenden Angeboten, Entscheidung nach Einsatz von geeigneten Evaluierungsverfahren. Berücksichtigung der rechtlichen Rahmenbedingungen.

4. Vermeidung bzw. Reduzierung der Risiken durch Planung einer Exit-Strategie bzw. des lokalen Backup-Service für wesentliche Applikationen (Vertragsgestaltung, Verwendung offener Datenformate).

5. Planung des laufenden Betriebes: Erarbeitung von Governance-Regeln (Management von unerwarteten Ausgaben, Budgetplanung, ungeplante Auswirkungen).

Von zentraler Bedeutung ist während der Projektplanung (Punkt 2) im Zusammenhang mit dem Einsatz von Cloud Computing die Analyse der „*Cloud-Fähigkeit*" von IT-Anwendungen bzw. den verarbeiteten Daten.

Aus organisatorischer Perspektive sind (bei Cloud Computing) folgende Aspekte zu berücksichtigen [BSCA10]:

- **Auswirkungen auf die Kontinuität der Geschäftstätigkeit:** Wann ist eine IT-Anwendung zu geschäftskritisch, um in die Cloud ausgelagert zu werden bzw. wann ist eine lokale Backup-Situation vorzusehen und wie kann damit ein alternatives Service im Ernstfall aufgebaut werden?

- **Informationssicherheit:** Werden Daten verarbeitet, die aufgrund gesetzlicher Bestimmungen oder nach der Einschätzung der Organisation nicht für die Nutzung von (Public-)Cloud Computing geeignet sind? Welche kryptographischen Funktionen vermeiden dieses Problem? – Ein besonderer Aspekt ist dabei die Wirksamkeit der Verschlüsselung, sofern diese auch gegenüber Interessen von mächtigen Institutionen und Staaten wirksam sein soll. Die Fragen, wer die Schlüsselerzeugung, Schlüsselhaltung und Anwendung der Schlüssel letztlich unter Kontrolle hat und in der Lage ist, diese zu schützen, ist in Bezug auf Souveränität essentiell. Allerdings ist für die meisten Cloud-Services nicht nur die reine Datenspeicherung (data at rest), sondern auch die temporär entschlüsselte Situation während der Verarbeitung von Daten in einem Cloud Service (data in transit) zu berücksichtigen.

- **Risikotoleranz:** Sind die Risiken eines Ausfalls der IT-Anwendung für eine Organisation tragbar? Gibt es einen Schwellenwert, der durch SLAs nicht garantiert werden kann?

- **Interdependenz von IT-Anwendungen:** Hat eine IT-Anwendung zu viele Abhängigkeiten mit bestehenden Services, um sinnvoll in eine Cloud ausgelagert zu werden?

- **Migrationsaufwand:** Was ist der maximal tolerierbare Aufwand für die Migration eines Service in die Cloud? Steht dies in Verhältnis zu den erwarteten Einsparungen (Kosten-Nutzen-Analyse)?

Generell gilt es, die Cloud-Fähigkeit von neuen IT-Anwendungen bereits in der Architekturphase und Vergabephase zu prüfen und bei positiver Einschätzung weitere Schritte zu setzen bzw. eine entsprechende Analyse durchzuführen (z.B. durch das skizzierte fünfstufige Vorgehensmodell).

Anhang 4: Wirtschaftliche Aspekte

Bereits heute wird ein erheblicher Anteil traditioneller IT-Dienstleistungen durch Cloud-basierte Services ersetzt bzw. ergänzt. Das Wirtschaftlichkeitsargument – also das Potential IT-Kosten nachhaltig zu senken – wird in diesem Zusammenhang als wichtiger Treiber für den Wandel in Richtung Cloud gesehen. Es gibt zunehmend Anwendungsszenarien (insbesondere, wenn es sich um Cross-Plattform fähige Anwendungen handelt), die ohne Cloud nicht umsetzbar sind.

Die Cloud Service Provider (CSP) realisieren die Kostenvorteile vor allem durch das Standardisieren von Services, das Bündeln von IT-Ressourcen und Automatisierung von Abläufen. Die Kalkulationen und Wirtschaftsmodelle sind allerdings für Kunden großer Cloud Provider kaum nachzuvollziehen. Zudem ist die Frage, was in die Wirtschaftlichkeitsbetrachtung einbezogen wird. Diese sieht deutlich anders aus, wenn auch die eventuell notwendigen Migrationskosten auf eine weitere Plattform aus strategischen oder Ausfallsgründen miteinbezogen werden muss oder wenn aus organisatorischen Gründen eine Ausfallsicherheit auf einer anderen Plattform (etwa um einem möglichen Cyber-Angriff auf eine Plattform vorzugreifen) vorzusehen ist. Auf Anbieterseite ermöglicht das Cloud-Konzept weitreichende Skaleneffekte. So sinken mit zunehmender Auslastung auf Anbieterseite die (Betriebs-) Kosten (Strom – GreenIT/CO2 Reduktion, Sicherheit, etc.) pro Server. Gleichzeitig können die Overhead-Kosten auf eine größere Zahl von Nutzern aufgeteilt werden. Der Kunde profitiert zudem durch ein höheres Maß an Flexibilität und budgetärem Planungsspielraum, da er die Ressourcen des CSP exakt seinem Bedarf entsprechend – also auch kurzfristig – in Anspruch nehmen kann. Investitionskosten zum Abdecken von Auslastungsspitzen können entfallen. Das Risiko, insbesondere das Sicherheitsrisiko wird zwar geringer aber dennoch zentralisiert und damit steigt auch der Nutzen eines erfolgreichen Angriffes.

Für die Verwaltung bedeutet Cloud Computing aus wirtschaftlicher Sicht:

- Standardisierte IT-Infrastruktur und -Dienste können unter den Rahmenbedingungen einer Cloud-Architektur und eines Cloud-Geschäftsmodells wirtschaftlicher zu beziehen bzw. zu erbringen sein. Die Anwendungen sind jedoch umfassend zu betrachten. Cloud-Fähigkeit, was die Struktur und Schnittstellen betrifft, ist unabhängig vom Umstand, ob derzeit Cloud eingesetzt wird, ein wichtiger Aspekt.

- Die Kostensituation bei funktionalen Anpassungen von Cloud-Services oder deren Integration in bestehende Geschäftsprozesse ist im Vergleich zu den Adaptionskosten herkömmlicher Architekturen weitgehend unbekannt (bzw. muss man im Detail unterscheiden für IaaS, PaaS und SaaS). Aufgrund des hohen Automatisierungsgrads der Cloud Services sind diese Kosten aber tendenziell höher anzusetzen.

- Massiv skalierende Public Cloud Services scheinen zumindest derzeit nicht anpassbar zu sein. Hier sind den Kostenvorteilen im Einkauf etwaige Effizienzverluste in der Nutzung der Standardservices ohne Anpassungen für die Verwaltung gegen zu rechnen. IT-Anwendungen sind als Werkzeug ja nicht nur aus einer Kostensicht im Einkauf, sondern vor allem auch hinsichtlich ihres Beitrags zur Effizienzsteigerung der Geschäftsprozesse der Verwaltung zu beurteilen (Anm.; Es werden eben – wie bei jeder externen Lösung, vgl. SAP – die vorhandenen bzw. möglichen Funktionalitäten und Geschäftsprozesse der externen Cloud Lösung

mitgekauft); für dieses Umfeld ungeeignete Prozesse können auch zu Kostensteigerungen (bis hin zu Umschulungsmaßnahmen) führen.

- Zusätzlich zu allfälligen Kostenvorteilen verändert sich bei Public Cloud Services für den Auftraggeber / Kunden des Cloud Services auch die Kostenstruktur grundlegend. Durch die nutzungsbedingte Verrechnung werden Investitionskosten durch Betriebskosten ersetzt, was entsprechende Auswirkungen auf die Budgetplanung hat. Für Private Cloud Services gilt dieses Argument unabhängig von der Größenordnung der Private Cloud bzw. Community Cloud nicht. Der Private Cloud Anbieter für eine große Organisation selbst muss investieren.

Die zu Grunde liegenden wirtschaftlichen Parameter sind aufgrund der zum Teil fehlenden Transparenz des technischen und organisatorischen Modells der CSP schwer zu beurteilen. Abgesehen von entsprechenden vertraglichen Vereinbarungen und SLAs sollten diese Bedenken rund um das Spannungsfeld zwischen Profit und Sicherheit mit in eine Vorab-Klassifizierung über die „Cloud-Fähigkeit" von Bereichen bzw. Daten einfließen.

Anhang 5: Technische Aspekte und Sicherheit

Technische Aspekte wie Virtualisierung, Provisioning, gemeinsame Nutzung von Ressourcen und Ausgleichen von Lastspitzen sowie Externalisierung von Investitionskosten sind Grundeigenschaften, die Cloud Computing ausmachen.

Bei der Beschreibung von Cloud Computing-Systemen haben sich u.a. **folgende technische Aspekte** etabliert.

Standardisierung

IT-Anwendungen haben eine Vielzahl von Schnittstellen bzw. unterhalten Schnittstellen zu anderen Anwendungen. Sind diese Schnittstellen standardisiert, ist ein Wechsel eines Anbieters einfacher, da der Anpassungsaufwand geringer sein müsste; von einer breiten Standardisierung sind wir allerdings noch weit entfernt - jedenfalls sind Projektaufwände zu kalkulieren.

Chance: Durch standardisierte Cloud-Umgebungen kann sich technisch gesehen ein Wettbewerb etablieren, der den Wechsel zwischen Anbietern einfacher macht. Die Standards der Schnittstellen bilden daher ein wichtiges Kriterium, um nicht in eine Abhängigkeit (LockIn) zu kommen. Für die Standardisierung gibt es bereits eine Reihe von Standards (z.B. OVF, SAML, SPML, XACML, LIAF) die durch die Cloud-Anbieter unterstützt werden sollten.

- Open Virtualization Format (OVF)
- Security Assertion Markup Language (SAML)
- OAuth, OpenID Connect
- Service Provisioning Markup Language (SPML)
- Extensible Access Control Markup Language (XACML)
- Liberty Identity Assurance Framework (LIAF)
- Breitere Aktivitäten:
    - NIST Cloud Standard Roadmap, Reference Architecture
    - ETSI TC Cloud
    - OASIS Cloud TCs
    - DMTF Cloud Standards
    - ITU Cloud Standard Roadmap

Mehr Informationen zu Standardisierungsaktivitäten finden sich im Cloud Standards Wiki[22].

Skalierbarkeit / Elastizität

Unter Skalierbarkeit versteht man die (automatische) Anpassbarkeit von Ressourcen an die – sich ändernden - Leistungsanforderungen von Auftraggebern/Kunden auch bei Lastspitzen (z.B. Dienstbeginn, Tagesabschluss, Monatsabschluss, Volkszählung, Wahlvorbereitung, Volksbefragung, ...).

Chance ist hier der Lastausgleich über mehrere Kunden oder Mandanten in der Cloud, da die Grundarchitektur dafür geeignet ist. Gleichzeitig kann es zum Risiko werden, wenn

[22] http://cloud-standards.org/wiki/index.php?title=Main_Page

nicht ausreichend Ressourcen vorgehalten werden und damit alle Kunden oder Mandanten beeinträchtigt werden.

ID- und Rechte-Management

Die Identitäts- und Rechteverwaltung ist wesentlicher Baustein der Zugangskontrolle in Cloud Computing Systemen. Um die bestehenden Sicherheitsbedenken auszuräumen, ist daher die Lösung des CSP genau zu hinterfragen wie er damit umgeht, dass fremde Administratoren Zugang zu Unternehmensdaten haben. Es muss die sichere Identifikation der Kunden der Cloud selbst wie auch die der Administratoren des CSP ermöglichen. Besonders auf die Absicherung der privilegierten Benutzerprofile des CSP muss geachtet werden. Hier muss es dem Kunden der Cloud ermöglicht werden, regelmäßige Audits (Zugriffe, Zugriffsprofile) durchführen zu können. Es sollten generell für die Authentisierung nur starke Verfahren für Kunden und CSP verwendet werden. Die Connectivity zu einem lokalen IDM (Identity Management) des Kunden ist sicherzustellen, da sonst erhebliche Zusatzaufwände und auch Risiken entstehen.

Das ID- und Rechte-Management kann auch bei einem Drittanbieter angesiedelt sein.

Mandantenfähigkeit

Zu den Grundeigenschaften einer Cloud-Architektur zählt die Mandantenfähigkeit. Die sichere Mandantenfähigkeit in der Cloud soll die Partitionierung einer virtualisierten Shared IT-Infrastructure ermöglichen, wie sie auch bei Server-Virtualisierung im modernen Rechenzentrum bereits eingesetzt wird. Dadurch ergibt sich die Chance, verschiedene Anwendungsszenarien (z.B.: Produktions- und Testbetrieb) abzubilden.

Sicherheitsstruktur

Um die Ressourcen der Kunden oder Mandanten (Daten, Anwendungen, Netze, …) zu schützen, ist eine durchgängige Sicherheitsarchitektur zu implementieren. Da Cloud Systeme mandantenfähig (multi-tenancy) sein müssen, ist eine sichere Trennung der Ressourcen von Kunden oder Mandanten in der Architektur abgebildet.

Cloud Management

Um den Betrieb von Cloud Services zu gewährleisten, sind vom CSP IT-Management-funktionen und Prozesse anzubieten, die sowohl die Einrichtung wie auch den Betrieb unterstützen. CSPs offerieren für ihre Services Werkzeuge in Form von Webportalen, die die Funktionen zur Verfügung stellen. Typischer Weise sind folgende Funktionen inkludiert:

- Steuerung von Services - dazu zählen z.B.:
  - das Starten
  - das Stoppen oder
  - Reboot
- Überwachung von Services - um die Leistungsfähigkeit/Leistungsdaten des CSP zu erheben.
- Sicherheit von Services - umfassen den sicheren Zugriff auf Services, Transparenz von Zugriff und die sichere Identifikation von Kunden und Administratoren des CSP.

Wünschenswert wären zudem Werkzeuge, mit denen die Cloud Ressourcen und die lokalen on-premise Ressourcen gleich verwaltet werden können.

Technische Revision

CSP müssen zum Durchsetzen von kundenspezifischen Sicherheitspolitiken dafür geeignete Prozesse anbieten. Es muss dem Kunden möglich sein, im Rahmen der Umsetzung seiner Sicherheitspolitik die benötigten Informationen/Zugriffe auf z.B. Log-Dateien oder Zugriffslisten zu haben, um insbesondere die eigene Compliance und die Einbindung der eigenen Monitoring-, Auditierung- und Logfile-Analyse-Lösungen zu gewährleisten.

Patch Management

Unter Patch Management wird die Planung und Installation von Patches (Software-Updates) zusammengefasst. Wichtig ist hier, dass Patches über die gesamte Umgebung zu definierten Zeitpunkten eingespielt werden.

Durch die standarisierte Cloud-Infrastruktur ergibt sich die Chance, das Patch Management bei höherem Effizienzgrad mit geringeren Ausfallzeiten zu bewerkstelligen. Als Schwierigkeit ist der Test der Verträglichkeit bzw. Kompatibilität von SW-Updates mit kundenspezifischen Anwendungen zu sehen.

Die wichtigsten Erkenntnisse aus den vorigen Punkten finden sich überblicksmäßig in der folgenden Zusammenfassung:

Zusammenfassung der technischen Aspekte

	Chance	**Risiken**
Standardisierung	Wettbewerb, Wechsel zwischen Anbietern	Ohne Standard Abhängigkeit von einzelnen CSP-Anbietern
Skalierbarkeit	Vorstellung nahezu grenzenloser Ressourcen durch CSP	Gleichzeitige Lastspitzen können im schlechtesten Fall zum Stillstand führen.
Identity- und Rechte-Management	Ist eine Kernanforderung an CSP und sollte damit „state of the art" durchgeführt werden.	Sicherheitsbedenken bei der Umsetzung der CSP, vor allem bei den privilegierten Benutzerkennungen (Administratoren)
Mandantenfähigkeit, Sicherheitsstruktur	Ist eine Kernanforderung an CSP und sollte damit „state of the art" durchgeführt werden.	Mangelnde Kontroll- und Einflussmöglichkeit.
Cloud Management	Standarddienste (& einheitliche Administrationskonsolen) werden durch komfortable Webportale zur Verfügung gestellt.	Einbindung der Werkzeuge an CSPs in kundenspezifische Prozesse noch nicht erprobt.

Technische Revision		Auftrennung der kundenspezfischen Daten (LogDateien etc.) muss vertraglich geregelt werden. Derzeit noch keine standardisierten Angebote (allerdings z.B. bei PaaS bereits eine Frage des Designs der Applikation)
Patch Management	Schnelles standardisiertes Ausrollen von Patches durch vereinheitlichte Infrastruktur	Schwierigkeit des Testens der Kompatibilität von Patches, Rücksichtnahme auf kundenspezifische Anforderungen.

Sicherheit

Cloud Computing wird durch Aspekte dominiert, die weit über die Grenzen des Landes und auch Europas hinweg beeinflusst werden. Es macht daher beschränkt Sinn, wenn jedes Land eigene Vorgaben und Überlegungen veröffentlicht. Daher wir hier auf die Arbeiten und Texte den Deutschen BSI verweisen, da diese auch mit Grundlage einer zukünftigen Cloud Zertifizierung im Rahmen der EU (Cyber Security Act) sein werden. Dieser C5 Kriterienkatalog ist auch wesentlicher Bestandteil des Fragenkataloges im Anhang.

Die finale Version des C5:2020 aus dem Jahr 2020 beinhaltet viele Neuerungen im Vergleich zur vorherigen Version. Für Prüfzeiträume, die am oder nach dem 15. Februar 2021 enden, empfiehlt das BSI, die Version C5:2020 aus dem Jahr 2020 anzuwenden, um aktuelle Entwicklungen ausreichend berücksichtigen zu können.

Download:

Kriterienkatalog Cloud Computing C5:2020
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020.pdf?__blob=publicationFile&v=2

Kriterien C5:2020 (Editierbares Format)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020_Editierbar.xlsx?__blob=publicationFile&v=3

Kreuzreferenztabelle
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/CloudComputing/Anforderungskatalog/2020/C5_2020_Referenztabelle.xlsx?__blob=publicationFile&v=4

Anhang 6: Prozesse (Geschäftsprozesse) - Aspekte

Cloud Computing als IT-Betriebsmodell ist nicht nur für IT-Abteilungen von Bedeutung, sondern für Unternehmen und die öffentliche Verwaltung insgesamt eine relevante Herausforderung. Durch den Einsatz von Cloud Computing kann eine ganzheitliche Änderung von Unternehmensstrategien und -strukturen erforderlich werden. Die Auslagerung von Teilen der eigenen Geschäftsprozesse an einen Dritten (CSP) ist mit signifikanten Änderungen in diesen Prozessen verbunden. Eine mögliche Folge ist die Notwendigkeit der Umverteilung von Rollen und Kompetenzen und damit Prozessen.

Die Zusammenarbeit von internen Prozessen und den Prozessen des CSP sind in einem Cloud Compliance Regelwerk (im Rahmen einer Dienstleistervereinbarung) transparent festzulegen und zu kontrollieren. Im Sinne der Aufgabendefinition und -überwachung wird auch in diesem Zusammenhang auf die Notwendigkeit des Abschlusses ausreichender Service Level Vereinbarungen (SLAs) und Operational Level Vereinbarungen (OLAs) verwiesen.

Strategische Aspekte der Prozessveränderung durch Cloud Computing

Prinzipiell verfügen viele bestehende Anwendungen, auch in der öffentlichen Verwaltung, die nicht als Cloud Service bezeichnet werden, über die typischen Anforderungen und Charakteristika von Cloud Services (z.B. gemeinsame Nutzung von Ressourcen über Vernetzung, Lizenzgebühren statt Investitionen für die Nutzer, Standardisierung). Bestehende Erfahrungen aus der Nutzung solcher Anwendungen, speziell im Zusammenhang mit Betrieb und Datenspeicherung über einen Auftragsverarbeiter und bei Anpassungen von Prozessen können auch bei der Evaluierung von potentiellen Cloud Services genützt werden.

Standardisierung ist der wesentlichste Faktor für Kostenersparnisse beim Einsatz von Cloud Computing. Spezifische Cloud Anwendungen sind ein Werkzeug zur effizienten Umsetzung dieser Standardisierung. Gerade Public Cloud Service unterliegen einem sehr hohen Standardisierungszwang, der bei einem Private Cloud Service nicht immer gegeben ist. Entsprechend dem Grad der Standardisierung der gewählten Cloud Lösung ist mit Änderungen in den Geschäftsprozessen und unterschiedlichen Kosten und Finanzierungsrisiken zu rechnen. Bei einem Einsatz von Cloud Services unterschiedlicher Dienstleister muss Interoperabilität zur Sicherstellung der Unabhängigkeit von einem bestimmten Anbieter in den Prozessen berücksichtigt werden. Bei Nutzung standardisierter Cloud Lösungen sollte durch den flexiblen Einsatz von Rechenleistung schnell auf Änderungen in den Geschäftsprozessen reagiert werden können. Compliance- und Governance-Prozesse werden in Unternehmen und der öffentlichen Verwaltung mit steigendem Einsatz von Cloud Services externer Dienstleister durch die Notwendigkeit der Sicherstellung und Kontrolle der Einhaltung von Datensicherheit und Rechtskonformität an Bedeutung gewinnen. Neben der gründlichen Ausarbeitung von SLAs zur Abdeckung der Anforderungen bei der Nutzung eines Cloud Services müssen auch die dazugehörigen Kontrollprozesse ausreichend definiert und umgesetzt werden.

Cloud Compliance

Es macht nicht Sinn, eine eigene österreichische Compliance Struktur aufzustellen und aufzubauen. Daher wird hier noch einmal auf den bereits unter dem Kapitel Sicherheit angeführten C5 Kriterienkatalog des Deutschen BSI verwiesen.

Weiters ist anzumerken, dass es nach Abschluss der Arbeiten der ENISA zur Cloud Zertifizierung und nach Annahme der Resultate als Zertifizierungsschema nach dem Cyber Security Act Zertifizierungen für Cloud geben wird, die auch im Umfeld Österreich anzuwenden sind.

Ein weithin offener Compliance Aspekt ist durch den Umstand gegeben, dass nahezu alle Cloud Angebote nur durch UserID und Passwort geschützt sind. Dies ist nicht nur in Hinblick auf die eIDAS Verordnung, sondern auch im Sinne einer wirksam umsetzbaren Zuordnung der Verantwortung ein erhebliches Thema.

Anhang 7: Gesamtbeurteilung

Cloud Computing ist keine Modeerscheinung der IKT-Branche, sondern vereint als nächsten Entwicklungsschritt die technischen und wirtschaftlichen Möglichkeiten, die konsequente Standardisierung bedingt. Daher erfordert diese Entwicklung massive Maßnahmen im rechtlichen und organisatorischen Bereich.

Die IT-Industrie drängt aufgrund eines klaren Businessmodells und aufgrund der mittlerweile vorwiegend genutzten mobilen Plattformen zum Einsatz von Cloud Computing und sieht damit eine Forcierung des Rollouts von E-Services. Zudem werden gewisse Verarbeitungen erst mit dem Einsatz einer öffentlichen Cloud ermöglicht. Durch geringere Einstiegshürden in Bezug auf Zeit und Ressourcen erhofft man sich ein erhöhtes Nutzungsvolumen der Public Cloud und damit höhere Gewinne.

Vor dem Einsatz muss man dennoch einige Punkte bedenken. Je nach gewähltem Modell (Private Cloud, Public Cloud, Hybrid Cloud) stellen sich die Auswirkungen des Veränderungsprozesses unterschiedlich dar. Im nächsten Kapitel sind alle Fragestellungen aus Sicht des Auftraggebers, die in dem Positionspapier identifiziert wurden, zusammengefasst.

Der Cloud-Monitor hat 2015 bereits das vierte Jahr die Cloud-Nutzung von deutschen Unternehmen betrachtet. Folgende vier zentrale Erkenntnisse aus Anwendersicht wurden gezogen: Die Cloud-Nutzung steigt langsam, aber stetig. Die Erfahrung mit Cloud-Computing ist überwiegend positiv. Sicherheitsbedenken und rechtliche Unklarheiten sind in erheblichem Maße vorhanden und bremsen die Marktdynamik. Dabei ist die allgemeine Cybersicherheit im Falle der Cloud deutlich gesteigert aber die Souveränität des Auftraggebers und der Nutzer kann gefährdet sein. Aufgrund fehlender Statistiken im Verwaltungsumfeld sind diese Erkenntnisse die beste Orientierung für die Entwicklung von Cloud in der Verwaltung.

Ähnlich dem Modell Portal-Verbund sollten künftige Entwicklungen im Hinblick auf den Investitionsschutz "Cloud-fähig" umgesetzt werden. Damit ist die Entscheidung, ob der Betrieb eines IT-Services in der Cloud oder klassisch im Rechenzentrum erfolgt, offen und kann jederzeit getroffen werden. Standardisierungen sollen der Cloud-Fähigkeit nicht entgegenstehen. Die Erkenntnisse aus diesem Dokument sind zu berücksichtigen.

Anhang 8: Entscheidungsfindungsprozess

Bevor man eine Entscheidung für die Nutzung von Cloud Computing trifft oder ein spezielles Modell auswählt, muss man in der Verwaltung die erforderlichen Grundlagen schaffen. In diesem Zusammenhang sind jedenfalls folgende Punkte zu klären:

Organisatorische Anforderungen
Ab wann ist eine IT-Anwendung zu geschäftskritisch, um in die Cloud ausgelagert zu werden? Wann ist der Schwellenwert für Ausfallzeiten erreicht?
Welche Daten disqualifizieren eine IT-Anwendung aufgrund der besonderen Sensitivität?
Welche Risiken sind für eine Organisation aufgrund von Service-Ausfällen tragbar?
Hat eine IT-Anwendung zu viele Abhängigkeiten, um sinnvoll in eine Cloud ausgelagert zu werden?
Was ist der maximal tolerierbare Aufwand für die Migration eines Verfahrens in die Cloud? Steht dies in Verhältnis zu den erwarteten Einsparungen?
Wie hoch ist die Dauer des Returns on Investment inkl. der Transitionskosten?
Rechtliche Anforderungen
Siehe DSGVO, Materiengesetze mit Geheimhaltungs- und Compliance-Anforderungen sowie Fragenkatalog in Kapitel 3
Technische Anforderungen und Sicherheit
Werden die im Einsatz befindlichen Schnittstellen unterstützt?
Werden starke Identifizierungsverfahren für Cloud Kunden und Administratoren genutzt?
Ist eine durchgängige Sicherheitsarchitektur implementiert? Wer hat die letztliche und alleinige Kontrolle über Erstellung, Verwahrung und Nutzung von kryptographischem Schlüsselmaterial (organisatorisch und technisch abgesichert)?
Können die für die Umsetzung der eigenen Sicherheitspolitik benötigten Zugriffe (z.B. Log Dateien, Zugriffslisten) gewährt werden?
Können Patches getestet werden und aus Kompatibilitätsgründen zurückgehalten werden?
Stellen kryptografische Methoden die Integrität der Daten sicher?
Welche Verfügbarkeiten können garantiert werden?
Wie skaliert die Cloud-Lösung?
Wie wird der Wechsel von einem Cloud-Anbieter zu einem anderen ermöglicht?

Anhang 9: Charakteristiken von Cloud Computing

- **On-Demand Self-Service/Self-provisioning of resources (Ressourcenmanagement durch Nutzer/Kunde):** Ein Kunde (s.o.) kann selbstständig und vollautomatisch Rechenressourcen, wie Rechenleistung oder Netzwerkspeicher, Anwendungen, Upgrades etc. abrufen und buchen, ohne dass hierzu eine Interaktion mit dem Service Provider nötig ist.

- **Broad Network Access:** Sämtliche Ressourcen sind breitbandig über das Internet oder Intranet angebunden. Der Zugriff erfolgt über Standardmechanismen, die eine Nutzung von Cloud-basierten Diensten mittels herkömmlicher Server oder auch Endgeräte wie PCs, Laptops, PDAs oder Smartphones ermöglichen.

- **Resource Pooling:** Die Rechenressourcen des Providers werden an einer Stelle gebündelt und mehreren Nutzern zur Verfügung gestellt.

- **Massive Scalability (Skalierbarkeit):** Je nach Anforderungen können Ressourcen im entsprechenden Umfang dem Kunden zur Verfügung gestellt werden.

- **Rapid Elasticity (Elastizität):** Ressourcen können in Echtzeit schnell und teilweise automatisiert auf die veränderten Bedürfnisse des Nutzers angepasst werden. Aus der Sicht der Nutzer stehen unbeschränkt Ressourcen zur Verfügung, die jederzeit und in jedem Umfang gekauft bzw. genutzt werden können. Dank der dynamischen Verteilung von Ressourcen und Diensten können bspw. Lastspitzen gut ausgeglichen werden.

- **Measured Service/Pay as you go (verbrauchsorientiertes Bezahlmodell):** Cloud Computing Systeme kontrollieren und optimieren die Zuteilung von Ressourcen vollautomatisiert. Der Ressourcenverbrauch wird kontinuierlich gemessen, kontrolliert und berichtet, um Transparenz für den Provider und den Kunden herzustellen. Nur die genutzten Dienste und Ressourcen werden abgerechnet - Nutzer zahlen in der Regel nur für tatsächlich abgerufenen Ressourcen und Dienste (je nach Vertragsmodell).

- **Multitenancy (Mehrmandantenfähigkeit):** Ressourcen und Dienste werden zwischen allen Kunden/Nutzern dynamisch aufgeteilt.

- **Push Notification:** senden von unaufgeforderten Mitteilungen auf Geräteebene zum Auslösen von Aktivitäten des Benutzers. Diese Kommunikation ersetzt zunehmend die Aufforderung zur Aktion per E-Mail oder andere klassische Verbindungen.

Anhang 10: Servicemodelle des Cloud Computings

Im Zusammenhang mit Cloud Computing existiert eine Klassifizierung der Services in drei unterschiedliche Modelle. Spätestens zum Zeitpunkt einer Überlegung der Nutzung in der Analyse des Services/der Anwendung anzustellen:

- **Infrastructure as a Service (IaaS):** Bei IaaS werden grundlegende Infrastrukturleistungen zur Verfügung gestellt (z.B. Rechenleistung, Speicherplatz), auf deren Basis der Nutzer individuelle Software wie Betriebssysteme oder Anwendungsprogramme betreiben kann. Der Nutzer ist nicht für das Management oder die Wartung der Infrastruktur zuständig, hat aber dennoch die Kontrolle über Betriebssysteme, Speicherverwaltung und Anwendungen. Auf die Konfiguration bestimmter Infrastrukturkomponenten, wie bspw. Host-Firewalls, hat er evtl. eine beschränkte Einflussmöglichkeit.

- **Platform as a Service (PaaS)**: Nutzer können auf Basis einer Cloud-Plattform Anwendungen entwickeln oder bereitstellen. Dazu werden entsprechende Frameworks und Entwicklungswerkzeuge zur Verfügung gestellt. Dabei hat der Nutzer die Kontrolle über die Anwendungen und individuelle Konfigurationsparameter der Bereitstellungsumgebung.

- **Software as a Service (SaaS):** Bei SaaS wird dem Nutzer eine Anwendung als Dienst zur Verfügung gestellt. Die Änderung nutzerspezifischer Konfigurationseinstellungen ist evtl. nur eingeschränkt durch den Nutzer möglich.

Zusätzlich werden aktuell weitere Ebenen diskutiert:

- **Business Process as a Service (BPaaS):** Geht aus der SaaS-Ebene hervor und wird durch eine stärkere Nähe zum Geschäftsprozess charakterisiert.
- **Data as a Service (DaaS)**
- **Network as a Service (NaaS)**

Anhang 11: Ausprägungen von Cloud Computing

In der Praxis sind drei grundsätzliche Ausprägungen für Cloud Computing zu unterscheiden. Sollte keine Unterscheidung angegeben sein, wäre trotzdem zum Zeitpunkt der Überlegung der Nutzung von Cloud Ausprägungen die Unterscheidung individuell anzuwenden bzw. hinsichtlich der Chancen und Risiken zu analysieren.:

- **Public Cloud:** Die Cloud-Infrastruktur ist öffentlich über Internettechnologien zugänglich und wird von einem CSP betrieben. In der Regel wird diese Ausprägung von einer sehr großen Nutzeranzahl in Anspruch genommen, wodurch sich entsprechende Skaleneffekte erzielen lassen. Durch die hohe Anzahl der Nutzer ist eine Individualisierung der Dienste und eine maßgeschneiderte Anpassung hier am wenigsten möglich.

- **Virtual Private Cloud:** ist eine spezifische Public Cloud Ausprägung, wobei mittels geeigneter Sicherheitsvorkehrungen dem Kunden eine abgekapselte IT-Infrastruktur zur Verfügung gestellt wird, die unter Verwendung von Secure VPN (Virtual Private Network) Technologie direkt mit dem Kunden-Netzwerk verbunden ist.

- **Private Cloud:** Die Cloud-Infrastruktur wird für einen einzelnen Auftraggeber bzw. vorgegebene Gruppe betrieben, die ausschließlichen Zugriff auf die Cloud hat. Sie kann die Infrastruktur selbst oder durch Dritte betreiben lassen. Skaleneffekte und Kosteneinsparungen werden reduziert, stärkere Individualisierungen der Dienste (d.h. Anpassung auf die Erfordernisse der Kunden) sind möglich, aus Sicht des Auftraggebers nimmt die Kontrolle über die Cloud zu.

- **Community Cloud:** Im Rahmen einer Community Cloud wird die Cloud-Infrastruktur gemeinsam von mehreren Organisationen genutzt, die ähnliche Interessen bzw. Ziele verfolgen. Das Management der Infrastruktur erfolgt durch die Organisationen selbst oder extern durch einen Dritten.

- **Hybrid Cloud:** Die hybride Variante einer Cloud-Infrastruktur ist eine Mischung zweier oder mehrerer Varianten. Dabei bleiben die unterschiedlichen Clouds eigenständige Einheiten, die jedoch mit standardisierter oder proprietärer Technologie miteinander verbunden werden. So wird die Daten- bzw. Anwendungsportabilität sichergestellt. Mittels einer Hybrid Cloud können die Vorteile mehrerer Varianten kombiniert und Kostenvorteile von Public Clouds mit Sicherheitsvorteilen von Private Clouds kombiniert werden. Allerdings ist hierbei auch eine strikte und somit oftmals kostspielige Trennung der Daten notwendig.

6 Annex

Linksammlung

[BITK 10]	BITKOM-Leitfaden-CloudComputing_Web Cloud Computing – „Was Entscheider wissen müssen", BITKOM, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., Albrechtstraße 10 A, 10117 Berlin-Mitte, Dr. Mathias Weber, Arbeitskreis Cloud Computing und Outsourcing, www.bitkom.org, bitkom@bitkom.org, 2010
[CCIS 10]	Cloud Computing in Schweizer Behörden „Vorstudie zu Cloud Computing in Schweizer Behörden", Heck Uwe, Müller Willy, Oktober 2010
[ECO N10]	EU Public Sector Cloud Economics „THE ECONOMICS OF THE CLOUD FOR THE EU PUBLIC SECTOR", Microsoft, Rolf Harms (rolfh@microsoft.com) or Michael Yamartino (michael.yamartino@microsoft.com), November 2010
[EGC C10]	E-Government und Cloud Computing „E-Government und Cloud Computing", E-Government Innovationszentrum, Dr. Thomas Rössler, thomas.roessler@egiz.gv.at, https://demo.egiz.gv.at/plain/content/download/678/3913/file/E- Government%20und%20 Cloud Computing.pdf, September 2010
[SRG C11]	Security and Resilience in Governmental Clouds „Security and Resilience in Governmental Clouds – Making an informed decision", ENISA, Catteddu Daniele, Jänner 2011
[WKI C10]	Wer klaut in der Cloud „Wer klaut in der Cloud – Chancen und Risiken des Cloud Computing", Detecon Consulting, Juli 2010

[DHRA10]	Der Himmel reißt auf "Der Himmel reißt auf" Thorsten Claus, Martin Jeske, Detecon Consulting, Februar 2010
[SWIS10]	Messmer_IT-Trends "IT Megatrends und Ihre Bedeutung für Geschäft und Gesellschaft" Bruno Messmer, Swisscom IT Services AG, September 2010
[CCMA10]	Cloud_Computing_Mindestsicherheitsanforderungen „BSI-Mindestsicherheitsanforderungen an Cloud ComputingAnbieter" Bundesamt für Sicherheit in der Informationstechnik, Bonn, E-Mail: cloudsecurity@bsi.bund.de, September 2010
[TVSR10]	kuppinger_ca_virtualization_security_report „CA Technologies Virtualization Security", Martin Kuppinger, KuppingerCole, service@kuppingercole.com, 2010
[GITC10]	government_in_the_clouds_200519 „Government in the Clouds", GARTNER Industry Research, Andrea Di Maio, Massimiliano Claps, Mai 2010
[CCÖV10]	Fraunhofer cloud_studie_vorabversion_20101129 „Cloud Computing für die öffentliche Verwaltung", ISPRAT-Studie, Dr. Peter H. Deussen, peter.deussen@fokus.fraunhofer.de, November 2010,
[BSCA10]	BURTON GROUP - Building a Solid Cloud Adoption Strategy: Success by Design "Building a Solid Cloud Adoption Strategy: Success by Design", Drue Reeves, dreeves@burtongroup.com, Mai 2010
[CCTR10]	BURTON GROUP - Cloud Computing: Transforming IT Cloud Computing: Transforming IT, Drue Reeves, dreeves@burtongroup.com, April 2010

[CCSE09]	BURTON GROUP - Computing Security in the Enterprise Cloud Computing Security in the Enterprise Cloud, Dan Blum, dblum@burtongroup.com, Juli 2009
[DCCS10]	BURTON GROUP - Developing a Cloud Computing Security Strategy "Developing a Cloud Computing Security Strategy", Dan Blum, dblum@burtongroup.com, Mai 2010
[PCEC09]	BURTON GROUP - Planning Considerations for Externalization and Cloud Computing Planning Considerations for Externalization and Cloud Computing, Mike Rollings, mrollings@burtongroup.com, Oktober 2009
[DSCC10]	BURTON GROUP - The Dark Side of Cloud Computing "The Dark Side of Cloud Computing", Drue Reeves, dreeves@burtongroup.com, Mai 2010
[SDCC10]	BURTON GROUP - Using Encryption to Protect Sensitive Data in Cloud Computing Environments "Using Encryption to Protect Sensitive Data in Cloud Computing Environments", Dan Blum, dblum@burtongroup.com, Mai 2010
[BSIC5]	Kriterienkatalog Cloud Computing C5 https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Kriterienkatalog/C5_AktuelleVersion/C5_AktuelleVersion_node.html
[CCSR]	ENISA Cloud Computing Security Risk Assessment „Cloud Computing", ENISA, Daniele Catteddu and Giles Hogben , Daniele.catteddu@enisa.europa.eu, giles.hogben@enisa.europa.eu, November 2009

[CCDS]	Cloud Computing und Datenschutz T. Weichert: Cloud Computing und Datenschutz, Unabhängiges Landeszentrum für Datenschutz Schleswig-Hohlstein. Abgerufen aus dem WWW am 15. Februar 2011 unter http://www.datenschutzzentrum.de/ Cloud Computing
[LCCR]	Leitfaden Cloud Computing Recht, Datenschutz & Compliance EuroCloud Deutschland_eco e. V., Leitfaden Cloud Computing Recht, Datenschutz & Compliance, 22-27. abrufbar unter http://www.eurocloud.de/dokument/

Änderungsprotokoll

Version: Cloud Computing Positionspapier 2016 - CloudComp-Pos-1.1.3 zu

Cloud Computing Positionspapier Cloud-Comp. 2.1.0

Datum: 01/2022

Autor: AG Cloud BLSG