WIK-Consult • Bericht

Studie für die Bundesnetzagentur

Strategische Bedeutung von Cloud-Diensten für die digitale Souveränität von KMU

Teil 1 – Marktübersicht Cloud-Anbieter (Az: 2021/008/Z25-3)

Autoren:

Martin Lundborg
Dr. Isabel Gull
Dajan Baischew

Bad Honnef, August 2022

WIK CONSULT

Impressum

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Deutschland
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
E-Mail: info@wik-consult.com
www.wik-consult.com

Vertretungs- und zeichnungsberechtigte Personen

Geschäftsführerin	Dr. Cara Schwarz-Schilling
Direktor	Alex Kalevi Dieke
Direktor Abteilungsleiter Netze und Kosten	Dr. Thomas Plückebaum
Direktor Abteilungsleiter Regulierung und Wettbewerb	Dr. Bernd Sörries
Leiter der Verwaltung	Karl-Hubert Strüver
Vorsitzende des Aufsichtsrates	Dr. Thomas Solbach
Handelsregister	Amtsgericht Siegburg, HRB 7043
Steuer-Nr.	222/5751/0926
Umsatzsteueridentifikations-Nr.	DE 329 763 261

Inhaltsverzeichnis

Abbildungen

Tabellen

Zusammenfassung

Das Ziel dieser Studie ist es, die Bedeutung von Cloud-Diensten, die insbesondere von international tätigen Hyperscalern angeboten werden, für die digitale Souveränität der KMU zu bewerten. Dieser Bericht ist der erste Teil von drei und beleuchtet den Cloud-Markt mit seinen relevanten Akteuren. Im zweiten Bericht wird der Begriff der digitalen Souveränität spezifiziert und erläutert, wie sich der Datenschutz auf die Datenkontrolle und Datenverwendung innerhalb von KMU auswirkt und welche Relevanz diese für KMU hat. Im dritten Bericht werden die Ergebnisse und Erkenntnisse über eine Umfrage aus der Praxis der KMU erfasst und analysiert.

Der Überblick über den EU-27-weiten und deutschen Cloud-Markt zeigt, dass die US-amerikanischen Hyperscaler ebenso wie auf dem globalen Markt die höchsten Marktanteile erlangt haben. Marktführer AWS (Amazon) hat auf dem europäischen Infrastructure-as-a-Service-Markt noch mehr Marktanteile (53 %) als auf dem globalen Markt (41 %). Allerdings können in vielen europäischen Ländern auch die nationalen Anbieter (wenn auch in einem begrenzten Ausmaß) Marktanteile behaupten, etwa die Deutsche Telekom, OVH und Orange.

Die Untersuchung der Produktmerkmale zeigt, dass die Unterschiede der vertraglich zugesicherten Qualitätsmerkmale, Preise und angebotenen komplementären Services nicht ausreichend groß sind, um die Verteilung der Marktanteile zu erklären. Insbesondere herrscht eine große Preiskomplexität am Markt. Durch unterschiedliche Preismodelle, eine Vielzahl von Services und individualisierbaren Modulen und Support-Möglichkeiten ist ein direkter Preisvergleich nur vereinzelt möglich. Diese kann auch ein Grund dafür sein, dass der Preis allein nicht entscheidungsrelevant für die Anbieterwahl ist bzw. nicht bedeutend genug, um die Marktstrukturen zu determinieren.

Wichtiger scheint anhand der Angebotsanalyse und Gesprächen mit Marktexperten, dass das gesamte Angebot an Zusatzdiensten, Software, Usability und die tatsächlich erbrachte (nicht die vertraglich zugesicherte) Performance eine wichtige Rolle bei der Anbieterwahl und damit der Marktstruktur haben. Anhand dieser Erhebungen lässt sich ebenso die Hypothese ableiten, dass Faktoren wie Vertrauen, empfundene Qualität, Migrationskosten, Empfehlungen der Beratungsunternehmen und Softwareanbietern/-Integratoren[1] sowie Skaleneffekte bei den Vertriebskanälen für die hohe Nachfrage der Nutzer ebenso relevant sind.

Anzumerken ist, dass die hohen Investitionssummen der Hyperscaler Vertrauen der Nutzer in deren Infrastruktur und Fähigkeit schaffen, weiterhin umfassende Angebote bereitzustellen.

1 Der Aufwand für die Einführung neuer Softwarelösungen ist oft geringer, wenn immer die gleiche Cloud-Plattform wie bisher verwendet wird. Deshalb empfehlen Beratungsunternehmen und Softwareanbieter oft Cloud-Anbieter, die sie bereits kennen.

In Bezug auf Datenschutz und Datensicherheit wurden wenige Unterschiede der AGBs und Leistungsbeschreibungen zwischen den Anbietern festgestellt. Durch den US-CLOUD Act aus dem Jahr 2018, welcher den Zugriff von US-Behörden auf Daten, die von US-amerikanischen Unternehmen gespeichert werden, unabhängig vom Speicherort erlaubt, besteht bei der Nutzung von Cloud-Diensten US-amerikanischer Unternehmen jedoch Rechtsunsicherheit bezüglich der Speicherung von personenbezogenen Daten. Dieser Problemstellung wird in Themenfeld 2 weiter nachgegangen.

Gaia-X könnte neue Bedingungen für den Cloud-Markt vor allem in Europa schaffen. Denn es schafft eine Interoperabilität, die es kleineren Cloud-Anbietern ermöglicht, im Verbund mit der flexiblen Kapazitätsbereitstellung der Hyperscaler zu konkurrieren. Auch erhöht das standardisierte Labelling von Gaia-X die Transparenz bei der Datenspeicherung und –verarbeitung, was zu einer verbesserten digitalen Souveränität der Nutzer führt.[2] Damit könnte Gaia-X größeres Vertrauen in Cloud-Anwendungen schaffen und damit insgesamt zu einer höheren Nutzungsrate von Cloud-Services führen. Für die Hyperscaler liegt das Interesse an Gaia-X im Wesentlichen in der Partizipation am europäischen Wachstumsmarkt. Da Gaia-X sich derzeit in einem konzeptionellen Stadium befindet, sind die Analysen der möglichen Auswirkungen durch Gaia-X eher theoretischer Natur.

2 Siehe Gaia-X (2021c), S. 4.

1 Einführung Themenfeld 1

Der Markt für Cloud-Anwendungen unterliegt einem starken Wachstum.[3] Laut DESI 2021 nutzen EU-weit 26 % der Unternehmen Cloud-Anwendungen, ein Wachstum von 10 Prozentpunkten gegenüber den zuletzt 2018 erhobenen Zahlen.[4] Dazu hat auch die Pandemiesituation wesentlich beigetragen.[5] Die Nutzungszahlen in Deutschland (20 %) sind weiterhin deutlich unter dem EU-Durchschnitt.[6] Ein Grund dafür dürften neben einer fehlenden Sensibilisierung für den Nutzen von Cloud-Anwendungen Sorgen der Unternehmen um die digitale Souveränität sein. Dieser Umstand wird in den drei Themenfeldern dieser Studie behandelt.

In diesem ersten von drei Teilen der Studie wird der globale, EU-weite und deutsche Markt für Cloud-Dienste mit seinen wesentlichen internationalen und nationalen Anbietern betrachtet.

Die Betrachtung der Marktanteile von Cloud-Diensten im Infrastructure-as-a-Service-Segment, dem zweit größten Public Cloud Segment gemessen am Umsatz (siehe Tabelle 3.1, Kapitel 3.3) zeigt, dass der Markt von amerikanischen (z. B. Amazon Web Services (AWS), Google Cloud Platform) und zum Teil chinesischen Anbietern (z. B. Huawei, Alibaba) dominiert wird. In der Studie wird vor diesem Hintergrund der Fragestellung nachgegangen, welche Gründe dafür verantwortlich sind, dass europäische Cloud-Anbieter den Anschluss im Cloud-Geschäft verloren haben und in welchen Bereichen Potenziale zum Markteinstieg liegen.

Dafür wurde in einer Desktop-Recherche nach einer Marktabgrenzung die Marktsituation in der EU-27 und in Deutschland analysiert. Umsatzzahlen, die Marktanteile und die Leistungsmerkmale der nach Marktanteilen in Deutschland relevanten Anbieter AWS, Microsoft Azure, Google Cloud Platform, IBM Cloud, Open Telekom Cloud und IONOS Cloud wurden für die Studie erhoben (siehe Kapitel 4). In einer vergleichenden Analyse wurde eine Anbieterlandkarte in Form einer Anbieter-Preis-Leistungsmatrix erstellt (siehe Kapitel 4). Um die zukünftige Entwicklung einschätzen zu können, werden mögliche Marktverschiebungen durch die Einführung von Gaia-X berücksichtigt (siehe Kapitel 5). Hier wird besonderes Augenmerk auf die Aktivitäten der Hyperscaler in diesem Zusammenhang und auf die möglichen Auswirkungen von Gaia-X auf die digitale Souveränität der Nutzer gelegt.

Die Ergebnisse bezüglich der Einschätzung der Marktstruktur, Marktentwicklungen und insbesondere das Entscheidungskalkül der Nutzer bei der Wahl der Cloud-Anbieter so-

---

3 Vgl. Gartner (2021).
4 Vgl. Digital Economy and Society Index (DESI) 2021, S. 53. Der Index definiert Cloud Computing als Nutzung von Anwendungen mittlerer Komplexität. Die Nutzung von z. B. Mail-Anwendungen über die Cloud ist darin nicht enthalten. Bei Anwendung einer breiteren Definition könnte diese Zahl demnach höher sein.
5 Vgl. BMWi (2021), S. 6 ff.
6 Vgl. Index für die digitale Wirtschaft und Gesellschaft (DESI) 2021 Deutschland, S.13.

wie die Strategie der Cloud-Anbieter bezüglich Gaia-X wurde durch Gespräche mit Experten im Markt beleuchtet. Ferner wurden in diesem ersten Teil der Studie Thesen abgeleitet, die nachfolgend im Projekt durch Unternehmensbefragungen (Arbeitspaket 3) überprüft wurden.

2 Anbieter- und Marktstruktur

Der Public-Cloud-Markt[7] hat in den letzten Jahren ein starkes Wachstum erfahren, das durch die steigende Zahl von Cloud-Nutzern und Anwendungsfällen angetrieben wurde. Dieses Wachstum wird sich in den kommenden Jahren fortsetzen, da das Potenzial für Cloud-Dienste noch nicht vollständig ausgeschöpft ist.[8]

Zunächst sollen in diesem Kapitel die Begrifflichkeiten und die zu untersuchenden Angebote definiert werden. Darauf folgen eine Analyse des weltweiten Public-Cloud-Marktes sowie eine Analyse für den EU-27-Markt und den deutschen Markt.

2.1 Begriffsklärung und Abgrenzungen

Das Bundesamt für Sicherheit und Informationstechnik definiert Cloud Computing wie folgt:

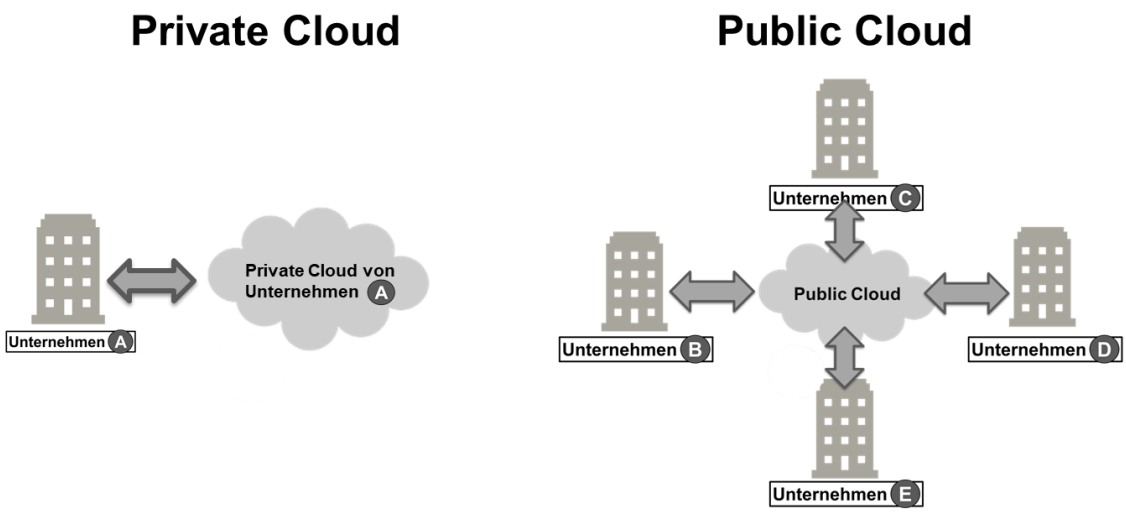
> *„Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.“*[9]

Damit unterscheidet sich Cloud Computing von On-Premise-Lösungen[10] grundsätzlich, da On-Premise-Datenspeicherung und -Rechenleistung im eigenen Netzwerk des Unternehmens liegen.

7 Siehe Definition in Kapitel 2.1
8 Statista (2021a).
9 Bundesamt für Sicherheit in der Informationstechnik (2020).
10 IT-Infrastruktur die vor Ort in den Betrieben implementiert wird.

Bei Cloud Computing wird zwischen Private und Public Cloud unterschieden.[11] Eine Public Cloud oder „öffentliche Cloud“ ist ein Cloud-Dienst, der von einem Cloud-Anbieter für mehrere Kunden angeboten wird. Die Private Cloud hingegen wird ausschließlich von einem Unternehmen oder einer einzigen Organisation betrieben. Dabei kann die Private Cloud vom Unternehmen selbst organisiert und betrieben oder von einem externen Cloud-Anbieter betrieben werden (siehe Abbildung 2-1).[12] Somit ermöglichen Public Clouds Skalierbarkeit und das gemeinsame Nutzen von Ressourcen, die über die Möglichkeiten eines einzelnen Unternehmens in den meisten Fällen hinausgehen.

Abbildung 2-1: Private versus Public Cloud



Quelle: WIK-Consult.

Die einzelnen Segmente der Public Cloud, welche auch als Servicemodelle bezeichnet werden, ergeben sich aus der Aufteilung von Aufgaben und Zuständigkeiten zwischen dem eigenen Unternehmen und dem Cloud-Anbieter. Die gewöhnlichen Servicemodelle werden als Infrastructure as a Service, Plattform as a Service und Software as a Service bezeichnet:[13]

- Infrastructure as a Service (IaaS) umfasst IT-Ressourcen wie Rechenleistung, Speicher, Netze oder die Virtualisierung von Hardware. Dieser Service wird besonders von IT-Administratoren eines Unternehmens beansprucht.
- Bei Platform as a Service (PaaS) werden neben der Bereitstellung von einer kompletten Infrastruktur standardisierte Schnittstellen angeboten, die von den Diensten des Unternehmens genutzt werden. Dem Kunden wird eine Plattform geboten,

11 Zusätzlich zu Public und Private Cloud kann die Community Cloud definiert werden, welche von einem Unternehmen und anderen Institutionen, die zur gleichen Gemeinschaft gehören und gemeinsame Anliegen haben (z.B. Forschungsgemeinschaften, Genossenschaften), geteilt wird.
12 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2020) und Haselmann et al. (2012), S. 30.
13 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2020) und KPMG (2021), S. 14.

um dort eigene Anwendungen zu entwickeln und laufen zu lassen. Somit wird dieser Service meist von Software-Entwicklern genutzt.

- Bei Software as a Service werden dem Kunden skalierbare onlinefähige Standardanwendungen angeboten. Somit umfasst Software as a Service Dienste aus IaaS und PaaS mit dem zusätzlichen Angebot von Software für Endkunden. SaaS-Zielgruppe sind somit Endnutzer.

Neben diesen drei unterschiedlichen Servicemodellen, in die grundsätzlich unterschieden werden kann, gibt es weitere „as a Service"-Begriffe, wie zum Beispiel Security as a Service, Business Process as a Service, Everything as a Service oder Künstliche Intelligenz as a Service. Meistens lassen sich diese Angebote jedoch grob in eines der drei wesentlichen Servicemodelle zuordnen.[14] Es sei außerdem zu beachten, dass die „as a Service"-Begriffe mitunter inflationär verwendet werden und die Begrifflichkeit mit unterschiedlichen Bedeutungen besetzt werden oder als eigenständiges Servicemodell gesehen werden. Ebenso kann der Begriff „Everyting as a Service", welcher mit „XaaS" abgekürzt wird, einmal als umfassender Begriff für alle Servicemodelle benutzt werden oder als Begriff bei dem das „X" lediglich ein Platzhalter für mögliche Services darstellt.[15]

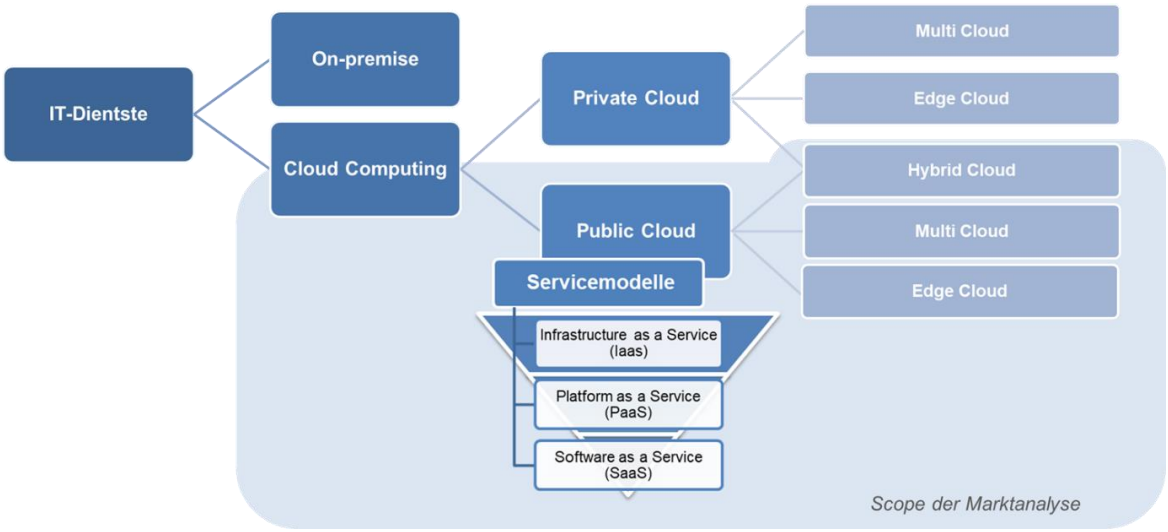
Weitere Betriebsformen des Cloud Computing sind Edge Cloud, Multi Cloud und Hybrid Cloud. Multi Cloud besteht aus mehr als einer Cloud-Lösung des gleichen Typs (Public oder Private) von unterschiedlichen Cloud-Anbietern. Hybrid Cloud hingegen umfasst die Implementierung mehrere Clouds unterschiedlicher Typen (Public und Private Cloud).[16]

Die Edge-Cloud als Sonderform des Cloud Computing bezeichnet das Heranbringen von Funktionalität und Zugänglichkeit der Cloud näher an den Ort, auch Netzwerkrand genannt, an dem Daten generiert und genutzt werden. Dadurch können zum Beispiel Latenzzeiten für zeitkritische Anwendungen verkürzt werden, aber auch sensible Daten näher an der Quelle aufbewahrt und Kosten für Datenübermittlung eingespart werden.[17] Da durch eine wachsende Anzahl an IoT-Geräte immer mehr Daten am Netzwerkrand generiert werden, steigt auch die Nachfrage nach Edge-Cloud-Computing, um Kosten, die durch die Übertragung entstehen, einzusparen. Im Hinblick auf Latenzzeiten adressiert Edge-Cloud-Computing besonders den wachsenden Markt der industriellen IoT-Anwendungen, in denen Echtzeitrechenleistung benötigt werden.

Ein Überblick über die Beziehungen der genannten Begrifflichkeiten wird in Abbildung 2-2 gegeben.

14 Vgl. Bundesamt für Sicherheit in der Informationstechnik (2020).
15 Vgl. Bedner (2013), S. 31 und Cloudcomputing Insider (2017).
16 Vgl. Red Hat (2021)
17 Vgl. Intel (2021).

Abbildung 2-2: Begriffsklärung Cloud Computing



Quelle: WIK-Consult.

2.2 Marktstruktur

Dieses Kapitel geht näher auf die Strukturen und Anbieter des weltweiten, EU-27-weiten und deutschlandweiten Cloud-Marktes ein. Ergebnis ist die Darstellung der relevanten Akteure anhand von Marktgröße und Marktanteilen in den bedeutendsten Cloud-Markt-Segmenten, welche im vorangegangenen Kapitel definiert wurden.

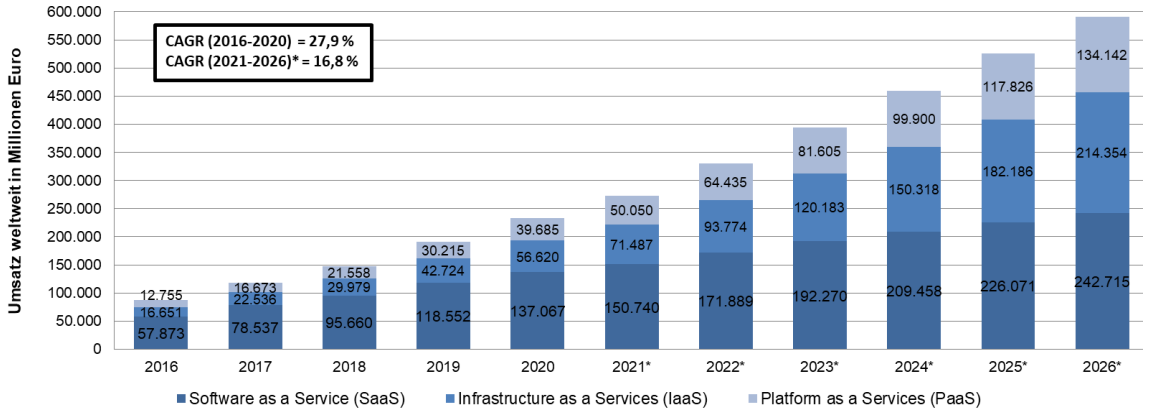
Im Jahr 2020 erzielte der gesamte Public Cloud-Markt 233,4 Mrd. Euro Umsatz.[18] Auch die vermehrte Nutzung dieser aufbauenden Angebote führt zu einem anhaltend exponentiellen Wachstum des globalen Cloud-Computing-Marktes, das auch für die kommenden Jahre prognostiziert wird.[19] Die Pandemiesituation im Jahr 2020 beschleunigte die Entwicklung der vermehrten Nutzung von Cloud-Services zusätzlich, z. B. um geschäftskritische Prozesse im Home Office aufrechtzuerhalten und die Kommunikation über Videokonferenzen zu ermöglichen.

Der weltweite Markt für Infrastructure as a Service (IaaS) ist allein zwischen den Jahren 2019 und 2020 um 33 % auf insgesamt 56,6 Milliarden Euro gewachsen (siehe Abbildung 2-3). Auf IaaS als reine Zurverfügungstellung von Speicher- und CPU-Infrastruktur bauen eine Reihe weiterer Services auf, die zu Public-Cloud-Anwendungen zählen. Dazu gehören der Bezug von Betriebssystemen und Entwicklungsumgebungen (Platform as a Service, PaaS) und Software (Software as a Service, SaaS) mit der Unterkategorie von Anwendungen mit künstlicher Intelligenz (KI as a Service, KaaS).[20]

18 Statista (2021a).
19 Vgl. KPMG (2021): The European Cloud Market: Key challenges for Europe and five scenarios with major impacts by 2027-2030.
20 Vgl. Microsoft (2020): Was ist SaaS? https://azure.microsoft.com/de-de/overview/what-is-saas/

In Abbildung 2-3 wird der weltweite Gesamtumsatz des Public-Cloud-Marktes mit den drei Segmenten IaaS, PaaS und SaaS im Zeitverlauf dargestellt. Insgesamt ist der Public-Cloud-Markt seit 2016 durchschnittlich um 27,9 % pro Jahr gewachsen und umfasste 2020 ein Umsatzvolumen von 233,4 Mrd. Euro. Die höchsten Umsätze werden in den Vereinigten Staaten (124,2 Mrd. Euro), China (16,1 Mrd. Euro), dem Vereinten Königreich (11,1 Mrd. Euro), Deutschland (10,5 Mrd. Euro) und Japan (8,4 Mrd. Euro) erwirtschaftet.[21]

Abbildung 2-3: Umsatz mit Public Cloud weltweit von 2016 bis 2020 und Prognose bis 2026, nach Segment



Quelle: Statista Technology Market Outlook (2021a). Mit * markierte Jahreszahlen stellen Prognosen dar.

Weltweit ist das Servicemodell IaaS in dem Zeitraum zwischen 2016 und 2020 am stärksten gewachsen, mit einer jährlichen durchschnittlichen Wachstumsrate von 35,8 %, gefolgt von PaaS mit einer jährlichen durchschnittlichen Wachstumsrate von 32,8 %. Das Segment SaaS hatte in diesem Zeitraum eine jährliche durchschnittliche Wachstumsrate von 24,1 %. Es wird prognostiziert, dass sich das relative Wachstum global abschwächt. Eine jährliche durchschnittliche Wachstumsrate zwischen 2021 und 2026 wird auf 16,8 % geschätzt.

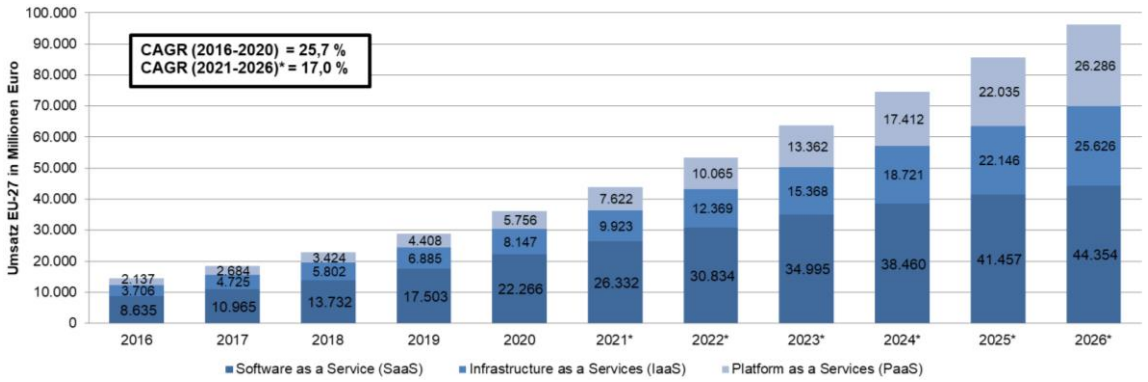
Trotz geringerer durchschnittlicher Wachstumsraten im SaaS-Segment ist dieses weltweit nach wie vor im Jahr 2020 das Umsatzstärkste mit einem Anteil von 59 %, verglichen mit IaaS (24 %) und PaaS (17 %) - siehe Abbildung 2-6).

Der Public-Cloud-Markt in der EU-27 erzielte 36,2 Mrd. Euro Umsatz im Jahr 2020 (siehe Abbildung 2-4). Damit werden 15,5 % des globalen Marktvolumens in der EU umgesetzt. Die umsatzstärksten europäischen Märkte sind Deutschland (10,5 Mrd. Euro), Frankreich (5,9 Mrd. Euro), Italien (3,3 Mrd. Euro), die Niederlande (3,2 Mrd. Euro) und Spanien (2,7 Mrd. Euro). Die Wachstumsraten liegen auf einem ähnlich hohen Niveau wie der globale Markt. Zwischen 2016 und 2020 stiegen die Umsätze pro Jahr im Durchschnitt um

21 Vgl. Statista (2021a).

25,7 %. Ebenso wird mit einem Abschwächen der Wachstumsraten gerechnet: Für die Jahre 2021 bis 2026 wird ein jährliches durchschnittliches Wachstum von 17,0 % erwartet.

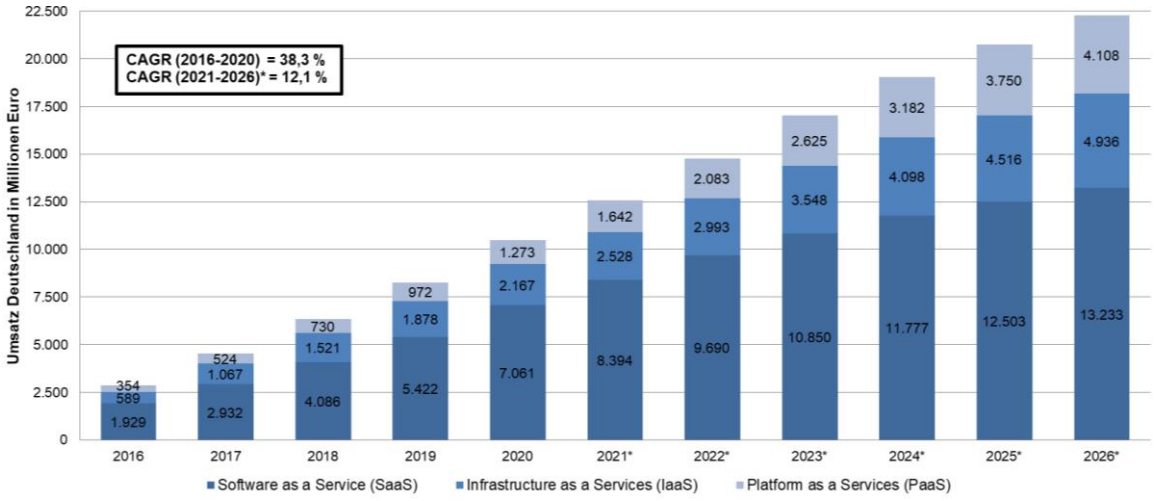
Abbildung 2-4: Umsatz mit Public Cloud in EU-27 von 2016 bis 2020 und Prognose bis 2026, nach Segment



Quelle: Statista Technology Market Outlook (2021a). Mit * markierte Jahreszahlen stellen Prognosen dar.

In der EU-27 ist eine ähnliche Umsatzaufteilung zwischen den drei Segmenten zu beobachten, verglichen mit dem globalen Public-Cloud-Markt. Das SaaS ist im Jahr 2020 das umsatzstärkste Segment mit 62 % (entspricht 22,3 Mrd. Euro), gefolgt von IaaS (22 %, entspricht 8,1 Mrd. Euro) und PaaS (16 %, entspricht 5,8 Mrd. Euro). In Abbildung 2-6 sind die Anteile dargestellt. Der deutsche Public Cloud-Markt ist, verglichen mit dem EU-27-Durchschnitt, mit einer jährlichen durchschnittlichen Wachstumsrate von 38,3 %, zwischen 2016 und 2020 besonders stark gewachsen. Wie Abbildung 2-5 zeigt, lag der Gesamtumsatz 2020 bei 10,5 Mrd. Euro. Möglicherweise dem bereits besonders starken Wachstum in den vergangenen vier Jahren geschuldet, werden für die nächsten fünf Jahre geringere Wachstumsraten, verglichen mit dem EU-27 Durchschnitt, erwartet. Diese sollen Prognosen zufolge im Durchschnitt bei 12,1 % jährlich liegen (für die Jahre 2021 bis 2026).

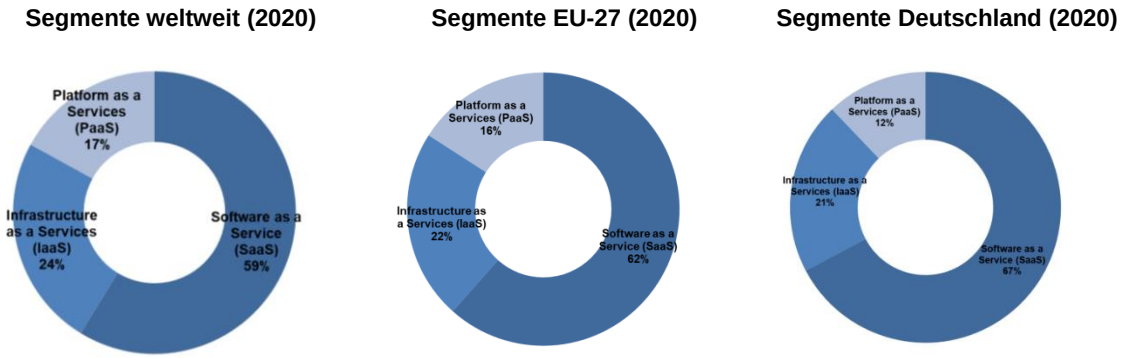
Abbildung 2-5: Umsatz mit Public Cloud in Deutschland von 2016 bis 2020 und Prognose bis 2026, nach Segment



Quelle: Statista Technology Market Outlook (2021a). Mit * markierte Jahreszahlen stellen Prognosen dar.

Abbildung 3-6 zeigt die Anteile der Segmente des Public-Cloud-Marktes. Sowohl im globalen Public-Cloud-Markt als auch im EU-27-weiten, dominiert das Servicemodell SaaS im Jahr 2020 in Deutschland mit 67 % Anteil am gesamten Cloud-Markt, was einem Umsatz von 13,2 Mrd. Euro entspricht. Der Marktanteil von SaaS am gesamten Cloud-Markt ist in Deutschland somit höher als im EU-27-weiten Durchschnitt und auch im globalen Durchschnitt. IaaS als zweitgrößtes Servicemodell erreicht im Jahr 2020 einen Umsatz von 4,9 Mrd. Euro (21 % Marktanteil). PaaS erreicht einen Umsatz von 4,1 Mrd. Euro (12 % Marktanteil).

Abbildung 2-6: Anteile Segmente weltweit und Europa von Cloud Computing nach Umsatz (2020)



Quelle: Statista Technology Market Outlook (2021a).

Dieser Überblick über die Marktgröße und die Marktentwicklung zeigt, dass der Markt für Cloud-Dienste sowohl weltweit als auch in Europa und Deutschland von zweistelligen jährlichen Wachstumsraten geprägt ist. Mehr als die Hälfte des Marktes besteht aus SaaS-Dienste, während IaaS und PaaS in etwa vergleichbar groß sind. Laut den Marktprognosen wird aber der Anteil SaaS vom Cloudmarkt in den kommenden Jahren sinken.

2.3 Marktanteile der relevanten Anbieter

Um den europäischen und den deutschen Markt isoliert zu betrachten, wurden über eine Literaturanalyse aktuelle Marktstudien und Monitorings sowie Jahresberichte und Finanzinformationen der relevanten Anbieter sowie Pressemeldungen einbezogen. Auf dieser Grundlage wurden transparente qualifizierte Schätzungen vorgenommen, die durch Gespräche mit Experten (Vertreter von Verbänden und Ansprechpartner aus wissenschaftlichen Institutionen, die im Beriech Wissenstransfer aktiv sind) validiert wurden.

Die Marktverteilung unter den Cloud-Anbietern unterscheidet sich stark zwischen den drei Servicemodellen.

Die Hyperscaler, dazu gehören vor allem Amazon, Microsoft, Google, Alibaba und Huawei, haben auf dem globalen Cloud-Markt deutliche Skalenvorteile. Denn IaaS und die darauf basierenden Services sind, wie viele andere digitale Services auch, durch hohe Fixkosten und geringe variable Kosten geprägt. Ein eigenes Ökosystem, das dem Nutzer unterschiedliche Services aus einer Hand anbietet, ist ein weiterer Vorteil der Hyperscaler.[22] Hinzu kommt, dass die aus Nutzersicht unbegrenzt flexiblen Kapazitäten bei einer gesicherten Grundauslastung deutlich besser gesteuert werden können. Die oben genannten Hyperscaler teilten im Jahr 2020 ca. 80 % des IaaS-Marktes unter sich auf, siehe Tabelle 2-1.

Tabelle 2-1: Marktanteil gemessen am Umsatz von IaaS, global (2019 und 2020)

Unternehmen	Umsatz 2020	Marktanteil 2020 (in Prozent)	Umsatz 2019	Marktanteil 2019 (in Prozent)	Wachstum 2019-2020 (in Prozent)
Amazon Web Services (AWS)	26,2	40,8	20,4	44,6	28,7
Microsoft Azure	12,7	19,7	8,0	17,4	59,2
Alibaba	6,1	9,5	4,0	8,8	52,8
Google Cloud Platform	3,9	6,1	2,4	5,2	66,1
Huawei	2,7	4,2	0,9	1,9	202,8
Andere	12,7	19,8	10,1	22,1	25,6
Gesamt	**64,3**	**100,0**	**45,7**	**100,0**	**40,7**

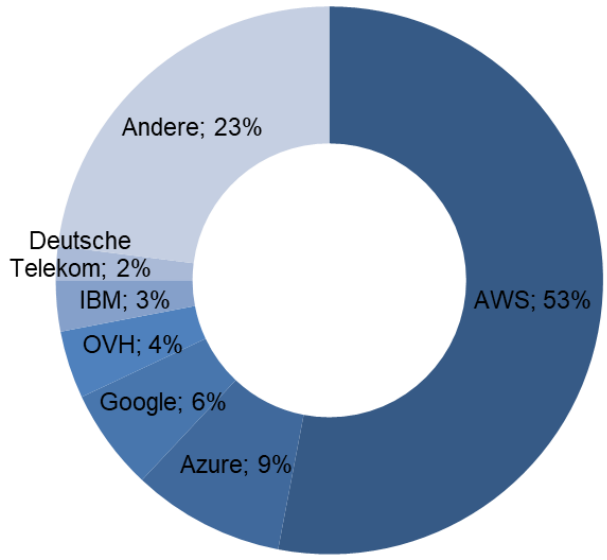
Quelle: Gartner (2021).

22 Vgl. Gull et al. (2020), S. 24 ff.

Der europäische Markt für IaaS, PaaS und Hosted Private Cloud wird hauptsächlich von den drei großen US-amerikanischen Hyperscalern AWS, Microsoft Azure und Google Cloud Platform dominiert. Die chinesischen Anbieter Alibaba und Tencent, die auf dem globalen Markt Anteile von knapp 10 % bzw. 4 % haben,[23] spielen in Europa hingegen eine untergeordnete Rolle. In den Bereichen IaaS, PaaS und Hosted Private Cloud stehen beispielsweise OVHCloud in Frankreich an dritter und die Deutsche Telekom in Deutschland an vierter Stelle.[24]

Abbildung 2-7 zeigt die Marktanteile der IaaS-Cloud-Anbieter in Europa 2020. Insgesamt handelt es sich bei den drei größten Anbietern in Europa mit einem gemeinsamen Marktanteil von 68 % um Unternehmen mit Sitz in den USA.

Abbildung 2-7: Marktanteile IaaS in Europa (2020)



Quelle: KPMG (2021).

Zwar haben die europäischen Anbieter, wie die Deutsche Telekom, OVH, Orange und Swisscom, ihren Umsatz in einem Zeitraum von vier Jahren mehr als verdoppelt, können aber nicht mit den Wachstumsraten und dem Investitionsvolumen der Hyperscaler mithalten.[25] Ebenso wird der Deutschen Telekom, vorgeworfen, von Beginn an im Jahr 2016 zusammen mit dem chinesischen Hersteller Huawei ihren Cloud-Dienst aufgebaut zu haben. Außerdem agiert die Deutsche Telekom auch als Reseller von Cloud-Diensten von

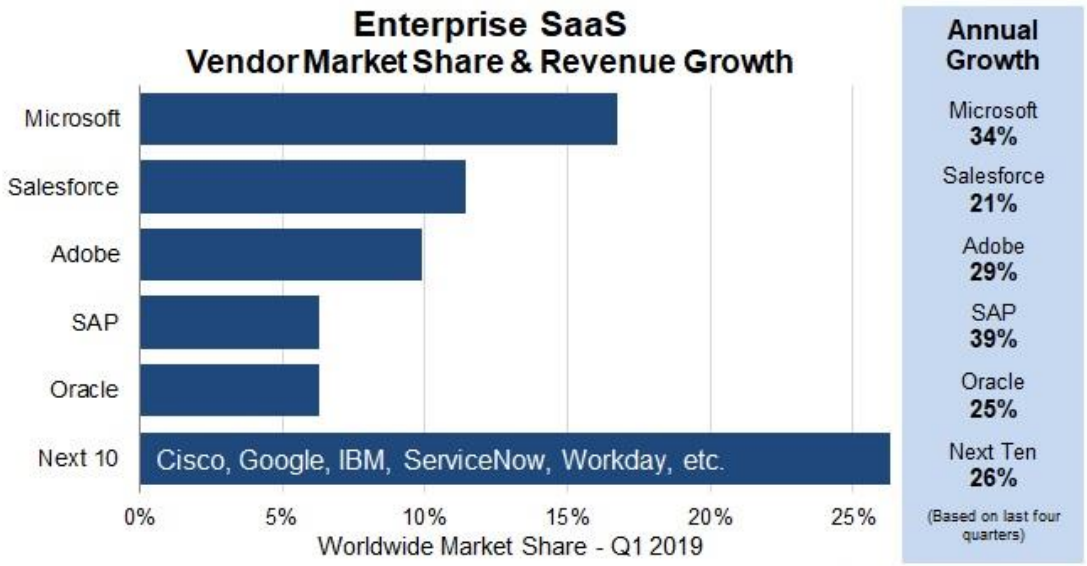
23 Synergy Research Group (2021a).
24 Synergy Research Group (2020a).
25 Synergy Research Group (2021b).

AWS und MS Azure[26]. Beides wirkt eher verstärkend als verringert auf die Abhängigkeit gegenüber nicht-europäischer Unternehmen.

Die Marktführer im IaaS und PaaS Segment in Deutschland sind AWS, Microsoft Azure, Google Cloud Platform, Deutsche Telekom, IBM und Oracle, konkrete Marktdaten liegen jedoch nicht vor.[27] Die Verteilung der Marktanteile im IaaS und PaaS-Segment sind somit besonders geprägt von wenigen Unternehmen mit sehr hohem Anteil und einer Vielzahl von Unternehmen mit sehr geringem Anteil.

Der Markt lässt sich differenzieren nach geografischen (z. B. Unternehmenssitz der Anbieter) und funktionalen Merkmalen (z. B. Angebotsportfolio, Funktionen und Geschäftsbedingungen der Anbieter). Funktional lassen sich z. B. die private und gewerbliche Nutzung von Cloud-Services und deren Angebotstiefe unterscheiden, also welche Marktsegmente von XaaS der Anbieter bedient. Bei den Marktanteilen von SaaS zeigt sich beispielsweise, dass Microsoft mit seiner Unternehmenssoftware Microsoft 365 und Business-Intelligence (BI) -Programmen Marktführer auf dem SaaS-Markt ist, siehe Abbildung 2-8.[28] Für den europäischen oder deutschen Markt liegen keine konkreten Marktverteilungen für das SaaS-Segment vor.

Abbildung 2-8: SaaS-Marktanteil und Umsatzwachstum



Quelle: Synergy Research Group (2020b).

26 Handelsblatt Kommentar, Europas Cloudanbietern fehlt gegenüber den US-Rivalen der Mut, online verfügbar unter https://www.handelsblatt.com/meinung/kommentare/kommentar-europas-cloudanbietern-fehlt-gegenueber-den-us-rivalen-der-mut/26962646.html, zuletzt abgerufen am 10.02.2022.

27 Vgl. Synergy Research Group (2020a).

28 Vgl. Kinsta (2021).

Zusammenfassend kann festgestellt werden, dass vor allem der Markt für IaaS und PaaS von wenigen Anbietern (Hyperscaler) sowohl weltweit, in EU-27 und in Deutschland geprägt sind. In Deutschland scheint der Markt sogar noch konzentrierter zu sein. Die drei größten Anbieter verfügen über etwa ca. 2/3 der Marktanteile.

Der Gesamtmarkt für SaaS ist dagegen deutlich heterogener mit einem vergleichbaren geringeren Grad der Konzentration. Mit Ausnahme von Microsoft sind andere Anbieter in dem SaaS-Markt, anders als in den IaaS- und PaaS-Märkten, prägend für den Gesamtmarkt. Die Anbieter im Saas-Markt sind Software-Anbieter, die sich von ihren Wettbewerbern mit ihren Applikationen differenzieren. Da die Applikationen auf unterschiedlichen Kundennutzen abstellen (z. B. im Vergleich Microsoft 365 vom Microsoft mit S4/Hana von SAP oder die CRM-Software von Salesforce) ist die Substituierbarkeit der Angebote in vielen Fällen nicht gegeben und es stellt sich die Frage der Marktabgrenzung bzw. ob der Markt für SaaS-Dienste als ein Markt oder als mehrere Märkte abzugrenzen sind.

3 Differenzierungsmerkmale und Anbietersteckbriefe

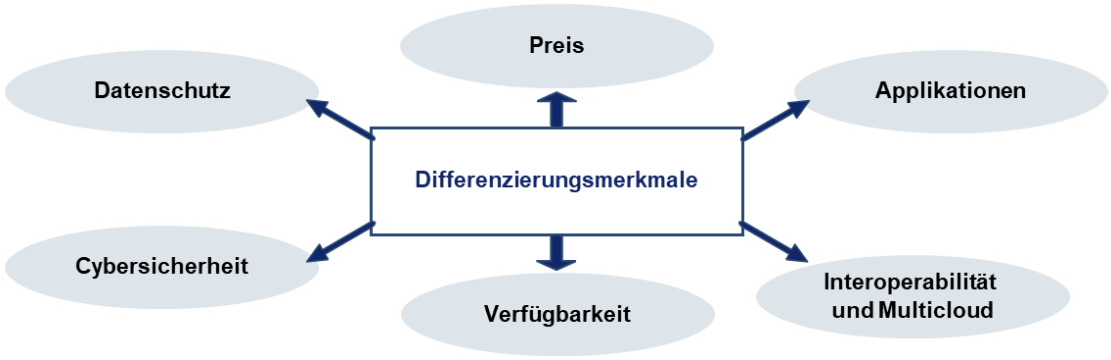
In diesem Kapitel werden die Ergebnisse der Desktoprecherche in Steckbriefform je Anbieter dargestellt. Dabei werden sowohl die Umsatz- und Renditezahlen sowie die Marktanteile als auch die Ausprägungen der Differenzierungsmerkmale am Markt gezeigt.

3.1 Wesentliche Differenzierungsmerkmale der Anbieter und Identifikation Cloud-Computing-Features

Mit dem Ziel, die wesentlichen Stellschrauben für die Marktstrukturen und Wettbewerbsdynamiken zu ermitteln, geht dieses Kapitel auf die folgenden Fragen ein: Welche sind die zentralen Differenzierungsmerkmale der wichtigsten Anbieter in Europa und deren Angebote, insbesondere in Bezug auf Leistungsbeschreibungen und AGBs? Wie werden der Datenschutz und die Datensicherheit in Bezug auf Unternehmensdaten geregelt? Daraus wird eine Stärken-Schwächen-Analyse der Anbieter in Kapitel 4 abgeleitet.

Die untersuchten Dimensionen der Differenzierungsmerkmale sind in Abbildung 3-1 dargestellt.

Abbildung 3-1: Differenzierungsmerkmale am Cloud-Markt



Quelle: WIK GmbH.

Zu wichtigen Differenzierungsmerkmalen und Features gehören insbesondere:

- Preis und Preisstrukturen: Bei Cloud-Infrastrukturen lassen sich Skalenerträge insbesondere bei Computing und Storage (Datenspeicher) erzielen. Durch eine dynamische Zuteilung der Ressourcen (Computing und Storage) können Leerkapazitäten besser vermieden werden als bei einer On-Premise-Lösung (Implementierung der Infrastruktur vor Ort bei Unternehmen). Somit können Cloud-Anbieter günstigere Angebote als vergleichbare On-Premise-Lösungen unterbreiten. Als gegenläufiger Effekt entstehen bei Cloud-Lösungen für die Datenübertragung höhere Kosten, die allerdings mit den über die Zeit sinkenden Netzkosten teilweise an Relevanz verloren haben.

- Verfügbare Software: Die Cloud-Anbieter integrieren eine Vielzahl an (Entwickler-)Tools und Softwarebibliotheken, z. B. Data-Analytics-Werkzeuge, Spracherkennung, Sprachausgabe, Recognition-Tools, Übersetzung, Textana-lyse, etc.[29] Dies erweitert die über die Cloud nutzbaren Funktionen und erhöht die Bindung des Nutzers an einen Anbieter.

- Interoperabilität, Möglichkeit zur Multi-Cloud-Lösungen und Datenmigration: Die Anbieter haben ein Interesse daran, den Vendor-Lock in für ihre Anwendungen zu verstärken, für Nutzer ist diese Abhängigkeit von einem Anbieter nachteilig. Stattdessen streben sie eher Multi-Cloud-Lösungen an.

- Verfügbarkeit und Ausfallsicherheit, Verfügbarkeit der Plattformen und redundante Implementierung der Datenspeicher: Dies sind die Grundbedingungen, die ein Nutzer an die Cloud-Anwendung stellt. In Abhängigkeit vom Anwendungsfall sind diese Aspekte der Verlässlichkeit der Services entscheidend.

29 Vgl. Gull et al. (2020), S. 39.

- Cybersicherheit: Die Einhaltung von Standards (z. B. ISO 27000 / ISO 27017, BSI C5): Standards helfen dem Nutzer, bestimmte Sicherheitsaspekte besser beurteilen zu können.

- Datenschutz: Alle US-amerikanischen Unternehmen unterliegen dem US CLOUD Act (Clarifying Lawful Overseas Use of Data Act), dem zufolge sie mitunter die bei ihnen gespeicherte Daten den US-Behörden für Ermittlungszwecke offenlegen müssen.[30] Das gilt unabhängig von der Berechtigung an den Daten und von deren Speicherort bzw. Server-Standort. Demnach haben Open Telekom Cloud und IONOS Cloud einen deutlichen Vorteil beim Datenschutz, da sie den europäischen Datenschutzrichtlinien, insbesondere der DSGVO unterliegen.

Zusammen mit den Leistungsbeschreibungen ist es erforderlich, die Entwicklungstendenzen zu berücksichtigen, um eine holistische Analyse durchführen zu können. Dazu gehören unter anderem folgende Umstände:[31]

- Ein steigender Trend zur Interoperabilität fördert offene Cloud-Ökosysteme, die kleinere Anbieter einschließen, und reduziert Lock-in-Effekte, die insbesondere bei den Ökosystemen der Hyperscaler bestehen.

- Neue Marktsegmente, wie Edge-Computing und spezifische Anwendungsfälle von KaaS (KI as a Service), eröffnen Wachstumspotenzial für alle Anbieter.

- Eine stärkere Regulierung kann zu einem Vorteil europäischer Anbieter führen, da diese z. B. beim Thema Datenschutz weiter fortgeschritten sind.

3.2 Anbietersteckbriefe

Die nachfolgenden Tabellen fassen die Daten zu den Leistungsmerkmalen je Anbieter zusammen.

Tabelle 4-1 zeigt den Steckbrief von Amazon Web Service, dem Marktführer weltweit und in Europa. Es ist ersichtlich, dass der Marktanteil in Europa noch deutlich höher ist als weltweit und AWS mit einer Umsatzrentabilität von ca. 38 % sehr profitabel ist. Die Angebote sind gekennzeichnet durch eine hohe Verfügbarkeit und viele komplementäre Services. Das Preisniveau liegt insgesamt leicht unter dem Niveau von Microsoft Azure.

30 Dieses US-Gesetz gestattet in bestimmten Grenzen und unter bestimmten Voraussetzungen den Zugriff der US-Behörden auf Daten in Rechenzentren außerhalb der USA, und zwar indem ein US-Unternehmen mit entsprechenden Außenstandorten angewiesen wird, die im Ausland gespeicherten Daten in die USA zu übertragen und hier an die Behörde herauszugeben.

31 Vgl. hier und im Folgenden KPMG (2021).

Tabelle 3-1: Steckbrief Amazon Web Service

	Amazon Web Service		
	weltweit	**EU**	**Deutschland**
Umsatz 2020 in Mio USD bzw. Mio EUR	35.448	7.372	1.749*
Marktanteil 2020	33,6%	53,0%	53,0%*
Rendite 2020 in Mio USD bzw. Mio EUR	13.531	2.359*	659*
Preisniveau	Preiseniveau insgesamt leicht unter Azure		
Anzahl Services	190 Cloud Services		
Anzahl der Regionen weltweit	24		
Verfügbarkeit	99,999%		
CPU-Performance	Höher als Azure und Google Cloud Platform, niedriger als Open Telekom Cloud		
Interoperabilität/Plattform für Multi-Cloud	mPlat Suit von AWS Market Place als Multi-Cloud-Conductor		
BSI C5-zertifiziert	Ja		
ISO Zertifikate	ISO 27001: ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO 9001:2015		
Besonderheiten in den AGBs	Nutzer ist für die Datenschutzmitteilungen und Einholung von Einwilligungen zur Verarbeitung personenbezogener Daten zuständig und sichert die Einhaltung dessen gegenüber AWS zu.		
Automatische Verschlüsselung von Daten	Automatische Verschlüsselung von Daten		
Kernkompetenzen	Developer Base, Erfahrung (seit 2006)		
Innovative Services	AWS IoT Greengrass erweitert AWS auf edge devices		

Quelle: Synergy Research Group (2020b), KPMG (2021), Fraunhofer (2021), Netapp.com (2021) Jahresberichte, AGBs und Unternehmens Website. Mit * gekennzeichnete Felder zeigen eine eigene Berechnung auf Basis der Durchschnittswerte der verfügbaren Zahlen.

Tabelle 3-2 zeigt den Steckbrief von Microsoft Azure. Nach Marktanteilen nimmt Azure Platz 2 hinter AWS ein. Die Umsatzrentabilität liegt ebenfalls bei ca. 38 %. Azure hat die höchste Anzahl an Cloud-Services unter den betrachteten Anbietern. Das Preisniveau ist gehoben.

Tabelle 3-2: Steckbrief Microsoft Azure

Microrsoft Azure			
	weltweit	**EU**	**Deutschland**
Umsatz 2020 in Mio USD bzw. Mio EUR	48.336	1.252	297*
Marktanteil 2020	18,0%	9,0%	9,0%*
Rendite 2020 in Mio USD bzw. Mio EUR	18.324	1.591*	765*
Preisniveau	Pay-as-you-go-Modelle sind ca. 20-15 % teurer als AWS und Google Cloud Platform, deutliche Rabatte gibt es bei Abo-Lösungen (bis zu 70 %), bei denen sich der Nutzer zwischen ein und drei Jahre bindet		
Anzahl Services	Ca. 260 Cloud Services		
Anzahl der Regionen weltweit	23		
Verfügbarkeit	99,95 % bis 99,99 % abhängig von der Anzahl der Verfügbarkeitszonen, die für die Leistung vom Nutzer gewählt wurde		
CPU-Performance	Geringer als AWS, in etwa auf einer Höhe mit Google Cloud Platform		
Interoperabilität/Plattform für Multi-Cloud	Mit Azure Arc wird eine Plattform zur Organisation von Multi-Cloud-Lösungen zur Verfügung gestellt		
BSI C5-zertifiziert	Erfüllt		
ISO Zertifikate	ISO 21001, ISO 27017, ISO 27018, ISO 27701, ISO 9001, ISO 2000:1:2011		
Besonderheiten in den AGBs	/		
Automatische Verschlüsselung von Daten	Serverseitige Verschlüsselung durch Azure (Server Side Encryption, SSE)		
Kernkompetenzen	Angebot eines zentralen Identity Managements		
Innovative Services	Azure IOT Edge		

Quelle: Synergy Research Group (2020b), KPMG (2021), Fraunhofer (2021), Netapp.com (2021), Cloud Mercato (2020), Jahresberichte, AGBs und Unternehmens Website. Mit * gekennzeichnete Felder zeigen eine eigene Berechnung auf Basis der Durchschnittswerte der verfügbaren Zahlen.

In Tabelle 3-3 ist der Steckbrief der Google Cloud Platform. Hier fällt insbesondere auf, dass das Preisniveau niedrig ist und die Umsatzrentabilität deutlich negativ ist, was auf eine nicht kostendeckende aggressive Preissetzungsstrategie hindeutet.

Tabelle 3-3: Steckbrief Google Cloud Platform

	Google Cloud Platform		
	weltweit	**EU**	**Deutschland**
Umsatz 2020 in Mio USD bzw. Mio EUR	5.170	835	198*
Marktanteil 2020	4,9%	6,0%	6,0%*
Rendite 2020 in Mio USD bzw. Mio EUR	-5.607	-905*	-215*
Preisniveau	geringes Preisniveau		
Anzahl Services	> 115		
Anzahl der Regionen weltweit	28		
Verfügbarkeit	99,99%		
CPU-Performance	Geringer als AWS, in etwa auf einer Höhe mit Microsoft Azure		
Interoperabilität/Plattform für Multi-Cloud	Bietet Flexibilität, Anwendungen in Hybrid- und Multi-Cloud-Umgebungen zu migrieren, zu erstellen und zu optimieren und gleichzeitig Anbieterabhängigkeit zu reduzieren, branchenführende Lösungen zu nutzen und behördliche Anforderungen zu erfüllen.		
BSI C5-zertifiziert	Erfüllt		
ISO Zertifikate	ISO 21001, ISO 27017, ISO 27018, ISO 27701, ISO 9001, ISO 2000:1:2011		
Besonderheiten in den AGBs	Kündigung wegen Inaktivität. Google behält sich das Recht vor, die Bereitstellung der Dienste für ein Projekt nach einer vorangekündigten Frist von 30 Tagen zu kündigen, wenn über einen Zeitraum von 60 Tagen (a) der Kunde nicht auf die Admin-Konsole zugegriffen hat oder das betreffende Projekt keine Netzwerkaktivität hatte und (b) bei diesem Projekt keine Gebühren für diese Dienste angefallen sind.		
Automatische Verschlüsselung von Daten	Verschlüsseln Daten bei der Übertragung zwischen den Einrichtungen sowie ruhende Daten, damit sie nur von autorisierten Rollen und Diensten mit überwachtem Zugriff auf die Verschlüsselungsschlüssel aufgerufen werden können.		
Kernkompetenzen	Preis und einfacher Umgang		
Innovative Services	Google Distributed Cloud erweitert die Infrastruktur und Dienste von Google Cloud auf das Edge-Netzwerk und Rechenzentren von Kunden.		

Quelle: Synergy Research Group (2020b), KPMG (2021), Cloud Mercato (2020), Procloud (2021), Jahresberichte, AGBs und Unternehmens Website. Mit * gekennzeichnete Felder zeigen eine eigene Berechnung auf Basis der Durchschnittswerte der verfügbaren Zahlen.

Tabelle 3-4 bildet den Steckbrief von IBM ab. Auffällig ist, dass IBM Multi-Cloud-Lösungen mit Microsoft Azure, AWS, Google Cloud Platform direkt vermarktet. Das Preisniveau ist hoch, insbesondere bei Support-Leistungen, und die Umsatzrentabilität liegt bei ca. 25 %.

Tabelle 3-4: Steckbrief IBM Cloud

	IBM Cloud		
	weltweit	**EU**	**Deutschland**
Umsatz 2020 in Mio USD bzw. Mio EUR	11.326	417	99*
Marktanteil 2020	4,1%	3,0%	5,5%*
Rendite 2020 in Mio USD bzw. Mio EUR	2.755	480*	152*
Preisniveau	Komplexe Preisstrukturen, teurer Support		
Anzahl Services	< 190		
Anzahl der Regionen weltweit	Etwas geringere globale Abdeckung als AWS		
Verfügbarkeit	99,9% auf 99,99% je nach Zone und Region		
CPU-Performance	/		
Interoperabilität/Plattform für Multi-Cloud	Direkte Vermarktung von Multi-Cloud-Lösungen mit Microsoft, AWS, Google		
BSI C5-zertifiziert	Erfüllt		
ISO Zertifikate	ISO 21001, ISO 27017, ISO 27018, ISO 27701, ISO 9001, ISO 2000:1:2011, ISO 2000, ISO 20243, ISO 22301, ISO 31000, ISO 45001		
Besonderheiten in den AGBs			
Automatische Verschlüsselung von Daten	Plattform für durchgängige Datenverschlüsselung vorhanden (IBM z15)		
Kernkompetenzen	/		
Innovative Services	/		

Quelle: Synergy Research Group (2020b), KPMG (2021), Cloud Mercato (2020), Procloud (2021), Jahresberichte, AGBs und Unternehmens Website. Mit * gekennzeichnete Felder zeigen eine eigene Berechnung auf Basis der Durchschnittswerte der verfügbaren Zahlen.

Tabelle 3-5 bildet den Steckbrief der Open Telekom Cloud ab. Auffällig ist hier, dass der Service ein negatives Jahresergebnis erzielt. Die Anzahl der Services ist auch bei Einbezug der Leistungen aus dem Ökosystem recht gering. Multi-Cloud-Lösungen mit Microsoft Azure, Google Cloud Platform und AWS werden direkt vermarktet. Das Preisniveau ist geringer als bei Microsoft Azure und AWS.

Tabelle 3-5: Steckbrief Open Telekom Cloud

Open Telekom Cloud			
	weltweit	**EU**	**Deutschland**
Umsatz 2020 in Mio USD bzw. Mio EUR	4178	/	/
Marktanteil 2020	/	2%	
Rendite 2020 in Mio USD bzw. Mio EUR	-650	/	/
Preisniveau	Unter den Hyperscalern		
Anzahl Services	40 (inkl. Ökosystem mit strategischen Partnerschaften mit AWS, Google Cloud Platform und MS Azure)		
Anzahl der Regionen weltweit	6 Verfügbarkeitszonen		
Verfügbarkeit	99,999%		
CPU-Performance	Höhere Performance als bei den Hyperscalern		
Interoperabilität/Plattform für Multi -Cloud	Multi-Cloud Strategie durch strategische Partnerschaften mit Microsoft Azure, Google Cloud Platform und AWS		
BSI C5-zertifiziert	Erfüllt		
ISO Zertifikate	ISO/IEC 27001/17/18 - 27701 geplant für Q4 2022, ISO 9001, ISO 14001, ISO/IEC 20000-1, ISO 22301		
Besonderheiten in den AGBs	Nein		
Automatische Verschlüsselung von Daten	Nein		
Kernkompetenzen	Open Telekom Cloud besonders für IaaS. Neben Vermarktung des eigenen Cloud-Angebotes (Open Telekom Cloud) werden Cloudangebote von AWS, Google Cloud Platform und MS Azure vermarktet (T-Systems). Standorte der Rechenzentren in Deutschland und den Niederlanden.		
Innovative Services	Cloud-Gaming-Plattform, die auf den neusten NVIDIA RTX Servern mit rechenstarken Grafikkarten basiert. Bauen zusätzlich eine Infrastruktur auf, die dezentrale Cloud-Kapazitäten in die Netze der Deutschen Telekom integriert („Edge Clouds“).		

Quelle: Synergy Research Group (2020b), KPMG (2021), Cloud Mercato (2020), Jahresberichte, AGBs und Unternehmens Website.

In Tabelle 3-6 ist der Steckbrief der Ionos Cloud dargestellt. Die Umsatzrentabilität beträgt ca. 24 %. Die Anzahl der Services recht gering. Multi-Cloud-Lösungen mit Microsoft Azure, Google Cloud Platform und AWS werden direkt vermarktet. Das Preisniveau ist geringer als bei Microsoft Azure und AWS. Auffällig ist, dass IONOS der einzige Anbieter ist, der nicht BSI C5-zertifiziert ist.

Tabelle 3-6: Steckbrief Ionos Cloud

Ionos Cloud			
	weltweit	**EU**	**Deutschland**
Umsatz 2020 in Mio USD bzw. Mio EUR	949	/	456
Marktanteil 2020	/	/	/
Rendite 2020 in Mio USD bzw. Mio EUR	229	/	/
Preisniveau	Unter den Hyperscalern		
Anzahl Services	40 (inkl. Ökosystem)		
Anzahl der Regionen weltweit	6 Rechenzentren verteilt auf Deutschland und die USA		
Verfügbarkeit	99,99%		
CPU-Performance	Höhere Performance als bei den Hyperscalern		
Interoperabilität/Plattform für Multi-Cloud	Direkte Vermarktung von Hybrid-Multi-Cloud-Lösungen von Microsoft, AWS, Google		
BSI C5-zertifiziert	Nein		
ISO Zertifikate	ISO 9001; ISO 27001		
Besonderheiten in den AGBs	nein		
Automatische Verschlüsselung von Daten	Nein		
Kernkompetenzen	IONOS legt bei Servern in Deutschland und Europa besonderen Wert auf die Einhaltung der deutschen und europäischen Datenschutzrichtlinien der DSGVO. Ihre Projekte können Sie somit DSGVO-konform betreiben und Ihre Daten sind vor Zugriff staatlicher Stellen geschützt; leistungsfähiges, flexibles und preisgünstiges Angebot und fokussiert auf den Mittelstand im europäischen Raum		
Innovative Services	/		

Quelle: Jahresberichte, AGBs und Unternehmens Website.

Die vergleichende Analyse der Anbieter und die Erstellung einer Anbieter-/ Leistungsmatrix folgen in Kapitel 5.

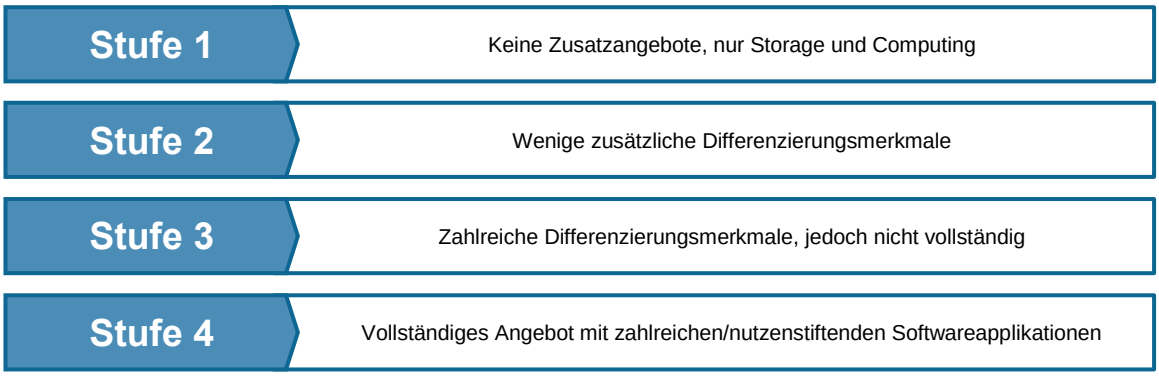
4 Analyse der Wettbewerbslandschaft

Mit den Ergebnissen aus den Markterhebungen wurden die Leistungen der Anbieter einander gegenübergestellt und analysiert. Aus der Analyse der Differenzierungsmerkmale wurde eine Anbieter-/Leistungsmatrix erstellt, inklusive der Produktmerkmale, Datenschutz- und Datensicherheitsaspekten sowie der Preispositionierung der relevanten Anbieter, die in Kapitel 4 beschrieben wurden.

4.1 Produktmerkmale

Die Angebote der Cloud-Anbieter für die Analyse werden den folgenden 4 Stufen zugeteilt (siehe Abbildung 4-1).

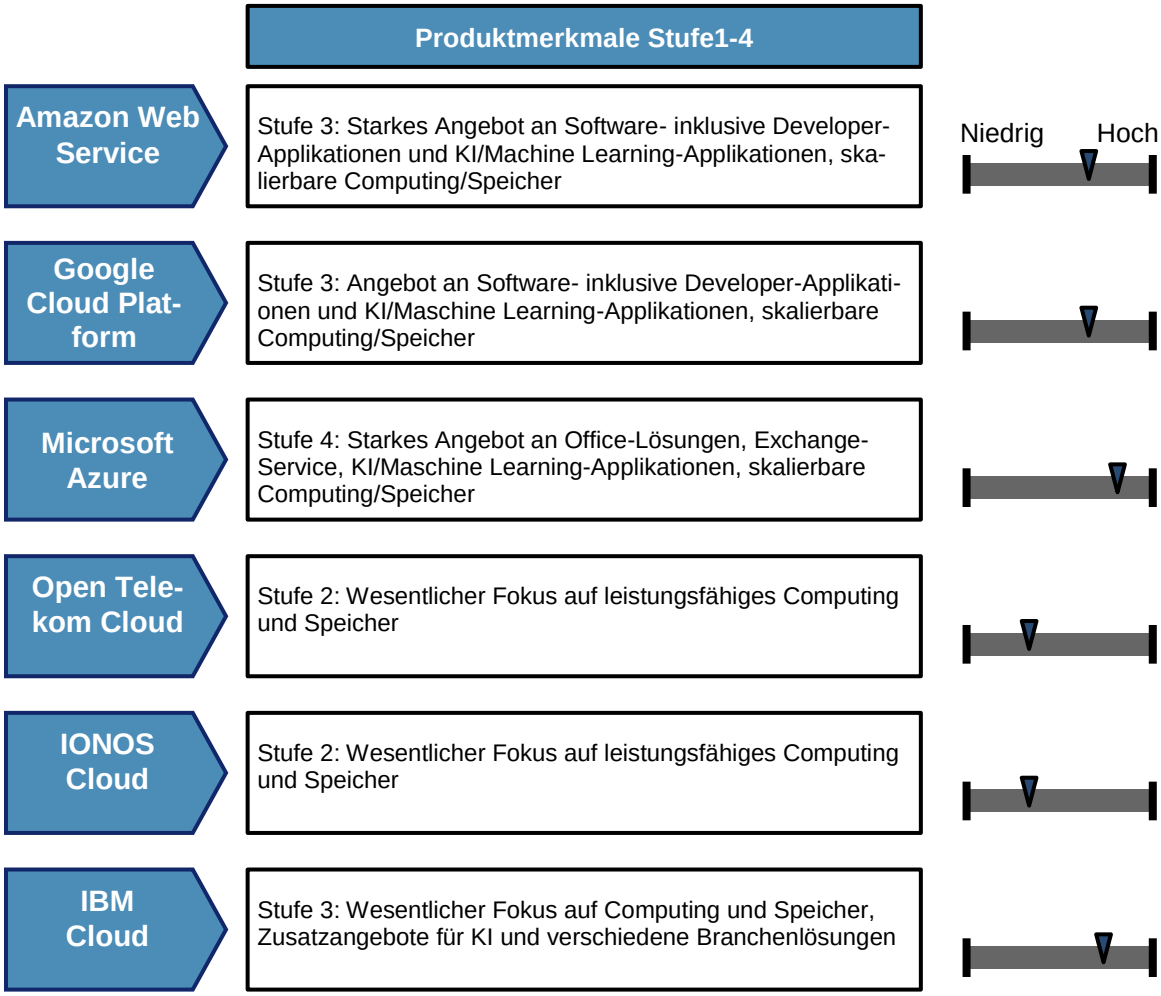
Abbildung 4-1: Einstufung der Marktpositionen anhand der Produktmerkmale



Quelle: WIK-Consult.

Gemäß der Anbieterdarstellung in Kapitel 4 ergibt sich folgendes Bild in der vergleichenden Analyse (siehe Abbildung 4-2).

Abbildung 4-2: Marktpositionierung der Cloud-Anbieter anhand der Produktmerkmale



Quelle: WIK-Consult.

Besonders die Hyperscaler können mit einer großen Produktpalette punkten. Die meisten Cloud-Services bietet Microsoft Azure an (ca. 260), das gleichzeitig auch globaler Marktführer im SaaS-Segment ist (siehe Kapitel 2.3). Darauf folgen AWS und IBM mit ca. 190 und Google Cloud Platform mit über 115. Durch strategische Partnerschaften können jedoch auch europäische Anbieter wie die Open Telekom Cloud und IONOS Cloud ergänzende Services im Endkunden-Segment anbieten, obgleich sie selbst stark auf IaaS fokussiert sind. Open Telekom Cloud und IONOS Cloud liegen bei ca. 40 inklusive der Angebote ihrer Partner im Ökosystem.

Diese Anzahl allein ist vermutlich jedoch nicht ausschlaggebend für eine Entscheidung für oder gegen einen Cloud-Anbieter. Bei den Hyperscalern machen fünf bis zehn Services ca. 70 % bis 80 % des Umsatzes aus. Bei AWS sind es sogar die Top-4-Services, die für 85 % des Umsatzes verantwortlich sind.[32]

32 Vgl. KPMG (2021), S. 30.

4.2 Verfügbarkeit

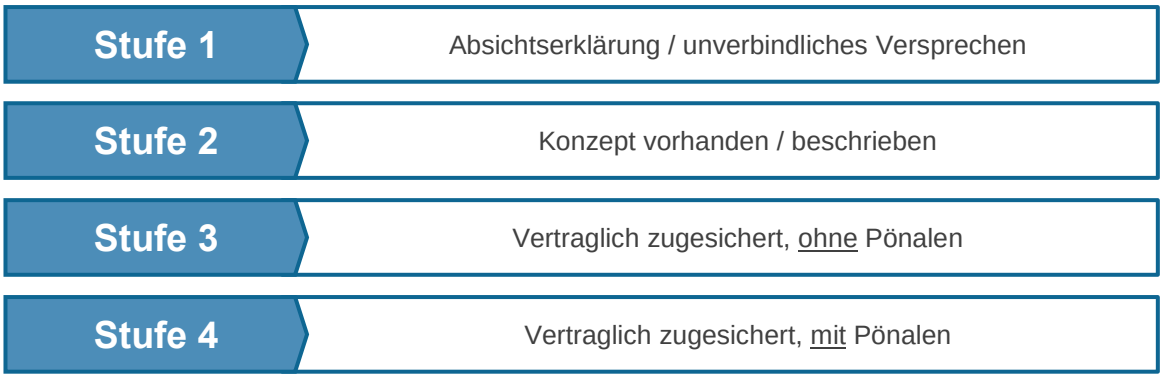
Bei der Verfügbarkeit liegen AWS und Open Telekom Cloud mit bis zu 99,999 % vorne. Das entspricht einer Ausfallzeit für Wartung etc. von ca. 0,09 Stunden pro Jahr. Google Cloud Platform und IONOS Cloud bieten 99,99 % Verfügbarkeit und Microsoft Azure abhängig vom gewählten Service zwischen 99,95 % und 99,99 %. IBM bietet ebenfalls in Abhängigkeit vom gewählten Service eine Verfügbarkeit zwischen 99,5 % und 99,99 % (siehe Kapitel 3.2).

Damit bietet AWS eine deutlich höhere Verfügbarkeit an, als die anderen Hyperscaler.

4.3 Datenschutz und Datensicherheit

Vergleichbar zu den Produktmerkmalen wurden die Angebote bezüglich Datenschutz und Datensicherheit in 4 Stufen zugeteilt (siehe Abbildung 4-3).

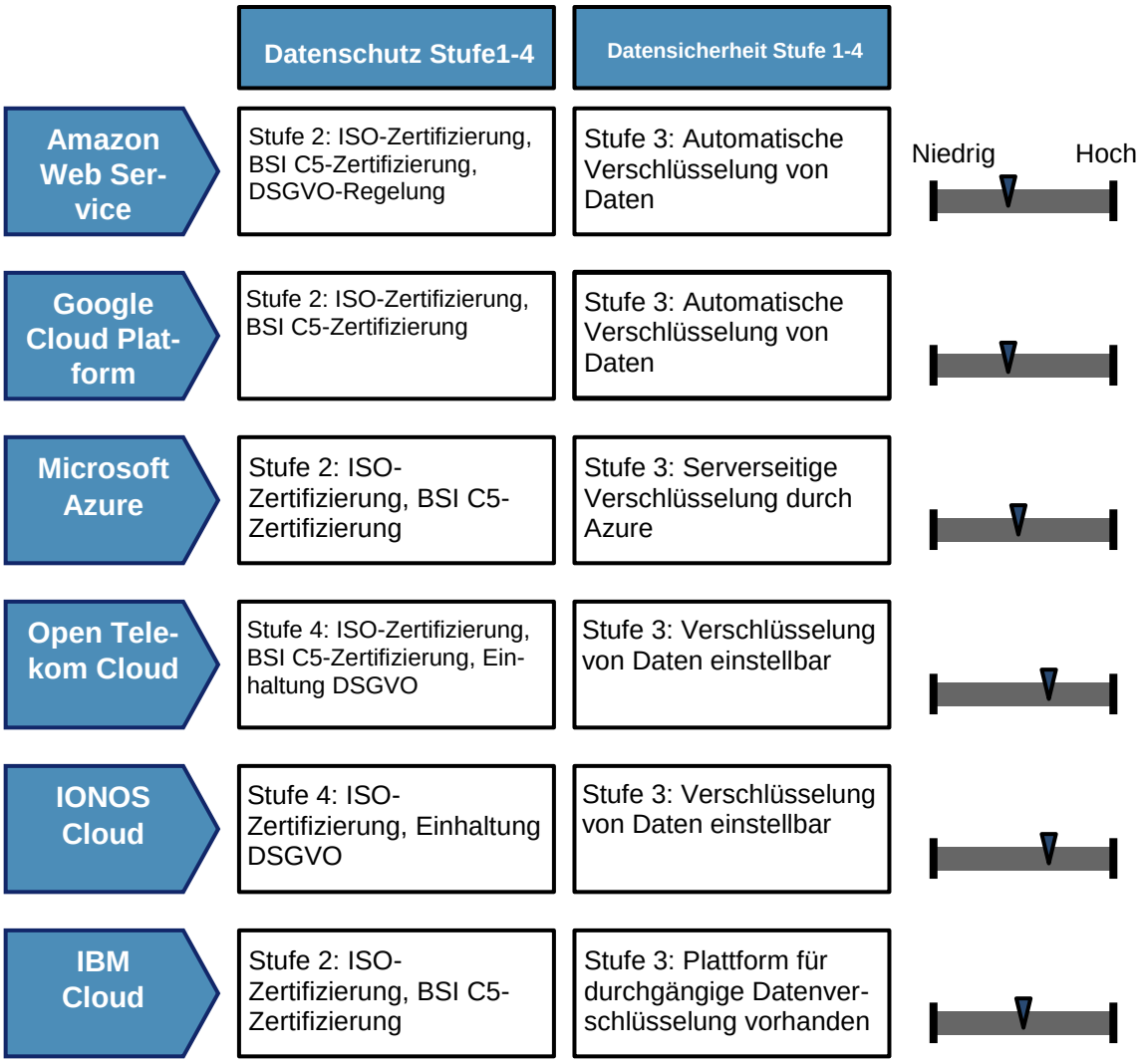
Abbildung 4-3: Einstufung der Marktpositionen anhand dem angebotenen Datenschutz- und Datensicherheitsniveau



Quelle: WIK-Consult.

Gemäß der Anbieterdarstellung in Kapitel 4 ergibt sich folgendes Bild in der vergleichenden Analyse (siehe Abbildung 4-4).

Abbildung 4-4: Marktpositionierung der Cloud-Anbieter bei Datenschutz und Datensicherheit



Quelle: WIK-Consult.

Die Sicherheit der Services lässt sich anhand der relevanten Zertifizierungen und der Verschlüsselung beurteilen. Mit der BSI C5-Zertifizierung hat das Bundesamt für Sicherheit in der Informationstechnik Kriterien zusammengestellt, anhand derer bestimmte Mindeststandards für Cloud-Anwendungen geprüft und testiert werden können.[33] Die Analyse der Anbieterinformationen und AGBs zeigt, dass alle Anbieter über mehrere ISO Zertifizierungen, insbesondere über die ISO/IEC 27001, die die Anforderungen an ein Informationssicherheits-Managementsystem spezifiziert verfügen. Alle betrachteten Anbieter bis auf IONOS Cloud werben mit der BSI C5-Zertifizierung.

33 Vgl. BSI (2020), S.11.

Eine entscheidende Frage stellt sich bei der Umsetzung bzw. Einhaltung der Zusagen der Anbieter. Alle US-amerikanischen Unternehmen unterliegen dem CLOUD Act, dem zufolge sie bei ihnen gespeicherte Daten den US-Behörden für Ermittlungszwecke offenlegen müssen. Das gilt unabhängig vom Eigentum an den Daten und von deren Speicherort bzw. Server-Standort. Demnach haben Open Telekom Cloud und IONOS Cloud einen deutlichen Vorteil beim Datenschutz, da sie den europäischen Datenschutzrichtlinien, insbesondere der DSGVO unterliegen.

Eine standardmäßige Verschlüsselung der Daten wird jedoch von den europäischen Anbietern nicht angeboten, diese muss entweder vom Kunden selbst vorgenommen werden oder zusätzlich nachgefragt werden.

4.4 Interoperabilität und Multi-Cloud

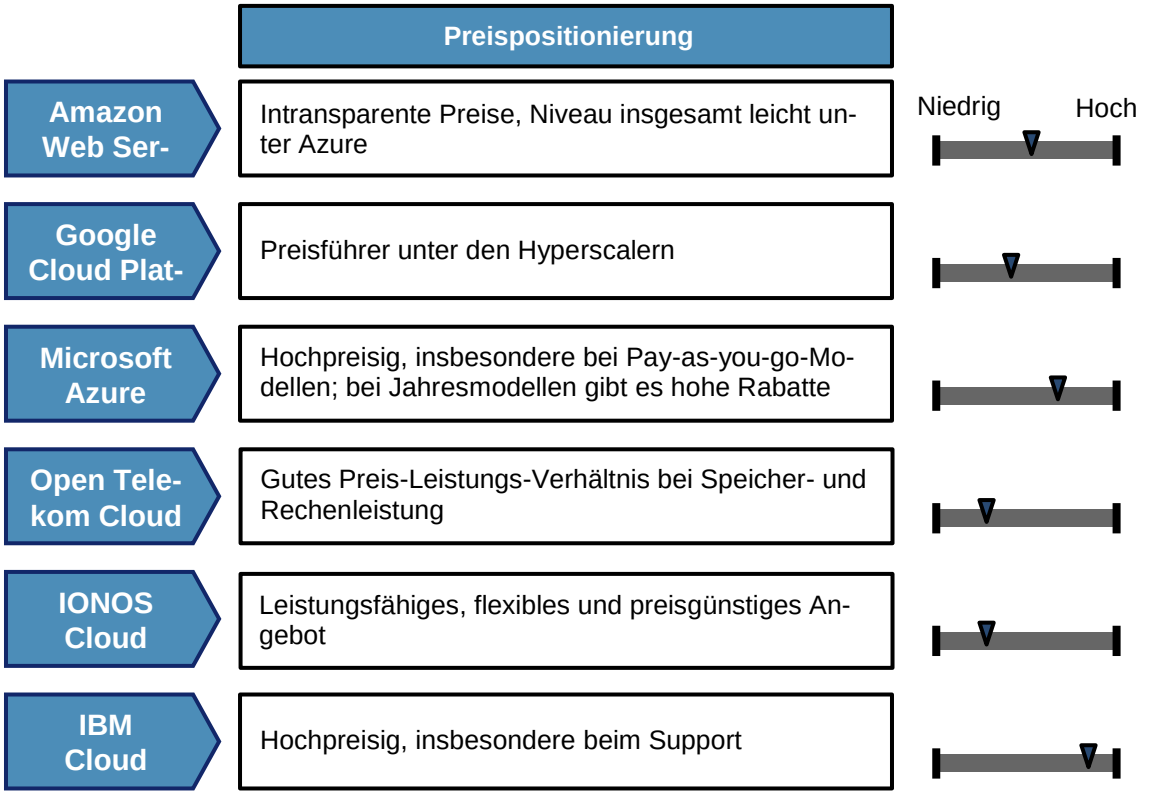
Die Hyperscaler stellen jeweils eigene Plattformen zur Organisation von Multi-Cloud-Lösungen zur Verfügung. IBM, Open Telekom Cloud und IONOS Cloud vermarkten Hybrid- und Multi-Cloud-Lösungen in Kombination direkt mit einem oder mehreren der Hyperscaler. Dies zeigt den steigenden Trend zur Interoperabilität und zu offenen Cloud-Ökosystemen und reduziert Lock-in-Effekte.

In diesem Zusammenhang könnte Gaia-X eine bedeutende Rolle in den kommenden Jahren spielen. Eine Analyse dazu ist in Kapitel 5 beschrieben.

4.5 Preispositionierung

Die Preissetzung bei Cloud-Services ist aufgrund der Vielzahl an Services, unterschiedlichen Bezahlmodellen und Support-Optionen oft intransparent. Die Desktop-Recherche in Kapitel 4 ergab im Vergleich folgendes Gesamtbild (siehe Abbildung 4-5).

Abbildung 4-5: Marktpositionierung der Cloud-Anbieter bei den Preisen



Quelle: WIK-Consult.

Die Recherche für diese Studie zeigt, dass die Preisgestaltung bei allen Hyperscalern komplex und intransparent ist. Im Durchschnitt ist Microsoft Azure der teuerste der drei, Google Cloud Platform mit Abstand der günstigste. AWS liegt leicht unter dem Preisniveau von Azure. Es gibt jedoch starke Schwankungen abhängig vom Individualisierungsgrad der Leistung, Pay-as-you-go oder Abo-Modellen und Inanspruchnahme von Support-Leistungen.

AWS belegt in einer Benchmark-Studie, die das Analystenhaus Cloud Mercato im Jahr 2020 im Auftrag von T-Systems durchgeführt hat, Platz zwei im Preis-Leistungs-Ranking nach der Open Telekom Cloud.[34] In dieser Studie wurde das Preis-Leistungsverhältnis der IaaS-Angebote Rechenleistung und Datenspeicherung der Anbieter AWS, Microsoft Azure, Google Cloud Platform und Open Telekom Cloud verglichen. Aufgrund der Vielzahl von Anwendungen und Preismodellen wurden jeweils zwei Angebote aus den Bereichen Rechenleistung und Datenspeicherung mit je einem Pay-as-you-go-Verbrauchsmodell und einer jährlichen Abrechnung in den Vergleich einbezogen.

34 Vgl. hier und im Folgenden Cloud Mercato (2020).

Die CPU-Leistung, also die Rechenleistung, wurde über die Software Geekbench 5 gemessen, die verschiedene Workloads über die jeweilige Cloud ausführte. Dabei waren die Dienste der Open Telekom Cloud am leistungsfähigsten, gefolgt von AWS. Azure und Google Cloud Platform sind danach ungefähr gleich auf. Die Bewertung der Rechenleistung über die Software ist allerdings nicht nachvollziehbar oder rekonstruierbar. Daher ist ein Bias zugunsten des Auftraggebers der Studie nicht auszuschließen.

Beim Preis-Leistungs-Verhältnis siegt der Studie nach ebenfalls die Open Telekom Cloud. Beim Pay-as-you-go-Verbrauchsmodell mit stündlicher Abrechnung folgt darauf Google, gefolgt von AWS. Bei der jährlichen Abrechnung wird AWS das zweitbeste Preis-Leistungs-Verhältnis nach der Open Telekom Cloud attestiert.

In einer Studie zu KI as a Service von WIK im Jahr 2020 wurden die Preise für KI-Applikationen untersucht. Dabei war die Schlussfolgerung, dass die Hyperscaler ihre Marktmacht durch große Finanzkraft und hohe Investitionen in Infrastruktur und Produktentwicklung leicht in andere Marktsegmente übertragen können. Die technischen Möglichkeiten selbst sind dabei weniger ausschlaggebend für ihre Marktdominanz. Vielmehr sind es die einfache Implementierung (Usability) und das Ökosystem inklusive Vertriebsnetz, die zu hohen Marktanteilen, insbesondere bei AWS und Microsoft Azure führen.[35] Daneben ergaben die für diese Studie geführten Expertengespräche[36] dass Meldungen über hohe Investitionen der Cloud-Anbieter von den Kunden mit steigendem Vertrauen in Infrastruktur und Angebotsqualität honoriert werden. Das fördert auch die Markenbildung.

Insgesamt ist somit festzustellen, dass das Preisniveau kein ausschlaggebendes Kriterium für den Nutzer bei der Wahl der Anbieter ist.

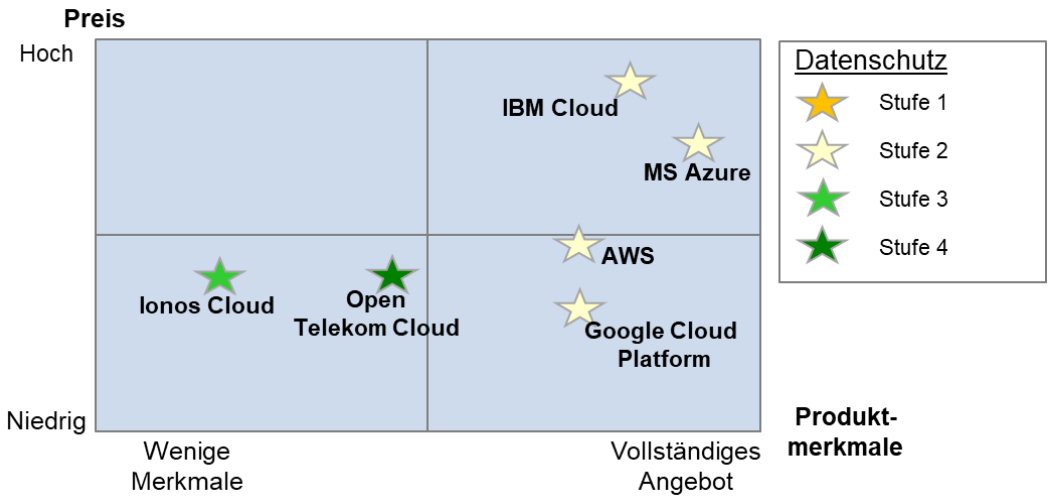
4.6 Anbieter-Preis-Leistungsmatrix und Zusammenfassung der Merkmale

Die folgende Anbieter-Preis-Leistungsmatrix fasst die Ergebnisse für die betrachteten Cloud-Anbieter nach der Einstufung in Bezug auf Produktmerkmale, Datenschutz und Datensicherheit sowie Preise zusammen.

35 Vgl. Gull et al. (2020), S 44 f.

36 Vertreter von Verbänden und Ansprechpartner aus wissenschaftlichen Institutionen, die im Beriech Wissenstransfer aktiv sind.

Abbildung 4-6: Preis-Produkt-Matrix



Quelle: WIK-Consult.

Die Untersuchung der AGBs, Leistungsbeschreibungen und Produktinformationen der betrachteten Anbieter zeigen, dass sich die Anbieter nur in wenigen Produktmerkmalen unterscheiden. Vielmehr liegen die Unterschiede in den angebotenen Services, Usability und Verfügbarkeit, während Preise nur eine begrenzte Auswirkung auf die Marktstruktur haben.

Die US-amerikanischen Anbieter bieten ein deutlich größeres Service-Angebot als IONOS Cloud und Open Telekom Cloud an. Unter den US-amerikanischen Anbietern positionieren sich IBM und Microsoft mit einer großen Anzahl an angebotenen Software-Applikationen während AWS zusätzlich mit einer höheren Verfügbarkeit punktet. Dennoch, die meisten Nutzer benutzen nur einen Bruchteil der Services, die die Hyperscaler anbieten. Ebenso stellen sich die deutschen Anbieter dem Wettbewerb mit günstigeren Preisen und besseren Datenschutzbestimmungen bzw. einer gewissen Rechtssicherheit besonders beim Speichern personenbezogener Daten.

Die Analyse ergibt außerdem, dass besonders der preisgünstige Hyperscaler Google Cloud Platform sowie Open Telekom Cloud derzeit Verluste im Cloud-Geschäft verbuchen müssen, während AWS und Microsoft sehr hohe Renditen erzielen.

Mögliche Erklärungen dafür sind, dass vor allem AWS als Marktführer über Skalenerträge und Kostenführerschaft, ein starkes Marketing- und Vertriebssystem verfügt, die Migrationskosten in die Cloud geringer sind als bei anderen Anbietern oder die Nutzer dazu tendieren, den Marktführer zu wählen. Dies kann wiederum auf zwei Überlegungen zurückzuführen sein. Zunächst sind die Leistungen und Preise relativ komplex, sodass viele Nutzer selbst keine fundierte Entscheidung treffen können. Daher könnten sie auf die

Entscheidung, die andere Nutzer bereits gefällt haben, vertrauen und ihnen zum Marktführer folgen. Es ist auch davon auszugehen, dass die Integratoren und IT-Dienstleister solche Cloud-Anbieter empfehlen, die sie schon kennen, um zusätzlichen Aufwand für die Einarbeitung in die Cloud-Angebote zu vermeiden. Des Weiteren ist eine Cloud-Strategie für ein Unternehmen aufgrund der hohen Migrationskosten eine langfristige Investition, für die möglichst ein Partner gewählt wird, der eine starke Marktposition innehat und damit die Wahrscheinlichkeit, dass dieser langfristig am Markt besteht, hoch ist, was ebenso unter „Vertrauen“ gefasst werden kann.

Aus den Erhebungen und Analyse leiten wir folgende Thesen ab:

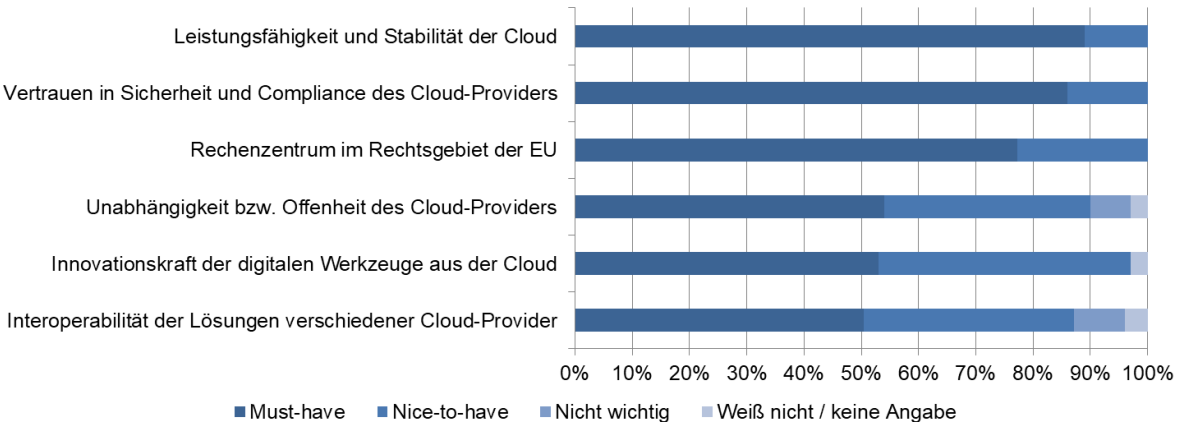
These 1: Die angebotene Software und dessen Usability bzw. User Experience sowie gefühltes Performance und nicht die Produktmerkmale (wie z. B. Datenschutz. Datensicherheit) sind für den Großteil der Cloud-Nutzer entscheidend bei der Anbieterauswahl.

These 2: Vertrauen ist aufgrund der Migrationskosten und der Komplexität ein entscheidendes Kriterium bei der Anbieterauswahl. Nutzer tendieren dazu, den Marktführer zu wählen.

These 3: Eine gute Usability ist ein entscheidender Wettbewerbsvorteil bei der Gewinnung von Nutzern.

Ergebnisse einer Befragung auf dem Jahr 2020 von 540 Unternehmen in Deutschland, die Cloud-Lösungen nutzen, ihren Einsatz planen oder diskutieren spiegeln diese drei Thesen deutlich wider (siehe Abbildung 4-7). Hierbei sei anzumerken, dass alle im Detail betrachteten Cloud-Anbieter mehrere Rechenzentren in Europa unterhalten.

Abbildung 4-7: Wie wichtig sind die folgenden Kriterien bei der Auswahl eines Cloud-Anbieters



Quelle: Bitkom Research (2021) via Statista. Basis: Unternehmen in Deutschland, die Cloud-Lösungen nutzen, planen oder diskutieren, n=540. Befragungszeitraum: 2020.

5 Potenzielle Wettbewerbsvorteile europäischer Anbieter und Marktverschiebungen durch Gaia-X

Dieses Kapitel gibt einen Überblick über den aktuellen Stand von Gaia-X und mögliche Auswirkungen auf den Cloud-Markt und die Hyperscaler sowie die digitale Souveränität der Nutzer von Cloud-Anwendungen, insbesondere KMU.

5.1 Hintergründe von Gaia-X

Mit Gaia-X kann in Europa ein neues Cloud-Ökosystem mit bestimmten Qualitätskriterien entstehen. Davon können Impulse für neue Wettbewerbsbedingungen ausgehen. Es besteht das Potential, die Wettbewerbsstrukturen und Differenzierungsmerkmale im Markt für cloudbasierte Anwendungen zu verändern. Dabei stellt sich die Frage, zu welchem Verhalten die Ankündigung des Projektes Gaia-X bei den Cloud-Anbietern – mit Fokus auf die Hyperscaler – geführt hat und wie sich diese gegenüber dem Projekt positionieren bzw. daran anpassen.

Gaia-X soll eine europäische Dateninfrastruktur schaffen, die die digitale Souveränität der EU-Mitgliedstaaten und der ansässigen Unternehmen schützt und Innovationen fördert. Dafür wird ein Ökosystem aus bestehenden Server-Strukturen geschaffen, innerhalb dessen die Nutzer entscheiden, wo ihre Daten gespeichert werden, und diese frei transferieren können (Portabilität). Die dezentralen Recheninfrastrukturen der Gaia-X Mitglieder soll interoperabel verbunden, über eine gemeinsame Benutzeroberfläche zugänglich gemacht und einheitlichen Open-Source-Standards und Benutzerregeln unterworfen werden. Infrastrukturdienste müssen dabei bestimmte Voraussetzungen bezüglich Datenschutz und Interoperabilität erfüllen und gegebenenfalls sich zertifizieren lassen, um Teil der Dateninfrastruktur zu werden.[37]

Das Gaia-X-Ökosystem besteht aus zwei wesentlichen Grundbestandteilen: dem Datenökosystem und dem Infrastrukturökosystem. Das Datenökosystem stellt Datenräume bereit, die auf gemeinsamen Regeln basieren. Das Infrastruktur-Ökosystem stellt die Infrastruktur von verschiedenen Anbietern zur Verfügung. In diesem Ökosystem soll es den KMU möglich sein, zwischen verschiedenen Anbietern zu wechseln oder auch Multi-Cloud-Lösungen zu implementieren.

Zusätzlich ermöglicht und fördert Gaia-X sogenannte föderierte Dienste. Dies sind festgelegte Regeln die es Teilnehmern erlaubt, in sicheren Datenräumen einen kontrollierten Daten- und Dienste-Austausch stattfinden zu lassen.[38]

Ein Grund für den Aufbau einer europäischen Dateninfrastruktur bezieht sich auf die potenzielle Abhängigkeit von Anbietern außerhalb der EU, insbesondere aus den USA, und

37 Vgl. Gaia-X (2021b).
38 Vgl. Gaia-X (2021b).

die potenzielle Verletzung des Datenschutzes bei der Speicherung von Daten bei in den USA ansässigen Anbietern aufgrund des US CLOUD Act.[39]

Für europäische Cloud-Anbieter bietet Gaia-X die Möglichkeit, innerhalb eines offenen Ökosystems Gesamtlösung in Kooperation mit anderen Akteuren anzubieten und über diesen Weg Verbundvorteile und Skalenerträge zu realisieren, die bisher als großer Wettbewerbsvorteil den Hyperscalern vorbehalten waren. Durch die Interoperabilität auf der Infrastrukturebene sollen nun auch kleinere Anbieter die Möglichkeit erhalten, den Nutzenden die Flexibilität bezüglich Kapazitäten bei Speicher- und Rechenleistung anzubieten, die diese sonst nur bei großen Anbietern bekommen würden.

Die große öffentliche Aufmerksamkeit, die das Projekt erhält, sensibilisiert darüber hinaus zusätzlich für die Themen Datensouveränität und Datensicherheit, die möglicherweise für die Wahl eines europäischen Anbieters sprechen könnten. Diese Aspekte haben großen Einfluss auf die digitale Souveränität der Nutzenden und werden in Abschnitt 5.3 tiefergehend betrachtet.

Die Transparenz der Leistungsbeschreibung durch einen Angebotskatalog, in dem alle Leistungen aller Anbieter über Gaia-X verzeichnet sind, ist ein weiterer Vorteil, der eine Marktverschiebung von den Hyperscalern hin zu Gaia-X-Services oder die generelle Ausweitung der Nutzung von Cloud-Services bei Unternehmen, die bisher solche noch nicht nutzen, begünstigen könnte.

Die Standardisierung, die mit Gaia-X einhergeht, erleichtert die digitale Transformation der Unternehmen bei der unternehmensübergreifenden Vernetzung. Gerade der Austausch von Daten über Unternehmensgrenzen hinweg erfordert eine multilaterale Zusammenarbeit, die nur durch eine Standardisierung und einen einheitlichen Zugang der Beteiligten zu den relevanten Daten möglich wird. Gerade hier kann Gaia-X die KMU mit vorhandenen Datenräumen unterstützen.

These 4: Die Interoperabilität, die durch GAIA X geschaffen wird, ermöglicht es kleineren Cloud-Anbietern, im Verbund mit der flexiblen Kapazitätsbereitstellung der Hyperscaler zu konkurrieren.

These 5: Die Transparenz in Bezug auf Datenverarbeitung und -Speicherung, die durch Gaia-X geschaffen wird, erhöht die digitale Souveränität der Nutzer.

These 6: Gaia-X schafft größeres Vertrauen in Cloud-Anwendungen und führt damit insgesamt zu einer höheren Nutzungsrate von Cloud-Services.

39 Vgl. hier und im Folgenden Baischew et al. (2020).

5.2 Aktivitäten der Hyperscaler im Zusammenhang mit Gaia-X

Zu den 22 europäischen Gründungsunternehmen der Gaia-X AISBL wurden 212 weitere Mitglieder im März 2021 aufgenommen, darunter die Hyperscaler AWS, Microsoft, Google und Alibaba.[40] Auch Oracle und Salesforce, die weltweit nennenswerte Marktanteile im SaaS-Segment haben (4,0 % bzw. 9,3 %)[41], sind Mitglieder.

Als Gründe für das Engagement gab AWS die Gewährleistung eines Höchstmaßes an Sicherheit und Datenschutz, die Achtung der Datenhoheit und der Zugang zu weltweit führender Technologie an.[42] Auch Microsoft gab als Beweggrund an, die Werte und die Vision von Gaia-X zu teilen und diese Wachstumschance für Europa unterstützen zu wollen.[43]

Daneben ist für die Hyperscaler die strategische Positionierung am wichtigen europäischen Wachstumsmarkt von Bedeutung. Der europäische Markt für IaaS und PaaS umfasst bereits ca. 13,9 Mrd. Euro[44] und wird in den nächsten Jahren weiterhin um über 20 % pro Jahr wachsen.[45] Dieses Wachstum könnte im B2B-Bereich durch die Souveränitätsvorteile, die Gaia-X für nutzende Unternehmen bringen soll, noch angeheizt werden. Denn durch Mindeststandards, Transparenz durch Labelling[46] und Interoperabilität könnten aktuelle Hemmnisse für Unternehmen, Cloud-Anwendungen zu nutzen, wie Datenschutzbedenken und die Angst vor Abhängigkeit von einem Anbieter, weiter abgebaut werden. Laut den für diese Studie geführten Expertengesprächen mit Verbänden die sich mit Gaia-X beschäftigen ist die Gewinnung von öffentlichen Verwaltungen als Nutzer ein gewichtiger Grund für die Hyperscaler, sich an Gaia-X zu beteiligen. In jedem Fall gilt es, durch eine Beteiligung an Gaia-X weiterhin am Marktwachstum teilzuhaben.

These 7: Für die Hyperscaler liegt das Interesse an Gaia-X im Wesentlichen in der Partizipation am europäischen Wachstumsmarkt.

5.3 Gaia-X und digitale Souveränität

Die Aufnahme der Hyperscaler aus den USA und China stößt teilweise auf Kritik, weil die Gaia-X-Initiative ursprünglich gerade wegen deren Marktmacht und den unterschiedlichen (nationalen) Datenschutzbestimmungen ins Leben gerufen wurde.[47] Kritiker befürchten, dass die datenbezogenen Mindeststandards, die derzeit noch in Verhandlung

40 Vgl. Gaia-X (2021a).
41 Vgl. Statista (2021b).
42 Vgl. AWS (2021).
43 Vgl. Microsoft (2020a).
44 Vgl. Synergy Research Group (2021b).
45 Vgl. Statista Technology Market Outlook (2021).
46 Siehe Gaia-X (2021c), S. 4.
47 Vgl. Germany Trade and Invest (2021).

sind, durch eine hohe Zahl an nicht europäischen Unternehmen[48], die an ihrem Hauptsitz z. B. anderen Datenschutzbestimmungen unterliegen, abgesenkt werden könnte.[49]

Aktuell ist die Situation bei US-amerikanischen Hyperscalern so, dass sie von US-(Strafverfolgungs-)Behörden auf der Grundlage des US CLOUD Acts dazu aufgefordert werden können, alle Daten und Informationen zu Kunden herauszugeben, die sich im Besitz, Gewahrsam oder unter ihrer Kontrolle befinden. Dies gilt unabhängig davon, ob es sich um personenbezogene Daten handelt und wo sich die Daten befinden, innerhalb oder außerhalb der Vereinigten Staaten (18 U.S.C. § 2713). Diese Verpflichtung steht in direktem Widerspruch zu den Grundsätzen und Anforderungen der europäischen DSGVO, weshalb auch die Verarbeitung von personenbezogenen Daten durch US-amerikanische Cloud-Anbieter mit Server-Standort in Europa wegen einer möglichen Datenübermittlung in die USA als problematisch gilt.[50] Bei Gaia-X ist geplant, diese Unterschiede durch abgestufte Labels zu berücksichtigen, in denen Konformitätskriterien zu Datensicherheit, Transparenz, Sicherheit, Portabilität und Flexibilität festgelegt werden.[51]

In Anbetracht dessen hält Amazon Web Service zwar einen Zusatz zur Datenverarbeitung vor, der besagt, dass AWS Dritten keinen Zugang zu den Nutzerdaten gewährt und falls notwendig, lediglich die Kontaktdaten des Nutzers weitergibt, damit diese die Daten direkt beim Kunden anfragen können.[52] Allerdings wird auch dieses Vorgehen den datenschutzrechtlichen Anforderungen aus der DSGVO nicht gerecht. Die Klausel entspricht bislang nicht den Standarddatenschutzklauseln (SCC) der EU-Kommission, die die Übertragung der Daten in Drittstaaten legitimieren könnten. Vorerst bleibt es dabei, dass es der US CLOUD Act den US-amerikanischen Ermittlungsbehörden ermöglicht, auf Daten zuzugreifen, die bei europäischen Tochterunternehmen US-amerikanischer Firmen oder auf Servern außerhalb der USA – etwa bei AWS – gespeichert sind. Insofern fehlt Unternehmen, die der DSGVO unterliegen, derzeit die rechtliche Grundlage für die

48 Siehe https://www.gaia-x.eu/members, zuletzt abgerufen am 11.02.2022.

49 Vgl. BMWK Pressemitteilung 15.09.2020 Bundesminister Altmaier zur Gründung der GAIA-X AISBL, online abrufbar unter https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2020/09/20200915-zitat-altmaier-zur-gruendung-der-gaia-x-aisbl.html, zuletzt abgerufen am 11.02.2022 und, z.B. Interview mit Yann Lechelle, CEO des Cloud Anbieters Scaleway, Gründungsmitglied aus Frankreich in Heise Magazin c't 1/2022 S.14, online abrufbar unter https://www.heise.de/select/ct/2022/1/2132816474156642787, zuletzt abgerufen am 11.02.2022.

50 EuGH Urt. v. 16.7.2020 – C 311/18, in: NJW 2020, 2613.

51 Siehe Gaia-X (2021c), S. 4.

52 Vgl. AWS-DSGVO-Zusatz zur Datenverarbeitung: Confidentiality of Customer Data. AWS will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends AWS a demand for Customer Data, AWS will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, AWS may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then AWS will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless AWS is legally prohibited from doing so.

Speicherung personenbezogener Daten bei US-amerikanischen Cloud-Anbietern wie AWS[53] was zugleich das Bedürfnis nach einer rein europäischen Lösung erhöht.

These 8: Gaia-X kann durch Labels Transparenz in Bezug auf den Datenschutz schaffen.

5.4 Gaia-X und KMU

Durch die Förderbekanntmachung „Innovative und praxisnahe Anwendungen und Datenräume im digitalen Ökosystem Gaia-X“ des BMWi von Februar 2021 werden Projekte gefördert, die den technologischen Bedarf und den ökonomischen Nutzen von Gaia-X verdeutlichen. Die 11 Projekte nutzen und entwickeln datenbasierte Business-Lösungen, wie neue Geschäftsmodelle oder Datenräume, die Interoperabilität und Portabilität von Daten ermöglichen.[54] Damit geht der inhaltliche Umfang dieser Projekte über IaaS und PaaS hinaus. Insbesondere unternehmensübergreifender Datenaustausch und -auswertung sollen mit diesen Use Cases erprobt und deren Nutzen für KMU verdeutlicht werden. Ein besonderer Fokus bei der Auswahl der Projekte liegt außerdem bei der Beteiligung von Start-ups und KMUs.

Die Schaffung von Datenräumen wird dadurch optimiert, dass vom Dateninhaber konfigurierbar ist, wer welche Daten über welche Infrastruktur wie nutzen darf. Somit können die Dateneigentümer besser überschauen, was mit ihren Daten passiert und wie sie die Hoheit über ihre Daten behalten können.

Dieser Aspekt kann dann über die potenzielle Erhöhung der Nutzung von IaaS und PaaS hinaus auch Kooperationen zu Data-Sharing und Data-Pooling zwischen KMU fördern. Diese Stärkung der Datenverfügbarkeit für KMU könnte wiederum als Enabler für die Einführung von Anwendungen mit Künstlicher Intelligenz in KMU fungieren.

Insgesamt verschaffen die Interoperabilität der Leistungen und die Vereinfachung der Portabilität der Daten von einem Anbieter zu einem andern den Nutzern einen höheren Autonomiegrad gegenüber Cloud-Anbietern. Dies kommt insbesondere KMU zugute, für die der Migrationsaufwand eine große Hürde bei der Implementierung von Cloud-Anwendungen darstellt, und deren Abhängigkeit vom einmal gewählten Anbieter damit relativ hoch ist.

53 Vgl. KPMG (2021).
54 Vgl. Bundesnetzagentur (2021).

6 Schlussfolgerungen

Grundlegend ist die Struktur des europäischen Marktes von IaaS und PaaS noch konzentrierter als die des globalen Marktes. AWS kommt auf einen Marktanteil von über 50 %, die asiatischen Anbieter spielen nur eine untergeordnete Rolle. Die nationalen Anbieter kommen auf dem Heimatmarkt jeweils auf einen Marktanteil im einstelligen Bereich.

Die vertraglich geregelten Differenzierungsmerkmale wie Datenschutz, Datensicherheit, vertraglich zugesicherte Performance/Qualität und Preise erklären für den Regelfall nicht den großen Marktanteil von AWS (mit Ausnahme der angebotenen Verfügbarkeit). Die Merkmale der Anzahl zusätzlichen Applikationen, Interoperabilität und Cybersicherheit bieten für den Nutzer der klassischen Cloud-Dienste keinen nennenswerten Vorteil bei AWS gegenüber den anderen Anbietern. Für Unternehmenskunden, die bereits Microsoft-Produkte nutzen, würde es bezüglich des Kriteriums „Applikationen“ sogar näherliegen, Azure als Cloud-Dienst zu nutzen. Bezüglich des Preises liegt AWS gemeinsam mit Microsoft Azure und IBM Cloud im höherpreisigen Segment und bezüglich des Datenschutzes, sind US-amerikanische Unternehmen ohnehin im Nachteil gegenüber europäischen Anbietern. Einzig die hohe Verfügbarkeit von 99,999 % ist ein deutlicher Wettbewerbsvorteil von AWS, den allerdings auch die Open Telekom Cloud bietet.

Dies legt die Überlegungen nahe, dass die Anbieterentscheidung von anderen Kriterien abhängt, wie einer besseren Usability und User Experience, der tatsächlichen (und nicht vertraglich zugesicherten Performance/Qualität), einem starken Marketing- und Vertriebssystem, den Migrationskosten, Vertrauen sowie Interoperabilität innerhalb der Wertschöpfungskette, die dazu führt, dass anderen Nutzern zum Marktführer gefolgt wird, da selbst keine fundierte Entscheidung getroffen werden kann.

Insbesondere beim Marketing- und Vertriebssystem ist es bemerkenswert, dass T-Systems (Deutsche Telekom) schwerpunktmäßig die Services der Hyperscaler vertreibt, anstatt ausschließlich die hauseigene Lösung anzubieten.

Vorteile der deutschen Anbieter, wie Open Telekom Cloud oder IONOS Cloud, sind hingegen die Möglichkeit zur Einhaltung der europäischen Datenschutzbestimmungen, und ein regionales Support- und Vertriebsnetz. Auf diesen Wettbewerbsvorteilen könnte insbesondere am heimischen Markt aufgesetzt werden, obgleich hohe Marktanteile dort auch nicht erzielt werden.

Im Zuge von Gaia-X werden Veränderungen auf dem Cloud-Markt, insbesondere was die digitale Souveränität angeht, erwartet, da ein höheres Maß an Transparenz und Interoperabilität geschaffen werden soll. Bisher haben sich die Hyperscaler zwar Gaia-X ebenso angeschlossen, in der Hoffnung, den Cloud-Markt in Europa weiter für sich ausbauen zu können.

Der aktuelle Stand von Gaia-X hat derzeit noch nicht das Stadium erreicht, um fundierte Aussagen zum tatsächlichen Einfluss auf den Cloud-Markt treffen zu können. Allerdings ist zu erwarten, dass das höhere Maß an digitaler Souveränität Hemmnisse bei der Cloud-Nutzung abbauen könnte und die Nachfrage nach Cloud-Services bei Unternehmen und insbesondere in der öffentlichen Verwaltung steigen lassen könnte. Mit Gaia-X könnte noch mehr Vertrauen der kleinen und mittleren Unternehmen in die Cloud aufgebaut werden und infolgedessen die Cloud-Nutzung in Deutschland insgesamt steigen.

7 Referenzen

AWS (2021): What's next for Europe's data revolution? AWS joins the Gaia-X initiative, https://aws.amazon.com/de/blogs/publicsector/what-next-europes-data-revolution-aws-joins-gaia-x-initiative/, zuletzt abgerufen am 23.11.2021

AWS-DSGVO-Zusatz zur Datenverarbeitung (2021): https://aws.amazon.com/de/compliance/gdpr-center/, zuletzt abgerufen am 23.11.2021

Back4App (2020): Top Cloud-Anbieter in Europa, https://blog.back4app.com/top-cloud-providers-in-europe/, zuletzt abgerufen am 23.11.2021

Baischew, D., Kroon, P., Lucidi, S. Märkel, C., Sörries, B. (2020): Digital Sovereignty in Europe – a first benchmark, Wik-Consult Report

Bedner, Mark; (Forum Wirtschaftsrecht) Cloud Computing. Technik, Sicherheit und rechtliche Gestaltung, 1.Aufl., Kassel, 2013.

Bitkom Research (2021): Cloud-Monitor 2021 – Eine Studie von Bitkom Research im Auftrag von KPMG, https://www.bitkom-research.de/system/files/document/Bitkom_KPMG_Charts_Cloud%20Monitor%202021_final.pdf, zuletzt abgerufen am 13.01.2022.

Bundesamt für Sicherheit in der Informationstechnik (BSI) (o.J.): Cloud Computing Grundlagen, online in: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/CloudComputing-Grundlagen.html, zuletzt abgerufen am 23.11.2021

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2020): Cloud Computing Compliance Criteria Catalogue – C5:2020 Kriterienkatalog Cloud Computing; Cloud Computing Compliance Criteria Catalogue – C5:2020 – Kriterienkatalog Cloud Computing (bund.de), zuletzt abgerufen am 23.11.2021

Bundesministerium für Wirtschaft und Energie (BMWi) (2021): Schwerpunktstudie Digitale Souveränität – Bestandsaufnahme und Handlungsfelder

Bundesnetzagentur (2021): Förderwettbewerb Gaia-X, https://www.bundesnetzagentur.de/DE/Sachgebiete/Digitalisierung/Foerderwettbewerb_GAIAX/start.html, zuletzt abgerufen am 23.11.2021

Cloudcomputing Insider (2017): Was ist XaaS? „Anything as a Service",https://www.cloudcomputing-insider.de/was-ist-xaas-anything-as-a-service-a-670272/, zuletzt abgerufen am 23.11.2021

Cloud Mercato (2020): Performance & Price/Performance Benchmark of IaaS Providers 2020

EuGH (2020): Urteil vom 16.7.2020, https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=EuGH&Datum=16.07.2020&Aktenzeichen=C-311/18, zuletzt abgerufen am 23.11.2021

EU Kommission (2021): Digital Economy and Society Index (DESI) 2021; https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021

EU Kommission (2021): Index für die digitale Wirtschaft und Gesellschaft (DESI) 2021 Deutschland; https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2021

Fraunhofer (2021): ISST-Report Cloud Transformation.pdf (fraunhofer.de)

Gaia-X (2021a): List of new Members to the Gaia-X AISBL: https://www.data-infrastructure.eu/GAIAX/Redaktion/EN/Downloads/gaia-press-release-march-31-list-en.pdf?__blob=publicationFile&v=3, zuletzt abgerufen am 23.11.2021

Gaia-X (2021b): https://www.gaia-x.eu/, zuletzt abgerufen am 23.11.2021

Gaia-X (2021c): Gaia-X Labelling Framework; https://gaia-x.eu/wp-content/uploads/files/2021-11/Gaia-X%20Labelling%20Framework_0.pdf, zuletzt abgerufen am 23.11.2021.

Gartner (2021): Oress Release: Gartner Says Worldwide IaaS Public Cloud Services Market Grew 40.7% in 2020; https://www.gartner.com/en/newsroom/press-releases/2021-06-28-gartner-says-worldwide-iaas-public-cloud-services-market-grew-40-7-percent-in-2020, zuletzt abgerufen am 23.11.2021

Germany Trade and Invest (2021): Gaia-X will Europas digitale Souveränität stärken, https://www.gtai.de/gtai-de/trade/specials/special/eu/gaia-x-will-europas-digitale-souveraenitaet-staerken-691602, zuletzt abgerufen am 23.11.2021

Gull, I., Schrade-Grytsenke, L., Lundborg, M. (2020): Cloud-Lösungen und KI-as-a-Service – Aktuelle und potenzielle Anwendungsszenarien und Marktentwicklungen, WIK Diskussionsbeitrag Nr.469

Handelsblatt (2021): Europas Cloudanbietern fehlt gegenüber den US-Rivalen der Mut, https://www.handelsblatt.com/meinung/kommentare/kommentar-europas-cloudanbietern-fehlt-gegenueber-den-us-rivalen-der-mut/26962646.html?ticket=ST-3656166-bVXA30oUx7ayTuOKz2TP-ap1, zuletzt abgerufen am 23.11.2021

Haselmann, Till; Hoeren, Thomas; Vossen, Gottfried (2012): Cloud Computing für Unternehmen, dpunkt Verlag GmbH

Intel (2021): Eine Edge-Cloud bringt Sie näher an Ihre Business-Intelligence heran; https://www.intel.de/content/www/de/de/edge-computing/edge-cloud.html, zuletzt abgerufen am 23.11.2021

Kinsta (2021): Cloud Marktanteil – ein Blick auf das Cloud-Ökosystem im Jahr 2021; https://kinsta.com/de/blog/cloud-marktanteil/, zuletzt abgerufen am 23.11.2021

KPMG (2021): The European Cloud Market: Key challenges for Europe and five scenarios with major impacts by 2027-2030.

Microsoft (2020): Was ist SaaS? https://azure.microsoft.com/de-de/overview/what-is-saas, zuletzt abgerufen am 23.11.2021

Microsoft (2020a): Microsoft announced as a member of Gaia-X, https://blogs.microsoft.com/eupolicy/2020/11/26/microsoft-announced-as-a-member-of-gaia-x/, zuletzt abgerufen am 23.11.2021

Netapp.com (2021): Google Cloud vs AWS: Comparing Price and Capabilities. https://cloud.netapp.com/blog/google-cloud-vs-aws-comparing-price-and-capabilities, zuletzt abgerufen am 23.11.2021.

Procloud (2021): Vergleich der Hyperscaler – Microsoft Azure vs Amazon AWS vs Google GCP. https://www.procloud.ch/vergleich-der-hyperscaler-microsoft-azure-vs-amazon-aws-vs-google-gcp/, zuletzt abgerufen am 23.11.2021.

Red Hat (2021): Was ist eine Multi-Cloud? https://www.redhat.com/de/topics/cloud-computing/what-is-multicloud, zuletzt abgerufen am 23.11.2021

Statista (2021a): Technology Market Outlook 2021; https://www.statista.com/outlook/tmo/public-cloud/worldwide?currency=EUR#global-comparison, Stand Oktober 2021, zuletzt abgerufen am 23.11.2021

Statista (2021b): Marktanteile der führenden Unternehmen am Umsatz mit Software-as-a-Service (SaaS) weltweit im Jahr 2020, https://de.statista.com/statistik/daten/studie/817910/umfrage/marktanteile-am-umsatz-mit-software-as-a-service-weltweit/, zuletzt abgerufen am 23.11.2021

Synergy Research Group (2020a): Amazon & Microsoft Lead the Cloud Market in all Major European Countries, https://www.srgresearch.com/articles/amazon-microsoft-lead-cloud-market-all-major-european-countries, zuletzt abgegerufen am 02.02.2022.

Synergy Research Group (2020b): SaaS Spending Hits $100 billion Annual Run Rate; Microsoft Extends its Leadership, https://www.srgresearch.com/articles/saas-spending-hits-100-billion-annual-run-rate-microsoft-extends-its-leadership, zuletzt abgerufen am 13.11.2021

Synergy Research Group (2021a): Quarterly Cloud Market Leaps to $42B – Amazon, Microsoft & Google Pocket 63% of Dollars Spent; https://www.srgresearch.com/articles/quarterly-cloud-market-leaps-to-42b-amazon-microsoft-google-pocket-63-of-dollars-spent, zuletzt abgerufen am 02.02.2022

Synergy Research Group (2021b): European Cloud Providers Double in Size but Lose Market Share; https://www.srgresearch.com/articles/european-cloud-providers-double-in-size-but-lose-market-share, zuletzt abgerufen am 13.11.2021

US-CLOUD Act (2018): https://www.congress.gov/bill/115th-congress/house-bill/4943, zuletzt abgerufen am 13.11.2021

WIK-Consult • Bericht

Studie für die Bundesnetzagentur

Strategische Bedeutung von Cloud-Diensten für die digitale Souveränität von KMU

Teil 2 – Digitale Souveränität und Cloud-Dienste (Az: 2021/008/Z25-3)

Autoren:

Dajan Baischew
Martin Lundborg
Christian Märkel
Dr. Marie-Christin Papen

Prof. Dr. Dagmar Gesmann-Nuissl
(Professorin an der TU Chemnitz)

Bad Honnef, August 2022

WIK CONSULT

Impressum

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Deutschland
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
E-Mail: info@wik-consult.com
www.wik-consult.com

Vertretungs- und zeichnungsberechtigte Personen

Geschäftsführerin	Dr. Cara Schwarz-Schilling
Direktor	Alex Kalevi Dieke
Direktor Abteilungsleiter Netze und Kosten	Dr. Thomas Plückebaum
Direktor Abteilungsleiter Regulierung und Wettbewerb	Dr. Bernd Sörries
Leiter der Verwaltung	Karl-Hubert Strüver
Vorsitzender des Aufsichtsrates	Dr. Thomas Solbach
Handelsregister	Amtsgericht Siegburg, HRB 7043
Steuer-Nr.	222/5751/0926
Umsatzsteueridentifikations-Nr.	DE 329 763 261

Inhaltsverzeichnis

Abbildungen

Tabellen

Zusammenfassung

Das Ziel dieser Studie ist es, die Auswirkungen auf die digitale Souveränität von KMU (kleinen und mittleren Unternehmen) im Zusammenhang mit der Nutzung von Cloud-Diensten, die insbesondere von international tätigen Hyperscalern angeboten werden, aufzuzeigen. Dieser Bericht ist der zweite Teilbericht von insgesamt drei Berichten und beleuchtet das Thema digitale Souveränität mit Fokus darauf, was unter dem Begriff verstanden wird, wie sich der Datenschutz auf die Datenkontrolle und Datenverwendung innerhalb von KMU auswirkt und mit welchen Unsicherheiten sich KMU konfrontiert sehen. Dabei wird auch der Aspekt der Übertragung von Daten in Drittstaaten außerhalb der EU beleuchtet. Des Weiteren wird aufgezeigt, inwieweit Cloud-Dienste die digitale Souveränität der KMU selbst beeinflussen.

Der Begriff „digitale Souveränität“ ist nicht eindeutig definiert und wird von verschieden Akteuren unterschiedlich aufgefasst. Allgemein adressiert digitale Souveränität in den öffentlichen Diskussionen sowohl eine makroökonomische bzw. geopolitische Ebene, bei dem es um die Souveränität der Staaten bzw. Rechtsräume geht, als auch eine mikroökonomische Ebene, bei der die Souveränität einzelner (Wirtschafts)-Akteure im Fokus steht. Während sich die Diskussionen um Cybersicherheit, Selbstbestimmung über die Daten und Datenschutz auf beiden Ebenen einspielen, wird die makroökonomische Ebene um geostrategische Aspekte ergänzt. Zusätzlich kann digitale Souveränität ausschließlich auf der Ebene der Individuen abgestellt sein, während andere Definitionen eher von einer Unternehmensperspektive ausgehen.

Auf makroökonomischer Ebene hat digitale Souveränität in den betrachteten Weltregionen EU, USA und China eine ähnliche, jedoch nicht identische Bedeutung. In allen drei betrachteten Weltregionen gibt es das Ziel, die eigene wirtschaftliche Resilienz zu erhöhen, indem die Region weniger abhängig von Ländern außerhalb ihres jeweiligen unmittelbaren Einflussbereichs werden.

Auf mikroökonomischer Ebene und besonders beim Thema der Selbstbestimmung von Individuen über ihre personenbezogenen Daten welche durch den Datenschutz reguliert sind, gibt es durchaus Unterschiede zwischen den Regionen. In den USA wird der Datenschutz auf Ebene der Bundesstaaten reguliert und variiert somit. Doch selbst im Bundesstaat Kalifornien, der in den USA als Vorreiter beim Thema Datenschutz angesehen werden kann und es in der Rechtslage durchaus inhaltliche Überschneidungen mit der europäischen DSGVO gibt, ist der Datenschutz aber dennoch weniger weitreichend, sodass Unternehmen in den USA ein weniger restriktiver Umgang mit personenbezogenen Daten vorgeschrieben wird. Hinzukommt, dass weitgehende Zugriffsrechte für US-Sicherheitsbehörden bestehen, welche einen Zugriff auch auf personenbezogene Daten ermöglichen. Dies gilt auch für Daten außerhalb der USA, wenn Zugriff auf diese Daten durch US-Unternehmen gegeben ist.

Der Datenschutz in China orientiert sich stark am DSGVO und wirkt sich entsprechend restriktiv auf die dortigen Unternehmen aus. Jedoch bestehen anders als in der EU weitreichende Gesetze für staatliche Behörden, den Datenschutz zu umgehen.

Für deutsche KMU schränkt der EU-Datenschutz den Datenzugriff und die Datenverwendung eher ein. Durch komplizierte und weitreichende Datenschutzvorgaben, entstehen daher rechtliche Unsicherheiten beim Umgang mit personenbezogenen Daten. Obgleich der Datenschutz für alle Unternehmen gilt, stehen KMU vor der Herausforderung, mit ihren begrenzten Ressourcen diese Vorgaben einzuhalten.

Neben der Datensouveränität der Individuen, die durch KMU eingehalten werden müssen, spielt Datensouveränität der Unternehmen eine Rolle im Zusammenhang mit Cloud-Lösungen. Wobei hier Datensouveränität der KMU im Kontext der Nutzung von Cloud-Diensten bedeutet, dass die in der Cloud liegenden Daten der KMU vor unerwünschten Zugriffen (inkl. Zugriffen durch Cloud-Anbieter, staatliche Behörden, Wettbewerber und weiteren Akteuren) geschützt sind, d.h. dass die KMU selbst über die Speicherung, Übertragung, Nutzung, Manipulation, Migration und Löschung ihrer Daten bestimmen und die Zugriffsrechte auf die Daten selbstbestimmt verwalten.

Cloud-Lösungen können die Datensouveränität der KMU erhöhen, in dem Cybersicherheit tendenziell verbessert wird und Datenzugriff und Datenverarbeitung durch befugte und kompetente Mitarbeiter des Unternehmens oder des Cloud-Anbieters für die KMU durchgeführt wird. Dennoch wird ein Kontrollverlust bei KMU wahrgenommen. Dieser kann begründet und unbegründet sein. Begründet ist er in jedem Fall dann, wenn Unternehmen „Lock-in-Effekte“ durch nicht gewährleistete Interoperabilität und Portabilität der Daten und Dienste ausgesetzt sind.

1 Einführung Themenfeld 2

Aus den Ergebnissen dieser Untersuchungen werden die wichtigsten Aspekte in Zusammenhang mit der digitalen Souveränität und der Nutzung von Cloud-Diensten in KMU für die Unternehmenserhebung, welche im dritten Teilbericht ausgewertet wird, abgeleitet.

Für die Untersuchungen wurden Desktoprecherchen zu verschiedenen Definitionen durchgeführt und das Verständnis der digitalen Souveränität für die drei betrachteten Weltregionen Europa, USA und China erörtert. Neben allgemeinen strategischen Positionen wir ein gesonderter Fokus auf Cloud-Dienste gesetzt. Die Ergebnisse sind in Kapitel 2 und 3 aufgeführt.

Für Kapitel 4 wurde ebenso eine Desktoprecherche und eine rechtliche Analyse durchgeführt, um die Besonderheiten des Datenschutzes als Teilaspekt der digitalen Souveränität in den drei betrachteten Weltregionen zu erfassen. Dabei wurde ebenso herausgearbeitet, in wieweit staatliche Behörden Zugriff auf die Daten ihrer Bürger und Unternehmen haben.

In Kapitel 5 und 6 wird auf die Lage der kleinen und mittleren Unternehmen eingegangen. Dabei wird zuerst auf die durch den Datenschutz entstehenden rechtlichen Unsicherheiten eingegangen und wie diesen entgegen gewirkt werden kann. Des Weiteren wird die digitale Souveränität der KMU analysiert und herausgearbeitet, inwiefern Cloud-Nutzung diese beeinflusst. Neben Desktoprecherche stützen sich die Ergebnisse auf Expertengespräche mit Ansprechpartnern aus dem Wissenstransferbereich, die sich mit Cloud-Diensten und KMU beschäftigen.

Die Arbeiten an Arbeitspaket 2 wurden zwischen Januar und März 2022 durchgeführt und spiegeln die aktuelle Lage zu diesem Zeitpunkt.

2 Definitionen digitaler Souveränität

Der Begriff „digitale Souveränität“ findet im politischen, öffentlichen und wissenschaftlichen Kontext immer mehr Verbreitung. Dennoch ist eine einheitliche Definition bzw. ein einheitliches Konzept bisher nicht vorhanden.[1] Daher werden in diesem Kapitel die verschiedenen Definitionen vorgestellt und anhand der Kriterien, die für KMU und Cloud-Dienste relevant sind, bewertet und passende Begriffsdefinitionen vorgeschlagen.

2.1 Unterschiedliche Auffassungen von digitaler Souveränität

Nachfolgende Beispiele illustrieren die unterschiedlichen Sichtweisen auf digitale Souveränität aus Politik und Wissenschaft:

> **Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Eine europäische Strategie für Daten - Eine europäische Datenstrategie (2020)[2]:** “Das Funktionieren des europäischen Datenraums wird davon abhängen, ob die EU hinreichend in Technologien und Infrastrukturen der nächsten Generation sowie in digitale Kompetenzen, wie z. B. in Datenkompetenz, investieren kann. Dies wiederum wird die technologische Unabhängigkeit Europas im Bereich der Schlüsseltechnologien und -infrastrukturen für die Datenwirtschaft stärken.”
>
> **Thierry Breton, EU-Kommissar für Binnenmarkt: Kommission stellt Strategien für Daten und Künstliche Intelligenz vor[3]:** “Our society is generating a huge wave of industrial and public data, which will transform the way we produce, consume and live. I want European businesses and our many SMEs to access this data and create value for Europeans – including by developing Artificial Intelligence applications. Europe has everything it takes to lead the ‘big data' race, and preserve its technological sovereignty, industrial leadership and economic competitiveness to the benefit of European consumers. […] [Technological sovereignty] is not a protectionist concept, it is simply about having European technological alternatives in vital areas where we are currently dependent.”
>
> **Margrethe Vestager Exekutiv-Vizepräsidentin für das Ressort “Ein Europa für das digitale Zeitalter” zur State of the Union[4]:** “The European vision for a digital future is one where technology empowers people. So today we propose a concrete plan to achieve the digital transformation. For a future where innovation works for businesses and for our societies. We aim to set up a governance framework based on an annual cooperation mechanism to reach targets in the areas of digital skills, digital infrastructures, digitalisation of businesses and public services.”

---

1 Vgl. Pohle (2020), BMWK (2021), S. 61ff und Baischew et al. (2020).

2 Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Eine europäische Strategie für Daten - Eine europäische Datenstrategie (2020). Wobei “technological sovereignty“ mit technischer Unabhängigkeit übersetzt wurde.

3 Europäische Kommission, 19.02.2020, online abrufbar unter https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273, zuletzt abgerufen am 02.02.2022.

4 Europäische Kommission, State of the Union: Commission proposes a Path to the Digital Decade to deliver the EU's digital transformation by 2030, 04.10.2021, online abrufbar unter https://ec.europa.eu/newsroom/representations/items/722345/de, zuletzt abgerufen am 02.02.2022.

Peter Altmaier, ehem. Bundesminister für Wirtschaft und Energie, bei seiner Rede auf dem Digital-Gipfel 2019[5]: "Daten werden der bedeutendste Rohstoff der Zukunft. Die europäische Wirtschaft benötigt dringend eine Infrastruktur, die Datensouveränität und breite Datenverfügbarkeit bei hohen Sicherheitsstandards gewährleistet."

Peter Altmaier, ehem. Bundesminister für Wirtschaft und Energie, bei einem Besuch in San Francisco, 2019[6]: "Germany has a right to digital sovereignty. Data clouds should not only be set up in the U.S. or China, but also in Germany so that European companies, which want secure and reliable data storage, have this option."

Fokusgruppe Digitale Souveränität (Bundesministerium für Wirtschaft und Energie) für den Digitalgipfel 2019[7]: Digitale Souveränität ist unverzichtbare Voraussetzung für unabhängiges staatliches und wirtschaftliches Handeln. Sie begünstigt Wirtschaftlichkeit, Wettbewerb, Agilität und die Fähigkeit, mit Risiken umgehen zu können. Digital souveräne Staaten und Organisationen können sich auf Grund geringerer Hersteller- oder Anbieterabhängigkeiten freier am Markt bedienen. Gleichzeitig ermöglicht digitale Souveränität, dass Unternehmen/Organisationen aufgrund niedrigerer Markteintrittsbarrieren selbst erfolgreicher als Anbieter in digitalen Ökosystemen agieren und somit Gestaltungs- und Innovationsspielräume erhalten können.

Julia Pohle, Konrad-Adenauer-Stiftung 2020[8]: "Die Souveränität eines demokratischen Staates besteht in der Sicherung der Selbstbestimmungsfähigkeit seiner Bürgerinnen und Bürger mit ihren unveräußerlichen Rechten. Sie dient damit dem Zweck, jedem Menschen zu ermöglichen, in seinen persönlichen Rechten respektiert zu werden und eigenverantwortlich zu handeln. [...] Die Spezifizierung „digital" im Konzept der „digitalen Souveränität" [...] verweist auf den gesamtgesellschaftlichen Transformationsprozess der Digitalisierung, der sich neben der allumfassenden Nutzung von Computertechnologie vor allem durch zwei zusammenhängende Entwicklungen auszeichnet: die Verbreitung und Nutzung digitaler Vernetzungstechnologie sowie die starke Zunahme digitaler Datensammlungen und grenzüberschreitender Datenströme."

Diese Aussagen zur digitale Souveränität zielen zum einen auf die geopolitische Ebene ab, bei der es um den Standort der Speicherung der Daten und die mit den Daten verbundenen Rechtsräumen ankommt sowie den Aufbau technologischen Know-Hows um Unabhängigkeit gegenüber anderen Staaten zu wahren (Makroebene), und zum zweiten auf die Souveränität der einzelnen Akteure, bei der es um die Sicherheit und Selbstbestimmung in Zusammenhang mit Daten und Infrastrukturen geht (Mikroebene).

---

5 Rede vom ehem. Bundeswirtschaftsminister Peter Altmaier während des Digital Gipfels 2019, Dortmund, 29.10.2019, https://www.de.digital/DIGITAL/Redaktion/EN/Meldungen/2019/20191028-altmaier-we-need-our-own-european-data-infrastructure.html, zuletzt abgerufen am 02.02.2022.

6 Ehem. Bundeswirtschaftsminister Peter Altmeier während eines Besuches in San Francisco, 9. July 2019, https://www.bloomberg.com/news/articles/2019-07-09/germany-makes-push-for-cloud-service-independent-of-u-s, zuletzt abgerufen am 02.02.2022.

7 Bundesministerium für Wirtschaft und Energie - Plattform „Innovative Digitalisierung der Wirtschaft", Fokusgruppe „Digitale Souveränität" im Rahmen des Digitalgipfels 2019, S. 6 Absatz 4.

8 Pohle, J. (2020), Digital sovereignty - A new key concept of digital policy in Germany and Europe, Konrad-Adenauer-Stiftung e. V, S. 6

Auffallend dabei ist die Betrachtung der digitalen Souveränität aus unterschiedlichen Perspektiven. Bei Pohle wird ausschließlich auf die Ebene der Individuen abgestellt, während die Fokusgruppe Digitale Souveränität auch aus Perspektive der Unternehmen den Begriff definiert. Dies kann durchaus zu Widersprüchen führen, welche im Verlauf der Studie herausgearbeitet werden. Ebenso macht es dieser Umstand notwendig, bei den Betrachtungen auf digitale Souveränität bei den unterschiedlichen Perspektiven zu differenzieren.

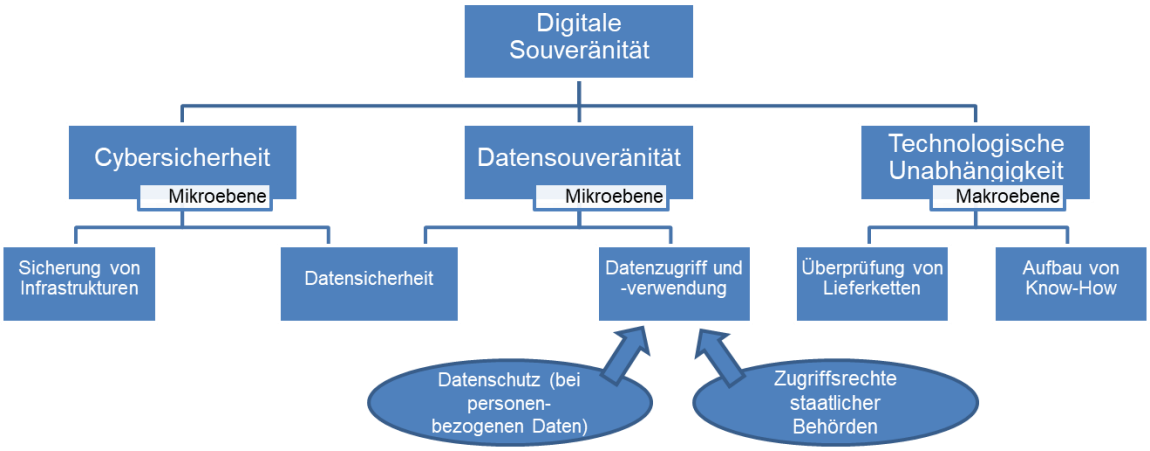
Ebenso auffallend ist, dass Begriffe wie technologische Souveränität teils als Synonym, teils als Oberbegriff und teils als Unterbegriff digitaler Souveränität verwendet werden. Datensouveränität hingegen scheint als ein Teilaspekt digitaler Souveränität verstanden zu werden. Im Zusammenhang dieser Studie wird technologische Souveränität mit digitaler Souveränität gleichgesetzt und Datensouveränität als Bestandteil digitaler Souveränität betrachtet. Eine exakte Taxonomie der Begriffe wie sie für diese Studie verwendet werden, folgt im nächsten Kapitel.

2.2 Taxonomie der Begriffe um digitaler Souveränität

Anhand von vorhandenen Begriffsdefinitionen in der Politik, in den öffentlichen Diskussionen und in der Wissenschaft, welche Auszugsweise im vorangegangen Kapitel aufgezeigt wurden, kristallisieren sich drei wesentliche Dimensionen der digitalen Souveränität heraus: Strategische Aspekte mit dem Ziel einer gewissen technologischen Unabhängigkeit (die eher die geopolitische „Makroebene“ adressieren), Cybersicherheit (die eher die auf Unternehmensebene stattfindet, daher eher die „Mikroebene“ adressiert) und Datensouveränität (die ebenso eher auf Unternehmens- und Individuumsebene stattfinden, daher eher die „Mikroebene“ adressiert). Abbildung 2-1 zeigt dieses Schema modellhaft auf, wobei zu beachten sei, dass sich die Dimensionen in vielen Aspekten stark Überschneiden und eine vollständige Trennung nicht möglich ist. Man könnte sich Abbildung 2-1 auch als Venn-Diagramm vorstellen, in dem alle drei Hauptdimensionen eine Schnittmenge bilden.

Die Dimension der Cybersicherheit bezeichnet die Resilienz digitaler Infrastruktur sowie der Abwehr von staatlich und nicht-staatlich organisierter Cyber-Spionage. Maßnahmen im Bereich der Cybersicherheit bestehen zum Beispiel in der Zertifizierung von Hard- und Software, aber auch in dem Aufstellen von Auswahlkriterien bei der Wahl von Hard- und Softwareherstellern für kritische Infrastrukturen.

Abbildung 2-1: Taxonomie der Begriffe unter digitaler Souveränität



Quelle: Eigene Darstellung.[9]

Datensouveränität setzt sich aus Datensicherheit sowie Datenzugriff und Datenverwendung zusammen. Auf Unternehmensebene wird Datenzugriff und Datenverwendung bei personenbezogenen Daten durch den Datenschutz reguliert, wobei Datenschutz und Datenverwendung ebenso von Zugriffrechten staatlicher Behörden abhängig sind.

Der Datenschutz stärkt die digitale Souveränität der Individuen. Für Unternehmen entstehen dadurch jedoch rechtliche Unsicherheiten mit dem Umgang personenbezogener Daten die ihnen zur Verfügung stehen. Daher muss Datensouveränität einmal aus der Perspektive der Individuen und einmal aus der Perspektive der Unternehmen betrachtet werden.

Eine Betrachtung der Datensouveränität aus der Perspektive der Individuen erfolgt in Kapitel 4 bei der Beleuchtung des Rechtsrahmens. In Kapitel 5 hingegen werden die aus dem Rechtsrahmen entstehenden rechtlichen Unsicherheiten für Unternehmen, inklusive KMU, in den Fokus gerückt.

Im Anschluss wird Datensouveränität speziell im Zusammenhang mit der Nutzung von Cloud-Diensten beleuchtet, wobei hier allein aus der Perspektive der Unternehmen betrachtet wird (Kapitel 6).

Datensouveränität findet in der öffentlichen Debatte besonders viel Anklang, aber auch politische Entscheidungsträger befassen sich umfassend mit Datensouveränität in Form von Strategien und Positionspapieren auf nationaler oder supranationaler Ebene (bspw. auf Ebene der EU). Technologische Unabhängigkeit zeichnet sich im staatlichen

9 Die Darstellung basiert auf die Recherche verschiedene Aussagen im Öffentlichen Raum. Eine einzige und eindeutige Definition und Taxonomie im öffentlichen Raum konnte nicht identifiziert werden. Die Darstellung stellt somit die Ergebnisse der Analyse der Studienautoren dar.

Bestreben nach widerstandsfähigen Lieferketten und dem Aufbau eigenem Know-How aus, um sicherzustellen, digitale Schlüsseltechnologie wie künstliche Intelligenz, High Performance Computing, Cloud und Datenräume und Cybersicherheit selbst entwickeln zu können.

3 Verständnis digitaler Souveränität im internationalen Vergleich

Wie in Abschnitt 2.2 dargestellt, spiegelt digitale Souveränität die zentralen Fragen wider, wie sich die Verfügbarkeit und Zugriffe digitaler Daten, Rechenleistung und Computernetzwerke auf die Souveränität von Staaten und die Privatsphäre des Einzelnen auswirkt. Diesen Fragen wird in allen der in dieser Studie betrachteten Weltregionen, EU, USA und China, nachgegangen. In der Tat ist diese Debatte fast so alt wie Computer und Computernetze selbst.[10]

Der Begriff „digitale Souveränität“ scheint jedoch eher für die Ziele der EU verwendet zu werden. Dennoch, neben der EU haben auch die USA und China das Ziel, ihre wirtschaftliche Widerstandsfähigkeit zu erhöhen, indem sie weniger abhängig von Ländern außerhalb ihres jeweiligen unmittelbaren Einflussbereichs werden. Die USA hat unter dem Motto "America first" des ehemaligen Präsidenten Donald Trump eine offen protektionistischere Haltung eingenommen.[11] China hat als Reaktion auf die US-Sanktionen mit seiner "Made in China 2025"-Strategie mehr Eigenständigkeit angekündigt. Im Folgenden werden diese Strategien und Positionen näher betrachtet.

In der EU

Über die drei „harten“ Hauptdimensionen Cybersicherheit, Datensouveränität und Technologische Unabhängigkeit hinaus wird in der EU digitale Souveränität als das Sicherstellen von europäischen Werten und Rechten für europäische Bürgerinnen in der digitalen Welt verstanden. Diese steht im besonderen Fokus „Europas digitaler Dekade“ und den digitalen Zielen für 2030 der Europäischen Kommission. Dabei umfassen die digitalen Ziele für 2030 eine sichere und nachhaltige digitale Infrastruktur, Kompetenzentwicklung von IKT-Expertinnen, ein digitaler Wandel in Unternehmen und eine Digitalisierung öffentlicher Dienste.[12]
Diese Ziele sollen digitale Souveränität stärken. Trotz globaler, wechselseitiger Abhängigkeit ist es somit ein Ziel der Europäischen Kommission, den Zugang zum europäischen Binnenmarkt zu regulieren und sicherzustellen, dass europäische Werte und Rechte nicht nur von europäischen Unternehmen, sondern auch von nicht-europäischen Unternehmen, die im EU-Binnenmarkt tätig sind, eingehalten werden. Ein weiteres Ziel ist es Forschungs- und Industriekapazitäten der EU im Bereich Digitalisie-

10 Für ein frühes Beispiel für die Erörterung aller drei Dimensionen, siehe Steinmüller, W. (1979). Legal problems of computer networks: A methodological survey. Computer Networks (1976), 3(3), 187-198. Die Debatte erhielt in den 1990er Jahren mehr Aufmerksamkeit, als das Internet bei den Verbrauchern populär wurde und Möglichkeit des Internets, unsere Lebensweise grundlegend zu verändern, sichtbar wurde. Siehe u.a., Perritt Jr, H. H. (1997). The Internet as a Threat to Sovereignty-Thoughts on the Internet's Role in Strengthening National and Global Governance. Ind. J. Global Legal Stud., 5, 423-442; Sassen, S. (1997). On the Internet and sovereignty. Ind. J. Global Legal Stud., 5, 545-559.

11 Siehe Gabler Wirtschaftslexikon, Url: https://wirtschaftslexikon.gabler.de/definition/america-first-politik-100609, abegrufen am 03.08.2022

12 Siehe Europäische Kommission – Europas digitale Dekade: digtiale Ziele für 2030, online abrufbar unter: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_de, zuletzt abgerufen am 17.03.2022.

rung zu stärken, da diese Technologien als Schlüsselfaktoren für künftige Innovationen und Wirtschaftswachstum gelten. Zentrale Ziele der der EU-Kommission sind:

- Sicherstellen der Einhaltung der geltenden Rechtsvorschriften, insbesondere der Grundrechte und
- die Schaffung von Rechtssicherheit um die Innovationstätigkeit zu erleichtern.

Neben zahlreichen Weißpapieren können als konkrete digitale Policies der EU zur Wahrung bzw. Erreichung digitaler Souveränität die Richtlinie aus dem Jahr 2016 zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystem in der Union („NIS-Directive“)[13], die DSGVO aus dem Jahr 2016[14], der Rechtsakt zur Cybersicherheit aus dem Jahr 2019[15], der Vorschlag für das Gesetz über Künstliche Intelligenz aus dem Jahr 2021[16], die Einführung des Digital Markets Act[17] und Digital Service Act[18] oder der Vorschlag eines European Chip Acts im Jahr 2022[19] gesehen werden.

Die Wahl besonders von chinesischen Herstellern (vor allem Huawei und ZTE) als Partner beim 5G-Rollout und der damit verbunden Fragen der Cybersicherheit von 5G-Netzten befeuerte die Debatte um digitale Souveränität ab dem Jahr 2019 zusätzlich. Der Unsicherheit über den Einsatz von chinesischer Hard- und Software wurde mit dem „EU-Instrumentarium“ für sichere 5G-Netze zu Beginn des Jahres 2020 („5G-Toolbox“) entgegengewirkt und zeichnet sich somit auch als eine konkrete Policy für die Stärkung der digitalen Souveränität innerhalb der EU ab.[20]

Das Thema digitale Souveränität wird stark auf EU-Ebene getragen. Eine Benchmarkstudie aus dem Jahr 2020, welche Dimensionen der digitalen Souveränität in den einzelnen Mitgliedsstaaten der EU sowie in UK untersucht, zeigt auf, dass alle untersuchten Länder die Wichtigkeit einer digitalen Transformation anerkennen und ambitionierte Pläne für einen Ausbau der bestehenden digitalen Infrastruktur sowie der Schulung von digitalen Fähigkeiten haben. Diese werden zumindest ein Fundament für digitale Souveränität bilden.[21]

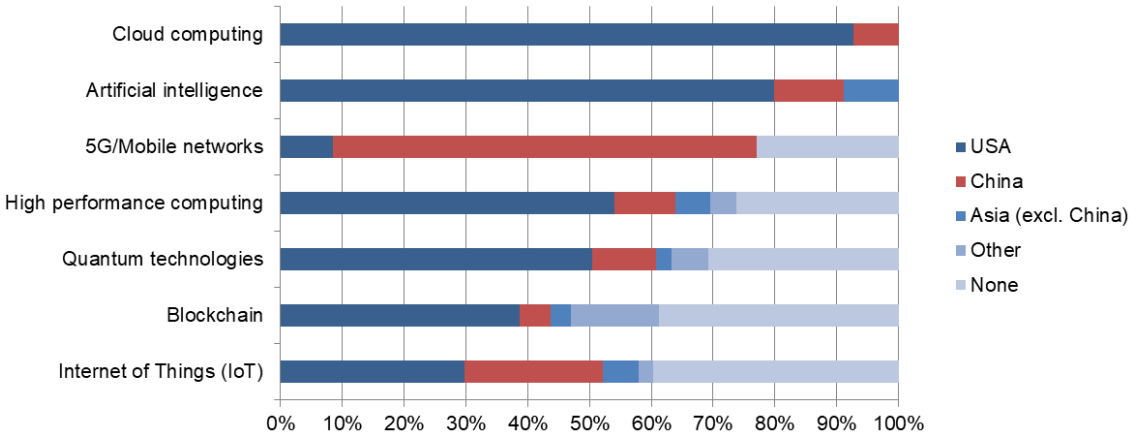
---

13 Online abrufbar unter https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32016L1148, zuletzt abgerufen am 17.03.2022.
14 Online abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679, zuletzt abgerufen am 17.03.2022.
15 Online abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32019R0881, zuletzt abgerufen am 17.03.2022.
16 Online abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0206, zuletzt abgerufen am 17.03.2022.
17 Online abrufbar unter https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_de, zuletzt abgerufen am 17.03.2022.
18 Online abrufbar unter https://ec.europa.eu/info/digital-services-act-ensuring-safe-and-accountable-online-environment_de, zuletzt abgerufen am 17.03.2022.
19 Online abrufbar unter https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en, zuletzt abgerufen am 17.03.2022.
20 Online abrufbar unter https://ec.europa.eu/commission/presscorner/detail/de/qanda_20_127, zuletzt abgerufen am 17.03.2022.
21 Baischew et al. (2020), S. 14.

Explizite Strategien, die digitale Souveränität im allgemeinen und Abhängigkeiten im speziellen adressieren, gibt es auf EU-Ebene und in den Ländern Deutschland und Frankreich. In den anderen Mitgliedsstaaten finden sich Aspekte digitaler Souveränität vor allem in allgemeinen Digitalisierungsstrategien wider.[22]

In Bezug zur Abhängigkeit gegenüber anderen Ländern und Regionen im Technologiebereich verdeutlicht Abbildung 3-1 die Handlungsmotivationen der EU und deren Mitgliedsstaaten. Dabei wurden Experten, die sich mit europäischer Technologie- und Digitalpolitik in den Regierungen befassen, zur Abhängigkeit der EU in unterschiedlichen Bereichen von den Ländern und Regionen USA, China, Asien (exkl. China), und Anderen befragt. Laut Expertenmeinungen ist die EU besonders abhängig von den USA in den Bereichen Cloud Computing, Künstliche Intelligenz, und High Performance Computing. Eine besonders hohe Abhängigkeit der EU scheint gegenüber China im Bereich 5G/Mobilfunknetze zu bestehen.

Abbildung 3-1: Abhängigkeit der EU gegenüber anderen Ländern laut Technik-Experten im Technologiebereich



Quelle: Deutsche Gesellschaft für Auswärtige Politik via Statista (2022). Befragungszeitraum Januar und Februar 2021, n=126. Befragte: Experten, die sich mit europäischer Technologie und Digitalpolitik in den Regierungen befassen.

Die Verteilung der größten Unternehmen der Digitalwirtschaft weltweit, untermauert diese Einschätzung. Die folgende Grafik zeigt die Marktkapitalisierung der größten 10 Unternehmen weltweit sowie ausgewählte Technologieunternehmen unter den 10 bis 100 größten Unternehmen. Unter den Top 10 sind 8 Unternehmen aus den USA und davon sind 7 amerikanische Technologieunternehmen. Das größte europäische Technologieunternehmen ist SAP auf Platz 100. Durch die sinkenden Aktienkurse in China sind Alibaba und Tencent aus dem Top 10 abgestiegen, gehören aber immer noch zu den 20 wertvollsten börsennotierten Unternehmen weltweit.

22 Stand Juli 2020, Baischew et al. 2020, S.16. Für einen ausführlichen Vergleich aller EU Mitgliedsstaaten und dem Vereinigten Königreich, siehe Baischew et al. 2020.

Tabelle 3-1: (Technologie-) Unternehmen nach Marktkapitalisierung

Rang	Unternehmen	Aktie	Markt-kapitalisierung (Mrd. USD)	Land
1	Apple	AAPL	2.699	USA
2	Saudi Aramco	2222.SR	2.288	Saudi-Arabien
3	Microsoft	MSFT	2.243	USA
4	Alphabet (Google)	GOOG	1.800	USA
5	Amazon	AMZN	1.643	USA
6	Tesla	TSLA	952	USA
7	Berkshire Hathaway	BRK-A	774	USA
8	NVIDIA	NVDA	666	USA
9	Meta (Facebook)	FB	605	USA
10	TSMC	TSM	554	Taiwan
13	Tencent	TCEHY	461	China
14	Visa	V	422	USA
17	Samsung	005930.KS	393	Südkorea
24	Mastercard	MA	335	USA
30	Alibaba	BABA	278	China
38	Broadcom	AVGO	245	USA
41	Cisco	CSCO	233	USA
44	Reliance Industries	RELIANCE.NS	223	Indien
45	Verizon	VZ	221	USA
46	Oracle	ORCL	216	USA
48	Adobe	ADBE	214	USA
49	Comcast	CMCSA	212	USA
50	Salesforce	CRM	211	USA
59	Intel	INTC	193	USA
68	QUALCOMM	QCOM	175	USA
72	Texas Instruments	TXN	167	USA
73	Netflix	NFLX	166	USA
74	AT&T	T	165	USA
80	T-Mobile US	TMUS	157	USA
84	China Mobile	0941.HK	148	China
95	PayPal	PYPL	134	USA
100	SAP	SAP	132	Deutschland

Quelle: Marktkapitalisierung auf der Basis der aktuellen Börsenkurse; https://companiesmarketcap.com/, zuletzt abgerufen am 22.02.2022

Große Abhängigkeit wird im Bereich Cloud gesehen. Diese stehen stark im Kontext digitaler Souveränität innerhalb der EU da Cloud Storage und Cloud Computing als Schlüsseltechnologien anerkannt werden. Neben Cloud Storage und Cloud Computing im Allgemeinen wird die Cloud Initiative Gaia-X im Speziellen ebenso im Kontext digitaler Souveränität gesehen, da Gaia-X sowohl die digitale Souveränität der Nutzer von Cloud Diensten als auch die Skalierbarkeit und Wettbewerbsfähigkeit der europäischen Anbieter von Cloud Diensten stärken soll.[23] Erläuterungen und Diskussionen dazu sind Themenfeld 1 zu entnehmen.

Neben Gaia-x können Anstrengungen zur Einhaltung beziehungsweise Erreichung von Datensouveränität auch in der öffentlichen Verwaltung gefunden werden. Maßnahmen für die deutsche Bundesregierung und Bundesverwaltung sind beispielsweise die Ver-

23 Vgl. https://gaia-x.eu/what-is-gaia-x, zuletzt abgerufen am 11.02.2022, BMWK Pressemitteilung 15.09.2020 Bundesminister Altmaier zur Gründung der GAIA-X AISBL, online abrufbar unter https://www.bmwi.de/Redaktion/DE/Pressemitteilungen/2020/09/20200915-zitat-altmaier-zur-gruendung-der-gaia-x-aisbl.html, zuletzt abgerufen am 11.02.2022.

schlüsselung der drahtgebundenen elektronischen Kommunikation mit Sichere Inter-Netzwerk Architektur (SINA), die sichere Kommunikation zwischen Netzwerken, das heißt auch mit Smartphones und Tablets, bietet.[24] Ein weiteres Beispiel aus der öffentlichen Verwaltung in Deutschland ist das Benutzen der Open-Source-Software von Nextcloud, einem deutschen Anbieter, um Datensouveränität beim Datenaustausch innerhalb des Bundes zu bewahren.

Ein neuartiger Ansatz zur Wahrung von Daten der öffentlichen Verwaltung im Allgemeinen ist die sogenannte „Data Embassy" von Estland. In der Digital Economy and Society Index (DESI) 2021 nimmt Estland in der Kategorie Digitale öffentliche Dienste Rang 1 unter den EU Mitgliedsstaaten ein[25], 99 % der Verwaltungsleistungen können vollständig digital vorgenommen werden. Die Data Embassy, welche ein Rechenzentrum und keine eigentliche Botschaft ist, dient als Erweiterung der Cloud des estländischen Staates und liegt in Luxemburg. Das Rechenzentrum, welches unter Hoheit des estländischen Staates liegt, wird als Back-up genutzt, ist aber auch fähig, die kritischsten Anwendungen laufen zu lassen, sollte es zu Ausfällen im Landesinneren kommen.[26] Das Rechenzentrum kann somit als Stärkung der Resilienz öffentlicher Daten und Dienste betrachtet werden.

Zusammenfassend kann fest gehalten werden, dass Digitale Souveränität in Europa als Problem wahrgenommen wird, auf der politischen/regulatorischen Agenda steht und dass Maßnahmen um die Unabhängigkeit zu erhöhen im regulatorischen und im Forschungsbereich unternommen wurden bzw. in der Umsetzung sind.

In den USA

Ein wichtiger Aspekt bei der digitalen Souveränität ist die Tatsache, dass wichtige Akteure der Digitalökonomie wie Meta (Facebook), Alphabet (Google), Apple, Microsoft, Amazon, IBM, NVIDIA, Oracle etc. ihren Sitz in den USA haben. Wie in Abbildung 3-1 zu sehen ist, führt dies gerade dazu, dass Akteure in der EU das Bild einer Abhängigkeit von den USA in Umfragen angeben. Für die USA stellt sich daher die Frage zu digitaler Souveränität und ausländischen Unternehmen weniger, mit Ausnahmen in der Halbleiterindustrie und im Mobilfunksegment.

Das Ziel von mehr Unabhängigkeit im Technologiesektor, Resilienzen im Cyberraum und Datensouveränität wird dennoch auch in den USA verfolgt.

---

24 Siehe Bundesamt für Sicherheit in der Informationstechnik, online abrufbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/SINA.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 11.02.2022.

25 DESI 2021, Estland, https://digital-strategy.ec.europa.eu/en/policies/desi-estonia, zuletzt abgerufen am 11.02.2022.

26 Siehe e-Governance in Estland, online abrufbar unter https://e-estonia.com/solutions/e-governance/data-embassy/,
zuletzt abgerufen am 11.02.2022 und OECD Case Study, The world's forst data embassy –Estonia, online abrufbar unter
https://www.oecd.org/gov/innovative-government/Estonia-case-study-UAE-report-2018.pdf, zuletzt abgerufen am 11.02.2022.

Beispielhaft für das Streben nach mehr Cybersicherheit, jedoch sicherlich auch mehr technologischer Unabhängigkeit, ist der Rückbau von chinesischem Telekommunikationsequipment in amerikanischen Netzwerken. Nach nachrichtendienstlichen Sicherheitsbedenken zum Einsatz von Equipment von chinesischen Unternehmen beim Aufbau der 5G-Netze verhinderte die FCC defacto den Kauf chinesischer 5G-Technologien, woraufhin das Supply Chain Reimbursment Program ins Leben gerufen wurde. Unter diesem Programm sollen Telekommunikationsnetzbetreiber die Kosten erstattet bekommen, die in angemessener Weise für die Entfernung, den Austausch und die Entsorgung von Kommunikationsgeräten und -diensten von ZTE und Huawei anfallen.[27]

Ein weiteres Beispiel für das Streben nach mehr technologischer Unabhängigkeit, besonders gegenüber China, ist der United States Innovation and Competition Act aus dem Jahr 2021. Dieser sieht vor, Investitionen in Grundlagen- und Spitzenforschung, Kommerzialisierung sowie Bildungs- und Ausbildungsprogramme in den Bereichen künstlicher Intelligenz, Halbleiter, Quantencomputer, fortgeschrittene Kommunikation, Biotechnologie und fortgeschrittene Energie zu tätigen, welche sich auf 110 Milliarden Dollar belaufen. Über 10 Milliarden Dollar wurden für die Einrichtung von zehn regionalen Technologiezentren und die Schaffung eines Programms zur Krisenbewältigung in der Lieferkette bewilligt.[28]

In China

China ist in den letzten zwei Dekaden zu einer Technologie-Superpower herangewachsen. Das e-Commerce Unternehmen Alibaba Group zählt zu den finanzstärksten Firmen der Welt[29] und bildet im Jahr 2020 25 % des gesamten e-Commerce Geschäftes weltweit ab und hat damit doppelt so viel e-Commerce Aktivität als Amazon.[30] Tencent, welches unter anderem aktiv in Geschäftsfeldern wie Sofortnachrichtendienste, Soziale Netzwerke, Onlinemedien, online Spiele sowie e-Commerce und Onlinewerbung ist, erreicht mit ihrer „Super-App“ WeChat 1,2 Mrd. monatliche aktive Nutzer, mehr als jede andere App der Welt.[31] Im Telekommunikationssektor ist China ebenso dominant:

---

27 The Verge, The cost of ripping and replacing Chinese cellular equipment has ballooned by billions, von Mitchell Clark, 04.02.2022, online abrufbar unter https://www.theverge.com/2022/2/4/22918611/rip-and-replace-hauwei-zte-fcc-cell-network-securty , zuletzt abgerufen am 23.03.2022.

28 Siehe Politico, Senate advances a rare bipartisan deal on countering China, von Andrew Desiderio, 17.05.2021, online abrufbar unter https://www.politico.com/news/2021/05/17/senate-bipartisan-deal-countering-china-489152, zuletzt abgerufen am 23.03.2022.

29 Siehe Forbes Global 2000 (2021), online abrufbar unter https://www.forbes.com/lists/global2000/#746710e25ac0, zuletzt abgerufen am 23.03.2022.

30 Gemessen an Gross Merchandise Value, siehe Activate Tech & Media Outlook 2022 via Statista, online abrufbar unter https://www.statista.com/statistics/664814/global-e-commerce-market-share/ und https://www.statista.com/statistics/885354/top-global-online-marketplaces-by-gmv/, zuletzt abgerufen am 17.03.2022.

31 Tencent.com via Statista, online abrufbar unter: https://de.statista.com/statistik/daten/studie/311381/umfrage/anzahl-der-monatlich-aktiven-nutzer-von-wechat-weltweit/, zuletzt abgerufen am 23.03.2022.

Huawei hat im Jahr 2020 einen Anteil im Netzwerkherstellermarkt von 37,3 %[32] und führt den 5G-Basisstationen-Markt an[33]. China ist ebenso Vorreiter bei Patenten im Zusammenhang mit dem nächsten Mobilfunkstandard 6G.[34]

Das Wachstum im Technologiesektor soll China ebenso erlauben, über das Verarbeitende Gewerbe hinaus neue Sektoren wie digitaler Gesundheitsfürsorge und Künstliche Intelligenz, Robotik und Big Data zu erschließen. Die Hälfte der 174 „Unicorns“ (Startups mit einem Wert von über 1 Mrd. USD) sind bereits in diesen Sektoren tätig.[35]

Auf dem Weg zur digitalen Vorherrschaft baut China eine umfassende Cyber-Unabhängigkeit auf, was die chinesische Digitalpolitik und den Entwicklungspfad von Chinas Politik in diesem Feld vorgibt. In globalen Kreisen drängt China auf ein staatszentriertes Verständnis von Souveränität, bei dem der Staat die höchste Autorität im digitalen Raum besitzt. Diese Vision wird hier durch den Ausbau der eigenen regulatorischen und technologischen Fähigkeiten verwirklicht. Dazu zählen u. a. stärkere Kontrollen des internationalen Datenverkehrs, der Online-Inhalte, des Online-Konsums und der Technologie-Anbieter.[36] Ziel ist es ebenso, Kartellgesetze auf den Weg zu bringen und Plattformen mit signifikanten Netzwerkeffekten die als Gatekeeper identifiziert wurden, zu regulieren. Dabei sollen unfaire Geschäftspraxen, wie das Erzeugen von Falschdaten (z. B. falsche Anzahl von „Clicks“ oder das Verschleiern negativer Produktbewertungen), der Einsatz von Algorithmen und anderen Techniken zur Beeinflussung von Nutzerentscheidungen oder das Ausnutzen von Geschäftsdaten von anderen Wettbewerbern bei Plattformen die selbst auch als Anbieter auf der eigenen Plattform auftreten (Plattformen mit Doppelrolle als Vermittler und Anbieter), unterbunden werden.[37]

China konzentriert sich auch auf die weitere Stärkung seiner Autonomie und Selbstständigkeit im digitalen Bereich, um die Abhängigkeit von Innovationen ausländischer digitaler Anbieter zu verringern.[38]

---

32 Itcandor.com via Statista, online abrufbar unter https://www.statista.com/statistics/540788/service-provider-network-market-share-by-vendor/, zuletzt abgerufen am 23.03.2022.

33 Trendforce.com via Statista, online abrufbar unter https://www.statista.com/statistics/1134472/global-mobile-base-station-vendor-market-share/, zuletzt abgerufen am 23.03.2022.

34 Nikkei.com, online abrufbar unter https://asia.nikkei.com/Business/Telecommunication/China-accounts-for-40-of-6G-patent-applications-survey, zuletzt abgerufen am 23.03.2022.

35 Stand 11.03.2022, siehe CBInsights, online abrufbar unter https://www.cbinsights.com/research-unicorn-companies, zuletzt abgerufen am 23.03.2022.

36 Vgl. The Diplomat, Tech Regulation in China Brings in Sweeping Changes, von Kai von Carnap und Valarie Tan, 21.12.2021, online abrufbar unter https://thediplomat.com/2021/12/tech-regulation-in-china-brings-in-sweeping-changes/, zuletzt abgerufen am 23.03.2022.

37 CNBC, China seeks to tighten rules on unfair internet competition, sending tech shares lower, von Arjun Kharpal, 17.08.2021, online abrufbar unter https://www.cnbc.com/2021/08/17/china-tech-regulation-draft-rules-ban-unfair-internet-competition-tencent-alibaba-slide.html, zuletzt abgerufen am 23.03.2022.

38 Vgl. https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537, siehe dazu auch staatliche Investitionen in die chinesische Halbleiterindustrie, https://www.handelsblatt.com/politik/international/halbleiter-chinas-milliardenschwere-aufholjagd-in-der-chipindustrie-stoesst-an-grenzen/27300398.html, und Software-Entwicklung (privatewirtschaftliche, teils getrieben von US-Sanktionen), heise.de, Wegen US-Sanktionen: Huawei will sich auf Software-

4 Rechtsrahmen für Datensouveränität im internationaler Vergleich zwischen der EU, den USA und China

In diesem Kapitel werden die rechtlichen Rahmenbedingungen des Datenschutzes sowie die Zugriffsrechte staatlicher Behörden auf personenbezogene Daten analysiert. Dies geschieht vor dem Hintergrund, dass diese Rahmenbedingungen sich auf die Unternehmensaktivitäten besonders im Zusammenhang mit der Nutzung von Cloud-Diensten auswirken.

Datensouveränität, wie eingangs erläutert, ist einer der drei Hauptdimensionen der digitalen Souveränität und besteht aus Datensicherheit einerseits sowie aus Datenzugriff und Datenverwendung andererseits. Datensicherheit, d. h. der Schutz vor Cyberangriffen, ist ebenso Teil der Cybersicherheit (siehe Abbildung 2-1).

Der Schutz personenbezogenen Daten sorgt für mehr Datensouveränität der Individuen, wirkt sich jedoch restriktiv auf die Datenzugriffe und Datenverwendungsmöglichkeiten von Unternehmen aus.

Ebenso wird die Datensouveränität von Individuen durch Zugriffsrechte staatlicher Behörden eingeschränkt, weshalb auch hierzu die Regelungen in allen drei betrachteten Weltregionen analysiert werden.

Die Erläuterung der in der EU geltenden Vorschriften sind besonders für die folgenden Kapitel relevant, da sie im Zusammenhang mit deutschen KMU und deren Nutzung von Cloud-Diensten und daraus resultierenden rechtlichen Unsicherheiten am bedeutsamsten sind.

Darüber hinaus werden vergleichbare Analysen für die USA und für China vorgenommen, da die dortigen Regularien sich ebenso auf den Umgang mit Daten innerhalb der EU auswirken können. Ferner kann durch den Ausblick in den USA und China ein breiteres Verständnis für die EU-Regularien gewonnen werden.

4.1 Datensouveränität in der EU

4.1.1 Datenschutz

Die Europäische Datenschutz-Grundverordnung DSGVO bildet seit Mai 2018 den Rechtsrahmen des Datenschutzes innerhalb der EU und schafft somit ein „level playing field“ zwischen den Mitgliedsstaaten im Europäischen Binnenmarkt. Die DSGVO soll ein hohes Schutzniveau für personenbezogene Daten sicherstellen, indem sie Anreize

Entwicklung konzentrieren, von Oliver Bünte, 25.05.2021, https://www.heise.de/news/Wegen-US-Sanktionen-Huawei-will-sich-auf-Software-Entwicklung-konzentrieren-6052950.html, zuletzt abgerufen am 23.03.2022.

für die Pseudonymisierung von personenbezogenen Daten schafft und damit die Identifizierung von Personen bei notwendigen Datenverarbeitungsvorgängen erschwert,[39] was die Datensouveränität der Verbraucher bewahrt. Die allgemeinen Voraussetzungen zur Datenverarbeitung, wie die Einwilligung auf Basis der Datenschutzerklärung[40], der Anspruch auf Auskunft im Umgang mit den personenbezogenen Daten,[41] aber auch das Recht auf Löschung personenbezogener Daten („Recht auf Vergessenwerden“)[42] stärken dabei den Verbraucher in seiner digitalen Selbstbestimmung – auch gegenüber den datenverarbeitenden Unternehmen.

Vor dem Hintergrund europäischer Abhängigkeit in den Technologiebereichen Cloud Storage und Cloud Computing gegenüber den USA, stellt sich die Frage, wie es sich mit dem Datenschutz verhält, wenn personenbezogene Daten gegenüber Empfängern in Drittländer (vor allen in die USA) offengelegt bzw. dort verarbeitet werden.

Grundsätzlich dürfen personenbezogene Daten nur an Länder außerhalb der EU oder des Europäischen Wirtschaftsraumes (EWR) übermittelt werden, wenn in diesen Drittländern das Schutzniveau der DSVGO erreicht wird.[43] Bezogen auf einige Länder wurde dies durch Angemessenheitsbeschluss[44] seitens der EU-Kommission ausdrücklich festgestellt.[45] Bei anderen – wie z. B. den USA oder China – gibt es diese Beschlussgrundlage nicht. Das Privacy Shield-Abkommen zwischen der EU und den USA aus dem Jahr 2016 hatte festgestellt, dass in den USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet wird. Mit dem Schrems II-Urteil des EuGH vom 16. Juli 2020 wurde der Privacy-Shield für ungültig erklärt.[46] Fehlt es an einem Angemessenheitsbeschluss oder einer vergleichbaren Übereinkunft kann die Übertragung personenbezogener Daten nur noch auf der Basis geeigneter Garantien[47] oder Ausnahmetatbeständen[48] erfolgen, oder sie muss – wenn beides nicht vorhanden ist – unterbleiben.[49]

---

39 BMWK (2022), Europäische Datenschutz-Grundverordnung, online abrufbar unter https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/europaeische-datenschutzgrundverordnung.html, zuletzt abgerufen am 11.02.2022. Eine Begriffsklärung ist in DSVGO Art. 4 Abs. 5 zu finden.

40 DSGVO Art. 6.

41 DSGVO Art. 15.

42 DSGVO Art. 17.

43 Vgl. DSGVO Art. 44 S. 2.

44 DSGVO Art. 45.

45 DSGVO Art. 45 Abs. 3. Eine Liste der Länder, zu denen ein Angemessenheitsbeschluss besteht, findet sich auf den Seiten der EU-Kommission: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_de, zuletzt abgerufen am 18.02.2022.

46 EuGH, Urteil vom 16. Juli 2020 – C-311/18 – (Schrems II).

47 DSGVO Art. 46.

48 DSGVO Art. 49.

49 Vergleich Bundesbeauftragte für Datenschutz und Informationsfreiheit: Praktische Auswirkungen der Rechtsprechung des EuGH auf den internationalen Datentransfer, online abrufbar unter https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Auswirkungen-Schrems-II-Urteil.html, zuletzt abgerufen am 11.02.2022.

Für den Datentransfer gibt es derzeit zwei mögliche Wege, die eingeschlagen werden könnten:

- Ein Datentransfer kann vorgenommen werden, wenn geeignete Garantien zwischen den am Datentransfer Beteiligten vorgesehen bzw. vereinbart sind. Diese müssen die wesentlichen Elemente des in der Europäischen Union geltenden Schutzes enthalten und bedürfen, sofern sie ausgehandelt werden, der Genehmigung durch die zuständigen Aufsichtsbehörde.[50] Nutzen die Vertragsparteien die von der EU-Kommission vorformulierten Standarddatenschutzklauseln[51] ist diese Genehmigung verzichtbar.[52]

  Für den Datentransfer hält die Kommission derzeit Module von Standarddatenschutzklauseln im Sinne des Art. 46 Abs. 2 lit. c DSGVO bereit, die die verschiedenen Typen von Übermittlungen abdecken.

  Datenexporteure und -importeure, die diese Standarddatenschutzklauseln des Kommissionsbeschlusses nutzen wollen, müssen also diese in ihre Vertragsbeziehung mit einbeziehen, was regelmäßig über AGB im Vertrag über die Auftragsverarbeitung stattfinden kann.

  Allerdings hat der EuGH auch festgestellt, dass die Standarddatenschutzklauseln alleine – je nach spezifischer Rechtslage und Situation im jeweiligen Drittland – gegebenenfalls nicht ausreichen, um ein angemessenes Datenschutzniveau sicherzustellen. Mitunter müssen zusätzliche technische und organisatorische Maßnahmen („zusätzliche Maßnahmen“ oder „supplementary measures“) ergriffen werden. Erheblich detaillierter als in den früheren Standardvertragsklauseln fallen deshalb die Regelungen zu den Rechten und Pflichten der Vertragsparteien mit Blick auf die Rechtslage des Empfängerlandes sowie auf Zugang von Behörden des Empfängerlandes zu den übermittelten Daten aus; diesem Thema widmen sich explizit die Klauseln 14 und 15. Der Datenexporteur hat z. B. zu prüfen, in welchem Umfang Behörden in einem Drittland die Möglichkeit haben, Zugriff auf die personenbezogene Daten zu nehmen, und ob den betroffenen Personen dagegen durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen (z. B. Anspruch auf rechtliches Gehör).[53] Gelangt er dabei zum Ergebnis, dass es sich aufgrund der besonderen Rechtslage und Situation im Drittland als unmöglich erweist, den Rechtsschutz nach europäischen Standard sicherzustellen, weil man z. B. Überwachungsgesetze in Drittstaaten nicht einfach durch vertragliche Regelungen außer Kraft setzen kann, dann muss der Datentransfer unterbleiben. Andererseits gilt: Können die Bedenken

50 DSGVO Art. 46 Abs. 3.
51 Siehe Europäische Kommission, 04.06.2021, Standardvertragsklausen für Verantwortliche und Auftragsverarbeiter in der EU / im EWR, online abrufbar unter unter https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors_de, zuletzt abgerufen am 11.02.2022.
52 DSGVO Art. 46 Abs. 2.
53 EuGH, Urteil vom 16. Juli 2020 – Az. C-311/18 – (Schrems II), Rn. 131, 187, 191.

durch zusätzliche Maßnahmen ausgeräumt werden, steht einem Datentransfer nichts mehr im Wege (z. B. weil die anfänglichen Bedenken zur Rückverfolgbarkeit durch den Einsatz von besonderen Verschlüsselungstechniken entgegnet werden kann, oder Daten in der Cloud A pseudonymisiert werden und sich der Schlüssel für die Ent-Pseudonymisierung in einer anderen Cloud, der Cloud B, hinterlegt wird).

- Lassen sich Garantien nicht vereinbaren, bleibt Art. 49 DSGVO. Er definiert eine begrenzte Zahl von Ausnahmetatbeständen, nach denen für ganz bestimmte, eng umrissene Situationen ein Datentransfer ins Drittland auch ohne Garantien und zusätzlichen Maßnahmen erlaubt sein soll.[54] Danach ist es prinzipiell auch denkbar eine vorherige Einwilligung in den jeweiligen Datentransfer einzuholen.[55] Diese Vorschrift ist allerdings eng auszulegen; der Europäische Datenausschuss (EDSA) vertritt hier eine sehr restriktive Auffassung und lässt genannten Ausnahmen überhaupt nur bei gelegentlichen oder sich nicht wiederholenden Übermittlungen zu,[56] weshalb die rechtfertigende Einwilligung bei der Inanspruchnahme von Cloud-Diensten regelmäßig als ausgeschlossen gilt.

Aus der in der DSGVO angelegten Systematik folgt, dass die Verantwortlichen in der Regel selbst bewerten müssen, ob bei Inanspruchnahme eines Cloud-Dienstes im Drittland die personenbezogenen Daten einen gleichwertigen Schutz wie in der EU genießen oder welche zusätzliche technischen oder organisatorischen Schutzmaßnahmen erforderlich werden (müssen), um den Verpflichtungen aus der DSGVO bzw. aus den vereinbarten Garantien vollumfänglich zu genügen.

Diese vorherige Einschätzung ist aber gerade für KMU schwierig, weshalb der EDSA Leitlinien zur Risikoanalyse zur Verfügung stellt, die einerseits bei der Bewertung der Situation im Drittland unterstützen sollen und zugleich risikoabhängig technische und organisatorische Maßnahmen vorschlagen, welche im Einzelfall von den Vertragspartnern eingesetzt werden können, um einen Datentransfer zu ermöglichen.[57] Diese Leitlinien werden bislang allerdings als viel zu bürokratisch und wenig anwenderfreundlich eingeschätzt.[58] Regelmäßig wird eine anwaltliche Unterstützung bei Bewertung der Ausgangssituation und der zu ergreifenden Maßnahmen erforderlich sein.

---

54 DSGVO 49 Abs. 1a.
55 DSGVO Art. 49 Abs. 1 lit. a).
56 EDSA, Leitlinien 2/2018 zu den Ausnahmen nach Art. 49 der Verordnung 2016/679 vom 25.5.2018; abrufbar unter https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_de.pdf, zuletzt abgerufen am 14.02.2021.
57 EDSA, Leitlinien 01/2020 v. 18. Juni 2021, abrufbar unter https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf, zuletzt abgerufen am 14.02.2021.
58 *Spies*, ZD 2021, 478, 479 ff.

4.1.2 Zugriffsreche staatlicher Behörden

Innerhalb der EU ist die Möglichkeit des behördlichen Zugriff auf personenbezogene Daten eines Unternehmens streng reglementiert. Insbesondere in strafrechtlichen Verfahren ist der Zugriff nur ausnahmsweise nach sorgfältiger Abwägung widerstreitender Interessen gestattet. Ferner ist diese eingeschränkte Zugriffsbefugnis auf den territorialen Zuständigkeitsbereich begrenzt; exterritoriale Zugriffsrechte – etwa auf Daten in den USA – bestehen in der Regel nicht, sondern könnten allenfalls durch entsprechende Rechtshilfegesuche/-abkommen gerichtlich erwirkt werden.[59]

4.2 Datensouveränität in den USA

4.2.1 Datenschutz

Anders als in der EU wird der Datenschutz in den USA auf bundesstaatlicher Ebene geregelt und darüber hinaus eher über Selbstverpflichtungen oder bereichs- bzw. branchenspezifisch reguliert (z. B. für die Bereiche Direktwerbung, Kreditauskünfte, Fitness-Tracker, Cloud Storage und -Computing).[60] Im Vordergrund dieser Regularien steht der Schutz der individuellen Privatsphäre (privacy) vor spezifischen oder systemischen Gefahren, nicht aber der Schutz der personenbezogenen Daten an sich (data protection), die allenfalls als eine Art Reflex mitgeschützt werden.[61] In den Regularien sind daher in erster Linie Aktualisierungspflichten oder Meldeverpflichtungen zum Schutz vor Sicherheitsverstößen festgelegt sowie die sich aus einer Verletzung dieser Pflichten ergebenden (Schadensersatz-) Ansprüche der Verbraucher und Verbraucherinnen näher ausgestaltet.[62] Über die Einhaltung dieser verbraucherschützenden Vorgaben wacht folgerichtig keine Datenschutzbehörde nach europäischem Vorbild, sondern die Federal Trade Commission (FTC).

Das Bestreben nach mehr Datenschutz kann im Bundesstaat Kalifornien beobachtet werden, in dem am 1.1.2023 der CALIFORNIA PRIVACY RIGHTS ACT in Kraft treten wird, in welchem zum einen die bisherigen Regelungen des CALIFORNIA CONSUMER PRIVACY ACT (CCPA) mit einfließen allerdings um Regelungen zum Schutz personenbezogener Daten ergänzt werden. Der CPRA findet Anwendung auf personenbezogene Daten, die ab dem 1.1.2022 erhoben und verarbeitet wurden. Den Unternehmen wird noch eine „grace period“ bis zum 1.1.2023 eingeräumt, d. h. nur Rechtsverletzungen die an oder nach diesem Termin stattfinden werden von den zuständigen Auf-

---

59 Jungkind, in: Wolff/Brink, BeckOK Datenschutzrecht, Art. 48 Rn. 10 ff.
60 Determann ZD 2021, 69.
61 Paul M. Schwartz, Preemption and Privacy, 118 Yale L.J. (2009), abrufbar unter http://digitalcommons.law.yale.edu/ylj/vol118/iss5/3 , zuletzt abgerufen am 18.02.2022.
62 Determann ZD 2021, 69.

sichtsgremien geahndet.[63] Der CCPA bleibt deshalb konsequenterweise noch bis zum 1.7.2023 in Kraft.

Die im CPRA vorgenommene Erweiterung um das Datenschutzrecht greift zahlreiche Regelungen auf, die man auch in der DSGVO findet, wie z. B. eine Definition von personenbezogenen Daten,[64] die in der weiteren Kategorisierung in „sensitiv personal information"[65] sogar noch über die Definition in Art. 9 DSGVO hinausgeht. Andererseits gibt es aber auch Abweichungen von der DSGVO. Der Schutz besonderer personenbezogener Daten ist weniger stark ausgeprägt als in der DSGVO. Das strenge Verbot mit Erlaubnisvorbehalt (Einwilligungsvorbehalt) nach Art. 6 Abs. 1 DSGVO gibt es im CPRA nicht; in den meisten Fällen ist ein Opt-out-Recht ausreichend,[66] während unter der DSGVO regelmäßig eine Opt-in-Einwilligung erforderlich ist. Für Unternehmen gibt es nach der CPRA keine Verpflichtung einen Datenschutzbeauftragten zu benennen, ferner sind die Bußgelder bei einem Verstoß gegen die CPRA äußerst gering und in keiner Weise mit dem Bußgeldrahmen des Art. 83 Abs. 4 und 5 DSGVO vergleichbar. Künftig wird ferner eine Aufsichtsbehörde für den Datenschutz eingerichtet, die „California Privacy Protection Agency",[67] der umfassende und weitreichende Aufgaben übertragen sind. Inhaltlich bemüht sich der CPRA deutlich stärker als die DSGVO, die Interessen der Unternehmen im Rahmen der erforderlichen Abwägungen zu den Persönlichkeitsinteressen der Verbraucher zu berücksichtigen.[68] Durch diesen Spielraum bei Entscheidungen über die Reichweite der Datensouveränität im Einzelfall bleibt eine gewisse Flexibilität erhalten, die man bei der Anwendung der DSGVO zuweilen vermisst.

Welche Auswirkungen die CPRA für den Datentransfer in die USA besitzen wird, bleibt abzuwarten. Sicher wird man der CPRA an sich ein adäquates Schutzniveau im Sinne des Art. 45 DSGVO bescheinigen können. Allerdings bleiben natürlich auch in Kalifornien die vom EuGH besonders kritisierten Zugriffsbefugnisse der US-amerikanischen Sicherheitsbehörden erhalten, was die Vorbehalte des EuGH, die er in seiner Schrems II-Entscheidung formuliert hat, gerade nicht beseitigen würde.

4.2.2 Zugriffsrechte staatlicher Behörden

In den USA gelten weitgehende Zugriffsrechte für die US-Sicherheitsbehörden. Grundlage dieser auch exterritorialen Zugriffsrechte war zunächst der USA PATRIOT Act[69], ein Gesetz, das nach den Anschlägen vom 11. September 2001 zur Terrorabwehr verabschiedet wurde und die Befugnisse der Sicherheitsbehörden massiv ausweitete. Mitt-

63 Lejeune, ITRB 2021, S. 13.
64 CPRA Sec. 1798.140 (m).
65 CPRA Sec. 1798.140 (z) (ae).
66 CPRA Sec. 1798.135 (c) (4).
67 CPRA Sec. 1798.199.10.
68 Ausführlich: Lejeune, ITRB 2021, S. 13, 14 ff.
69 Pub. L. 107-56, 115 Stat. 272.

lerweile ist der USA FREEDOM ACT[70] als Nachfolgegesetz in Kraft getreten, allerdings ist der Einfluss der Sicherheitsbehörden auf den Datenverkehr nach dem CLOUD-ACT[71] gleich geblieben. Diese können ohne richterliche Anordnung auf alle Daten zugreifen, die auf Servern in den USA gespeichert sind.[72] Ebenso kann sich ein Herausgabeverlangen auch auf E-Mails und andere Kommunikationsinhalte von Cloud-Storage- und Cloud-Computing-Dienste erstrecken, die dem Zugriff und der Kontrolle von US-Unternehmen unterliegen, sich jedoch auf ausländischen Servern befinden. Gerade deshalb erweist sich der Datentransfer aus der EU in die USA als besonders problematisch[73], jedoch auch das Verwenden amerikanischer Cloud-Anbieter.

Der CLOUD-Act stellt klar, dass US-Anbieter elektronischer Kommunikations- oder Remote-Computing-Dienste dazu verpflichtet sind, sämtliche in ihrem Besitz, Gewahrsam oder ihrer Kontrolle (posession, custody or control) befindlichen Daten offenzulegen und zwar unabhängig davon, ob die Daten innerhalb oder außerhalb der USA gespeichert sind (Title 18 U. S. C. § 2713). Der CLOUD Act eröffnet den betroffenen Unternehmen die Möglichkeit, das Herausgabeverlangen unter gewissen Voraussetzungen abzulehnen (sog. motion to quash).[74] Eine Ablehnung ist nach Title 18 U. S. C. § 2703(h)(2)(A) möglich, wenn das Herausgabeverlangen Daten von Nicht-US-Bürgern oder nicht in den USA ansässigen Personen betrifft und zudem die Offenlegung das erhebliche Risiko der Verletzung der Gesetze einer „qualifizierten ausländischen Regierung“ (qualifying foreign government) begründet. Als „qualifizierte ausländische Regierungen“ gelten jedoch nur Staaten, mit denen die USA ein Executive Agreement im Sinne von Title 18 U. S. C. § 2523 abgeschlossen haben, wozu die EU nicht gehört.[75] Beim Fehlen eines Executive Agreements sieht der CLOUD Act nach § 103(c) nur sehr beschränkte Möglichkeiten zur Abwehr des Herausgabeverlangens vor.

Der exterritoriale Anwendungsbereich der Zugriffsrechte ist demnach weit. Selbst wenn die zur Herausgabe verlangten Daten bei Anbietern außerhalb der USA gespeichert sind, können – wie aufgezeigt – Zugriffsrechte von US-Behörden bestehen. Zur Begründung des Zugriffsrecht reicht jeglicher Mindestkontakt eines Cloud-Storage oder Cloud-Computing-Dienstes zu den USA aus, zum Beispiel im Konzernverbund aber auch die vorrübergehende Anwesenheit eines Mitarbeiters in den USA.[76]

---

70 Pub. L. 114-23, 129 Stat. 268, abrufbar unter: https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf, zuletzt abgerufen am 8.02.2022.
71 Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, Stat. 2383 abrufbar unter https://www.congress.gov/bill/115th-congress/senate-bill/2383/text, (zuletzt abgerufen am 8.2.2022; ausfüphrlich dazu Gausling MMR 2018, 578.
72 Foreign Intelligence Surveillance Act i.V.m. der Executive Order 12333.
73 EuGH, Urteil vom 16. Juli 2020 – C-311/18 – (Schrems II).
74 Ausführlich: Determann/Nebel CR 2018, 408, 410.
75 Ein solches Executive Agreement besteht allein mit dem Vereinigten Königreich.
76 Voigt, MMR 2014, 158, 160.

Darüber hinaus kann – selbst wenn kein rechtlicher oder tatsächlicher Anknüpfungspunkt eines Cloud-Anbieters zu den USA besteht, die Herausgabe von Daten im Zuge eines Rechtshilfeabkommens erfolgen, wobei dann – ähnlich wie in Deutschland – Straftaten die Grundlage eines solchen Herausgabeabkommens bilden müssen. Solche Verpflichtungen stehen regelmäßig außerhalb des Datenschutzes.

4.3 Datensouveränität in China

4.3.1 Datenschutz

In China ist im Jahr 2021 das PERSONAL INFORMATION PROTECTION LAW (PIPL)[77] in Kraft getreten, das als erstes umfassendes Datenschutzgesetz Chinas gilt.

Das PIPL regelt die Verarbeitung personenbezogener Daten durch staatliche Einrichtungen, Unternehmen oder Einzelpersonen in China und zielt nach Art. 1 PIPL darauf ab, personenbezogene Daten besser zu schützen und über standardisierte Datenverarbeitungsvorgänge ein bereichsübergreifendes Datenschutzregime zu schaffen. Im Grunde sind viele Regelungen des PIPL mit denen der DSGVO vergleichbar,[78] seien es die Definitionen von personenbezogenen oder sensiblen Daten,[79] die Definition der Verarbeitungsvorgänge,[80] die einzuhaltenden Grundsätze[81] als Voraussetzungen für eine Datenverarbeitung,[82] die Rechte der Betroffenen,[83] die Regelungen zum Datentransfer ins Ausland,[84] der (unabhängigen) Aufsicht[85] oder die Möglichkeit Bußgelder bei Verletzung der PIPL-Vorschriften festzusetzen.[86] Allerdings gibt es auch bedeutende Unterschiede.[87] In erster Linie ist dies die exterritoriale Wirkung[88] des PIPL. Es soll auch Verarbeitungsvorgänge außerhalb Chinas erfassen, die die nationale Sicherheit oder die legitimen Interessen Chinas und seiner Bürger berühren; exterritorial ausgeführte Datenverarbeitungsvorgänge (z. B. in einem deutschen Unternehmen) unterfallen danach ebenfalls den Vorgaben des PIPL sowie dem DSL.[89]

---

77 Stanford University, Digichina, Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021, online abrufbar unter https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/, zuletzt abgerufen am 14.02.2022; und China-Briefing.com, The PRC Personal Information Protection Law (Final): A Full Translation, online abrufbar unter https://www.china-briefing.com/news/the-prc-personal-information-protection-law-final-a-full-translation/, zuletzt abgerufen am 14.02.2022

78 Eine Synopse zu den vergleichbaren Regelungen findet sich in: Johannes, ZD 2022, 90, 96 ff.

79 PIPL Art. 4 und 28.

80 PIPL Art. 4 Abs. 2.

81 PIPL Art. 5 bis 9.

82 PIPL Art. 13 und 14.

83 PIPL. Art. 44 ff.

84 PIPL Art. 38 ff.

85 PIPL Art. 60 ff.

86 Nach Art. 66 Abs. 2 PIPL können Bußgelder in Höhe von bis zu 50 Millionen Yuan (ca. 6,5 Millionen Euro) oder fünf Prozent des Jahresumsatzes verhängt werden.

87 Tabellarische Übersicht bei Johannes, ZD 2022, 90, 91.

88 PIPL Art. 3.

89 DSL Art. 2 Abs. 2.

Kapitel 3 PIPL enthält z. B. Regeln für die grenzüberschreitende Bereitstellung personenbezogener Daten. Diese ist nach Art. 38 PIPL nur in bestimmten Fällen erlaubt: entweder nach einer von der Cyberspace Administration of China (CAC) organisierten Sicherheitsüberprüfung oder nach einer Zertifizierung durch eine von der CAC akkreditierten Stelle oder nach Abschluss einer Vereinbarung mit dem Empfänger im Ausland auf der Grundlage eines vom CAC formulierten Standardvertrags oder durch speziellere gesetzliche Erlaubnis. Damit soll sich zugleich für Unternehmen außerhalb der VR China die Verarbeitung personenbezogener Daten chinesischer Bürger erschweren. Außerdem dürfen Daten, die im Festlandgebiet der VR China gespeichert sind, nicht ohne die Erlaubnis der chinesischen Behörden an die Justiz oder Exekutive anderer Länder übergeben werden,[90] während sich diese Behörden umgekehrt erhebliche Zugriffsrechte auf die Daten ausländischer Personen sichern.

Überhaupt können die Vorkehrungen des PIPL an zahlreichen Stellen durch Verwaltungsvorschriften unter Berufung auf nationale Sicherheitsinteressen außer Kraft gesetzt und Ausnahmen zu Gunsten von bestimmten Verarbeitungsvorgängen geschaffen werden u. a. zur Videoüberwachung, der Datenlokalisation, dem Profiling und Blacklisting,[91] so dass der zunächst eingeräumte Datenschutz quasi „durch die Hintertüre“ kassiert werden kann.

4.3.2 Zugriffsrechte staatlicher Behörden

Neben dem PIPL ist die Datensicherheit sowie die Zugriffsrechte der chinesischen Behörden weitgehend im DATA SECURITY LAW (DSL)[92] angesprochen, welches als Datensicherheitsgesetz dem Schutz und der Sicherheit wichtiger Daten mit Bedeutung für die nationale Sicherheit dient und darin u. a. umfassende Zugriffsbefugnisse chinesischer Sicherheitsbehörden auf alle Formen von erhobenen Daten definiert.[93]

Das wichtigste Element des DSL ist das sog. Datenklassifizierungssystem (Art. 21 DSL), mit dem die chinesische Regierung verschiedene Arten von Daten auf der Grundlage ihrer Bedeutung klassifizieren und einen Schutz- und Sicherheitsstandard für jede Datenklasse veröffentlichen wird; derzeit ist das noch nicht geschehen. Darüber hinaus legt es aber auch Sicherheitsverpflichtungen für Datenverarbeitende im Allgemeinen fest (Art. 27 ff. DSL, u. a. Einrichtung eines Managementsystems für Datensicherheit, regelmäßige Risikobewertung, Berichts- und Meldepflichten), die durch nationale Leitlinien weiter ausgestaltet werden. Nach Art. 33 DSL müssen Vermittler von Datentransaktionen die Identität der an der Transaktion beteiligten Parteien überprüfen, eine Be-

90 PIPL Art. 41.
91 Profiling ist das Anlegen von Datensätzen über Personen. Blacklisting ist das Sammeln von „negativen Daten“, um eine Person von bestimmten Aktivitäten, Zugängen u.ä. auszuschließen.
92 Stanford University, Digichina, Translation: Data Security Law of the People’s Republic of China (Effective Sept. 1, 2021), online abrufbar unter https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/,zuletzt abgerufen am 14.02.2022.
93 DSL Art. 35 und 36.

schreibung der Datenquelle einholen und eine Dokumentation vorlegen. Unternehmen, die Datentransaktionen durchführen wollen, müssen erforderlichenfalls die spezialgesetzlich vorgeschriebenen Lizenzen oder Qualifikation erwerben.[94] Die Verantwortlichen müssen bei Anfragen der Organe der öffentlichen Sicherheit und der nationalen Sicherheitsorgane kooperieren, was eben auch die Herausgabe von Daten mit einschließt.[95]

Dabei gilt das DSL nach Art. 2 Abs. 2 DSL auch für Datenverarbeitungsaktivitäten außerhalb Chinas. Es sollen bestimmte, gegen die Interessen Chinas und seiner Bürger gerichtete und extraterritorial ausgeführte Datenverarbeitungsaktivitäten dem Sanktionsmechanismus des DSL unterliegen. Insofern müssen auch ausländische Unternehmen, die Daten über chinesische Bürger verarbeiten oder deren Datenverarbeitungsvorgänge sich auf die VR China bzw. chinesische Einrichtungen oder Bürger auswirken, die Sicherheitsverpflichtungen des DSL erfüllen, um Sanktionen zu entgehen.

Insofern sichert sich auch China – aber deutlich weitergehender als die USA – über das DSL umfangreiche Zugriffsrechte auf Daten, die in Europa zu chinesischen Bürgern oder Institutionen gesammelt werden. Zur Begründung des Zugriffsrechts chinesischer Behörden reichen demnach rechtliche, aber auch rein tatsächliche Kontakte eines exterritorialen Cloud-Storage oder Cloud-Computing-Dienstes zu China aus.

4.4 Zwischenfazit internationaler Vergleich Datensouveränität

Datensouveränität der Individuen, verstanden als Schutz personenbezogener Daten und dem Zugriff staatlicher Behörden auf diese Daten ist in allen drei betrachteten Weltregionen reguliert. EU-Bürger werden dabei besonders stark geschützt. Dies geschieht:

- einerseits durch den Schutz personenbezogener Daten vor ungewollten Datenzugriffen und Datenverwendungen durch Unternehmen, und
- anderseits vor dem Zugriff staatlicher Behörden denen nur ausnahmsweise bei strafrechtlichen Verfahren und nach sorgfältiger Abwägung widerstreitender Interessen der Zugriff gestattet wird.

Individuen in China werden ebenso vor dem Datenzugriff und der Datenverwendung von Unternehmen geschützt, wobei sich das PIPL stark an der DSGVO orientiert. Unternehmen in China sind somit ähnlich starken Restriktionen ausgesetzt, personenbezogene Daten zu verwenden. Jedoch sorgen umfangreiche staatliche Zugriffsrechte für eine geringe Datensouveränität der chinesischen Bürger und Unternehmen, da staatlichen Behörden weitreichende Rechte gewährt werden, auf (personenbezogene) Daten zuzugreifen und diese zu verwenden.

94 DSL Art. 34.
95 DSL Art. 35.

Da der Datenschutz in den USA auf bundestaatlicher Ebene reguliert ist, kann dieser stark variieren. Der Datenschutz im Bundesstaat Kalifornien, zum Beispiel, weißt Ähnlichkeiten zur DSGVO auf, ist jedoch weniger restriktiv gegenüber Unternehmen. Wo nach der DSGVO ein strenges Verbot mit Erlaubnisvorbehalt (Einwilligungsvorbehalt) gilt (Opt-in-Einwilligungen), ist im kalifornischen Recht in den meisten Fällen ein Opt-out ausreichend. Ebenso gibt es, anders als in der EU, für Unternehmen keine Verpflichtung einen Datenschutzbeauftragten zu benennen. Ferner sind die Bußgelder bei einem Verstoß in keiner Weise mit dem Bußgeldrahmen des DSGVO vergleichbar.

Eine Zusammenfassung wird in Tabelle 4-1 vorgenommen.

Aus dieser Zusammenfassung stellen sich hauptsächlich zwei Fragen für den weiteren Verlauf der Studie. Zum einen stellt sich die Frage, in wie weit rechtliche Unsicherheiten für deutsche KMU bei der Anwendung der DSGVO entstehen. Zum anderen, welche Implikationen für KMU durch Zugriffsrechte von US-Sicherheitsbehörden auf Daten die durch amerikanische Unternehmen gespeichert werden entstehen, besonders vor dem Hintergrund der großen Marktanteile amerikanischer Unternehmen im europäischen Cloud-Markt.

Tabelle 4-1: Datensouveränität im internationalen Vergleich (EU, USA und China)

	EU	USA	VR China
Datenschutz personenbezogene Daten	Umfassender Schutz durch DSGVO Daten muss/sollte in der EU bleiben	Auf Bundesstaatenebene reguliert, variieren daher Ähnliche Definitionen von personenbezogenen Daten zur DSGVO Gegenüber Unternehmen jedoch weitaus weniger restriktiv: opt-out Möglichkeiten reichen an vielen Stellen aus und Bußgelder bei nicht Einhaltung sehr viel geringer	Ähnliche Definitionen von personenbezogenen Daten zur DSGVO Unternehmen sind starken Restriktionen auferlegt, wie sie Daten chinesischer Bürger verwenden dürfen
Zugriff auf Daten durch staatliche Behörden	Stark reglementiert: in strafrechtlichen Verfahren ist der Zugriff ausnahmsweise nach sorgfältiger Abwägung widerstreitender Interessen gestattet	Weitgehende Zugriffsrechte für die US-Sicherheitsbehörden Auch bei Daten außerhalb der USA wenn US-Unternehmen Zugriff darauf haben	Weitreichende Zugriffsrechte auf Daten von Ausländern innerhalb Chinas PIPL kann an zahlreichen Stellen durch Verwaltungsvorschriften unter Berufung auf nationale Sicherheitsinteressen außer Kraft gesetzt werden und Ausnahmen zu Gunsten von bestimmten Verarbeitungsvorgängen geschaffen werden

Quelle: WIK-Consult

5 Rechtliche Unsicherheiten für KMU bei der Nutzung von Cloud-Diensten durch DSGVO und staatlichen Zugriffsrechten

5.1 Definition KMU

Vor dem Hintergrund das der Schutz personenbezogener Daten alle Unternehmen in Deutschland betrifft, stellt sich die Fragen, wie sich diese Thematik auf die kleinen und mittleren Unternehmen auswirkt. Die KMU ist in Deutschland ein wichtiger Wirtschaftsfaktor; Die KMU stellen ca. 3,5 Millionen Betriebe und generieren rund 61 % der Nettowertschöpfung in Deutschland.[96]

Für quantitative Merkmale gibt es in der KMU-Literatur verschiedene Definitionen. In den Beschreibungen werden zwar dieselben Faktoren (Zahl der Mitarbeiter und Umsatz bzw. Bilanzsumme) herangezogen, jedoch unterschiedliche Grenzwerte festgelegt. Die EU[97] geht davon aus, dass ein Unternehmen nicht mehr als 249 Beschäftigte und einen jährlichen Umsatz von höchstens 50 Millionen Euro oder eine Bilanzsumme von 43 Millionen Euro hat.

Die Abgrenzung des Instituts für Mittelstandsforschung (IfM) liegt bei bis zu 499 Beschäftigten und einem Umsatz von weniger als 50 Millionen Euro pro Jahr. Das IfM unterteilt hierbei in Kleinstunternehmen (maximal 9 Beschäftigte und weniger als 2 Mio. EUR Umsatz pro Jahr), kleine Unternehmen (maximal 49 Beschäftigte und weniger als 10 Mio. EUR Umsatz) und mittlere Unternehmen (maximal 499 Beschäftigte und weniger als 50 Mio. EUR Umsatz pro Jahr).[98] Zur Darstellung der Merkmale des deutschen KMU-Sektors wird auf die folgende Beschreibung des IfM Bezug genommen.

5.2 Rechtliche Unsicherheiten

Im Bereich der Datensouveränität aus Perspektive der Individuen sind rechtliche Rahmenbedingungen beim Speichern und Verarbeiten von personenbezogenen Daten, auch für KMU relevant. Beispiele von personenbezogenen Daten bei den KMU sind unter anderen die Kundendaten, Zuliefererdaten und Mitarbeiterdaten. Basis für die rechtlichen Rahmenbedingungen beim Speichern und Verarbeiten personenbezogener Daten ist die DSGVO. Sie bezieht sich auf die Verarbeitung personenbezogener Daten und muss u. a. von Unternehmen angewandt werden, die diese Daten in Deutschland verarbeiten. Das gilt auch für Kleinunternehmen und Freiberufler, die zum Beispiel nur eine eigene Webseite betreiben oder geschäftsüblichen Kundenkontakt pflegen. Aufgrund der thematischen Komplexität stellt sich für KMU häufig die Frage, ob und in wel-

96 Institut für Mittelstandsforschung (IfM), online abrufbar unter https://www.ifm-bonn.org/statistiken/mittelstand-im-ueberblick/kennzahlen-der-kmu-nach-definition-des-ifm-bonn/kennzahlen-deutschland, zuletzt abgerufen am 07.09.2021.
97 EU-Empfehlung 32003H0361.
98 IfM Bonn, 2016.

chem Rahmen welche Schutzmaßnahme geleistet werden muss (z. B. Datenschutzerklärung und Auftragsdatenverarbeitungsverträge).[99]

Kompliziert wird es dann, wenn nicht sichergestellt wird, dass die personenbezogenen Daten, die in der Cloud gespeichert und verarbeitet werden, auch in Deutschland bzw. im Binnenmarkt bleiben. Die Vorgehensweise zur Beantwortung der Frage, welche Schutzmaßnahme im Fall einer Weitergabe der Daten außerhalb der EU geleistet werden müssen, ist für die KMU durch die DSGVO vorgegeben:

1. Stufe:

Auf der ersten Stufe hat der Datenexporteur eine eigene Rechtsprüfung durchzuführen und auf dieser Grundlage festzustellen, ob die personenbezogenen Daten, die unter den Standardverträgen transferiert werden würden, im Drittland wesentlich gleichwertig geschützt sind. Bezugspunkt für diese Prüfung sind immer nur die übertragenen Daten, sodass auch nur für diese das Schutzniveau garantiert sein muss. Eine Bewertung der gesamten Rechtsordnung des Drittlandes ist also nie durchzuführen – allerdings sind diejenigen Regelungen zu bewerten, die auf die konkret übermittelten Daten anwendbar sind. Der Blick auf die konkreten Daten gilt jedoch nicht nur für das Land, das die Daten empfängt; vielmehr muss der Datenexporteur auch die gesamte Transportstrecke im Blick behalten, um das Schutzniveau bestimmen zu können. Ferner muss festgestellt werden, inwiefern betroffenen Personen im Drittland durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen, um sich gegen den Zugriff auf die Daten zu schützen. Da die Bewertung für jeden Einzelfall, d. h. für jeden Datensatz, durchzuführen ist, können sich für ein und dasselbe Empfängerland durchaus unterschiedliche Resultate ergeben.

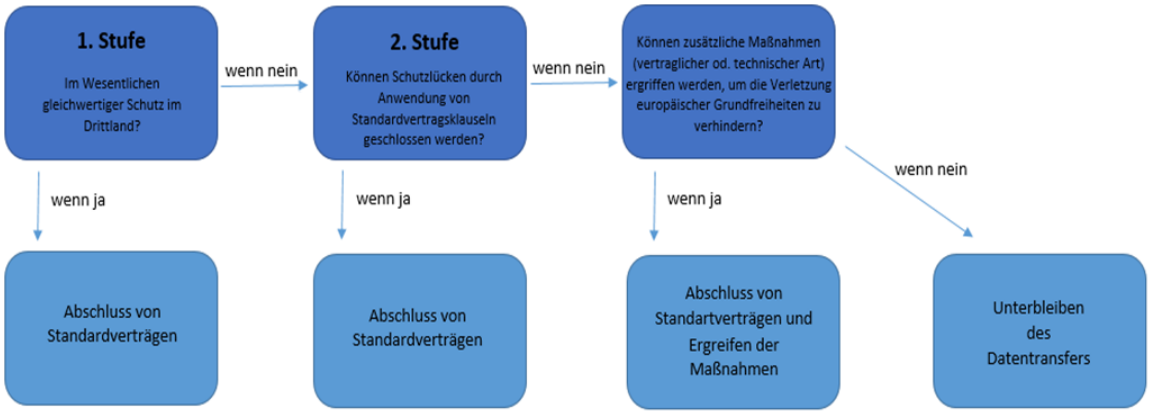
2. Stufe:

Wenn bei der Bewertung auf der ersten Stufe ein angemessenes Schutzniveau im Drittland festgestellt wird, reicht es für den Datenexporteur aus, die Standardverträge abzuschließen, um seine Pflicht aus Art. 46 DSGVO zu wahren. Wenn es hierbei jedoch Zweifel gibt, muss er in einem zweiten Schritt prüfen, ob die Schutzlücken, die er entdeckt hat, durch die Bestimmungen, die die Standardvertragsklauseln vorsehen, geschlossen werden. Besonders zu berücksichtigen – auch im Hinblick auf das Schrems II-Urteil – ist, dass auch Standardverträge als vertragliche Regelungen nur zwischen den Parteien wirken. Auf gesetzliche Pflichten, denen der Empfänger womöglich unterliegt, können sie naturgemäß keinen Einfluss haben (z. B. die Pflicht, Daten an Behörden weiterzugeben). Zudem können die Klauseln auch nicht gegen Zugriffe beim Transport

99 Siehe Betriebe-machen.de, online abrufbar unter https://betrieb-machen.de/datenschutz-fuer-kleinunternehmen-und-freiberufler/ und https://betrieb-machen.de/eugh-cookies/, zuletzt abgerufen am 23.03.2022.

der Daten zum Empfänger schützen, da die Verantwortlichen (z. B. die Netzbetreiber) keine Vertragspartei sind. Für das aufgrund des Urteils besonders im Blick zu behaltende Rechtsschutzsystem können die Verträge ohnehin keine Auswirkung haben. Die Verwendung von Standardverträgen kann daher nur einen Ausschnitt an geeigneten Garantien im Sinne der DSGVO liefern, etwa wenn bei der Datenverarbeitung des Datenimporteurs selbst besondere Gefahren bestehen. Weiteren Schutz können auch Standardvertragsklauseln nicht gewähren – mit der Konsequenz, dass der Verantwortliche neben den Standardverträgen weitere Maßnahmen ergreifen muss. Solche Maßnahmen können sowohl vertraglicher als auch technischer Natur sein. Sofern beispielsweise durch eine Verschlüsselung sichergestellt werden kann, dass staatliche Stellen auf die Daten nicht zugreifen und dadurch die Verletzung europäischer Grundfreiheiten verhindert wird, und somit ein im Wesentlichen gleichwertiges Schutzniveau hergestellt werden kann, darf der Datentransfer erfolgen, andernfalls nicht.

Abbildung 5-1: Prüfung eines angemessenen Datenschutzniveaus durch Standardvertragsklauseln



Quelle: Eigene Darstellung.

Die KMU sind nicht nur verpflichtet, eine Prüfung des angemessenen Schutzniveaus bezüglich aller Verarbeitungsvorgänge anzustellen (sog. Datenmapping“), sondern sie müssen dieses auch dokumentieren, vgl. Art. 5 Abs. 2 DSGVO. Die genaue Form „wie“ eine solche Dokumentation erfolgen soll, ist nicht vorgeschrieben, weshalb es sich anbietet, auf Vorgehensweise zu rekurrieren, die aus dem Qualitätsmanagement bekannt sind.

Es kann davon ausgegangen werden, dass diese rechtliche Situation für KMU eine Herausforderung darstellt. Stehen größeren Unternehmen meist ganze Abteilungen zur Bewältigung rechtlicher Fragestellungen zur Verfügung, sind in kleineren Unternehmen versierte Einzelpersonen oder die Geschäftsführung mit den Fragestellungen befasst.

Dabei ziehen rechtliche Gegebenheiten und Urteilsverkündungen im Bereich Datenübertragung und -schutz schnell einen oft auch komplexen Handlungsbedarf nach sich.

Für die KMU bei der Nutzung von Cloud-Diensten können folgende rechtlichen Unsicherheiten festgehalten werden:

- In allen Regionen sind bei der Nutzung von Cloud-Diensten die Datensouveränität der Individuen relevant und unterliegt ähnlichen, aber nicht den gleichen Bedingungen. Für KMU die Cloud-Dienste in mehreren Regionen nutzen, ist die Berücksichtigung der verschiedenen Bedingungen wichtig, um die Daten angemessen zu schützen.
- In Bezug auf Datenschutz in Deutschland stammen rechtliche Vorgaben im Wesentlichen aus der DSGVO.
- Für KMU die ihre Daten in der EU speichern und verarbeiten, besteht entweder die Möglichkeit, die ausschließliche Speicherung und Verarbeitung in der EU mit dem Cloud-Anbieter zu vereinbaren, oder mit dem Anbieter Regelungen zu treffen, im Fall dass die Daten außerhalb des Binnenmarkts gespeichert und verarbeitet werden. In beiden Fällen können Datensouveränität nur gelebt werden, wenn es in den Vereinbarungen zwischen Anbieter und KMU geregelt wird.
- Durch Schremms II ist die Rechtslage für KMU unübersichtlich geworden und rechtliche Unsicherheiten bestehen in Bezug auf zukünftige Gerichtsentscheidungen.
- Auf die KMU kommen des Weiteren durch die DSGVO Prüf- und Dokumentationspflichten zu. KMU müssen in der Lage sein, diese Pflichten umzusetzen. Jedoch gelten die Regelungen unabhängig davon, ob die Daten in der Cloud oder im eigenen Betrieb gespeichert und verarbeitet werden.
- Zusätzliche rechtliche Rahmenbedingen neben DSGVO ergeben sich für KMU, je nachdem in welcher Branche sie aktiv sind und vor allem, ob sie als Betreiber kritischer Infrastrukturen aktiv sind.[100]
- Wenn deutsche KMU Daten in den USA oder in China speichern, besteht grundsätzlich immer eine zusätzliche Gefahr, dass Behörden in den USA bzw. China auf die Daten Zugriff bekommen.
- Gerade vor dem Hintergrund des großen Marktanteils von amerikanischen Cloud-Anbietern am europäischen Markt besteht die zusätzliche Gefahr, dass amerikanische Sicherheitsbehörden Zugriff auf in der EU gespeicherte Daten haben. Jedoch scheint laut Expertenmeinungen[101] diese Tatsache KMU weniger bekannt und wird als allgemeine Angst vor Ausspähattacken amerikanischer Geheimdienste gesehen.

100 Diese Aussage wurde in Expertengesprächen für diese Studie bestätigt. Bei den Befragten handelt es sich um Ansprechpartner aus dem Wissenstransferbereich, die sich mit Cloud-Diensten und KMU beschäftigen.

101 Bei den Befragten handelt es sich um Ansprechpartner aus dem Wissenstransferbereich, die sich mit Cloud-Diensten und KMU beschäftigen.

6 Digitale Souveränität für KMU

In den vorangegangenen Kapiteln wurde digitale Souveränität aus der Perspektive der Individuen betrachtet, wobei der Datenschutz deren digitale Souveränität stärkt, jedoch rechtliche Unsicherheiten bei den Unternehmen schafft. Im folgenden Kapitel wird digitale Souveränität aus der Perspektive der KMU näher betrachtet. Konkrete Unterschiede ergeben sich dabei bei der Datensouveränität, da es hierbei vielmehr um die Kontrolle des Datenzugriffs und der Datenverwendung geht und weniger um den Datenschutz personenbezogener Daten.

6.1 Technologische Unabhängigkeit und Cybersicherheit

Ausgehend von der Taxonomie des Begriff der digitalen Souveränität in Kapitel 2 spielen technologische Unabhängigkeit sowie Cybersicherheit ebenso eine wichtige Rolle für KMU.

Auf der geopolitischen Ebene der digitalen Souveränität mit dem Ziel der technologischen Unabhängigkeit, ist zu beobachten, dass die KMU häufig auf den Import von Technologiegütern aus dem Ausland angewiesen sind. Nicht zuletzt zeigt der globale Mangel an Halbleitern und die damit verbunden Lieferverzögerungen von in Deutschland hergestellten Endprodukten, die Abhängigkeit der deutschen Wirtschaft von Drittstaaten beim Bezug von elektronischen Bauteilen, Leiterplatten und Elektronikkomponenten (inkl. Halbleitern).[102] Bezüglich der Speicherung von Daten können ebenso Abhängigkeiten bestehen, z. B. bei der Beschaffung von Hardware für Serverkomponenten. Dies gilt für Cloud-Anbieter aber auch für On-Premise-Lösungen.

Für Bereitsteller kritischer Infrastruktur können beispielsweise besonders Themen der Cybersicherheit relevant sein. Allerdings wachsen mit der Digitalisierung innerhalb der KMU auch die Herausforderungen, entsprechende Resilienz zu gewährleisten und somit großen Wert auf Cybersicherheit zu legen. Cloud-Lösungen könnten hier tendenziell die Cybersicherheit der Unternehmen stärken, da den Cloud-Anbietern ganz andere Ressourcen zur Verfügung stehen, Angriffe vorzubeugen oder abzuwehren.[103]

Im Rahmen der im September 2021 erschienen Cybersicherheitsstrategie des Bundesministeriums des Innern und für Heimat (BMI) im „Handlungsfeld 2“ wird explizit auf die Rolle der Wirtschaft und insbesondere der KMU eingegangen.[104] Hierbei sollen

---

102 Vgl. ifo Konjunkturprognose (2021), VDA Pressemitteilung (2021), online abrufbar unter https://www.vda.de/de/presse/Pressemeldungen/211005_Deutscher-Pkw-Markt-im-September--Rund-ein-Viertel-weniger-Neuzulassungen, und VDI Pressemitteilung (2021), online abrufbar unter https://www.vdi-nachrichten.com/technik/produktion/lieferengpaesse-belasten-maschinenbau-in-nrw/, zuletzt abgerufen am 13.01.2022.

103 Diese Aussage wurde in Expertengesprächen für dieser Studie bestätigt.

104 Bundesministerium des Innern, für Bau und Heimat (2021): Cybersicherheitsstrategie für Deutschland 2021, online abrufbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 13.01.2022.

(staatliche) Rahmenbedingungen gesetzt werden, um kritische Infrastruktur, aber auch Unternehmen vor Ransomeware-Angriffen oder anderen Schadprogrammen zu schützen. Dabei soll auch die Zusammenarbeit von Wirtschaft und Behörden gestärkt werden. Entsprechende Maßnahmen umfassen eine Unterstützung von KMU bei der Digitalisierung und der IT-Sicherheit. Denn besonders im Hinblick auf Cyberangriffe beurteilt das BMI, dass KMU diesen „[…] Herausforderungen aufgrund von Mängeln an Ressourcen und Wissen nicht ausreichend gewachsen“ sind.[105]

Für die sogenannten Hidden Champions, also KMU mit einem hohen Exportanteil und bedeutenden Marktanteilen in Nischenmärkten, ist Cybersicherheit ebenso besonders wichtig, um ihr Prozesswissen vor Cyberangriffen aus dem Ausland zu schützen.

6.2 Datensouveränität für KMU in Zusammenhang mit Cloud-Diensten

Für die Nutzung von Cloud-Diensten im Mittelstand ist vor allem die Frage der Datensicherheit und die Kontrolle über Datenzugriffe und Datenverwendung der eigenen Daten entscheidend. Für diese Studie wurde auf dieser Basis die folgende Definition von Datensouveränität in Zusammenhang mit Cloud und KMU formuliert:

> Datensouveränität der KMU im Kontext der Nutzung von Cloud-Diensten bedeutet, dass die in der Cloud liegenden Daten der KMU vor unerwünschten Zugriffen (inkl. Zugriffen durch Cloud-Anbieter, staatliche Behörden, Wettbewerber und weiteren Akteuren) geschützt sind, d. h. dass die KMU selbst über die Speicherung, Übertragung, Nutzung, Manipulation, Migration und Löschung ihrer Daten bestimmen und die Zugriffsrechte auf die Daten (inklusive personenbezogener Daten) selbstbestimmt verwalten.

Für die Frage, inwieweit die Datensouveränität durch Cloud-Nutzung beeinflusst wird, wurden Expertengespräche[106] im Rahmen dieser Studie geführt.

Aus den Expertengesprächen ging hervor, dass Daten, die bei etablierten Cloud-Anbietern abgespeichert sind, meist besser vor Cyberangriffen (von außerhalb und aus dem Unternehmen selbst heraus), Serverabstürzen oder sonstigen äußeren Einflüssen wie Brand oder Überschwemmungen geschützt sind, als jene, auf unternehmensinternen On-Premise Lösungen. Hiervon geht ein positiver Effekt der Cloud-Nutzung auf die Datensouveränität im Mittelstand aus.

Ebenso kann die Datensouveränität gesteigert werden, indem befugten Mitarbeitern durch Cloud-Lösungen die Möglichkeit gegeben wird, auf Unternehmensdaten vereinfacht zuzugreifen, zum Beispiel von unterwegs oder aus dem Homeoffice heraus. Dem Unternehmen können durch Cloud-Lösungen ebenso Möglichkeiten gegeben werden, Unternehmensdaten umfangreicher zu verarbeiten.

---

105 BMI (2021), S. 61, Absatz 1.

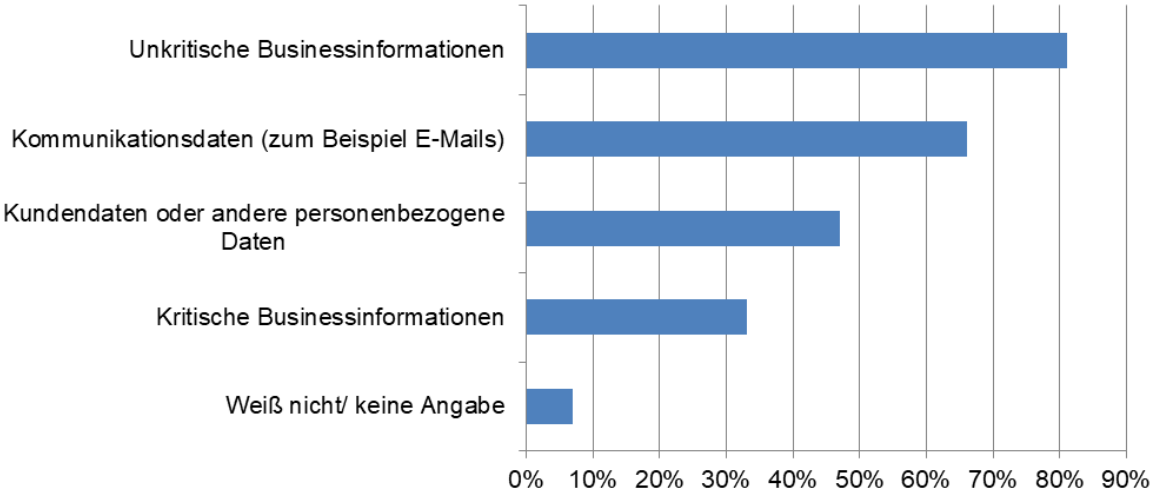
106 Bei den Befragten handelt es sich um Vertreter relevanter Verbände und Ansprechpartner aus dem Wissenstransferbereich, die sich mit Cloud-Diensten und KMU beschäftigen.

Dennoch wird ein Kontrollverlust beim Datenzugriff und der Datenverwendung von den KMU wahrgenommen, welcher begründet und unbegründet sein kann. Kommt es zu Serverausfällen bei Cloud-Anbietern oder können Mitarbeiter des Unternehmens aufgrund von Verbindungsproblemen keine Verbindung zu den Cloud-Servern aufbauen, dann gefährdet dies die Datensouveränität des Unternehmens. Ebenso können Kontrollverluste über den Datenzugriff entstehen, wenn Cloud-Anbieter keine Interoperabilität und Portabilität der Daten gewährleisten und „Lock-in"-Effekte entstehen.

Kontrolle über den Datenzugriff und die Datenverwendung ist daher eher gegeben, wenn Unternehmen Infrastrukturen und Entwickler-Plattformen (IaaS und PaaS) nutzen können und ihre eigene Software dazu entwickeln. So können „Lock-in"-Effekte eher noch entgangen werden. Diese setzt jedoch hohe IT-Kompetenzen im Unternehmen voraus.

Beispielhaft zeigt Abbildung 6-1, dass neben unkritischen Geschäftsinformation, die unter den in Cloud-Lösungen gespeicherten Daten laut Unternehmensbefragung am häufigsten abgelegt werden, auch Kommunikationsdaten, Kundendaten und kritische Geschäftsinformationen auf Cloud-Lösungen abgelegt werden (bei der Betrachtung werden alle Unternehmensgrößen beachtet, nicht nur KMU). Es zeigt sich, dass Unternehmen zwischen Daten differenzieren und abwägen, welche sie in Cloud-Lösungen speichern wollen.

Abbildung 6-1: Welche der Art von Daten werden auf der Cloud gespeichert



Quelle: Statista (2022). Basis: Unternehmen in Deutschland die Public-Cloud-Lösungen nutzen, n=226. Befragungszeitraum November 2018 bis Januar 2019.

Ein weiterer Kontrollverlust bei der Nutzung von Cloud-Lösungen kann durch den Datenzugriff staatlicher Behörden erfolgen, was jedoch laut Expertenmeinung für KMU weniger im Vordergrund steht. Eine Umgehung dessen kann neben der serverseitigen Verschlüsselung eine Ende-zu-Ende Verschlüsselung sein, bei der nur das Unternehmen selbst über den Schlüssel verfügt. Jedoch kann in solchen Fällen ein Support auf Seiten der Cloud-Anbieter nur sehr eingeschränkt erfolgen.

Eine abschließende Prüfung, inwieweit Cloud-Lösungen die digitale Souveränität der KMU beeinflusst, kann durch die Unternehmensbefragung im nächsten Arbeitspaket durchgeführt werden.

Exkurs: Allgemeine Nutzung von Cloud-Diensten bei KMU

Mit der voranschreitenden digitalen Transformation der KMU gewinnen Cloud-Dienste an Bedeutung. Im Jahr 2020 nutzten 32 % der kleinen und mittlere Unternehmen Cloud-Dienste, im Vergleich zur Vorbefragung in 2018 ergibt dies eine Steigerung von 10 Prozentpunkten.

Da es mehrere Argumente für KMU gibt, auf Cloud zu setzen, besteht hier zumindest in der Theorie erhebliches Potential. Viele KMU leiden unter Fachkräftemangel und/oder haben keine eigene IT-Abteilung und setzen auf externe IT-Dienstleister. Mit Cloud-Diensten besteht die Chance, die Digitalisierung mit weniger eigenen Fachkräfte voranzutreiben.

Cloud-Lösungen können KMU die Möglichkeit bieten, auch mit geringerem IT-Wissen beispielsweise cloudbasierte KI-as-a-Service Anwendungen zu nutzen. Weitere Chancen identifizieren Lindner und Leyh[107] im Rahmen eines Themenclusters zu Cloud-Computing in KMU. Dabei werden auch Studien, die sich mit KMU in anderen Ländern befassen, betrachtet. Beispielsweise beleuchten Yu et al.[108] die Chancen von Cloud-Computing in China und befragten dort 107 KMU. Ein großer Vorteil wird in der Cloud-Nutzung bei der Arbeit von verschiedenen Standorten gesehen. Zudem kann eine flexible Skalierung vorgenommen werden. Werth et al.[109] erwarten eine bedeutende Nutzung von Cloud-Lösungen in deutschen Consultingunternehmen. Diese Branche erscheint insbesondere wegen der hohen Reisetätigkeit als gutes Einsatzgebiet. Hier kann mithilfe von Cloud-Lösungen eine hohe Erreichbarkeit geschaffen werden, die einen Wettbewerbsvorteil darstellen kann. Insgesamt leiten Lindner und Leyh[110] aus der Nutzung von Cloud-Diensten Vorteile wie den unbegrenzte Zugriff auf Dokumente und Daten und damit die Möglichkeit des ortsunabhängigen Arbeitens ab.

107 Lindner und Leyh (2019).
108 Yu et al. (2018).
109 Werth et al. (2016).
110 Lindner und Ley (2019).

Aus einer Studie im Bereich Handwerk[111] wird deutlich, dass befragte Handwerksunternehmen große, bisher nicht ausgeschöpfte, Potenziale von Cloud-Technologie in ihrer Branche sehen. Diese Abweichung von aktueller Nutzung und erwarteter zukünftiger Relevanz zeigt, dass aus der Perspektive der KMU noch Hemmnisse bestehen, Cloud-Technologien einzusetzen.

Eines dieser Hemmnis bei der Digitalisierung und die Nutzung von Cloud-Diensten stellen die Sicherheitsbedenken dar. Im Cloud-Monitor 2021 nannten 41 % der Unternehmen mit weniger als 100 Mitarbeitern „Schwierigkeiten bei der Umsetzung unserer Security-Anforderungen“ als Hindernis bei der Integration von Public-Cloud-Lösungen.[112] Dies bestätigt auch eine studienübergreifende Analyse: Es herrscht große Unsicherheit in nahezu allen Unternehmen insbesondere bezüglich der IT-Sicherheit und des Cloud-Computings.[113] Mit Standards zur digitalen Souveränität, wie zum Beispiel bei Gaia-X, kann das erforderliche Vertrauen geschaffen werden, um dieses Hemmnis zu beseitigen.

Viele KMU geben mangelnde Finanzierungsmöglichkeiten[114] oder die Befürchtung von Fehlinvestitionen[115] als Digitalisierungshemmnis an. Mit Cloud-Infrastruktur und -Diensten bekommen die KMU eine Lösung die geringere Anfangsinvestitionen, mehr Flexibilität, Skalierbarkeit und einen schnellerer Einsatz als eine Lösung auf dem eigenen Firmengelände („On Premise“) bietet. Die Kosten für eine Cloud-Nutzung sind leichter abzuschätzen und zu Steuern, beispielsweise wenn die Kapazitäten nur dann in Anspruch genommen werden, wenn sie auch aktiv genutzt werden. Diese Vorteile von Cloud-Angeboten können die Hemmnisse bei der Digitalisierung der KMU abbauen.

111 Runst et al. 2020a.
112 KMPG in Zusammenarbeit mit bitkom research (2021), Cloud-Monitor 2021.
113 Brockhaus et al. 2020.
114 Deutsche Industrie- und Handelskammertag DIHK (2021).
115 Priyadarshinee et al. (2017). Diese Studie bezieht sich zwar auf indische KMU, lässt jedoch auch lauf Lindner und Leyh (2019) Schlüsse für deutsche KMU zu.

7 Schlussfolgerungen

Eine Analyse zur digitalen Souveränität muss aus unterschiedlichen Perspektiven vorgenommen werden. Auf Individuumsebene steigert der Datenschutz die Datensouveränität. Für Unternehmen schafft der Datenschutz jedoch eher Rechtsunsicherheit und kann beim Umgang mit Daten einschränkend wirken.

- Unternehmen in den USA sind weniger restriktiven Datenschutzgesetzen ausgesetzt und freier beim Umgang mit personenbezogenen Daten. Unternehmen in China sind einem stärkeren Datenschutz ausgesetzt als in den USA aber weniger starkem Datenschutz als in der EU. Hinzukommt in China, dass eine größere Bandbreite an staatlichen Zugriffsmöglichkeiten auf die Daten besteht.
- Für KMU, die ihre Daten in der EU speichern und verarbeiten, besteht entweder die Möglichkeit, die ausschließliche Speicherung und Verarbeitung in der EU mit dem Cloud-Anbieter zu vereinbaren, oder mit dem Anbieter Absprachen über die vertraglichen oder technischen Schutzmechanismen zu treffen, im Fall dass die Daten außerhalb des Binnenmarkts gespeichert und verarbeitet werden.
- Auf die KMU kommen des Weiteren durch die DSGVO Prüf- und Dokumentationspflichten zu. KMU müssen in der Lage sein, diese Pflichten umzusetzen. Jedoch gelten die Regelungen unabhängig davon, ob die Daten in der Cloud oder im eigenen Betrieb gespeichert und verarbeitet werden.
- Gerade vor dem Hintergrund des großen Marktanteils von amerikanischen Cloud-Anbietern am europäischen Markt besteht die zusätzliche Gefahr, dass amerikanische Sicherheitsbehörden Zugriff auf in der EU gespeicherte Daten haben. Ende-zu-Ende-Verschlüsselungen können diesen Zugriff unterbinden, was jedoch die Supportmöglichkeiten der Cloud-Anbieter erschwert.
- „Lock-in“-Effekte können für die KMU dann entstehen, wenn Interoperabilität und Portabilität der Daten durch die Cloud-Anbieter nicht gewährleistet ist. Dies schränkt die Datensouveränität der KMU ein. Jedoch eröffnen sich den KMU durch die Nutzung von Cloud-Lösungen neue Datenzugriffs- und Datenverarbeitungsmöglichkeiten, bei gleichzeitiger tendenzieller Verbesserung der Cybersicherheit.

Inwieweit Cloud-Lösungen KMU in ihrer digitalen Souveränität fördern oder ob Unternehmen eine Gefährdung ihrer digitalen Souveränität durch Cloud-Nutzung sehen, wird anhand der Ergebnisse aus der Unternehmenserhebung im nächsten Themenfeld analysiert.

8 Referenzen

Baischew, D., Kroon, P., Lucidi, S. Märkel, C., Sörries, B. (2020): Digital Sovereignty in Europe – a first benchmark, Wik-Consult Report, online verfügbar unter https://www.wik.org/fileadmin/Studien/2021/Digital_Sovereignty_Report.pdf, zuletzt abgerufen am 13.01.2022.

BMI (2021): Cybersicherheitsstrategie für Deutschland 2021, online verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=1, zuletzt abgerufen am 13.01.2022.

BMWK (2021). Schwerpunktstudie Digitale Souveränität – Bestandsaufnahme und Handlungsfelder, online verfügbar unter https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.pdf?__blob=publicationFile&v=6, zuletzt abgerufen am 02.02.2022.

Brockhaus, C. P., Bischoff, T. S., Haverkamp, K., Proeger, T., Thonipara, A. (2020): Digitalisierung von kleinen und mittleren Unternehmen in Deutschland - ein Forschungsüberblick. Göttinger Beiträge zur Handwerksforschung No. 46.

Deutsche Industrie- und Handelskammertag DIHK (2021): Digitalisierung mit Herausforderungen – Die IHK-Umfrage zur Digitalisierung online verfügbar unter https://www.dihk.de/resource/blob/35410/e090fdfd44f3ced7d374ac3e17ae2599/ihk-digitalisierungsumfrage-2021-data.pdf zuletzt abgerufen am 25.03.2022.

EU (2003). SME definition, online verfügbar unter https://ec.europa.eu/growth/smes/sme-definition_de, zuletzt abgerufen am 21.03.2022.

IfM Bonn (2016). KMU-Definition des IfM Bonn, online verfügbar unter https://www.ifm-bonn.org/definitionen-/kmu-definition-des-ifm-bonn, zuletzt abgerufen am 21.03.2022.

Heinrich Böll Stiftung (2021). Digitale Souveränität – Die EU im Wettlauf um Einfluss und Führungsrolle, online verfügbar unter https://www.boell.de/de/2021/02/10/digitale-souveraenitaet-die-eu-im-wettlauf-um-einfluss-und-fuehrungsrolle?dimension1=ds_aupo21, zuletzt abgerufen am 02.02.2022.

Ifo Konjunkturprognose (2021). Lieferengpässe und Coronawelle bremsen deutsche Wirtschaft aus, online verfügbar unter https://www.ifo.de/node/67010, zuletzt abgerufen am 07.02.2022.

KPMG/Bitkom research (2021): Cloud-Monitor 2021, online verfügbar unter https://www.bitkom-resarch.de/system/files/document/Bitkom_KPMG_Charts_Cloud%20Monitor%202021_final.pdf zuletzt abgerufen am 25.03.2022.

Lindner, D. Leyh, C. (2019): Digitalisierung von KMU – Fragestellungen, Handlungsempfehlungen sowie Implikationen für IT-Organisation und IT-Servicemanagement. HMD 56, S. 402-418, https://doi.org/10.1365/s40702-019-00502-z.

Pohle, Julia (2020). Digitale Souveränität - Ein neues digitalpolitisches Schlüsselkonzept in Deutschland und Europa, Konrad Adenauer Stiftung, online verfügbar unter https://www.kas.de/documents/252038/7995358/Digitale+Souver%C3%A4nit%C3%A4t.pdf/c04017b5-11d6-94b5-5e50-ce9f71829b1e?version=1.0&t=1608034330280, zuletzt abgerufen am 02.02.2022.

Priyadarshinee P, Raut RD, Jha MK, Kamble SS (2017) A cloud computing adoption in Indian SMEs: Scale development and validation approach. Journal of High Technology Management Research 28(2), S. 221–245.

Runst, P., & Proeger, T. (2020): Digitalisierungsmuster im Handwerk-Eine regionale und sektorale Analyse des Digitalisierungs-Checks des Kompetenzzentrums Digitales Handwerk (No. 39). Göttinger Beiträge zur Handwerksforschung.

Schwartz, P. M. (2009): Preemption and Privacy, 118 Yale L.J., abrufbar unter: http://digitalcommons.law.yale.edu/ylj/vol118/iss5/3 , zuletzt abgerufen am 18.02.2022.

Statista (2022): Welche der folgenden Daten speichert Ihr Unternehmen in der Public Cloud?; https://de.statista.com/statistik/daten/studie/714288/umfrage/umfrage-in-deutschen-unternehmen-zu-gespeicherten-daten-in-der-public-cloud/, zuletzt abgerufen am 23.11.2021.

Voigt, P. (2014): Weltweiter Datenzugriff durch US-Behörden, Auswirkungen für deutsche Unternehmen bei der Nutzung von Cloud-Diensten, MMR 2014, 158.

Werth D, Greff T, Scheer W (2016): Consulting 4.0 – Die Digitalisierung der Unternehmensberatung. HMD 53, S. 55–70.

Yu Y, Li M, Li X, Zhao JL, Zhao D (2018): Effects of entrepreneurship and IT fashion on SMEs' transformation toward cloud service through mediation of trust. Information Management 55(2), S. 245–257.

WIK-Consult • Bericht

Studie für die Bundesnetzagentur

Strategische Bedeutung von Cloud-Diensten für die digitale Souveränität von KMU

Teil 3 – Empirische Erhebung KMU zu Cloud-Diensten und digitaler Souveränität (Az: 2021/008/Z25-3)

Autoren:

Serpil Taş
Dr. Lukas Wiewiorra

Claus Mayerböck
(uzbonn)

Bad Honnef, August 2022

WIK CONSULT

Impressum

WIK-Consult GmbH
Rhöndorfer Str. 68
53604 Bad Honnef
Deutschland
Tel.: +49 2224 9225-0
Fax: +49 2224 9225-63
E-Mail: info@wik-consult.com
www.wik-consult.com

Vertretungs- und zeichnungsberechtigte Personen

Geschäftsführerin	Dr. Cara Schwarz-Schilling
Direktor	Alex Kalevi Dieke
Direktor Abteilungsleiter Netze und Kosten	Dr. Thomas Plückebaum
Direktor Abteilungsleiter Regulierung und Wettbewerb	Dr. Bernd Sörries
Leiter der Verwaltung	Karl-Hubert Strüver
Vorsitzender des Aufsichtsrates	Dr. Thomas Solbach
Handelsregister	Amtsgericht Siegburg, HRB 7043
Steuer-Nr.	222 / 5751 / 0926
Umsatzsteueridentifikations-Nr.	DE 329 763 261

Inhaltsverzeichnis

Abbildungen

Tabellen

Zusammenfassung

Das Ziel dieser Studie ist es, die Bedeutung von Cloud-Diensten, die insbesondere von international tätigen Hyperscalern angeboten werden, für die digitale Souveränität von KMU (kleinen und mittleren Unternehmen) zu bewerten. Dieser Bericht ist der dritte von drei Teilberichten und beleuchtet die Praxis der KMU im Umgang mit Cloud-Diensten Hierfür wurden KMU in Deutschland befragt. Die Ziehung der Stichprobe erfolgte auf der Grundlage von Quoten für ausgewählte Merkmale der Grundgesamtheit, um für diese eine repräsentative Zusammenstellung der KMU-Landschaft in Deutschland zu ermöglichen.

Cloud-Dienste werden zunehmend relevanter – auch für KMU in Deutschland. Vor allem KMU, die in der Branche Information und Kommunikation tätig sind, sowie KMU, die Finanz- und Versicherungsdienstleistungen oder freiberufliche, wirtschaftliche, technische und wissenschaftliche Dienstleistungen erbringen, verwenden bereits heute mehrheitlich Cloud-Dienste.

Die Nutzung wird häufig durch die Aussicht, mit Hilfe von Cloud-Diensten einen geräte-, zeit- und ortsunabhängigen Zugriff auf Daten und Anwendungen zu erlangen, motiviert. Ein weiterer wichtiger Motivator ist zudem der erleichterte Daten- und Informationsaustausch innerhalb des Unternehmens, der durch Cloud-Dienste möglich wird. Dies wird besonders relevant, wenn Mitarbeiter an verschiedenen Standorten tätig sind. Es zeigt sich, dass Unternehmen mit mehreren Standorten tendenziell eher Cloud-Dienste adoptieren als Unternehmen mit einer geringen Anzahl an Standorten.

Eine einheitliche Cloud-Strategie gibt es unter den KMU jedoch nicht. Vielmehr scheinen Cloud-Dienste aber auch Cloud-Anbieter je nach individuellen Bedürfnissen miteinander kombiniert zu werden. Relevant sind jedoch insbesondere Cloud-Dienste auf der Softwareebene. Auf dieser Ebene werden den KMU vorgefertigte Softwarelösung angeboten, die über die Cloud-Infrastruktur des Anbieters betrieben werden.

Im Wesentlichen werden Cloud-Dienste von KMU derzeit zur reinen Datenspeicherung bzw. -sicherung und / oder für Office- und Kollaborationsanwendungen verwendet. Gespeichert und verarbeitet werden sowohl personen- als auch unternehmensbezogene Daten. Beide Datentypen können kritisch für das Unternehmen sein. Personenbezogene Daten sind zudem durch die Datenschutz-Grundverordnung in Europa besonders geschützt. Daher spielte bzw. spielt für nahezu alle der KMU, die Cloud-Dienste aktuell verwenden oder dies planen, Daten- und Informationssicherheit sowie Datenschutz eine entscheidende Rolle bei der Auswahl des Cloud-Anbieters. Nichtsdestotrotz entscheidet sich ein nicht unbedeutender Anteil an KMU für Dienste nicht-europäischer Cloud-Anbieter, obwohl viele dieser KMU Nachteile in der IT- / Informations- und Datensicherheit sehen sowie Bedenken hinsichtlich der Rechtssicherheit und des Mangels an Transparenz haben.

1 Einführung: Themenfeld 3

Im Mittelpunkt dieses Teilberichts steht eine empirische Erhebung zur Nutzung von Cloud-Diensten unter KMU sowie zur Relevanz der digitalen Souveränität in diesem Kontext. Zu diesem Zweck wurde eine Befragung von KMU in Deutschland von Anfang Mai bis Anfang Juni durchgeführt. Die Befragung wurde als CATI-Befragung mit Hybrid-Option aufgesetzt.[1] Zu diesem Zweck wurde die Stichprobe repräsentativ anhand von Quoten für ausgewählte Merkmale der Grundgesamtheit ausgestreut.

Die nachfolgenden Kapitel fassen die Ergebnisse der Befragung zusammen. Nach einer Einleitung in die Methodik in Kapitel 2, folgt in Kapitel 3.1 eine Bestandsaufnahme der Nutzung von Cloud-Diensten unter KMU. Die Kapitel 3.2 und 3.3 befassen sich mit dem Kenntnisstand der KMU zu Datenschutz- und Datensicherheitsregelungen sowie ihrer Einstellung zur digitalen Souveränität.

Der Teilbericht schließt mit einem Kapitel, welches die Schussfolgerungen aus der Analyse zusammenfasst.

1 Die KMU hatten ebenfalls die Möglichkeit den Fragebogen online auszufüllen, sollten ein Telefonat von Seiten der KMU nicht möglich sein.

2 Methodik

Um die Nutzung von Cloud-Diensten unter KMU in Deutschland zu bewerten, wurden mittels eines Unternehmensbefragung Primärdaten erhoben. Der Fragebogen wurde konzipiert, um Erkenntnisse zu der Adoption von Cloud-Diensten, den Hemmnissen und Treibern bei der Nutzung von Cloud-Diensten, dem Kenntnisstand der KMU zu Datenschutz- und Datensicherheitsregelungen, sowie dem Verständnis und der Einstellung von KMU zu digitaler Souveränität abzuleiten.

In den nachfolgenden Abschnitten werden die Stichprobe, die Datenerhebung sowie das Fragebogendesign beschrieben.

2.1 Grundgesamtheit und Stichprobe

Die Zielgruppe für die Untersuchung waren KMU in Deutschland, basierend auf der Definition der Europäischen Kommission. Die Europäische Kommission grenzt KMU von Großunternehmen durch Schwellenwerte im Jahresumsatz und in der Beschäftigungszahl ab. So gehören Unternehmen, die weniger als 250 Mitarbeiter beschäftigen und einen Jahresumsatz von bis zu 50 Millionen Euro verzeichnen, zu den KMU in Deutschland.[2] Aktuellen Statistiken zu folge fallen etwa 3,5 Millionen Unternehmen unter diese Definition; dies entspricht etwas mehr als 99 % des gesamten Unternehmensbestands in Deutschland.[3]

Im Rahmen der Befragung wurden Vertreter von insgesamt 505 KMU in Deutschland aus neun verschiedenen Branchen telefonisch interviewt.[4] Bei der Stichprobenziehung wurde ein zweistufiges Verfahren angewandt. Zunächst wurde eine Bruttostichprobe an geschichteten, zufällig gezogenen Unternehmensadressen aus einer Unternehmensdatenbank entnommen.[5] In einem zweiten Schritt wurden aus dieser Bruttostichprobe die Interviewpartner der KMU rekrutiert.

Um eine Zusammenstellung der Stichprobe zu gewährleisten, die die KMU-Landschaft in Deutschland angemessen abbildet, wurde die Ziehung einer Quotenstichprobe veranlasst. Die Quotenstichprobe gehört zu den „nicht-zufälligen Stichproben“. Bei einer Quotenstichprobe werden mit Hilfe einzelner Merkmale, über die Vorabinformation der Grundgesamtheit vorliegen, durch Quoten die Strukturen der Grundgesamtheit in der Stichprobe nachgebildet, um anschließend Rückschlüsse auf die Grundgesamtheit ziehen zu

2 Vgl. IfM Bonn (2022a).
3 Vgl. IfM Bonn (2022b).
4 Mit eine Stichprobengröße von ca. 500 lassen sich die KMU in Deutschland angemessen abbilden. Bei der Wahl dieser Stichprobengröße wurde eine Fehlermarge von maximal + / -5 % und ein Konfidenzniveau von mindestens 95 % angesetzt.
5 Die Adressen wurden bei der Creditreform Datenbanken und Services erworben. Insgesamt wurden 6.127 Adressen aus der Datenbank beschafft. Die eingekauften Adressen wurden sowohl für den Pretest als auch für das Hauptfeld verwendet. Das Bruttosample wurde inklusive Informationen zum Namen des Unternehmens, Adresse, Telefonnummer, Ansprechpartner der 1. Führungsebene, Branche des Unternehmens (inkl. WZ-Code), Anzahl an Angestellten und Jahresumsatz geliefert.

können. Die Ausstreuung der Stichprobe für diese Studie erfolgte hauptsächlich nach dem Merkmal „Branchenverteilung“.[6] Die nachfolgende Abbildung gibt die Verteilung der Grundgesamtheit im Vergleich zur Stichprobe wieder. Da einzelne Branchen[7] weniger stark in der Grundgesamtheit vertreten sind, wurde eine Mindestfallzahl von 30 Befragungen pro Branche festgelegt.[8]

Tabelle 2-1: Merkmale – Stichprobe vs. Grundgesamtheit

	Cluster	Klassifikation der Wirtschafts-zweige (WZ-Codes)	Verteilung in der Stichprobe*	Verteilung in der Grundgesamt-heit
Branchen	Verarbeitendes Gewerbe, Bergbau und Gewinnung von Steinen und Erden, sonstige Industrie	B, C, D und E	8,71 %	8,92 %
	Baugewerbe	F	10,30 %	11,05 %
	Handel, Verkehr und Lagerei	G, H und I	24,55 %	27,49 %
	Information und Kommunikation	J	6,14 %	3,87 %
	Erbringung von Finanz- und Versicherungsdienstleistungen	K	6,14 %	2,12 %
	Grundstücks- und Wohnungswesen	L	6,14 %	5,34 %
	Erbringung von freiberuflichen, wissenschaftlichen und technischen Dienstleistungen sowie von sonstigen wirtschaftlichen Dienstleistungen	M und N	19,21 %	21,49 %
	Erziehung und Unterricht, Gesundheits- und Sozialwesen	P und Q	9,11 %	9,36 %
	Sonstige Dienstleistungen	R und S	9,70 %	10,37 %
	Gesamt	B-N, P-S	100 % (Anzahl: 505)	100 % (Anzahl: 3.535.705)
	Kategorien		**Verteilung in der Stichprobe***	**Verteilung in der Grundgesamt-heit**
Unternehmensgrößen	Kleinstunternehmen		83,56 %	86,60 %
	Kleinunternehmen		12,28 %	10,95 %
	Mittlere Unternehmen		4,16 %	2,45 %
	Gesamt		100 % (Anzahl: 505)	100 % (Anzahl: 3.535.705)

Quelle: WIK-Consult / uzbonn. IfM Bonn (2022): Branchenstruktur der Unternehmen nach Unternehmensanzahl in 2019 in Deutschland, https://www.ifm-bonn.org/fileadmin/data/redaktion/statistik/mittelstand_im_einzelnen/dokumente/Unt_2019_D_BR-STR.pdf [letzter Zugriff: 10.06.2022]. Die Wirtschaftszweige A (Land- und Forstwirtschaft, Fischerei), O (öffentliche Verwaltung, Verteidigung; Sozialversicherung), T (Private Haushalte mit Hauspersonal; Herstellung von Waren und Erbringung von Dienstleistungen durch private Haushalte für den Eigenbedarf ohne ausgeprägten Schwerpunkt), U (Exterritoriale Organisationen und Körperschaften) wurden in der Untersuchung nicht beachtet. *ungewichtete Daten.

6 Obwohl anderes als beim Merkmal „Branchenverteilung“ keine harten Quoten für das Merkmal „Unternehmensgröße“ festgelegt wurde, wurde bei der Ziehung eine der Grundgesamtheit angemessen Verteilung der Stichprobe nach Unternehmensgrößen angestrebt.

7 Die Wirtschaftszweige wurden entsprechend der Aggregate für die volkswirtschaftliche Gesamtrechnung in Branchen zusammengefasst.

8 Die Mindestanzahl wurde festgelegt, um Gruppenvergleiche zu ermöglichen.

Aufgrund der leichten Diskrepanzen zwischen den Populationsparametern „Branche“ und „Unternehmensgröße“ und den realisierten Stichprobenmerkmalen, die aus der verzerrten Ausstreuung der Stichprobe im Hinblick auf die Branchen resultiert, wurden für die Auswertungen Poststratifikationsgewichte berechnet und angewandt. Die Poststratifikationsgewichtung ist eine Technik, die in der Marktforschung eingesetzt wird, um Diskrepanzen zwischen Populationsparametern und realisierten Stichprobenmerkmalen zu minimieren.[9]

2.2 Datenerhebung

Die Befragung wurde als eine CATI-Erhebung mit Hybridoption umgesetzt. Es wurden vorrangig telefonische Interviews (CATI[10]) durchgeführt. Der Fragebogen war jedoch ebenfalls online (CAWI[11]) verfügbar. Letzteres diente dazu KMU, die sich an einer telefonischen Befragung nicht beteiligen konnten, dennoch die Möglichkeit zu geben, teilzunehmen. Insgesamt wurden allerdings lediglich N=4 Beobachtungen online erhoben.

Da die meisten befragten Unternehmen sehr klein waren, stammte die Zielperson in den KMU überwiegend aus der Geschäftsleitung. Etwa 67 % der Interviewpartner gaben an, zur Geschäftsführung oder dem Vorstand zu gehören. 11 % der Interviewpartner gehörten zur Geschäftsbereichsleitung oder Abteilungsleitung. Die restlichen Interviewpartner waren Teamleiter, Mitarbeiter oder andere.

Die Daten wurden von Anfang Mai bis Anfang Juni 2022 erhoben.

2.3 Fragebogendesign

Der Fragebogen besteht aus fünf thematischen Abschnitten. Der erste Abschnitt erfasst Information zur Nutzung von Cloud-Diensten. Die KMU wurden zunächst gebeten Auskunft über den Stand der Nutzung zu geben. Die Antworten auf diese Fragen dient dazu, die KMU im Hinblick auf die aktuelle Adoption von Cloud-Diensten in drei Nutzungsgruppen einzuordnen: 1) KMU, die Cloud-Dienste nutzen; 2) KMU, die keine Cloud-Dienste nutzen und eine Nutzung von Cloud-Diensten planen; 3) KMU, die keine Cloud-Dienste nutzen und eine Nutzung nicht planen. Diese Gruppierung ermöglicht im Verlauf der Befragung (zumindest) einzelne Fragen spezifischer auf die jeweilige Befragungsgruppe auszurichten, da davon auszugehen war, dass sich die Einstellungen und der Kenntnisstand der Befragten zum Thema Cloud-Dienste und digitaler Souveränität zwischen den oben definierten Gruppen unterscheidet.

9 Vgl. Kulas et al. (2018).
10 CATI, Computer-assisted telephone interviewing.
11 CAWI, Computer-assisted web interviewing.

Im zweiten Befragungsabschnitt werden Fragen zur Art des Cloud-Dienstes und zum Cloud-Anbieter gestellt. Darüber hinaus werden die Nutzungsgründe bzw. die Gründe der Nicht-Nutzung von Cloud-Diensten allgemein erfasst. Dazu gehört die Identifikation der Hemmnisse und Treiber der Adoption von Cloud-Diensten bei KMU. Die Bedürfnisse der KMU hinsichtlich der Ausgestaltung sowie der Nutzung von Cloud-Diensten spielt in diesem Zusammenhang eine wichtige Rolle und wird ebenfalls erfragt. Hierzu werden die Befragten gebeten, auf einer fünfstufigen Likert-Skala anzugeben, wie wichtig ihnen unterschiedliche betriebsrelevante Leistungen sowie Kriterien aus dem Bereich Sicherheit und Datenschutz bei der Wahl des Cloud-Anbieters waren und sind.

Der dritte Befragungsabschnitt dient der Erfassung des Kenntnisstands der KMU zu Datenschutz- und Datensicherheitsregelungen im Zusammenhang mit Cloud-Diensten. Für die Ermittlung der Kenntnisse wurden subjektive Messgrößen verwendet, zu der die Selbsteinschätzung gehört. In diesem Fall werden die Befragten gebeten ihren Wissensstand selbst einzustufen.

Der vierte Befragungsabschnitt befasst sich mit dem Thema digitale Souveränität. Zunächst sollen Assoziationen der KMU zu diesem Begriff und ihr Verständnis darüber erfasst werden. Daraufhin wird erörtert, welche Bedeutung KMU den Cloud-Diensten und der digitalen Souveränität für ihre Wettbewerbs- und Innovationsfähigkeit beimessen und welche Bedenken sie haben. Letztlich wird ihr Interesse an sicheren europäischen Infrastrukturen erfragt.

Der Fragebogen schließt mit einigen Fragen zur Unternehmensstruktur. Hierzu gehören Fragen, die verschiedene unternehmensspezifische Merkmale und Kennzahlen erfassen, wie Mitarbeiteranzahl, Standorte, Jahresumsatz, Wirtschaftszweige, etc.

Vor der Feldphase wurde der Fragebogen im Rahmen eines Pretests überprüft. Der Fragebogen befindet sich im Anhang dieses Berichts.

3 Befragungsergebnisse

Die folgenden Abschnitte dokumentieren die Ergebnisse aus der Befragung. Kapitel 3.1 fasst die aktuelle Nutzung von Cloud-Diensten unter KMU zusammen. Es wird ein Überblick über die Adoption von Cloud-Diensten, der unterschiedlichen Modelle und der einzelnen Anbieter gegeben. Zudem wird herausgearbeitet, welche Faktoren bei der Wahl des Cloud-Anbieters eine Rolle gespielt haben. Zudem folgt ein Einblick über die Motive und Hemmnisse der Adoption von Cloud-Diensten.

Kapitel 3.2 befasst sich hingegen mit dem Kenntnisstand der KMU zu Datenschutz- und Datensicherheitsregelungen, die für sie sowohl in der EU und Deutschland als auch in nicht-europäischen Staaten wie den USA gelten.

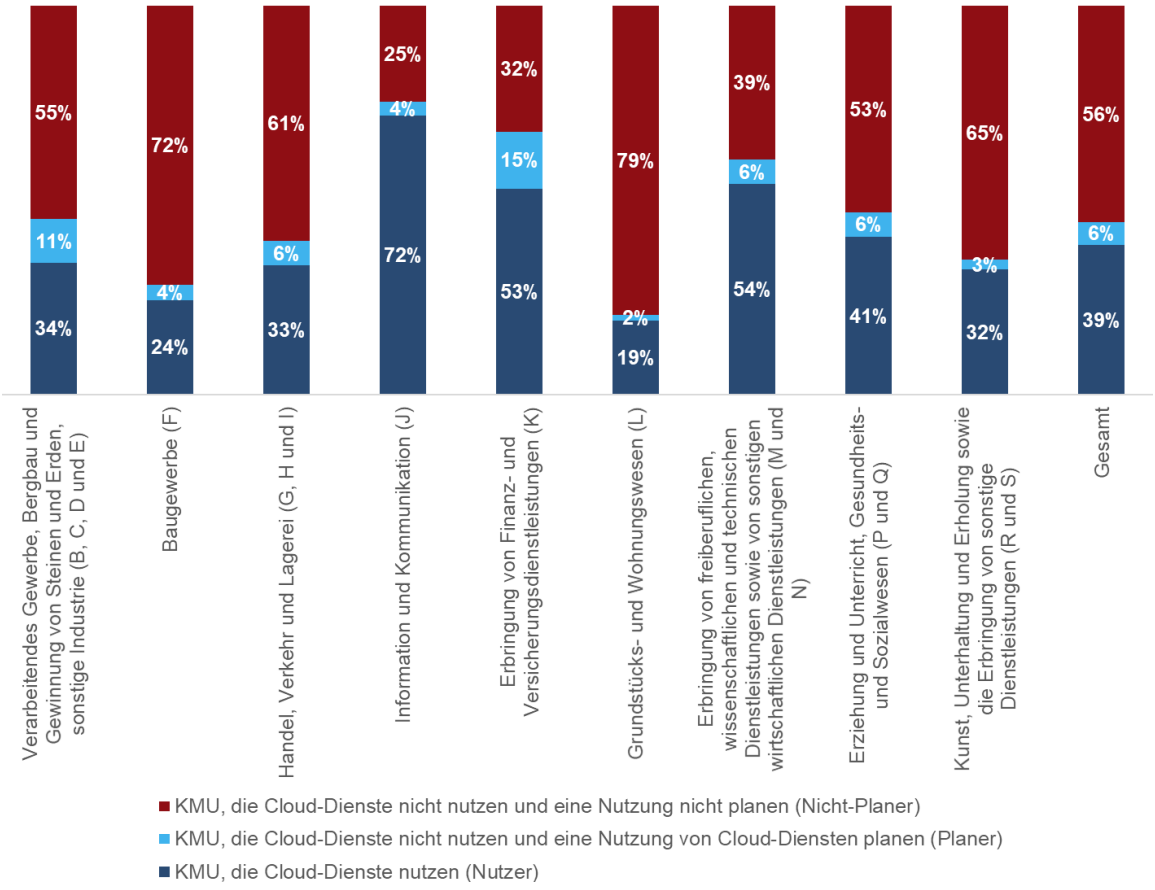
Das letzte Kapitel 3.3 geht auf die Bedeutung von digitaler Souveränität für KMU ein. Es wird untersucht, was KMU unter dem Begriff verstehen und welche Rolle digitale Souveränität in ihren Entscheidungen in Zusammenhang mit Cloud-Diensten spielt.

3.1 Nutzung von Cloud-Diensten

Nahezu 40 % der befragten KMU in Deutschland nutzt derzeit mindestens einen Cloud-Dienst; weitere 6 % planen zumindest zukünftig Cloud-Dienste zu verwenden (siehe Abbildung 3-1).

Mit Blick auf die einzelnen Branchen werden teilweise sehr starke Unterschiede in der Adoption von Cloud-Diensten deutlich. Mehr als 70 % der KMU, die in der Branche Information und Kommunikation tätig sind und immerhin jeweils mehr als 50 % der KMU, die Finanz- und Versicherungsdienstleistungen oder freiberufliche, wirtschaftliche, technischen und wissenschaftliche Dienstleistungen erbringen, verwenden heute bereits Cloud-Dienste. Dem gegenüber nutzen lediglich unter 25 % der KMU im Baugewerbe bzw. 20 % der KMU im Grundstücks- und Wohnungswesen Cloud-Dienste.

Abbildung 3-1: Nutzung von Cloud-Dienst nach Branchen



Quelle: WIK-Consult / uzbonn. N=505. Basis: Alle Befragte.

Die KMU, die aktuell Cloud-Dienste in Deutschland nutzen, sind im Durchschnitt bereits seit etwa 4,5 Jahre Anwender.[12] Etwa 61 % der KMU, die eine Nutzung von Cloud-Diensten planen, ziehen eine Einführung innerhalb eines Jahres in Betracht. Ca. 37 % würden Cloud-Dienste zu einem späteren Zeitpunkt einführen.[13]

Adoption von Cloud-Diensten

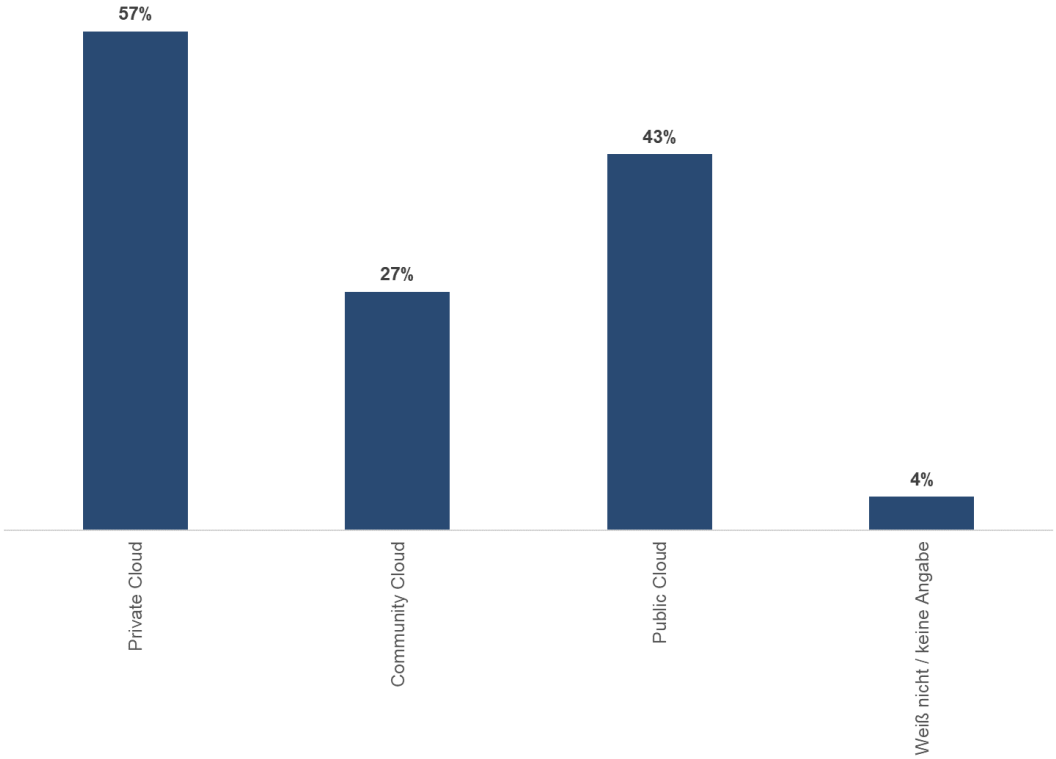
Im ersten Teilbericht dieser Studie wird erläutert, dass sich Cloud-Dienste in unterschiedliche Modelle aufteilen. Cloud-Dienste untergliedern sich zum einen nach der Art der Bereitstellung und zum anderen im Hinblick auf die jeweils gebotenen Services. Bei den Bereitstellungsmodellen werden häufig Private, Community und Public Cloud voneinander abgegrenzt, die sich u.a. in der Nutzergruppe unterscheiden. Bei der Public Cloud

12 5 % getrimmtes Mittel. N=203. Ohne Berücksichtigung von Fällen, die „weiß nicht / keine Angabe“ angegeben haben. Basis: KMU, die Cloud-Dienste nutzen.

13 N= 32. Basis: KMU, die eine Nutzung non Cloud-Diensten planen. Die restlichen KMU machen keine Angabe zum Zeitpunkt der Einführung von Cloud-Diensten.

liegt eine offene Nutzergruppe vor. Die Cloud-Infrastruktur wird in der Regel von mehreren Unternehmen geteilt, wobei jedem Unternehmen eigene virtuelle Kapazitäten zur Verfügung gestellt werden.[14] Die Private Cloud hingegen ist durch eine geschlossene Nutzergruppe charakterisiert. Die Cloud-Infrastruktur steht ausschließlich einem Unternehmen zur Verfügung bzw. wird für dieses betrieben.[15] Bei der Community Cloud wird die Cloud-Infrastruktur von Unternehmen und Institutionen, die gemeinsame Anliegen haben (z.B. Unternehmensnetzwerke, Genossenschaften), geteilt.[16]

Abbildung 3-2: Bereitstellungs- / Liefermodelle



Quelle: WIK-Consult / uzbonn. N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.

KMU, die auf die Cloud umgestellt haben oder eine Cloud-Strategie einführen wollen, entscheiden sich laut den Befragungsergebnissen am ehesten für eine Private Cloud (57 %) oder eine Public Cloud (43 %).[17] Seltener findet die Community Cloud-Lösung

14 Vgl. Arockiam et al. (2011), Biebl (2012).
15 Vgl. Biebl (2012).
16 Vgl. Arockiam et al. (2011).
17 Ähnliche Verhältnisse bei der Nutzung lassen sich auch in anderen Studien, wie bei KPMG (2022), finden. Laut KPMG (2022) nutzen im Jahr 2022 etwa 67 % Private-Cloud-Computing und weitere 14 % planen die Nutzung. Public-Cloud-Computing werden von 47 % der Unternehmen verwendet. 28% planen die Nutzung von Public-Cloud-Computing. Es ist anzumerken, dass KPMG im Unterschied zu dieser Studie nicht ausschließlich KMU befragt hat. Dort wurden Unternehmen mit 20 oder mehr Beschäftigten befragt. Dennoch sollten die in dieser Studie aufgeführten Ergebnisse zu den Bereitstellungsmodellen vorsichtig interpretiert werden. Aufgrund sehr heterogener Bezeichnungen bei der Vermarktung

Anwendung (siehe Abbildung 3-2). Nicht alle KMU entschieden sich jedoch ausschließlich für eine Form der Bereitstellung. Etwa 25 % verwenden bzw. planen mindestens zwei verschiedene Modelle zu verwenden.[18]

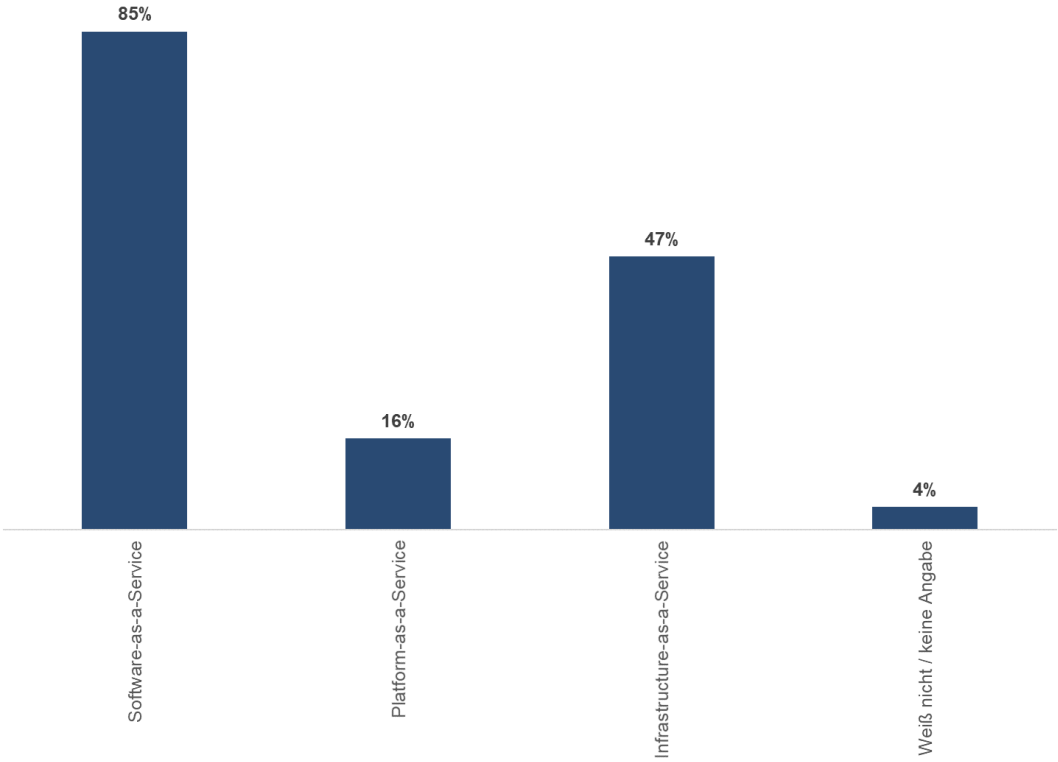
Bei den Servicemodellen lassen sich ebenfalls drei wesentliche Formen abgrenzen, nämlich Software-as-a-Service (SaaS), Plattform-as-a-Service (PaaS) und Infrastructure-as-a-Service (IaaS). Im ersten Teilbericht wird gezeigt, dass der SaaS-Markt der umsatzstärkste Cloud-Markt ist. Unter den KMU gehören Dienste der Softwareebene zu den am häufigsten verwendeten Cloud-Diensten. Beim SaaS Cloud-Modell werden den Anwendern vorgefertigte Softwarelösungen angeboten, die über die Cloud-Infrastruktur des Cloud-Anbieters betrieben werden.[19] Bekannte Beispiele dieser Art von Lösungen sind Office- bzw. Kollaborationsanwendungen wie Microsoft 365, Google Workspace oder cloudbasierte CRM-, HR-, DMS-, ERP-, Sicherheitsanwendungen etc. u.a. von Anbietern wie Salesforce, SAP, Datev, Oracle, Amagno und Sophos. Etwa 85 % der KMU verwenden oder planen die Verwendung verschiedener vorgefertigter Softwarelösungen (siehe Abbildung 3-3).

Knapp 50 % der KMU abonnieren Cloud-Dienste der Infrastrukturebene (IaaS) oder planen ein Abonnement (siehe Abbildung 3-3). Auf dieser Ebene werden den KMU in der Regel IT-Ressourcen wie Rechenleistung, Speicher oder Netze zur Verfügung gestellt.[20] Beispiel sind Elastic Computing Cloud oder Simple Storage Service von Amazon Web Services sowie Compute Engine oder Cloud Storage von Google Cloud. Der Anwender ist befähigt, Betriebssystem und weitere Software beliebig zu installieren und zu betreiben, hat jedoch nur wenig bis gar keinen Zugriff auf oder Kontrolle über Netzwerkkomponenten oder die physikalischen IT-Infrastrukturen.[21]

von Cloud-Diensten, könnten für die Befragten Schwierigkeit bei der korrekten technischen Abgrenzung der Bereitstellungsmodelle bestehen.

18 N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.
19 Vgl. Labes (2012), Hoberg et al. (2012), Bayrak et al. (2011).
20 Vgl. Biebl (2012), Bento & Bento (2011).
21 Vgl. Biebl (2012), Bento & Bento (2011).

Abbildung 3-3: Servicemodelle



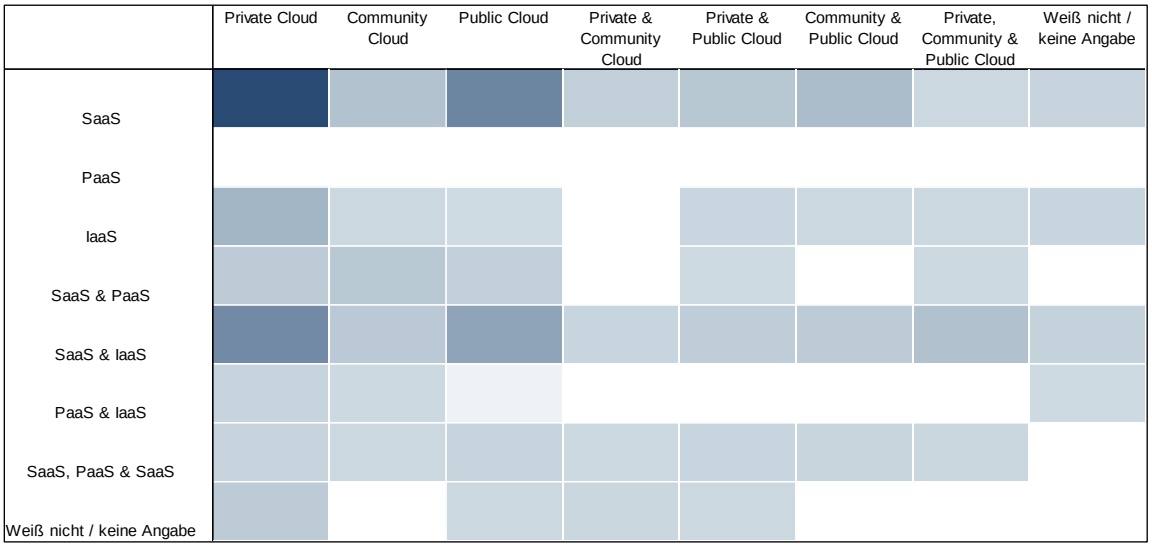
Quelle: WIK-Consult / uzbonn. N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.

Am seltensten finden Cloud-Dienste der Plattformebene Anwendung. Nur etwa 16 % der KMU, die Cloud-Dienste bereits verwenden oder dies für die Zukunft planen, entscheiden sich für PaaS-Lösungen (siehe Abbildung 3-3). Bei dieser Art des Service wird dem Anwender eine integrierten Laufzeit- oder Entwicklungsumgebung für Anwendungen bereit gestellt.[22] PaaS-Lösungen werden häufig von Entwicklern verwendet. Beispiele hierfür sind Google App Engine der Google Cloud oder AWS Elastic Beanstalk von Amazon Web Services.

Eine einheitlich angewandte Cloud-Strategie lässt sich aus den Befragungsdaten nicht eindeutig erkennen. Vielmehr neigen KMU offenbar dazu Service- und Bereitstellungsmodelle je nach Bedürfnis zu kombinieren.

22 Vgl. Biebl (2012).

Tabelle 3-1: Kombination von Service- und Bereitstellungsmodellen



Quelle: WIK-Consult / uzbonn. N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen. Lesehilfe: Schattierungen geben die Verteilung unterschiedlicher Kombinationen von Service- und Bereitstellungsmodelle wieder. Je dunkler die Blauschattierung, desto höher ist der Anteil der KMU, die die jeweilige Kombination nutzt oder plant zu nutzen. Am häufigsten vertreten ist die Cloud-Strategie, die aus einer Private Cloud in Kombination mit einer Softwarelösung steht (18 %). Die weißen Schattierungen entsprechen einem Anteil von (nahezu) 0 %.

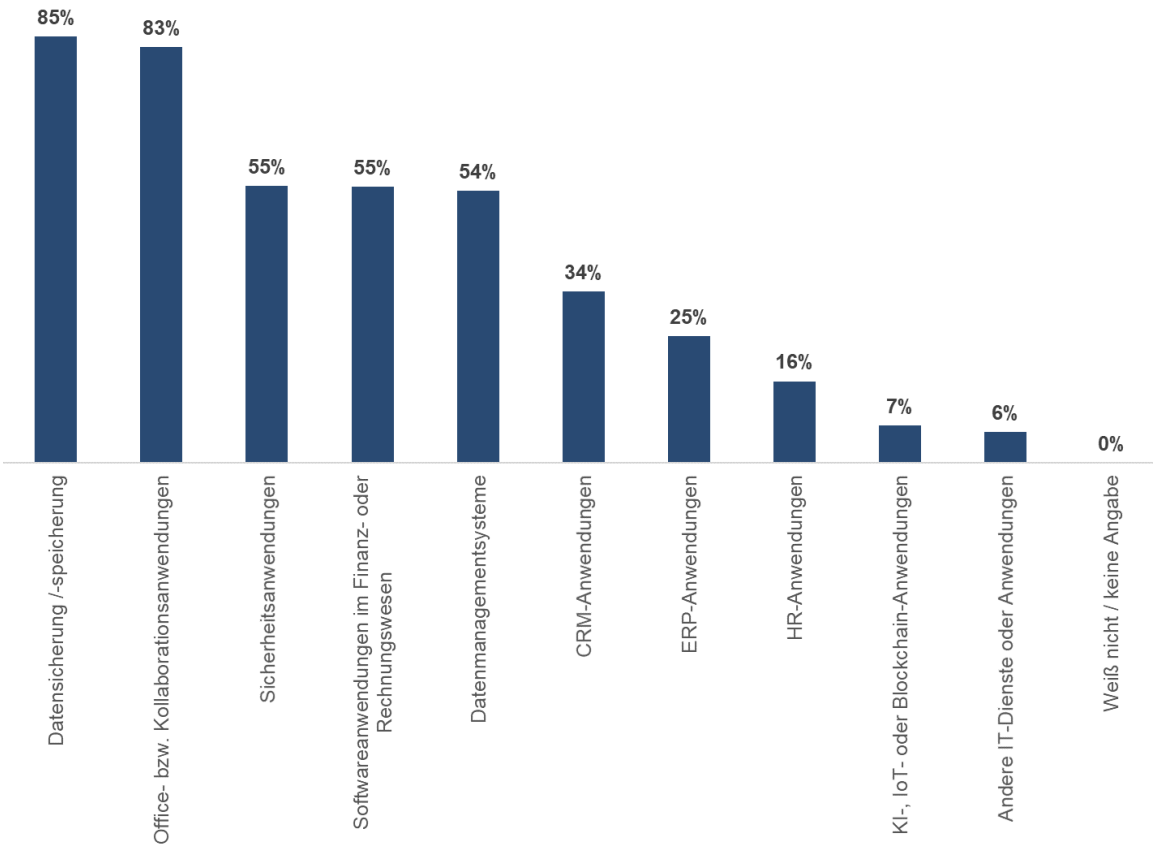
Anwendungsfälle

Die Mehrheit der KMU nutzt oder plant Cloud-Dienste vor allem zur reinen Datenspeicherung bzw. -sicherung und / oder für Office- und Kollaborationsanwendungen (inkl. Web- und Videokonferenzanwendungen), wie Microsoft 365, zu verwenden (85 % bzw. 83 %). Für KMU sind dies die klassischen Anwendungsfälle für Cloud-Dienste. Des Weiteren beziehen etwa jeweils 55 % der KMU Sicherheitsanwendungen, Softwareanwendung im Finanz- und Rechnungswesen sowie Systeme zum Datenmanagement aus der Cloud oder ziehen den Bezug in Betracht. Spezialanwendung für CRM, ERP und HR sowie neuerer Technologien wie KI, Blockchain und IoT werden vergleichsweise wenig genutzt oder in Betracht gezogen. Laut einer Befragung von KPMG (2021) konnten diese Bereiche in den letzten Jahren jedoch einige Zugewinne bei der Nutzung erzielen.[23] Denkbar wäre es, dass Cloud-Dienste dieser Art in Zukunft an Relevanz gewinnen (siehe Abbildung 3-4).

KMU verwenden Cloud-Dienste insgesamt für etwa 4,2 Anwendungsfälle.[24]

23 KMPG (2021) befragte Unternehmen mit 20 oder mehr Beschäftigten in Deutschland.
24 5 % getrimmtes Mittel. Der Median liegt hingegen bei 4 Anwendungsfällen. N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.

Abbildung 3-4: Anwendungsfälle

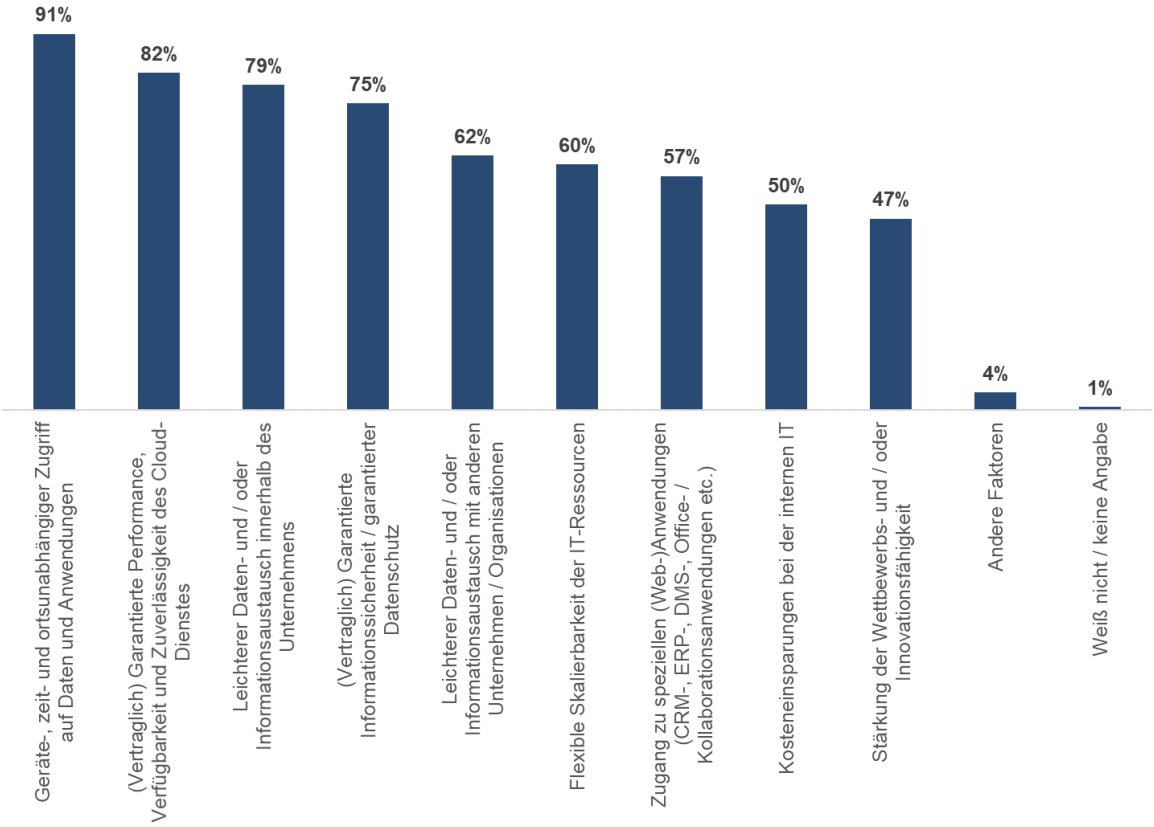


Quelle: WIK-Consult / uzbonn. N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.

Motivation

Die Nutzung selbst wird zumeist durch die Aussicht, mit Hilfe von Cloud-Diensten einen geräte-, zeit- und ortsunabhängigen Zugriff auf Daten und Anwendungen zu erlangen, motiviert. Für 91 % der KMU, die bereits Cloud-Dienste verwenden oder dies planen, ist dieser Aspekt ein wesentlicher Motivator. Ein weiterer wichtiger Motivator ist zudem der erleichterte Daten- und Informationsaustausch innerhalb des Unternehmens, der durch Cloud-Dienste möglich wird. Dies wird besonders relevant, wenn Mitarbeiter an verschiedenen Standorten arbeiten. Es zeigt sich, dass Unternehmen mit mehreren Standorten tendenziell eher Cloud-Dienste adoptieren als Unternehmen mit einer geringen Anzahl an Standorten. Für jeweils 75 % bzw. 82 % der KMU ist die vertraglich zugesicherte und garantierte Informationssicherheit, der Datenschutz und die Performance Grund für die Nutzung von Cloud-Diensten. Vergleichsweise zweitrangige Gründe für KMU sind hingegen die Stärkung der Wettbewerbs- und Innovationsfähigkeit sowie Kostenersparnisse der internen IT (siehe Abbildung 3-5).

Abbildung 3-5: Gründe für die Nutzung von Cloud-Diensten



Quelle: WIK-Consult / uzbonn. N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.

Entscheidungskriterien für die Wahl des Cloud-Anbieters

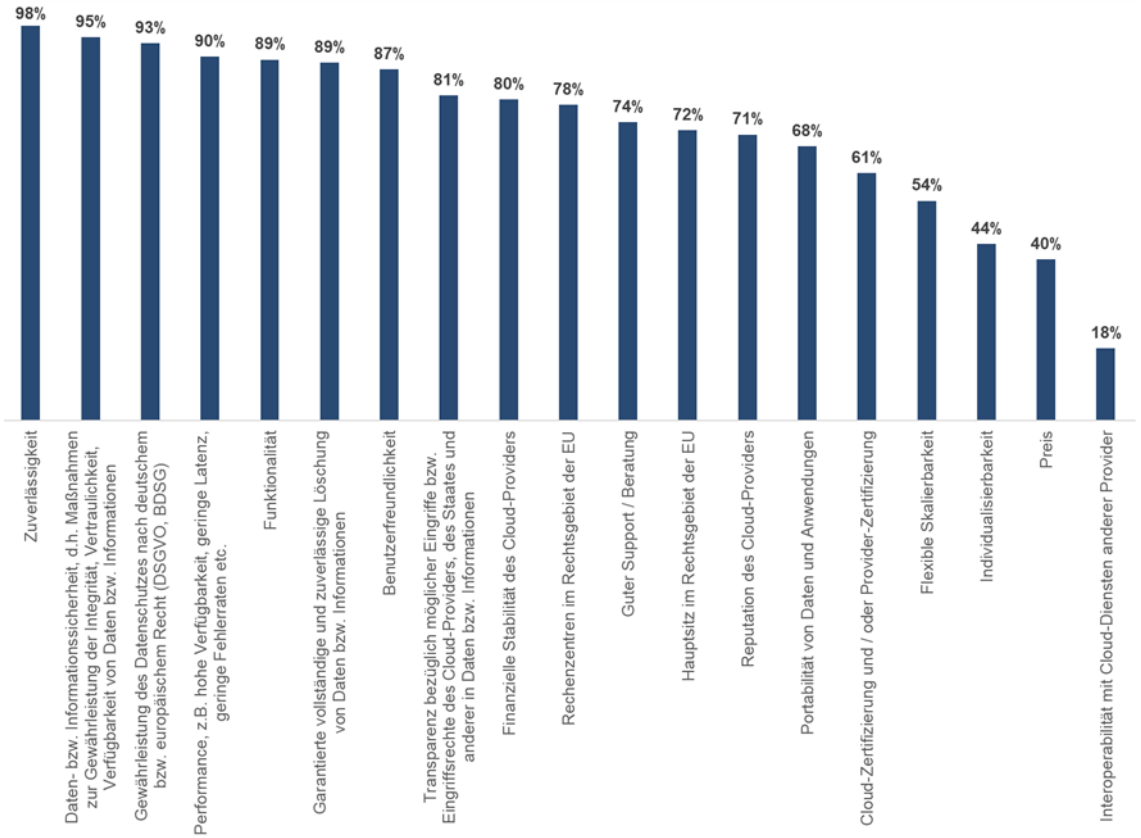
Die geringe Relevanz von monetären Faktoren bei Entscheidungen im Zusammenhang mit Cloud-Diensten bei KMU ist auch bei den Antworten der KMU zur Frage, wie wichtig der Preis für die Wahl des Cloud-Anbieters war bzw. ist, ersichtlich. Im Vergleich zu anderen Kriterien wirkt der Preis eher unbedeutend (siehe Abbildung 3-6). Dabei belaufen sich die Ausgaben der KMU, die Cloud-Dienste abonnieren oder abonnieren möchten, im Mittel auf etwa 6.000 Euro jährlich.[25]

Bereits im ersten Teilbericht werden Differenzierungsmerkmale von Cloud-Diensten herausgearbeitet. Die Untersuchung ergibt, dass vor allem die Preisgestaltung bei den wichtigsten Cloud-Anbietern komplex und intransparent ist und damit für Anwender wenig hilfreich für das Treffen einer fundierten Entscheidung. Die Befragungsergebnisse zeigen, dass insgesamt weniger KMU, die Cloud-Dienste nutzen oder die Einführung einer Cloud-Strategie planen, den Preis als wichtig für die Wahl des Anbieters einstufen als die

25 5 % getrimmtes Mittel. Der Median liegt hingegen bei 1500 Euro. N=191. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.

Performance und Zuverlässigkeit der Dienste sowie die Gewährleistung von Daten- und Informationssicherheit und des Datenschutzes (siehe Abbildung 3-6).[26]

Abbildung 3-6: Wichtigkeit unterschiedlicher Faktoren für die Wahl des Cloud-Anbieters (Anteil der Angaben „wichtig“ bis „sehr wichtig“)



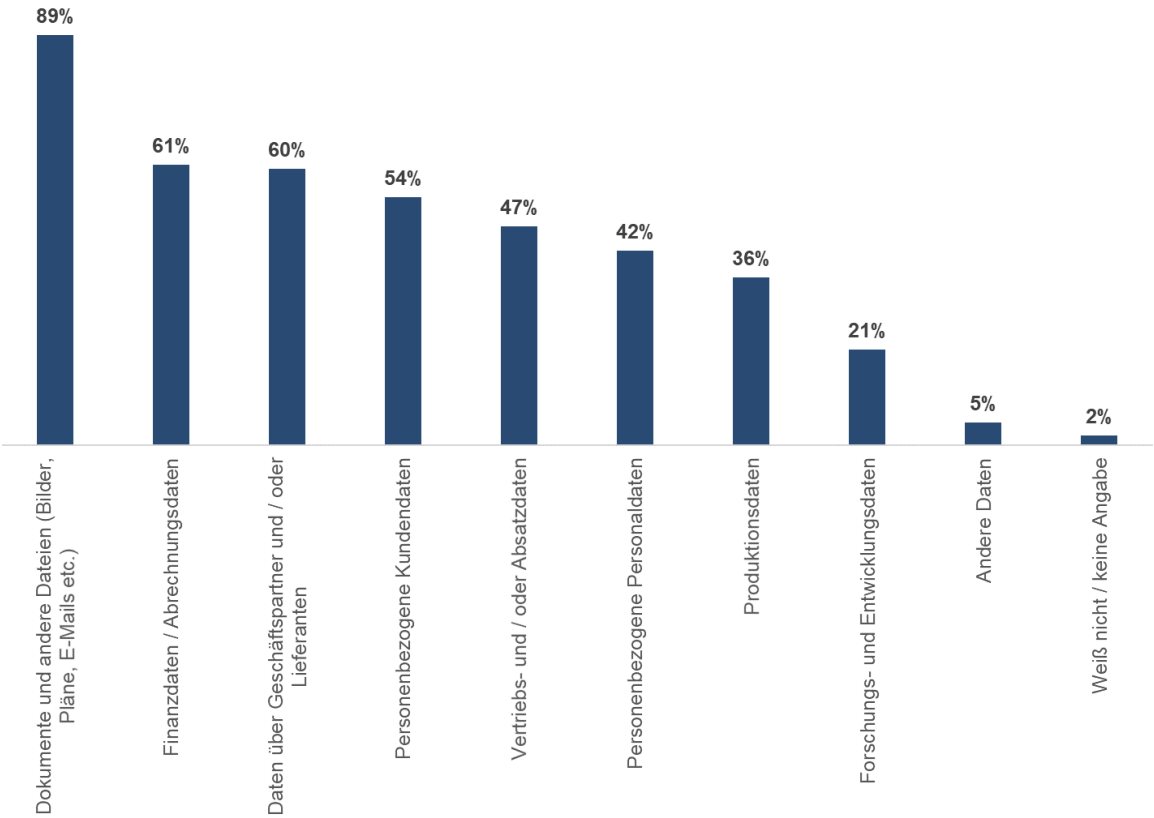
Quelle: WIK-Consult / uzbonn. N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.

Da KMU sowohl sensible, personenbezogene, aber auch unternehmensbezogene Daten und Informationen in der Cloud ablegen und verarbeiten, ist die Daten- und Informationssicherheit und der Datenschutz besonders wichtig. Vor allem personenbezogene Daten, sei es von Kunden oder Mitarbeitenden, sind stark durch Rechtsregelungen geschützt. Unternehmensdaten sind wertvoll und können auch geschäftskritisch sein, wenn sie für den reibungslosen Betrieb eines Unternehmens unerlässlich sind. Beispiele für unternehmenskritische Daten können Produktionsdaten, Finanzdaten oder Forschungs- und Entwicklungsdaten sein. Wenn geschäftskritische Daten, veröffentlicht, manipuliert oder entwendet werden, kann dies erhebliche negative Folgen für das Unternehmen mit sich ziehen.[27]

26 In zwei Studien von KPMG (2020, 2021) gelten ebenfalls Performance in diesem Fall die Leistungsfähigkeit und Stabilität der Cloud sowie Vertrauen in Sicherheit und Compliance als die wichtigsten Kriterien (97 % bzw. 95 %).

27 Vgl. Gries (2021), Ochs (2018).

Abbildung 3-7: Arten von Daten, die in der Cloud gespeichert und verarbeitet werden



Quelle: WIK-Consult / uzbonn. N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.

Etwa 60 % der KMU, die Cloud-Dienste nutzen oder eine Nutzung planen, hinterlegen derzeit oder ziehen das Hinterlegen von personenbezogene Kunden- oder Mitarbeiterdaten in der Cloud in Betracht (siehe Abbildung 3-7). Diese Daten müssen, wie oben beschrieben, rechtlich besonders geschützt werden. Verwunderlich ist daher nicht, dass Datenschutz sowie die Daten- und Informationssicherheit für jeweils mehr als 90% der KMU wichtig bis sehr wichtig für die Wahl des Cloud-Anbieters sind. Dennoch entscheiden sich etwa 70 % der KMU, die Cloud-Dienste abonnieren oder ein Abonnement planen, für nicht-europäische Anbieter – insbesondere für US-amerikanische Anbieter, welche nicht der europäischen Regelungen und Standards unterliegen.[28] Als Nachteil nicht-europäischer Anbieter wird zumeist die Rechtsunsicherheit (in Bezug auf die DSGVO, BDSG, und Gerichtbarkeit), die mit der Nutzung einhergeht und sowie Bedenken hinsichtlich der / des IT- / Information- und Datensicherheit / -schutz angeführt.[29]

28 N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen. Es ist zu beachten, dass etwa 55 % der KMU die Cloud-Dienste europäischer Anbieter nutzen. Es gibt ein Anteil an KMU, die sowohl europäische als auch nicht-europäische Dienste nutzen oder dies planen.

29 Die Frage nach den Nachteilen von nicht-europäischen Cloud-Anbietern im Vergleich zu europäischen Anbietern wurde als offene Frage gestellt. Die qualitativen Antworten wurden nachträglich kate-

Knapp 90 % der KMU, die Cloud-Dienste nutzen oder eine Nutzung planen, beabsichtigen oder speichern und verarbeiten bereits heute Unternehmensdokumente und andere Dateien in der Cloud. Einige KMU geben zudem an, Cloud-Dienste auch speziell für Finanz- und Abrechnungsdaten zu verwendet oder verwenden zu wollen. Seltener finden sich jedoch KMU, die ausdrücklich Produktionsdaten oder Forschungs- und Entwicklungsdaten in der Cloud ablegen oder ablegen wollen.

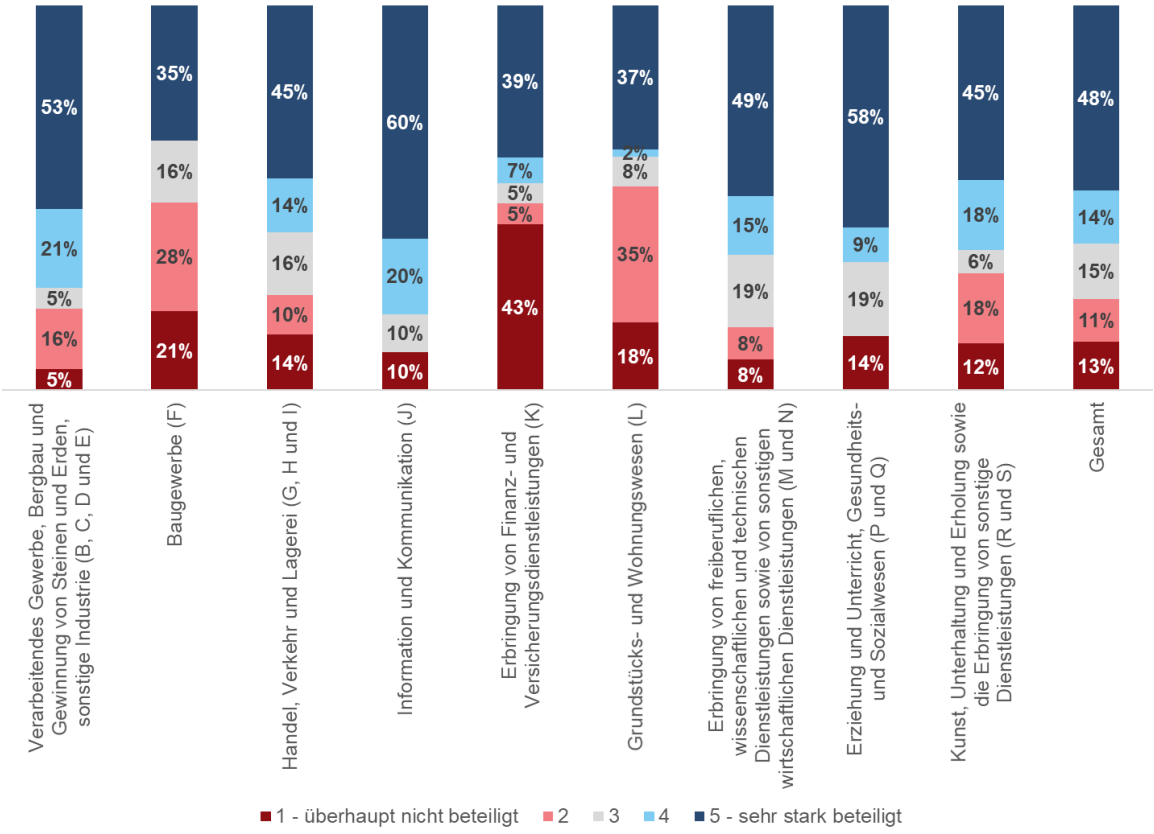
Im ersten Teilbericht wird argumentiert, dass eine Cloud-Strategie für ein Unternehmen aufgrund der hohen Migrationskosten eine langfristige Investition darstellt, für die möglichst ein Partner gewählt wird, der eine starke Marktposition innehat und langfristig am Markt bestehen kann. Dies trifft vor allem zu, wenn es sich um IaaS- oder PaaS-Lösungen handelt oder wenn verschiedene Bereitstellungs- und Servicemodelle miteinander verbunden werden. Marktführer haben zumeist den Vorteil, dass sie über Skalenerträge und Kostenführerschaft sowie ein starkes Marketing- und Vertriebssystem verfügen, wodurch die Migrationskosten in die Cloud geringer sind als bei anderen Anbietern. Bei SaaS-Lösungen kommt zudem hinzu, dass sich vereinzelt defacto Standards in verschiedenen Bereichen, wie zum Beispiel Microsoft 365, herausgebildet haben, auf die Anwender automatisch zurückgreifen.[30] Es ist auch davon auszugehen, dass die Integratoren und IT-Dienstleister solche Cloud-Lösungen und -Anbieter empfehlen, die sie schon kennen, um zusätzlichen Aufwand für die Einarbeitung in die Cloud-Angebote zu vermeiden.

Etwa 50 % der KMU, die aktuell Cloud-Dienste verwenden oder zukünftig verwenden werden, haben oder holen sich derzeit Unterstützung von IT-Dienstleistern – sowohl bei der Auswahl des Cloud-Dienstes bzw. -Anbieters als auch bei der Implementierung und Betreuung der Dienste. Etwa 13 % geben sogar alles in die Hände des Dienstleisters und sind überhaupt nicht beteiligt. Dies trifft insbesondere für KMU zu, die Finanz- und Versicherungsdienstleistungen erbringen (siehe Abbildung 3-8). Aus den Daten wird jedoch nicht ersichtlich, ob der Beratungsbedarf mit der Komplexität der Cloud-Strategie steigt. Dies scheint eher Einzelfallabhängig zu sein.

gorisiert. Etwa 40 % der KMU äußerten Bedenken hinsichtlich der / des IT- / Information- und Datensicherheit / -schutz (Zitate: „Datensicherheit ist evtl. nicht gegeben“, „Fehlender Datenschutz“, „Kein garantierter Datenschutz“, „Sorge um Fremdzugriff“, „Wirtschaftsspionage“, „Ausspähung ist 'Tür und Tor' geöffnet“). Etwa 20 % der KMU geben Rechtsunsicherheit als Nachteil an (Zitate: „Bedenken, dass das europäische Recht eingehalten wird“, „Gerichtsbarkeit nicht in der EU“, „Keine Rechtssicherheit“, „Regressfähigkeit“). Jeweils 5 % der KMU bemängeln die grundsätzliche Intransparenz (Zitate: „Keine Informationen“, „Völlige Intransparenz“), die Performance (Zitate: „Keine Verfügbarkeit“, „Schlechter Ping“, „Eine garantierte Verfügbarkeit ist nicht immer gegeben“) und den Support (Zitate: „Sprachliche Barriere“, „Erreichbarkeit bei Problemen“). Für 3 % der KMU ist Abhängigkeit (Zitate: „Abhängigkeit von amerikanischen Firmen“, „Abhängigkeit vom Anbieter, wenn ich keinen Zugriff mehr habe“) und für 2 % der Preis / die Kosten ein Nachteil. Letztlich hatten 16 % KMU andere Gründe, die nicht eindeutig zuordbar waren. 40 % der KMU machten keine Angaben. (N=377, Basis: KMU, die sich mit dem Thema Cloud befasst haben.)

30 Neben dem Preis, der Leistung und der Performance sehen einige KMU bei den großen, nicht-europäischen Anbietern auch ihre Präsenz bzw. Verbreitung und häufig die damit in Verbindung gebrachte Innovationsfähigkeit als Vorteil an.

Abbildung 3-8: Eigenbeteiligung bei der Auswahl des Cloud-Dienstes bzw. -Anbieters sowie bei der Implementierung und Betreuung während des Betriebs des Cloud-Dienstes



Quelle: WIK-Consult / uzbonn. N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen. Etwa 1 % gab „weiß nicht / keine Angabe“ an. Diese wurden bei der Berechnung der Anteile nicht berücksichtigt.

Etwa 80 % bzw. 70 % der KMU, die aktuell oder zukünftig Cloud-Dienste verwenden, sehen die finanzielle Stabilität und Reputation des Cloud-Anbieters als wichtig für ihre Entscheidung an (siehe Abbildung 3-6). Zwei Aspekte deren Bedeutung im Teilbericht 1 herausgearbeitet wird und allgemein als Vorteile großer, nicht-europäischer Cloud-Anbieter gesehen werden.

Die Frage nach den Vorteilen von großen, nicht-europäischen Cloud-Anbietern im Vergleich zu europäischen Anbietern wurde als offene Frage gestellt. Die qualitativen Antworten wurden nachträglich kategorisiert. Neben dem Preis, der Leistung und der Perfor-

mance sehen einige KMU bei den großen, nicht-europäischen Anbietern auch ihre Präsenz bzw. Verbreitung und häufig die damit in Verbindung gebrachte Innovationsfähigkeit als Vorteile an.[31]

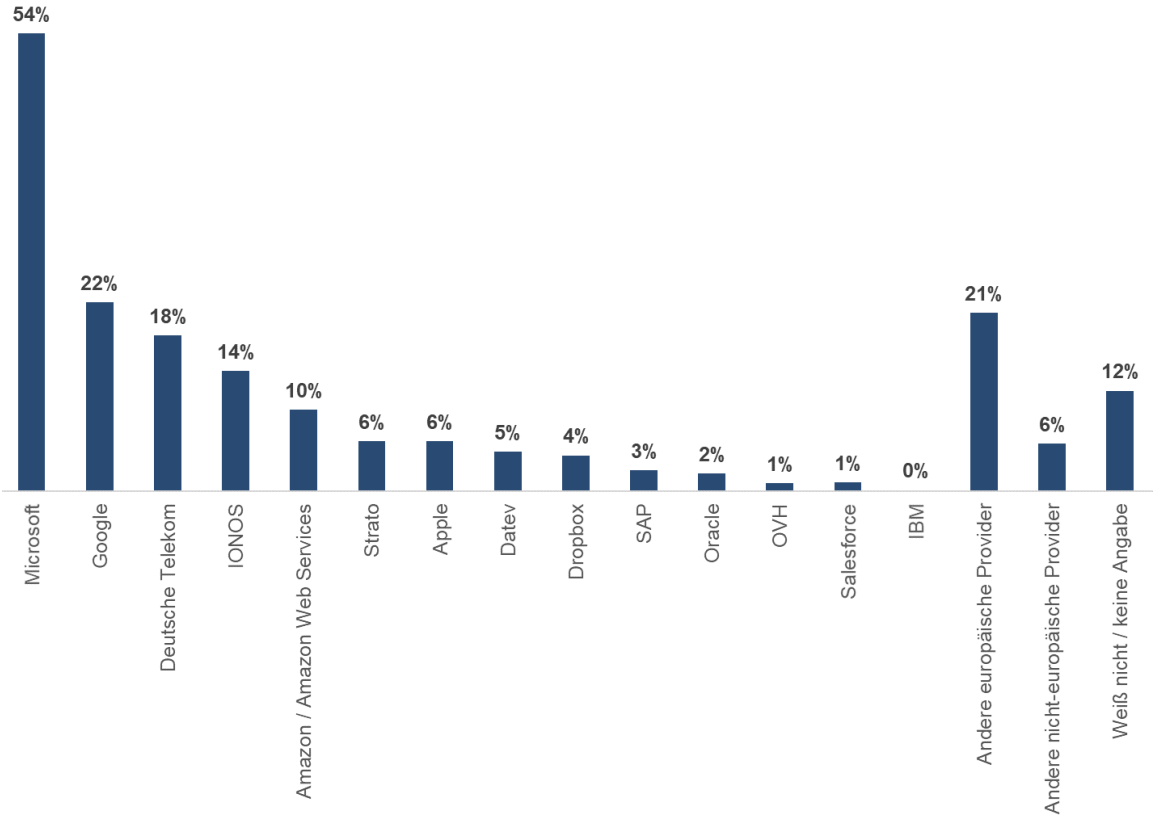
Mit Abstand am beliebtesten und weitesten verbreitet unter KMU sind die Dienste des Cloud-Anbieters Microsoft (siehe Abbildung 3-9). Bei der Ausweisung der Marktanteile von SaaS im Teilbericht 1 zeigt sich, dass Microsoft mit seiner Unternehmenssoftware Microsoft 365 und Business-Intelligence (BI) -Programmen Marktführer auf dem SaaS-Markt ist.

Die anderen beiden großen, internationalen Anbieter Google und Amazon Web Services werden von jeweils 22 % bzw. 10 % der KMU genutzt oder in Betracht gezogen. Vor allem Amazon Web Services, welches die meisten Marktanteile für IaaS hat, steht bei den KMU hinten an, da für diese vielmehr die Softwareebene interessant ist. Beliebte europäische Anbieter sind vor allem die Deutsche Telekom sowie IONOS. Da die Deutsche Telekom auch als Reseller von Cloud-Diensten von Amazon Web Services und Microsoft Azure agiert, ist der Anteil von 18 % mit Vorsicht zu interpretieren.

Abbildung 3-9 zeigt darüber hinaus, dass die Cloud-Landschaft mit den Diensten, für die sich KMU interessieren, sehr heterogen ist. Es existieren sehr viele kleinere Anbieter.

31 Etwa 11 % der KMU sehen Vorteile im Preis bzw. im Preis-Leistungsverhältnis von großen, nicht-europäischen Anbietern. Grob 9 % der KMU stufen die Performance, 6 % die Funktionalität, 3 % die Skalierbarkeit der Dienste als besser im Vergleich zu europäischen Cloud-Diensten ein. Ca. 2 % der KMU loben die Benutzerfreundlichkeit und 1 % den Support. Etwa 3 % bzw. 5 % der KMU sehen Vorteile in der Verbreitung und Innovationsfähigkeit der Dienste. Letztlich hatten 8 % KMU andere Gründe, die nicht eindeutig zuordbar waren. 70 % der KMU machten keine Angaben. (N=377, Basis: KMU, die sich mit dem Thema Cloud befasst haben.)

Abbildung 3-9: Cloud-Anbieter



Quelle: WIK-Consult / uzbonn. N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.

Eine vergleichsweise weniger entscheidende Rolle bei der Wahl des Cloud-Anbieters scheint für die KMU aktuell Interoperabilität zu spielen. Dabei fördern Interoperabilität zusammen mit der Gewährleistung von Portabilität der Daten offene Cloud-Ökosysteme, die kleinere Anbieter einschließen, und reduzieren Lock-in-Effekte, die insbesondere bei den Ökosystemen der Hyperscaler bestehen. Studien von KPMG (2020, 2022) zeigen jedoch, dass Interoperabilität zunehmend wichtiger für Unternehmen wird. KPMG (2020, 2022) befragte im Jahr 2020 und 2022 deutsche Unternehmen mit 20 und mehr Beschäftigten nach der Wichtigkeit unterschiedlicher Faktoren bei der Wahl des Cloud-Anbieters. Während im Jahr 2020 etwa 51 % Interoperabilität als Must-have einstufen sind es in 2022 etwa 62 %.[32]

32 Vgl. KPMG (2020), KPMG (2022).

Vor- und Nachteile nicht-europäischer Cloud-Anbieter

Etwa 70 % der KMU abonnieren oder planen Dienste nicht-europäischer Cloud-Anbieter zu abonnieren.[33]. Dabei sehen KMU sowohl Vor- als auch Nachteile in der Nutzung von Diensten dieser Anbieter. Einige dieser Vor- und Nachteile wurden bereits in den obigen Abschnitten angesprochen. Dieser Abschnitt fasst vor allem die Vor- und Nachteile großer, nicht-europäischer Anbieter aus Sicht ihrer Nutzer und der, die es zukünftig werden könnten, zusammen.

Insgesamt benennen mehr KMU Nach- als Vorteile nicht-europäischer Cloud-Anbieter (63 % zu 37 %). Zu den Top drei häufig genannten Vorteilen gehört der Preis bzw. das Preis-Leistungsverhältnis (14 %), die Performance (13 %) und die Funktionalität (12 %). Zu den Top drei Nachteilen gehört die IT- / Informations- und Datensicherheit (41 %), die Rechtsunsicherheit (DSVCO, BDSG und Gerichtbarkeit) (23 %) und der Mangel an Transparenz (9 %).[34]

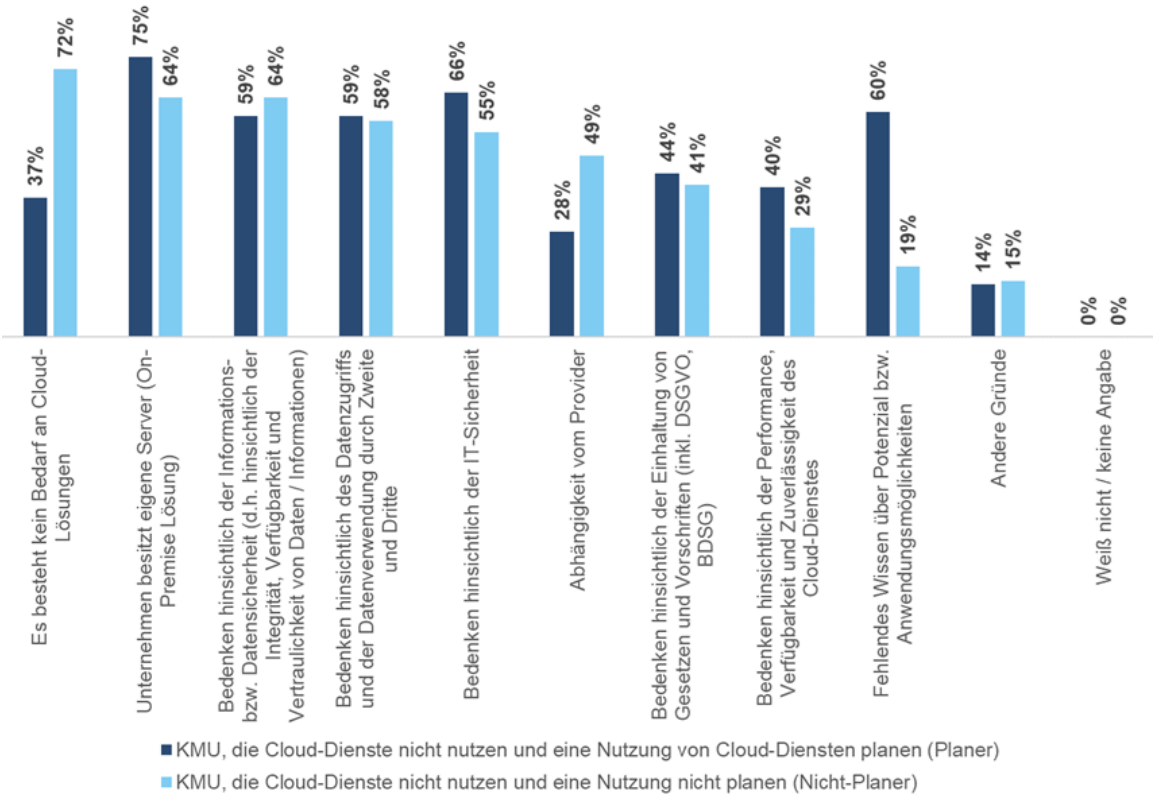
Gründe für die Nicht-Nutzung von Cloud-Diensten

Etwa 62 % der KMU in Deutschland nutzen aktuell keine Cloud-Dienste; knapp 10 % von diesen planen zumindest eine Einführung von Cloud-Diensten in der Zukunft und 42 % haben sich bisher noch nicht mit einer möglichen Nutzung von Cloud-Diensten befasst. Weitere 47 % haben sich aktiv gegen eine Nutzung von Cloud-Diensten entschieden.[35]

Die meisten der KMU, die sich zumindest mit dem Thema „Cloud“ auseinandergesetzt haben, nutzen bisher keine Cloud-Dienste, da es noch keinen akuten Bedarf gibt oder die Unternehmen eigene Server besitzen. Weitere Hemmnisse sind Bedenken hinsichtlich der Sicherheit in Bezug auf die IT, Daten und Information sowie in Anbetracht möglicher Datenzugriffe von außen. Ein fehlendes Wissen über Potenziale bzw. Anwendungsmöglichkeiten hat bisher vor allem die KMU, die die Einführung einer Cloud-Strategie planen, zurückgehalten (siehe Abbildung 3-10).

33 Es handelt sich ausschließlich um US-amerikanische Cloud-Anbieter. N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.
34 N= 162. Basis: KMU, die Cloud-Dienste nicht-europäischer Anbieter nutzen oder dies planen.
35 Die restlichen KMU machen keine Angabe. N=302. Basis: KMU, die keine Cloud-Dienste nutzen.

Abbildung 3-10: Hemmnisse



Quelle: WIK-Consult / uzbonn. N=175. Basis: KMU, die Cloud-Dienste nicht nutzen, aber sich mit der Thematik auseinandergesetzt haben.

Darüber hinaus haben im Schnitt etwa 15 % eine Reihe von anderen Gründen für die Nicht-Nutzung von Cloud-Diensten angegeben. Unter den Antworten befinden sich eine kleine Anzahl an Aussagen, die darlegen, dass Cloud-Dienste aufgrund der langesamen bzw. schlechten Breitbandverbindung nicht erworben wurden.

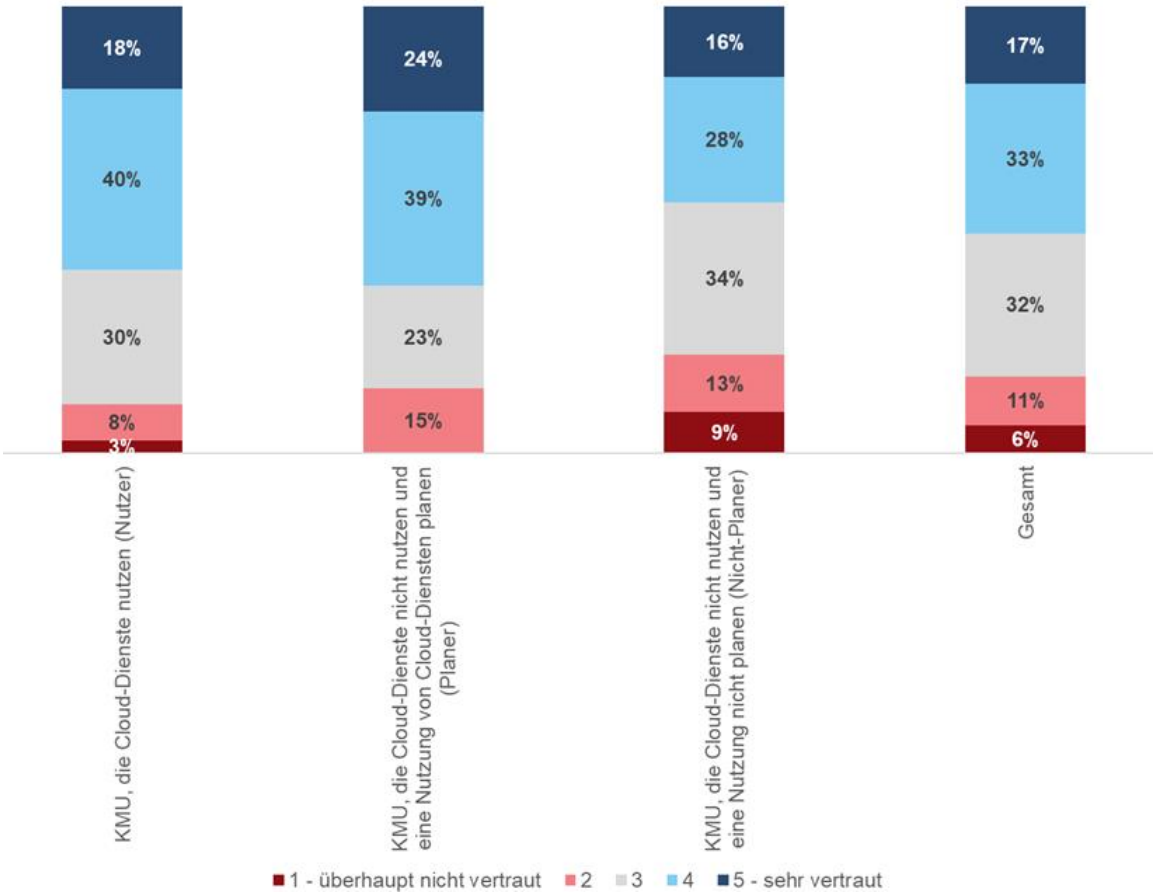
Im nachfolgenden Kapitel wir der Kenntnisstand von KMU zu Datenschutz- und Datensicherheitsregelungen untersucht.

3.2 Kenntnisstand zu Datenschutz- und Datensicherheitsregelungen

Teilbericht 2 befasst sich bereits eingehend mit den rechtlichen Bedingungen für Datenschutz, denen die KMU in Deutschland grundsätzlich unterliegen. Vor allem die Europäische Datenschutz-Grundverordnung (DSGVO) bildet seit ihrer Verabschiedung im Mai 2018 den Rechtsrahmen des Datenschutzes innerhalb der EU und dient dazu, ein hohes Schutzniveau für personenbezogene Daten natürlicher Personen innerhalb Europas sicherzustellen. Der Kenntnisstand zu Datenschutz-Grundverordnung variiert stark zwi-

schen den KMU, die bereits Cloud-Dienste nutzen oder dies zumindest planen und denjenigen, die eine Nutzung aktuell nicht in Betracht ziehen. Erstere sind deutlich vertrauter mit der Verordnung als letztere (siehe Abbildung 3-11).

Abbildung 3-11: Vertrautheit mit der DSGVO



Quelle: WIK-Consult / uzbonn. N=505. Basis: Alle KMU. Etwa 1 % gab „weiß nicht / keine Angabe“ an. Diese wurden bei der Berechnung der Anteile nicht berücksichtigt.

Wie im zweiten Teilbericht erläutert, legt die Verordnung unter anderem fest, dass „personenbezogene Daten nur an Länder außerhalb der EU oder des Europäischen Wirtschaftsraumes (EWR) übermittelt werden, wenn in diesen Drittländern das Schutzniveau der DSGVO erreicht wird, um natürliche Personen und ihre Daten zu schützen.“[36] Für einige Länder hat die Europäische Kommission durch einen Angemessenheitsbeschluss dies ausdrücklich festgestellt. Für die USA, wo die Mehrheit der großen, internationalen Cloud-Anbieter wie Google, Amazon Web Services und Microsoft ihren Hauptsitz haben, gibt es diese Beschlussgrundlage nicht bzw. nicht mehr. Zunächst hatte das Privacy Shield-Abkommen zwischen der EU und den USA aus dem Jahr 2016 zwar bestätigt,

36 Siehe Ausarbeitung in Teilbericht 2, S. 15.

dass in den USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet wird. Jedoch wurde das Abkommen mit dem Schrems-II-Urteil des EuGH vom 16. Juli 2020 für ungültig erklärt.[37]

Nichtsdestotrotz nutzen viele KMU in Deutschland Cloud-Dienste, die von US-amerikanischen Anbietern zur Verfügung gestellt werden oder planen diese zu nutzen (70 %).[38]

Für die Mehrheit der Nutzer von Cloud-Diensten, die bereits vor dem Schrems-II-Urteil Cloud-Dienste nutzen und angeben, US-amerikanischer Anbieter zu verwenden, hatte das Urteil keine Auswirkungen bzw. Konsequenzen (60 %). Lediglich 11 % haben nach dem Urteil ihre internen Regelungen zur Speicherung bzw. Verarbeitung kritischer Daten und Information angepasst. Wenige haben Verträge verändert oder gar den Cloud-Anbieter gewechselt (8 % bzw. 4 %).[39] Dabei speichern und verarbeiten aktuell bereits 61 % der KMU, die Cloud-Dienste nutzen, personenbezogene Kunden- oder Personaldaten in der Cloud; darunter auch eine Vielzahl an KMU, die US-amerikanische Cloud-Dienste verwenden.[40]

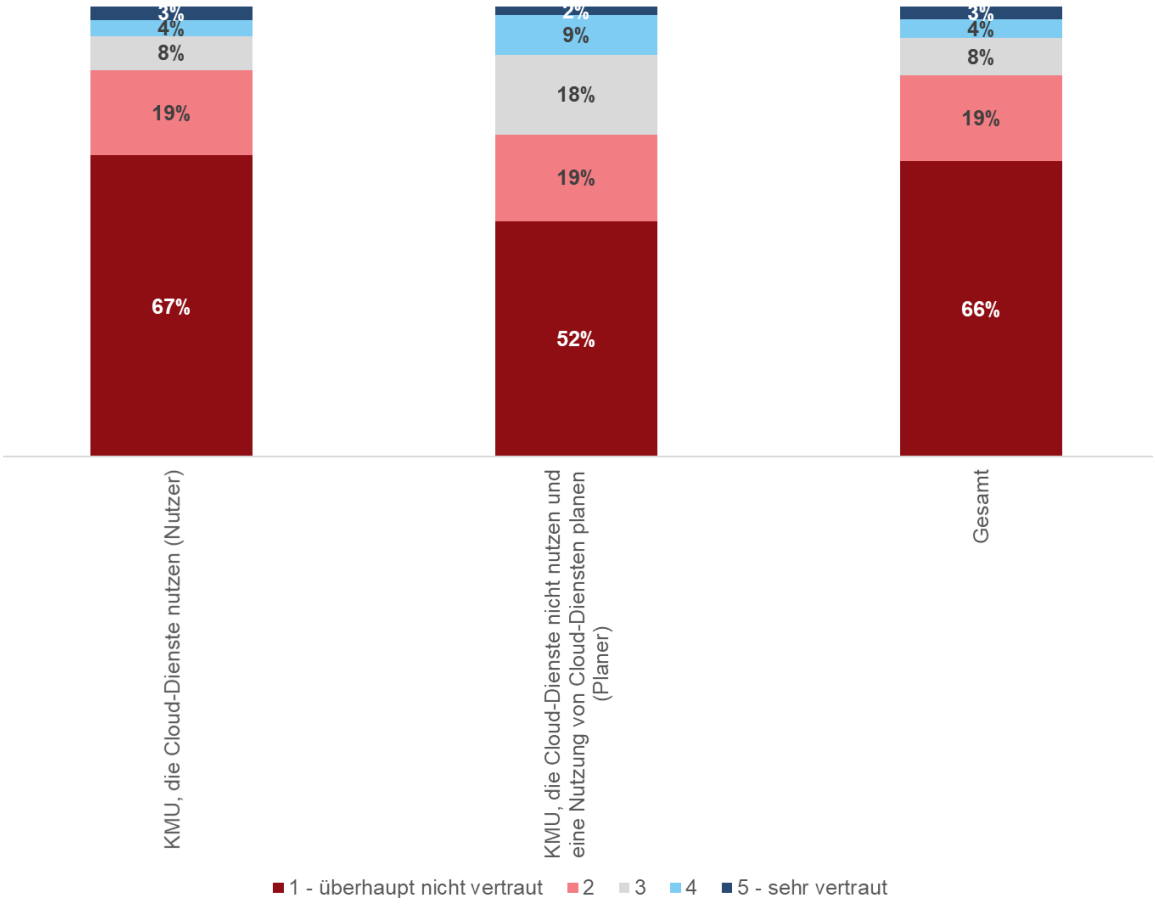
Diese Reaktionen weichen maßgeblich von den Reaktionen größerer Unternehmen auf das Schrems-II-Urteil ab. In einer Befragung von KPMG (2021), wofür Unternehmen mit 20 oder mehr Beschäftigten in Deutschland befragt wurden, gaben 60 % an, dass das Urteil eine Auswirkung auf die Cloud-Strategie hatte. Die meisten passten vor allem ihre technischen und organisatorische Maßnahmen an.[41]

Ähnlich geringe Reaktionen wie auf das Schrems-II-Urteil lassen sich bei den KMU im Hinblick auf den im Jahre 2018 verabschiedeten CLOUD Act erkennen, welches US-Anbieter dazu verpflichtet, US-Behörden sämtliche in ihrem Besitz, Gewahrsam oder ihrer Kontrolle befindlichen Daten offenzulegen und zwar unabhängig davon, ob die Daten innerhalb oder außerhalb der USA gespeichert sind.[42] Auch diese Gesetzgebung hatte für die KMU, die zu jenem Zeitpunkt bereits Cloud-Dienste nutzen und angeben, US-amerikanischer Anbieter zu verwenden, nach eigenen Angaben keine Auswirkungen (64 %).[43] Allgemein geben die KMU, ob sie nun US-amerikanische Cloud-Dienste bereits nutzen oder dies in der Zukunft planen, zudem zu, wenig bis überhaupt nicht mit den Inhalten und Konsequenzen des CLOUD Acts vertraut zu sein (80 %) (siehe Abbildung 3-12).

---

37 Siehe Ausarbeitung in Teilbericht 2, S. 15 f.
38 N=235. Basis: KMU, die Cloud-Dienste nutzen oder eine Nutzung planen.
39 N=124. Basis: KMU, die Cloud-Dienste US-amerikanischer Anbieter nutzen und Cloud-Dienste länger als 22 Monate verwenden.
40 N=203. Basis: KMU, die Cloud-Dienste nutzen.
41 Vgl. KPMG (2021).
42 Siehe Ausführungen in Teilbericht 2.
43 14 % der KMU haben ihre internen Regelungen zur Speicherung bzw. Verarbeitung kritischer Daten angepasst, weiter 11 % änderten ihre Verträge und 4 % wechselten ihren Anbieter. Letztlich zogen 2 % andere Konsequenzen und 17 % machten keine Angabe zu den Konsequenzen. N=78. Basis: KMU, die Cloud-Dienste US-amerikanischer Anbieter nutzen und Cloud-Dienste länger als 50 Monate verwenden.

Abbildung 3-12: Vertrautheit mit dem US CLOUD Act



Quelle: WIK-Consult / uzbonn. N=162. Basis: KMU, die US-amerikanische Cloud-Anbieter nutzen oder planen zu nutzen. Etwa 6 % gab „weiß nicht / keine Angabe“ an. Diese wurden bei der Berechnung der Anteile nicht berücksichtigt.

3.3 Digitale Souveränität

Nicht nur die Stärkung der digitalen Souveränität von natürlichen Personen, sondern auch die der Wirtschaft ist angesichts der starken Positionen von US-amerikanischen Unternehmen in der Forschung als auch im politischen Diskurs eine häufig wiederkehrende Thematik. Dennoch fehlt es bisher an einer einheitlichen Definition, wie im Teilbericht 2 herausgearbeitet wird.

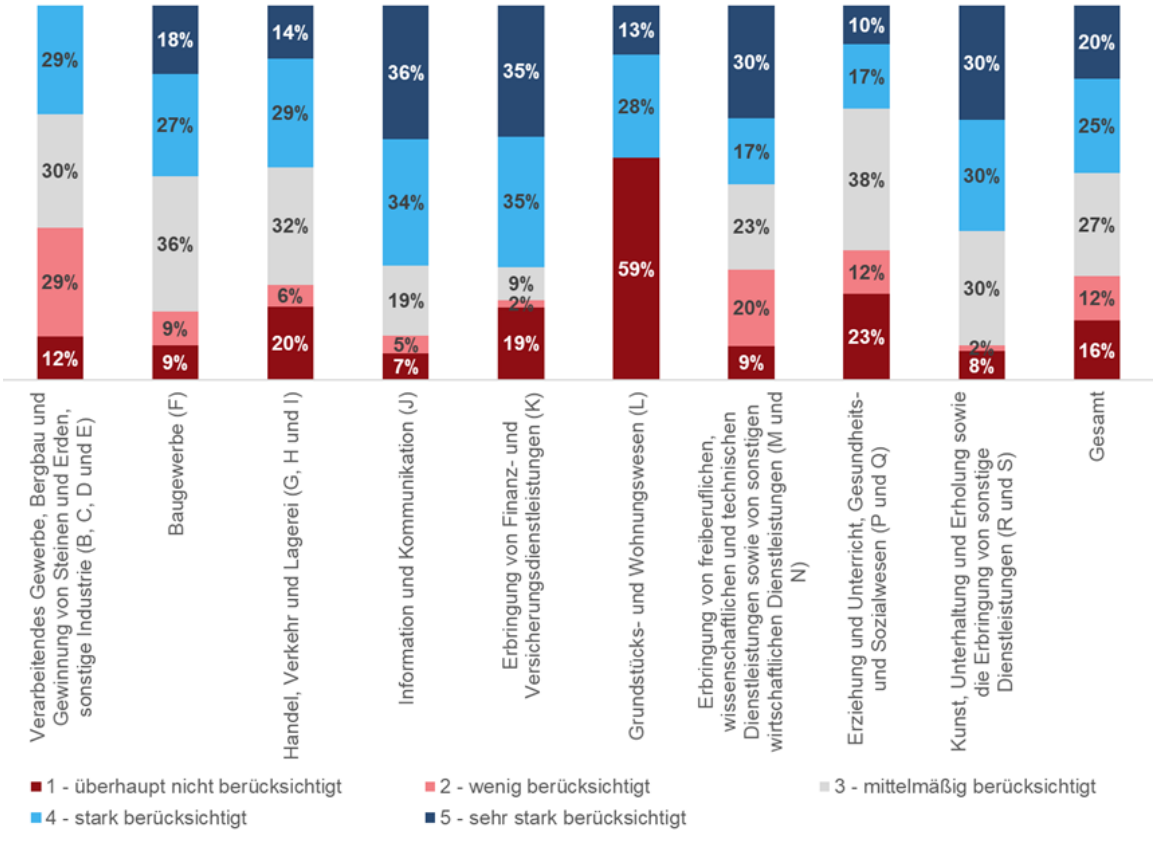
Möglicherweise ist für viele KMU der Begriff „Digitale Souveränität“ auch daher heute noch nicht in Gänze greifbar. Insgesamt ist der Begriff 65 % der KMU nicht bekannt. Die restlichen KMU, die den Begriff zumindest kennen, haben mitunter unterschiedliche Auffassungen dazu, was digitale Souveränität für sie bedeutet. Selten werden die verschiedenen Dimensionen – Cybersicherheit, Datensouveränität und technologische Unabhängigkeit – der digitalen Souveränität gemeinsam genannt. Die Antworten beziehen sich

vermehrt nur auf eine Dimension, wobei die Datensouveränität offenkundig am häufigsten während der Befragung genannt wurde. So gab ein KMU an, unter digitaler Souveränität zu verstehen, „dass […] die Daten unabhängig von Zugriffen eigenverantwortlich [verwaltet werden] und, dass niemand Zugriff erlangt“. Einige andere KMU gaben Antworten wie „ich [bin] der Herr meiner Daten […]“ oder „ich [habe] die Hoheit über meine Daten […]“.

Trotz der generellen Unkenntnis der KMU im Hinblick auf die Bedeutung des Begriffs „Digitale Souveränität“, zeigt sich dennoch, dass diejenigen KMU, die ein Verständnis zum Thema „Digitale Souveränität“ aufbringen, diese tendenziell bei der Entscheidung, Cloud-Dienste zu verwenden oder nicht zu verwenden, berücksichtigen. Für 40 % der KMU spielte die digitale Souveränität bei der Entscheidung eine starke bis sehr starke Rolle. Weitere knapp 25 % berücksichtigten die digitale Souveränität zumindest mittelmäßig stark bei ihrer Entscheidung. Für knapp ein Viertel der KMU hingegen wurde die digitale Souveränität wenig bis überhaupt nicht bei der Entscheidung beachtet.[44] Allgemein lassen Anwender von Cloud-Diensten ihre digitale Souveränität eher in die Entscheidung einfließen als KMU, die keine Cloud-Dienste nutzen und dies auch bisher nicht planen. Deutliche Unterschiede lassen sich so auch in den einzelnen Branchen finden (siehe Abbildung 3-13).

44 N=179. Basis: KMU, die Verständnis zum Thema digitale Souveränität aufbringen.

Abbildung 3-13: Berücksichtigung der digitalen Souveränität bei der Entscheidung, Cloud-Dienste zu nutzen



Quelle: WIK-Consult / uzbonn. N=179. Basis: KMU, die Verständnis zum Thema digitale Souveränität aufbringen. Etwa 7 % gab „weiß nicht / keine Angabe“ an. Diese wurden bei der Berechnung der Anteile nicht berücksichtigt.

Für die eigenen Wettbewerbs- und Innovationsfähigkeit empfinden die KMU ihre digitale Souveränität im Durchschnitt jedoch als weniger wichtig. Lediglich 28 % der KMU, die den Begriff „Digitale Souveränität“ kennen, sehen digitale Souveränität als wichtig bis sehr wichtig für ihre Wettbewerbsfähigkeit an. Für die Innovationsfähigkeit liegt der Anteil bei 25 %. Daneben messen etwa 50 % an KMU der digitalen Souveränität sowohl in Bezug auf die Innovations- als auch Wettbewerbsfähigkeit ihres Unternehmens keine Rolle oder nur eine geringe zu.[45] Das Bild ändert sich leicht, wenn nur die Anwender von Cloud-Diensten betrachtet werden. Für die KMU, die aktuell Cloud-Dienste nutzen, ist die digitale Souveränität für die Innovations- und Wettbewerbsfähigkeit tendenziell immerhin wichtiger als für den Durchschnitt der KMU in Deutschland (37 % bzw. 38 %). Ein direkter Zusammenhang zwischen der Komplexität der Cloud-Strategie und der Einstellung der

45 N=179. Basis: KMU, die Verständnis zum Thema digitale Souveränität aufbringen.

KMU zur Rolle der digitalen Souveränität für ihre Wettbewerbs- und Innovationsfähigkeit, lässt sich jedoch nicht feststellen.[46]

Dabei ist das Hauptziel „der Erhalt und die Stärkung der digitalen Souveränität der Wirtschaft die Gewährleistung der Handlungsfähigkeit und Zukunftsfähigkeit“[47] der Unternehmen und damit der Wettbewerbs- und Innovationsfähigkeit. Digitale Souveränität wie sie vom BMWK (urspr. BMWi) beschrieben wird, wird maßgeblich durch zwei Komponenten erreicht. Zum einen wird sie durch die Verfügbarkeit von bzw. der Zugang zu Technologien und Daten erreicht und zum anderen durch die selbstbestimmte, reflektierte, verantwortungsvolle Nutzung von digitalen Technologien und Daten.[48] Beides kann, wie im zweiten Teilbericht bereits herausgearbeitet, in gewissem Maß ein Zielkonflikt darstellen. Das Angebot von Cloud-Anbieter ermöglicht KMU zwar jenen Zugang zu neuen Diensten und Technologen, dennoch haben die KMU Zweifel und Bedenken hinsichtlich des sicheren und selbstbestimmten Umgangs mit den Informationen und Daten, die über die angebotenen Dienste verarbeitet und gespeichert werden.

Insgesamt scheint aus Sicht der KMU eine gewisse Gefährdung der digitalen Souveränität von Cloud-Diensten auszugehen (73 %)[49], obwohl etwa 67 % diese Gefährdung als eher gering bis mittelmäßig einstufen.[50] Etwa 20 % der KMU sind sogar der Ansicht, dass überhaupt keine Gefährdung der digitalen Souveränität von Cloud-Diensten ausgeht.[51] In den Daten sind keine eindeutigen Unterschiede in der Einstellung nach Komplexität der Cloud-Strategie zu erkennen.

Diejenigen KMU, die davon ausgehen, dass Cloud-Dienste die digitale Souveränität von Unternehmen gefährden - wenn auch nur zu einem geringen Maße - führten hierfür Gründe wie erhöhte Abhängigkeit von Cloud-Anbietern, mangelnde IT- / Daten- und Informationssicherheit sowie mangelnder Datenschutz an.[52] In Bezug auf das Abhängigkeitsargument wird von einigen KMU betont, dass Cloud-Dienste sich zu einem gewissen Maß ihrer Kontrolle entziehen und bestehende Sicherheits- und Datenschutzkonzepte hingenommen werden müssen, obwohl sie selten nachvollziehbar seien.[53] In Zusammenhang mit IT- und Datensicherheit sowie Datenschutz führen einige KMU neben der

46 Bereits in Kapitel 3.1 wird festgestellt, dass die Steigerung der Wettbewerbs- und Innovationsfähigkeit ein zweitrangiger Motivator für die Nutzung von Cloud-Diensten ist.
47 BMWi (2021), S.37.
48 Vgl. BMWi (2021).
49 N=179. Basis: KMU, die Verständnis zum Thema digitale Souveränität aufbringen.
50 N=133. Basis: KMU, die Verständnis zum Thema digitale Souveränität aufbringen und davon ausgehen, dass Cloud-Dienste zumindest eine geringe Gefährdung für die digitale Souveränität mitbringen.
51 N=179. Basis: KMU, die Verständnis zum Thema digitale Souveränität aufbringen.
52 So wurde von einzelnen KMU angeführt, dass eine Gefährdung der digitalen Souveränität durch die Abhängigkeit von Firmen, Anbietern und Global Playern entsteht.
53 Zitate: „Abhängigkeit vom Anbieter, […] [wodurch es zu] Abhängigkeit von vorgegebenen Strukturen [kommt]“, „Aufgrund [einer] […] gewissen Abhängigkeiten von Firmen / Global Playern“, „Die Abhängigkeit [und die Tatsache, dass] […] man nicht eingreifen kann [..]“, „Es bleibt eine gewisse Abhängigkeit in Sicherheitssystemen“, „Man ist abhängig von der Sicherheit und vom Zugriff anderer“, „Weil man von Dienstleistern abhängig ist, die möglicherweise ihre eigenen Regelungen haben“, „Weil [Cloud-Dienste] […] zu umfangreich [..] [sind], um eine gewisse Übersicht zu behalten und die Kontrollfähigkeit bei der Nutzung auszuüben“, „Weil [Cloud-Dienste] […] unkontrollierbar bleib[en] für die Nutzer“, „Weil ich auf den Cloud-Dienst nur beschränkten Einfluss habe […] [und] keine direkte Kontrolle“, „Da wo wir auf

generellen Besorgnis, dass die IT- und Datensicherheit nicht gegeben oder Datenschutz nicht eingehalten wird, aus, dass Cloud-Dienste anfällig für Hackerangriffe, Wirtschafts- und Industriespionage sowie Fremdzugriffe wären.[54]

Auf europäischer Ebene existiert derzeit ein Projekt, welches eine europäische Dateninfrastruktur schaffen soll, die die digitale Souveränität der EU-Mitgliedstaaten und der ansässigen Unternehmen schützt und Innovationen fördert. Das Projekt, Gaia-X, wird in Teilbericht 1 eingehend beschrieben. Doch den wenigsten KMU ist das Projekt bisher bekannt (7 %). Tendenziell kennen mehr KMU, welche Cloud-Dienste bereits nutzen oder dies planen, Gaia-X (10 % bzw. 15 %) als KMU, die derzeit keine Cloud-Dienste nutzen und dies auch nicht planen (4 %).[55]

Die KMU, die das Projekt Gaia-X kennen, erhoffen sich dadurch vor allem mehr Vertrauen in digitale Anwendung durch erhöhte Datensouveränität und -sicherheit (75 %). Zudem wird durch Gaia-X erwartet, dass es zu einer schnellen Entwicklung digitaler Innovationen kommt. Jeweils etwa 40 % der KMU hoffen auf eine höhere Datenverfügbarkeit, eine Steigerung des Wissens- und Erfahrungsaustausches (z.B. in der Cloud) sowie auf die Entwicklung neuer Geschäftsmodelle und Dienstleistungen. Letztlich erhoffen sich 30 % durch Gaia-X Wettbewerbsvorteile und 11 % denken das Gaia-X weitere andere Vorteile haben könnte. Etwa 16 % gehen von keinen Vorteilen durch Gaia-X für Ihr Unternehmen aus.[56]

Cloud-Dienste angewiesen sind, die aber nicht mit dem Datenschutz vereinbar sind, sind wir eingeschränkt, weil es manchmal keine Alternativen gibt."

54 Zitate: „Datensicherheit ist nicht gegeben. Die Folgen [daraus] sind Wirtschaftskriminalität, Sicherheitsdienste die Daten zusammen führen ohne den eigenen Willen", „Datenschutzproblematik, Angriffen von externen Hackern", „Die Cloud-Dienste sind nicht sicher, es gibt genügend Hacker die Daten klauen", „Es sind durch die Cloud-Nutzung Hackerangriffe möglich", „Fremder und unbemerkter Zugriff möglich", „Keine Sicherheit durch außereuropäische Anbieter", „Keine gewährleistete Einhaltung der Datenschutzgrundverordnungen", „Ich kann nicht jeden Datenstrom nachvollziehen, es bleibt eine gefühlte Sicherheitslücke", „Wegen der Datensicherheit", „Weil [Cloud-Dienste] […] dazu [einladen] […], Daten unsorgsamer zu behandeln und es viel mehr Einfallstore gibt für Datenklau und Fehleranfälligkeit[en]", „Weil […] [die Cloud-Dienste] irgendwo gehackt werden können. Die letzte Schwachstelle können die Mitarbeiter [sein], da kann viel verloren gehen. [Schlagwörter:] Industriespionage usw. […]".

55 Anteile der Kenner. N=505. Basis: Alle KMU.

56 N=38. Basis: KMU, die Gaia-X kennen. Es wurden auch KMU zu den erhofften Auswirkungen von Gaia-X auf die Anwendung von digitalen Technologien in ihren Unternehmen befragt, die Gaia-X nicht kennen (N=467). Im Laufe der Befragung wurde dieser Gruppe erklärt, was Gaia-X ist und bezweckt. Ergebnis: Mehr Vertrauen in digitale Anwendungen durch erhöhte Datensouveränität und -sicherheit (52 %), schnellere Entwicklung digitaler Innovationen (41 %), höhere Datenverfügbarkeit (37 %), Steigerung des Wissens-, und Erfahrungsaustausches z.B. in der Cloud (35 %), Wettbewerbsvorteile (23 %), neue Geschäftsmodelle / Dienstleistungen / Produkte (29 %), andere Auswirkungen (5 %), keine Auswirkungen (28 %), weiß nicht / keine Angabe (8 %). Aufgrund der vorgetragenen Definition könnten diese Antworten verzerrt sein.

4 Schlussfolgerungen

Insgesamt zeigt sich, dass für KMU der SaaS-Markt besonders relevant ist. Anders als beim IaaS- und PaaS-Markt, bei denen wenige Anbieter besonders hohe Marktanteile verbuchen, verwenden KMU Dienste verschiedenster Cloud-Anbieter. An der Spitze steht jedoch Microsoft, das mit seiner Unternehmenssoftware Microsoft 365 und Business-Intelligence (BI)-Programmen insgesamt Marktführer auf dem SaaS-Markt ist und auch von KMU mehrheitlich verwendet wird. So bleiben die anderen beiden großen internationalen Anbieter Google und Amazon Web Services aber auch europäische Anbieter insgesamt bei den KMU hinter Microsoft zurück.

Die Cloud-Anbieter auf dem SaaS-Markt bieten mitunter jedoch sehr unterschiedliche Lösungen an, die nicht direkt mit Diensten anderer Cloud-Anbieter substituierbar oder vergleichbar sind. So lässt sich eine CRM-Cloud-Anwendung von Salesforce nicht durch eine Office- oder Kollaborationsanwendungen von Microsoft substituieren. Würde der SaaS-Markt nach Anwendungsfällen unterteilt werden, könnte der Markt wohlmöglich konzentrierter ausfallen.

Bei der Auswahl des Cloud-Anbieters ist der Preis vielmehr zweitrangig für KMU. Sie legen vor allem Wert auf die Performance sowie eine hohe Zuverlässigkeit. Dafür geben sie etwa 6.000 Euro jährlich für Cloud-Dienste aus. Da KMU sowohl sensible, personenbezogene, aber auch unternehmensbezogene Daten und Informationen in der Cloud ablegen und verarbeiten, ist die Daten- und Informationssicherheit und der Datenschutz ebenfalls besonders wichtig bei der Auswahl. Jeweils mehr als 90 % der KMU, die Cloud-Dienste verwenden oder eine Nutzung in Betracht ziehen, stufen diese beiden Aspekte als wichtig bis sehr wichtig bei der Entscheidung für einen Cloud-Provider ein. Vor allem personenbezogene Daten, sei es von Kunden oder Mitarbeitenden, sind stark durch Rechtsregelungen in Europa geschützt. Dennoch entscheiden sich etwa 70 % der KMU, die Cloud-Dienste abonnieren oder ein Abonnement planen, für nicht-europäische Anbieter – im Speziellem US-amerikanische Anbieter. Diese müssen nicht den europäischen Regelungen und Standards unterliegen. Dabei sehen die meisten dieser KMU mehr Nachteile als Vorteile nicht-europäischer Cloud-Anbieter. Zu den Top drei benannten Nachteilen gehört die IT- / Informations- und Datensicherheit, die Rechtsunsicherheit (DSGVO, BDSG und Gerichtbarkeit) und der Mangel an Transparenz. Auch die Vertrautheit mit den US-amerikanischen Regelung, wie dem CLOUD Act, ist sehr gering. Zudem geben die meisten KMU, die US-amerikanische Cloud-Dienste vor dem CLOUD Act nutzten, an, dass die Verabschiedung des Gesetzes keine Auswirkung auf ihre Nutzung der Cloud-Dienste hatte. Ähnliches gilt für das Schrems-II-Urteil. Dabei speichern und verarbeiten aktuell bereits 61 % der KMU, die Cloud-Dienste nutzen, personenbezogene Kunden- oder Personaldaten in der Cloud; darunter auch eine Vielzahl an KMU, die US-amerikanische Cloud-Dienste verwenden.

Dennoch wird deutlich, dass KMU nicht ausschließlich auf Dienste nicht-europäischer Cloud-Anbieter zurückgreifen. Etwa 55 % der KMU, die Cloud-Dienste nutzen oder dies planen, verwenden oder ziehen die Nutzung europäischer Cloud-Anbieter in Betracht – entweder ausschließlich oder parallel zu einem Dienst eines nicht-europäischen Anbieters. Eine einheitliche Cloud-Strategie scheint es bei den KMU insgesamt nicht zu geben. Vielmehr neigen KMU offenbar dazu Service- und Bereitstellungsmodelle sowie Cloud-Anbieter je nach Bedürfnis zu kombinieren.

Ein wichtiges Ziel Europas ist die Stärkung der digitalen Souveränität der Wirtschaft, um unter anderem die Wettbewerbs- und Innovationsfähigkeit europäischer Unternehmen zu festigen. Doch KMU wissen mitunter nicht, was digitale Souveränität ist oder was es für sie bedeutet. Gerade einmal 35 % der KMU in Deutschland ist der Begriff „Digitale Souveränität“ bekannt. Diese Gruppe berücksichtigt die digitale Souveränität ihres Unternehmens zwar hinreichend stark in der Abwägungsentscheidung, ob Cloud-Dienste verwendet werden oder nicht, doch geht die Mehrheit insgesamt nicht davon aus, dass digitale Souveränität sehr wichtig für ihre Wettbewerbs- und Innovationsfähigkeit ihres Unternehmens ist. Für die KMU, die Cloud-Dienste verwenden oder dies planen, ist die Steigerung der Wettbewerbs- oder Innovationsfähigkeit gleichfalls ein eher zweitrangiger Motivator für die Nutzung von Cloud-Diensten.

Dieses Ergebnis könnte gegebenenfalls auf die Tatsache zurückgeführt werden, dass für KMU vor allem SaaS-Lösungen relevant sind, die zwar notwendig sind, um Unternehmensprozesse effizient zu gestalten und so womöglich Wettbewerbsnachteile aufzuholen, aber weniger zu einem zusätzlichen Wettbewerbsvorteil führen. So wenden KMU Cloud-Dienste vorrangig schlicht zur Speicherung bzw. Sicherung von Daten sowie speziell für Office- und Kollaborationsanwendungen an. Die zweite Gruppe an Anwendung, die aus der Cloud bezogen werden oder deren Bezug in Betracht gezogen wird, sind Sicherheitsanwendungen, Softwareanwendung im Finanz- und Rechnungswesen sowie Systeme zum Datenmanagement. Spezialanwendung für CRM, ERP und HR sowie neuerer Technologien wie KI, Blockchain und IoT werden aktuell noch vergleichsweise wenig genutzt oder in Betracht gezogen, könnten in der Zukunft jedoch an Relevanz gewinnen.

Insgesamt scheint aus Sicht der KMU dennoch eine gewisse Gefährdung der digitalen Souveränität von Cloud-Diensten auszugehen, auch wenn diese als eher gering bis mittelmäßig einstuft wird. Abhilfe könnte Gaia-X schaffen, doch ist dieses Projekt bisher nur sehr wenigen KMU bekannt.

5 Referenzen

Arockiam, L.; Monikandan, S.; Parthasarathy G. (2011): Cloud Computing: A Survey. International Journal of Internet Computing, 1(2), S.26-33.

Bayrak, E.; Conley, J.P.; Wilkie, S. (2011). The Economics of Cloud Computing. The Korean Economic Review, 27 (2), S.203-230.

Bento, A.; Bento, R. (2012). Cloud Computing: A new Phase in Information Technology Management. Journal of Information Technology Management, 22(1), S. 39-46.

Biebl, J. (2012): Wofür steht Cloud Computing eigentlich?. Wirtschaftsinformatik & Management, 4, S.22-29.

BMWi (2021): Schwerpunktstudie Digitale Souveränität. Bestandsaufnahme und Handlungsfelder. https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/schwerpunktstudie-digitale-souveranitaet.html, zuletzt abgerufen am 23.06.2022.

Gries, U. (2021): Welche Datensätze würden Sie schützen? https://www.it-daily.net/it-sicherheit/datenschutz-grc/welche-datensaetze-wuerden-sie-schuetzen, zuletzt abgerufen am 23.06.2022.

Hoberg, P.; Wollersheim, J.; Böhm, M.; Krcmar, H. (2012): Cloud Computing: Überblick und Herausforderungen für das Controlling. Controlling: Zeitschrift für erfolgsorientierte Unternehmenssteuerung, 24(6), S.294-300.

IfM Bonn (2022a): KMU-Definition des IfM Bonn, https://www.ifm-bonn.org/definitionen/kmu-definition-der-eu-kommission [letzter Zugriff: 10.06.2021].

IfM Bonn (2022b): Mittelstand im Überblick, https://www.ifm-bonn.org/statistiken/mittelstand-im-ueberblick/kennzahlen-der-kmu-nach-definition-des-ifm-bonn/kennzahlen-deutschland [letzter Zugriff: 10.06.2021]

KPMG (2020): Cloud-Monitor 2020. Die Integrationsfähigkeit und Interoperabilität der Cloud stärken. In Zusammenarbeit mit bitkom research. https://hub.kpmg.de/studie-cloud-monitor-2020?utm_campaign=Cloud-Monitor %202020&utm_source=AEM, zuletzt abgerufen am 23.06.2022.

KPMG (2021): Cloud-Monitor 2021. Die Goldenen Zwanziger für die Cloud?. In Zusammenarbeit mit bitkom research. https://hub.kpmg.de/cloud-monitor-2021, zuletzt abgerufen am 23.06.2022.

KPMG (2022): Cloud-Monitor 2022. Das Potenzial von der Kosteneffizienz bis zur Energieeffizienz. In Zusammenarbeit mit bitkom research. https://hub.kpmg.de/cloud-monitor-2022, zuletzt abgerufen am 23.06.2022.

Kulas, J.T.; Robinson, D.H.; Smith, J.A.; Kellar, D.Z. (2018): Post-Stratification Weighting in Organizational Surveys: A Cross-Disciplinary Tutorial. Human Resource Management, 57, S.419-436.

Labes, Stine (2012): Grundlagen des Cloud Computing – Konzept und Bewertung von Cloud Computing. Technische Universität Berlin. Projektbericht IKM. Band 01. Universitätsverlag der TU Berlin: Berlin.

Lakshminarayanan, R.; Kumar, B.; Raju, M. (2013): Cloud Computing Benefits for Educational Institutions. https://arxiv.org/ftp/arxiv/papers/1305/1305.2616.pdf, zuletzt abgerufen am 20.06.2022.

Ochs, M. (2018): Informationsschutz in Liefernetzwerken (Supply Chain Risk Management). Blog des Fraunhofer-Institut für Experimentelles Software Engineering. https://www.iese.fraunhofer.de/blog/informationsschutz-in-liefernetzwerken-supply-chain-risk-management/, zuletzt abgerufen am 23.06.2022.

Anhang – Fragebogen[57]

Abschnitt 1 – Einleitung
Seite
#Fragentyp: Text *# Anzeige-Logik: Alle Befragte*
Vielen Dank für Ihre Bereitschaft zur Teilnahme an dieser Befragung. Ziel der Befragung ist eine Bestandsaufnahme der Nutzung von Cloud-Diensten unter kleinen und mittelständischen Unternehmen. Die Befragung wird etwa 20 Minuten in Anspruch nehmen. Alle Antworten auf diesem Fragebogen werden vertraulich behandelt, d.h. die Antworten werden in keiner Weise mit Ihren persönlichen Daten in Verbindung gebracht. Die Antworten werden ausschließlich für Forschungszwecke verwendet. Die Befragung wurde von der Bundesnetzagentur beauftragt. Durchgeführt wird die Befragung von der WIK-Consult GmbH und dem Umfragezentrum Bonn. Für Rückfragen stehen wir jederzeit gerne zur Verfügung. WIK-Consult GmbH Frau Serpil Taş Tel.: +49 2224 92 25-96 e-mail: s.tas@wik-consult.com
Abschnitt 2 – Adoption von Cloud-Diensten
Seite
#Fragentyp: Text *# Anzeige-Logik: Alle Befragte*
Unter Cloud-Diensten versteht man IT-Infrastrukturen und Anwendungen (z.B. Speicherplatz, Rechenleistung, Entwicklungsumgebungen oder Anwendungssoftware), die als **Dienstleistung über das Internet** bereitgestellt werden und für den Nutzer geräte- und ortsunabhängig zugänglich sind (z.B. über Programmierschnittstellen (API), Webseiten oder Apps). Bei der Nutzung von Cloud-Diensten werden gespeicherte oder verarbeitete Daten bzw. Informationen in der Regel auf externen Servern gelagert. Beispiele für Cloud-Dienste: • cloudbasierte CRM-, HR-, DMS-, ERP-, Sicherheitsanwendungen u.a. von Salesforce, SAP, Datev, Oracle, Amagno, Sophos etc. • cloudbasierte Office- / Kollaborationsanwendungen wie Microsoft 365 (z.B. SharePoint, Skype, Teams, oneDrive), Google Worksuit (z.B. Docs, Gmail, Drive etc.), Zoom, Adobe Creative Cloud etc. • Speicherplatz, Rechenleistung und / oder Entwicklungsumgebungen von Amazon Web Services (AWS), IBM Cloud, Google Cloud, Microsoft Azure etc.

57 Hier ist der CATI-Fragebogen angehangen. Änderungen die für die Online-Version des Fragebogens vorgenommen wurden, sind entsprechend gekennzeichnet. Die zusätzlichen Erläuterungen wurden bei der CATI-Befragung entweder je nach Bedarf oder immer den Befragten vorgelesen. Bei der Online-Befragung wurden sie zumeist durch Mouseover umgesetzt.

Seite
#Fragentyp: Single Choice *# Anzeige-Logik: Alle Befragte*
[q01] Nutzt Ihr Unternehmen derzeit mindestens einen Cloud-Dienst? <1> Ja <2> Nein <777> Weiß nicht / keine Angabe
Seite
#Fragentyp: Freitext - Anzahl [keine negative Zahlen erlaubt, Dezimalzahlen erlauben] *# Anzeige-Logik: Wenn q01==1 [Befragte, die Cloud-Dienste nutzen]*
[q02] Wie lange nutzen Sie bereits Cloud-Dienste in Ihrem Unternehmen? *[Anzahl]* Jahre *[Anzahl]* Monate <777> Weiß nicht / keine Angabe
Seite
#Fragentyp: Single Choice *# Anzeige-Logik: Wenn q01==2,777 [Befragte, die Cloud-Dienste nicht nutzen oder „weiß nicht / keine Angabe“ angegeben haben]*
[q03] Diskutiert oder plant Ihr Unternehmen die Nutzung von Cloud-Diensten? <1> Ja <2> Nein <777> Weiß nicht / keine Angabe
Seite
#Fragentyp: Single Choice *# Anzeige-Logik: Wenn q03==2,777 [Befragte, die „Nein“ oder „weiß nicht / keine Angabe“ angegeben haben]*
[q04] Sie haben soeben angegeben, dass Sie die Nutzung von Cloud-Diensten weder diskutieren noch planen. Welche der folgenden Aussagen treffen auf Ihr Unternehmen zu? <1>Wir haben uns noch nicht mit einer möglichen Nutzung von Cloud-Diensten in unserem Unternehmen befasst. <2>Wir haben uns gegen die Nutzung von Cloud-Diensten entschieden. <777> Weiß nicht / keine Angabe
Seite
#Fragentyp: Single Choice *# Anzeige-Logik: Wenn q03==1 [Befragte, die eine Nutzung diskutieren / planen]*

[q05] Wann werden Sie Cloud-Dienste in Ihrem Unternehmen voraussichtlich einführen?

<1>In ca. 1-3 Monaten
<2>In ca. 4-6 Monaten
<3>In ca. 7-12 Monaten
<4>Zu einem späteren Zeitpunkt
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Single Choice
 # Anzeige-Logik: Wenn q01==1 [Nutzer]

[q07] Wie stark war bzw. ist Ihr Unternehmen bei der Wahl des Cloud-Dienstes bzw. Cloud-Providers sowie der Implementierung und Betreuung während des Betriebs der Cloud-Dienste beteiligt?

Bitte antworten Sie auf einer Skala von 0 bis 10.
Die 0 steht für "überhaupt nicht beteiligt" (d.h. Sie haben die Wahl des Cloud-Dienstes / Providers sowie die Implementierung und Betreuung während des Betriebs einem IT-Dienstleister überlassen).
Die 10 steht für "sehr stark beteiligt" (d.h. Sie haben die Wahl des Cloud-Dienstes / Providers sowie die Implementierung und Betreuung während des Betriebs selbstständig übernommen).

<666> Trifft nicht zu - unser Unternehmen nutzt nur von z.B. Auftraggebern, Lieferanten etc. vorgegebene Cloud-Dienste
<777> Weiß nicht / keine Angabe

[Anpassung der Frage für CAWI:
[q07] Wie stark war bzw. ist Ihr Unternehmen bei der Wahl des Cloud-Dienstes bzw. Cloud-Providers sowie der Implementierung und Betreuung während des Betriebs der Cloud-Dienste beteiligt?

<1> 0 - überhaupt nicht beteiligt (Wir haben die Wahl des Cloud-Dienstes / Providers sowie die Implementierung und Betreuung während des Betriebs einem IT-Dienstleister überlassen).
<2>1
<3>2
<4>3
<5>4
<6>5
<7>6
<8>7
<9>8
<10> 9
<11> 10 – sehr stark beteiligt (Wir haben die Wahl des Cloud-Dienstes / Providers sowie die Implementierung und Betreuung während des Betriebs selbstständig übernommen).
<666> Trifft nicht zu - unser Unternehmen nutzt nur von z.B. Auftraggebern, Lieferanten etc. vorgegebene Cloud-Dienste
<777> Weiß nicht / keine Angabe]

Seite

#Fragentyp: Single Choice

 # Anzeige-Logik: Wenn q07==666 [Nutzer, die keine eigenen Cloud-Dienste verwenden]

[q03a] Diskutieren oder planen Sie in Ihrem Unternehmen die Einführung von Cloud-Diensten?

<1> Ja
<2> Nein
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Single Choice

 # Anzeige-Logik: Wenn q03a==1 [Befragte, die die Nutzung planen]

[q04a] Wann werden Sie Cloud-Dienste in Ihrem Unternehmen voraussichtlich einführen?

<1>In ca. 1-3 Monaten
<2>In ca. 4-6 Monaten
<3>In ca. 7-12 Monaten
<4>Zu einem späteren Zeitpunkt
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Single Choice

 # Anzeige-Logik: Wenn [q01==2,777 UND q03 == 1] ODER q03a==1 [Planer]

[q08] Wie stark ist Ihr Unternehmen bei der Wahl des Cloud-Dienstes bzw. Cloud-Providers sowie der Implementierung und Betreuung während des Betriebs der Cloud-Dienste beteiligt bzw. wird es voraussichtlich beteiligt sein?

Bitte antworten Sie auf einer Skala von 0 bis 10.
Die 0 steht für "überhaupt nicht beteiligt" (d.h. Sie werden die Wahl des Cloud-Dienstes / Providers sowie die Implementierung und Betreuung während des Betriebs einem IT-Dienstleister überlassen).
Die 10 steht für "sehr stark beteiligt" (d.h. Sie werden die Wahl des Cloud-Dienstes / Providers sowie die Implementierung und Betreuung während des Betriebs selbstständig übernehmen).

<777> Weiß nicht / keine Angabe

[Anpassung der Frage für CAWI:

[q08] Wie stark ist Ihr Unternehmen bei der Wahl des Cloud-Dienstes bzw. Cloud-Providers sowie der Implementierung und Betreuung während des Betriebs der Cloud-Dienste beteiligt bzw. wird es voraussichtlich beteiligt sein?

<1> 0 - überhaupt nicht beteiligt (Wir werden die Wahl des Cloud-Dienstes / Providers sowie die Implementierung und Betreuung während des Betriebs einem IT-Dienstleister überlassen).
<2>1

<3>2
<4>3
<5>4
<6>5
<7>6
<8>7
<9>8
<10> 9
<11> 10 – sehr stark beteiligt (Wir werden die Wahl des Cloud-Dienstes / Providers sowie die Implementierung und Betreuung während des Betriebs selbstständig übernehmen).
<666> Trifft nicht zu - unser Unternehmen nutzt nur von z.B. Auftraggebern, Lieferanten etc. vorgegebene Cloud-Dienste
<777> Weiß nicht / keine Angabe]

Seite

#Fragentyp: Single Choice
 # Anzeige-Logik: Do not show question, test mode, sort respondents into three groups

[q06] Filter: Der Filter dient der Gruppierung der befragten KMU in eine der drei Nutzergruppen.

<1> *[Wenn q01==1 UND q07!=666]* KMU, die Cloud-Dienste bereits nutzen
<2>*[Wenn (q01==2,777 UND q03==1) ODER q03a==1]* KMU, die eine Nutzung von Cloud-Diensten diskutieren / planen
<3>*[Wenn (q01==2 UND q03==2,777) ODER [q01==777 UND q03==2] ODER [q03a==2,777]* KMU, die keine Cloud-Dienste nutzen und die Nutzung nicht diskutieren / planen
<4>*[Wenn q01==777 UND q03==777]* KMU, die nicht wissen ob sie Cloud-Dienste nutzen oder eine Nutzung planen

Abschnitt 3 –Treiber und Hemmnisse der Nutzung von Cloud-Diensten, Nutzungsmuster

Seite

#Fragentyp: Multiple Choice, randomisiert
#Anzeige-Logik: Wenn q06==1,2 [Nutzer und Planer]

[q09] Welche der folgenden Faktoren motivieren in Ihrem Unternehmen den Einsatz von Cloud-Diensten?

<1>Flexible Skalierbarkeit der IT-Ressourcen
<2>Kosteneinsparungen bei der internen IT *[Erläuterung: z.B. in IT-Infrastruktur, Hardware, Software, IT-Support, IT-Administration, Informationssicherheit]*
<3>Geräte-, zeit- und ortsunabhängiger Zugriff auf Daten und Anwendungen
<4>Zugang zu speziellen (Web-)Anwendungen (CRM-, ERP-, DMS-, Office- / Kollaborationsanwendungen etc.)
<5>(Vertraglich) Garantierte Informationssicherheit bzw. garantierter Datenschutz
<6>(Vertraglich) Garantierte Performance, Verfügbarkeit und Zuverlässigkeit des Cloud-Dienstes
<7>Leichterer Daten- und / oder Informationsaustausch innerhalb des Unternehmens

<8>Leichterer Daten- und / oder Informationsaustausch mit anderen Unternehmen bzw. Organisationen

<9>Stärkung der Wettbewerbs- und / oder Innovationsfähigkeit

<666> Andere Faktoren: *[Freitextfeld] (fixiert)*

<777> Weiß nicht / keine Angabe *(fixiert)*

Seite

#Fragentyp: Multiple Choice, non-randomisiert [Reihenfolge der Nennung: Privat, Community, Public Cloud]

#Anzeige-Logik: Wenn q06==1[Nutzer]

[q10] Welche der folgenden Cloud Bereitstellungsmodelle nutzt Ihr Unternehmen?

<1>Private Cloud *[Erläuterung: Die Cloud-Infrastruktur steht ausschließlich Ihrem Unternehmen zur Verfügung.]*

<2>Community Cloud *[Erläuterung: Die Cloud-Infrastruktur wird von Ihrem Unternehmen und anderen Institutionen, die zur gleichen Gemeinschaft gehören und gemeinsame Anliegen haben (z.B. Unternehmensnetzwerke, Genossenschaften), geteilt.]*

<3>Public Cloud *[Erläuterung: Die Cloud-Infrastruktur wird von mehreren Unternehmen geteilt und jedem Unternehmen werden eigene virtuelle Kapazitäten zur Verfügung gestellt.]*

<666> Andere: *[Freitextfeld]*

<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Multiple Choice, nicht randomisiert

#Anzeige-Logik: Wenn q06==1 [Nutzer]

[q11] Welche Art Cloud-Dienstleistung nutzt Ihr Unternehmen? Nutzen Sie…

<*1*>Vorgefertigte Anwendungsprogramme, die über die Cloud-Infrastruktur des Anbieters betrieben werden *[Erläuterung: Beispiele sind: Office-, Kollaborationsanwendungen wie Microsoft 365 (also z. B. SharePoint, Skype, Teams, oneDrive), Google Worksuit (z.B. Docs, Gmail, Drive etc.), Zoom, Adobe Creative Cloud oder cloudbasierte CRM-, DMS-, ERP-, Sicherheitsanwendungen etc. u.a. von Salesforce, SAP, Datev, Oracle, Amagno oder Sophos. Diese Dienste sind auch bekannt als: Software as a Service (SaaS)]*

<2>IT-Ressourcen wie Rechenleistung, Speicher, Netze oder die Virtualisierung von Hardware *[Erläuterung: Beispiele sind: Elastic Computing Cloud, Simple Storage Service (von Amazon Web Services), Compute Engine, Cloud Storage (z. B. Google Cloud). Diese Dienste sind auch bekannt als: Infrastructure as a Service (IaaS)]*

<3>Integrierte Laufzeit- oder Entwicklungsumgebung für Ausführung und Entwicklung unternehmenseigener Anwendungen *[Erläuterung: Beispiele sind: Google App Engine (Google Cloud), AWS Elastic Beanstalk (von Amazon Web Services). Diese Dienste sind auch bekannt als: Platform as a Service (PaaS)]*

<777> Weiß nicht / keine Angabe

[Anpassung der Frage für CAWI:

[q11] Welche Art Cloud-Dienstleistung nutzt Ihr Unternehmen?

<1>Vorgefertigte Anwendungsprogramme, die über die Cloud-Infrastruktur des Anbieters betrieben werden (Fachbegriff: Software as a Service (SaaS)) *[Erläuterung: Beispiele sind: Office-, Kollaborationsanwendungen wie Microsoft 365 (also z. B. SharePoint, Skype, Teams, oneDrive), Google Worksuit (z.B. Docs, Gmail, Drive etc.), Zoom, Adobe Creative Cloud oder cloudbasierte CRM-, DMS-, ERP-, Sicherheitsanwendungen etc. u.a. von Salesforce, SAP, Datev, Oracle, Amagno oder Sophos.]*

<2>IT-Ressourcen wie Rechenleistung, Speicher, Netze oder die Virtualisierung von Hardware (Fachbegriff: Infrastructure as a Service (IaaS)) *[Erläuterung: Beispiele sind: Elastic Computing Cloud, Simple Storage Service (von Amazon Web Services), Compute Engine, Cloud Storage (z. B. Google Cloud).]*

<3>Integrierte Laufzeit- oder Entwicklungsumgebung für Ausführung und Entwicklung unternehmenseigener Anwendungen (Fachbegriff: Platform as a Service (PaaS)) *[Erläuterung: Beispiele sind: Google App Engine (Google Cloud), AWS Elastic Beanstalk (von Amazon Web Services).]*

<777> Weiß nicht / keine Angabe]

Seite

#Fragentyp: Multiple Choice, randomisiert

#Anzeige-Logik: Wenn q06==1 [Nutzer]

[q12] Welche der folgenden IT-Dienste oder Anwendungen nutzen Sie derzeit in der Cloud?

<1>Datensicherung bzw. Datenspeicherung

<2>Office- / Kollaborationsanwendungen (inkl. Web- und Videokonferenz-Anwendungen)

<3>ERP-Anwendungen *[Erläuterung: ERP steht für Enterprise Resource Planning und bezeichnet eine Softwarelösung zur Ressourcenplanung.]*

<4>CRM-Anwendungen *[Erläuterung: CRM steht für Customer Relationship Management und bezeichnet eine Softwarelösung zur systematischen Gestaltung der Beziehungen und Interaktionen mit Kunden.]*

<5>HR-Anwendungen *[Erläuterung: HR steht für Human Resources]*

<6>Datenmanagementsysteme

<7>Sicherheitsanwendungen (z.B. Anti-virus Programme)

<8>KI-, IoT- oder Blockchain-Anwendungen

<9>Softwareanwendungen im Finanz- oder Rechnungswesen

<666> Andere IT-Dienste oder Anwendungen: *[Freitextfeld] (fixiert)*

<777> Weiß nicht / keine Angabe *(fixiert)*

[Anpassung der Frage für CAWI:

[q12] Welche IT-Dienste oder Anwendungen nutzen Sie derzeit in der Cloud?

<1>Datensicherung / -speicherung

<2>Office- / Kollaborationsanwendungen (inkl. Web- und Videokonferenz-Anwendungen)

<3>ERP-Anwendungen *[Erläuterung: ERP steht für Enterprise Resource Planning und bezeichnet eine Softwarelösung zur Ressourcenplanung.]*

<4>CRM-Anwendungen *[Erläuterung: CRM steht für Customer Relationship Management und bezeichnet eine Softwarelösung zur systematischen Gestaltung der Beziehungen und Interaktionen mit Kunden.]*

<5>HR-Anwendungen *[Erläuterung: HR steht für Human Resources]*

<6>Datenmanagementsysteme

<7>Sicherheitsanwendungen (z.B. Anti-virus Programme)

<8>KI-, IoT- oder Blockchain-Anwendungen *[Erläuterung: IoT: Internet of Things]*
<9>Softwareanwendungen im Finanz- oder Rechnungswesen
<666> Andere IT-Dienste oder Anwendungen: [Freitextfeld] (fixiert)
<777> Weiß nicht / keine Angabe (fixiert)]

Seite

#Fragentyp: Multiple Choice, randomisiert
#Anzeige-Logik: Wenn q06==1 [Nutzer]

[q13] Bei welchen der folgenden Provider hat Ihr Unternehmen Cloud-Dienste angemietet bzw. abonniert?

<1>Amazon / Amazon Web Services (AWS)
<2>Microsoft
<3>Google
<4>Deutsche Telekom *[Erläuterung: OpenCloud, MagentaCloud, TelekomCloud]*
<5>IBM
<6>OVH
<7>IONOS
<8>Salesforce
<9>SAP
<10> Oracle
<666> Andere europäische Provider: *[Freitextfeld]* (fixiert)
<667> Andere nicht-europäische Provider: *[Freitextfeld]* (fixiert)
<777> Weiß nicht / keine Angabe *(fixiert)*

[Anpassung der Frage für CAWI:
[q13] Bei welchem bzw. welchen Providern hat Ihr Unternehmen die Cloud-Dienste angemietet / abonniert?

<1>Amazon / Amazon Web Services (AWS)
<2>Microsoft
<3>Google
<4>Deutsche Telekom [Erläuterung: OpenCloud, MagentaCloud, TelekomCloud]
<5>IBM
<6>OVH
<7>IONOS
<8>Salesforce
<9>SAP
<10> Oracle
<666> Andere europäische Provider: *[Freitextfeld] (fixiert)*
<667> Andere nicht-europäische Provider: *[Freitextfeld] (fixiert)*
<777> Weiß nicht / keine Angabe *(fixiert)*]

Seite

#Fragentyp: Single Choice

#Anzeige-Logik: Wenn q13==667 UND q13!=1,2,3,5,8,10 [Nutzer eines nicht-europäischen Providers, der gleichzeitig keinen US-amerikanischen Provider in 13 ausgewählt hat]

[q13a] Sie haben angegeben, Cloud-Dienste eines nicht-europäischen Providers zu nutzen. Handelt es sich dabei um einen US-amerikanischen Provider?

<1>Ja
<2>Nein
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Multiple Choice, randomisiert

#Anzeige-Logik: Wenn q06==1 [Nutzer]

[q14] Welche Daten werden in Ihrem Unternehmen in der Cloud gespeichert und / oder verarbeitet? Sind das…

<1>Finanzdaten bzw. Abrechnungsdaten
<2>Personenbezogene Kundendaten
<3>Daten über Geschäftspartner und / oder Lieferanten
<4>Produktionsdaten
<5>Forschungs- und Entwicklungsdaten
<6>Personenbezogene Personaldaten
<7>Vertriebs- und / oder Absatzdaten
<8>Dokumente und / oder Bildmaterial
<666> Andere Daten *[Erläuterung: z.B. anonymisierte / pseudonymisierte Kunden- oder Personaldaten und andere Betriebsdaten]*: *[Freitextfeld] (fixiert)*
<777> Weiß nicht / keine Angabe *(fixiert)*

[Anpassung der Frage für CAWI:
[q14] Welche Daten werden in Ihrem Unternehmen in der Cloud gespeichert und / oder verarbeitet?

<1>Finanzdaten bzw. Abrechnungsdaten
<2>Personenbezogene Kundendaten
<3>Daten über Geschäftspartner und / oder Lieferanten
<4>Produktionsdaten
<5>Forschungs- und Entwicklungsdaten
<6>Personenbezogene Personaldaten
<7>Vertriebs- und / oder Absatzdaten
<8>Dokumente und / oder Bildmaterial
<666> Andere Daten *[Erläuterung: z.B. anonymisierte / pseudonymisierte Kunden- oder Personaldaten und andere Betriebsdaten]*: *[Freitextfeld] (fixiert)*
<777> Weiß nicht / keine Angabe *(fixiert)*]

Seite

#Fragentyp: Multiple Choice, nicht randomisiertd [Reihenfolge der Nennung: Privat, Community, Public Cloud]

#Anzeige-Logik: Wenn q06==2 [Planer]

[q15] Welche der folgenden Cloud Bereitstellungsmodelle zieht Ihr Unternehmen in Betracht?

<1>Private Cloud *[Erläuterung: Die Cloud-Infrastruktur steht ausschließlich Ihrem Unternehmen zur Verfügung.]*

<2>Community Cloud *[Erläuterung: Die Cloud-Infrastruktur wird von Ihrem Unternehmen und anderen Institutionen, die zur gleichen Gemeinschaft gehören und gemeinsame Anliegen haben (z.B. Unternehmensnetzwerke, Genossenschaften), geteilt.*

<3>Public Cloud *[Erläuterung: Die Cloud-Infrastruktur wird von mehreren Unternehmen geteilt und jedem Unternehmen werden eigene virtuelle Kapazitäten zur Verfügung gestellt.]*

<666> Andere: *[Freitextfeld]*

<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Multiple Choice, nicht randomisiert

#Anzeige-Logik: Wenn q06==2 [Planer]

[q16] Welche Art Cloud-Dienstleistung zieht Ihr Unternehmen in Betracht?

*<1>*Vorgefertigte Anwendungsprogramme, die über die Cloud-Infrastruktur des Anbieters betrieben werden *[Erläuterung: Beispiele sind: Office-, Kollaborationsanwendungen wie Microsoft 365 (also z. B. SharePoint, Skype, Teams, oneDrive), Google Worksuit (z.B. Docs, Gmail, Drive etc.), Zoom, Adobe Creative Cloud oder cloudbasierte CRM-, DMS-, ERP-, Sicherheitsanwendungen etc. u.a. von Salesforce, SAP, Datev, Oracle, Amagno oder Sophos. Diese Dienste sind auch bekannt als: Software as a Service (SaaS)]*

*<2>*IT-Ressourcen wie Rechenleistung, Speicher, Netze oder die Virtualisierung von Hardware *[Erläuterung: Beispiele sind: Elastic Computing Cloud, Simple Storage Service (von Amazon Web Services), Compute Engine, Cloud Storage (z. B. Google Cloud). Diese Dienste sind auch bekannt als: Infrastructure as a Service (IaaS)]*

<3>Integrierte Laufzeit- oder Entwicklungsumgebung für Ausführung und Entwicklung unternehmenseigener Anwendungen *[Erläuterung: Beispiele sind: Google App Engine (Google Cloud), AWS Elastic Beanstalk (von Amazon Web Services) INT: Diese Dienste sind auch bekannt als: Platform as a Service (PaaS)]*

<777> Weiß nicht / keine Angabe

[Anpassung der Frage für CAWI:

[q16] Welche Art Cloud-Dienstleistung zieht Ihr Unternehmen in Betracht?

*<1>*Vorgefertigte Anwendungsprogramme, die über die Cloud-Infrastruktur des Anbieters betrieben werden (Fachbegriff: Software as a Service (SaaS)) *[Erläuterung: Beispiele sind: Office-, Kollaborationsanwendungen wie Microsoft 365 (also z. B. SharePoint, Skype, Teams, oneDrive), Google Worksuit (z.B. Docs, Gmail, Drive etc.), Zoom, Adobe Creative Cloud oder cloudbasierte CRM-, DMS-, ERP-, Sicherheitsanwendungen etc. u.a. von Salesforce, SAP, Datev, Oracle, Amagno oder Sophos.]*

<2>IT-Ressourcen wie Rechenleistung, Speicher, Netze oder die Virtualisierung von Hardware (Fachbegriff: Infrastructure as a Service (IaaS)) *[Erläuterung: Beispiele sind: Elastic Computing Cloud, Simple Storage Service (von Amazon Web Services), Compute Engine, Cloud Storage (z. B. Google Cloud).]*

<3>Integrierte Laufzeit- oder Entwicklungsumgebung für Ausführung und Entwicklung unternehmenseigener Anwendungen (Fachbegriff: Platform as a Service (PaaS)) *[Erläuterung: Beispiele sind: Google App Engine (Google Cloud), AWS Elastic Beanstalk (von Amazon Web Services).]*

<777> Weiß nicht / keine Angabe]

page break

#Fragentyp: Multiple Choice, randomisiert

#Anzeige-Logik: Wenn q06==2 [Planer]

[q17] Welche der folgenden IT-Dienste oder Anwendungen planen Sie in der Cloud zu nutzen?

<1>Datensicherung bzw. -speicherung

<2>Office- bzw. Kollaborationsanwendungen (inkl. Web- und Videokonferenzanwendungen)

<3>ERP-Anwendungen *[Erläuterung: ERP steht für Enterprise Resource Planning und bezeichnet eine Softwarelösung zur Ressourcenplanung.]*

<4>CRM-Anwendungen *[Erläuterung: CRM steht für Customer Relationship Management und bezeichnet eine Softwarelösung zur systematischen Gestaltung der Beziehungen und Interaktionen mit Kunden.]*

<5>HR-Anwendungen *[Erläuterung: HR steht für Human Resources*]

<6>Datenmanagementsysteme

<7>Sicherheitsanwendungen (z.B. Anti-Virus Programme)

<8>KI-, IoT- oder Blockchain-Anwendungen

<9>Softwareanwendungen im Finanz- oder Rechnungswesen

<666> Andere IT-Dienste oder Anwendungen: *[Freitextfeld] (fixiert)*

<777> Weiß nicht / keine Angabe *(fixiert)*

[Anpassung der Frage für CAWI:

[q17] Welche der folgenden IT-Dienste oder Anwendungen planen Sie in der Cloud zu nutzen?

<1>Datensicherung / -speicherung

<2>Office- / Kollaborationsanwendungen (inkl. Web- und Videokonferenz-Anwendungen)

<3>ERP-Anwendungen *[Erläuterung: ERP steht für Enterprise Resource Planning und bezeichnet eine Softwarelösung zur Ressourcenplanung.]*

<4>CRM-Anwendungen *[Erläuterung: CRM steht für Customer Relationship Management und bezeichnet eine Softwarelösung zur systematischen Gestaltung der Beziehungen und Interaktionen mit Kunden.]*

<5>HR-Anwendungen *[Erläuterung: HR steht für Human Resources]*

<6>Datenmanagementsysteme

<7>Sicherheitsanwendungen (z.B. Anti-virus Programme)

<8>KI-, IoT- oder Blockchain-Anwendungen *[Erläuterung: IoT: Internet of Things]*

<9>Softwareanwendungen im Finanz- oder Rechnungswesen

<667> Andere IT-Dienste oder Anwendungen: [Freitextfeld] (fixiert)

Weiß nicht / keine Angabe (fixiert)]

Seite
#Fragentyp: Multiple Choice, randomisiert *#Anzeige-Logik: Wenn q06==2 [Planer]*
[q18] Bei welchen der folgenden Provider plant Ihr Unternehmen Cloud-Dienste anzumieten bzw. zu abonnieren? <1>Amazon / Amazon Web Services (AWS) <2>Microsoft <3>Google <4>Deutsche Telekom *[Erläuterung: OpenCloud, MagentaCloud, TelekomCloud]* <5>IBM <6>OVH <7>IONOS <8>Salesforce <9>SAP <10> Oracle <666> Andere europäische Provider: *[Freitextfeld] (fixiert)* <667> Andere nicht-europäische Provider: *[Freitextfeld] (fixiert)* <777> Weiß nicht / keine Angabe *(fixiert)* [Anpassung der Frage für CAWI: [q18] Bei welchem bzw. welchen Providern plant Ihr Unternehmen die Cloud-Dienste anzumieten / zu abonnieren? <1>Amazon / Amazon Web Services (AWS) <2>Microsoft <3>Google <4>Deutsche Telekom [Erläuterung: OpenCloud, MagentaCloud, TelekomCloud] <5>IBM <6>OVH <7>IONOS <8>Salesforce <9>SAP <10> Oracle <666> Andere europäische Provider: *[Freitextfeld] (fixiert)* <667> Andere nicht-europäische Provider: *[Freitextfeld] (fixiert)* <777> Weiß nicht / keine Angabe *(fixiert)*]
Seite
#Fragentyp: Single Choice *#Anzeige-Logik: Wenn q18==667 UND q18!=1,2,3,5,8,10 [Befragter, der einen nicht-europäischen Providers zu nutzen plant, der gleichzeitig keinen US-amerikanischen Provider in 17 ausgewählt hat]*

[q18a] Sie haben angegeben, die Nutzung von Cloud-Diensten eines nicht-europäischen Providers in Betracht zu ziehen. Handelt es sich dabei um einen US-amerikanischen Provider?

<1>Ja
<2>Nein
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Multiple Choice, randomisiert
#Anzeige-Logik: Wenn q06==2 [Planer]

[q19] Welche Daten plant Ihr Unternehmen in der Cloud zu speichern und / oder zu verarbeiten?

<1>Finanzdaten bzw. Abrechnungsdaten
<2>Personenbezogene Kundendaten
<3>Daten über Geschäftspartner und / oder Lieferanten
<4>Produktionsdaten
<5>Forschungs- und Entwicklungsdaten
<6>Personenbezogene Personaldaten
<7>Vertriebs- und / oder Absatzdaten
<8>Dokumente und / oder Bildmaterial
<666> Andere Daten *[Erläuterung: z.B. anonymisiert / pseudonymisiert Kunden- oder Personaldaten und andere Betriebsdaten]*: *[Freitextfeld] (fixiert)*
<777> Weiß nicht / keine Angabe *(fixiert)*

Seite

#Fragentyp: Freitextfeld - Zahl [keine negativen Werte erlauben, Dezimalzahlen erlauben]
#Anzeige-Logik: Wenn q06==1 [Nutzer]

[q20] Wie hoch sind Ihre jährlichen Ausgaben für die Cloud-Dienste? Sollten Sie sich nicht sicher sein, dann schätzen Sie bitte.

[Zahl] Euro
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Freitextfeld - Zahl [keine negativen Werte erlauben, Dezimalzahlen erlauben]
#Anzeige-Logik: Wenn q06==2 [Planer]

[q21] Wie hoch schätzen Sie Ihre jährlichen Ausgaben für die Cloud-Dienste ein?

[Zahl] Euro
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Single Choice
#Anzeige-Logik: Wenn q06==1,2 [Nutzer und Planer]

[q22] Wie wichtig war bzw. ist Ihrem Unternehmen der Preis bei der Auswahl des Cloud-Providers auf einer Skala von 1=überhaupt nicht wichtig bis 5=sehr wichtig?

<1>Überhaupt nicht wichtig
<2> XXX
<3> XXX
<4> XXX
<5> Sehr wichtig
<777> Weiß nicht / keine Angabe

[Anpassung der Frage für CAWI:
[q22] Wie wichtig war / ist Ihrem Unternehmen der Preis bei der Auswahl des Cloud-Providers?

<1>Überhaupt nicht wichtig
<2> XXX
<3> XXX
<4> XXX
<5> Sehr wichtig
<777> Weiß nicht / keine Angabe]

Seite

#Fragentyp: Single Choice, randomisiert
#Anzeige-Logik: Wenn q06==1,2 [Nutzer und Planer]

[q23] Wie wichtig waren bzw. sind Ihnen die folgenden „betriebsrelevanten Leistungen“ bei der Wahl des Cloud-Providers auf einer Skala von 1=überhaupt nicht wichtig bis 5=sehr wichtig?

-[q23_1] Performance, z.B. hohe Verfügbarkeit, geringe Latenz, geringe Fehlerraten etc.
-[q23_2] Flexible Skalierbarkeit
-[q23_3] Zuverlässigkeit
-[q23_4] Portabilität von Daten und Anwendungen
-[q23_5] Interoperabilität mit Cloud-Diensten anderer Provider
-[q23_6] Funktionalität
-[q23_7] Individualisierbarkeit
-[q23_8] Benutzerfreundlichkeit
-[q23_9] Guter Support bzw. Beratung

<1>Überhaupt nicht wichtig
<2>XXX
<3>XXX
<4>XXX
<5>Sehr wichtig
<777> Weiß nicht / keine Angabe

[Anpassung der Frage für CAWI:

[q23] Wie wichtig waren bzw. sind Ihnen die folgenden „betriebsrelevanten Leistungen“ bei der Wahl des Cloud-Providers?

[q23_1] Performance, z.B. hohe Verfügbarkeit, geringe Latenz, geringe Fehlerraten etc.
[q23_2] Flexible Skalierbarkeit
[q23_3] Zuverlässigkeit
[q23_4] Portabilität von Daten und Anwendungen
[q23_5] Interoperabilität mit Cloud-Diensten anderer Provider
[q23_6] Funktionalität
[q23_7] Individualisierbarkeit
[q23_8] Benutzerfreundlichkeit
[q23_9] Guter Support bzw. Beratung

<1>Überhaupt nicht wichtig
<2> XXX
<3> XXX
<4> XXX
<5> Sehr wichtig
<777> Weiß nicht / keine Angabe]

Seite

#Fragentyp: Single Choice, randomisiert
#Anzeige-Logik: Wenn q06==1,2 [Nutzer und Planer]

[q24] Wie wichtig waren bzw. sind Ihnen die folgenden Leistungen und Kriterien hinsichtlich „Sicherheit, Datenschutz und Organisation des Cloud-Providers“ bei der Wahl des Cloud-Providers auf einer Skala von 1=überhaupt nicht wichtig bis 5=sehr wichtig?

-[q24_1] Garantierte vollständige und zuverlässige Löschung von Daten bzw. Informationen
-[q24_2] Daten- bzw. Informationssicherheit, d.h. Maßnahmen zur Gewährleistung der Integrität, Vertraulichkeit, Verfügbarkeit von Daten bzw. Informationen
-[q24_3] Gewährleistung des Datenschutzes nach deutschem bzw. europäischem Recht (DSGVO, BDSG)
-[q24_4] Transparenz bezüglich möglicher Eingriffe bzw. Eingriffsrechte des Cloud-Providers, des Staates und anderer in Daten bzw. Informationen
-[q24_5] Rechenzentren im Rechtsgebiet der EU
-[q24_6] Hauptsitz im Rechtsgebiet der EU
-[q24_7] Finanzielle Stabilität des Cloud-Providers
-[q24_8] Reputation des Cloud-Providers
-[q24_9] Cloud-Zertifizierung und / oder Provider-Zertifizierung

<1>Überhaupt nicht wichtig
<2>XXX
<3>XXX
<4>XXX
<5>Sehr wichtig
<777> Weiß nicht / keine Angabe

[Anpassung der Frage für CAWI:

[q24] Wie wichtig waren bzw. sind Ihnen die folgenden Leistungen und Kriterien hinsichtlich „Sicherheit, Datenschutz und Organisation des Cloud-Providers“ bei der Wahl des Cloud-Providers?

[q24_1] Garantierte vollständige und zuverlässige Löschung von Daten bzw. Informationen

[q24_2] Daten- bzw. Informationssicherheit, d.h. Maßnahmen zur Gewährleistung der Integrität, Ver-traulichkeit, Verfügbarkeit von Daten bzw. Informationen

[q24_3] Gewährleistung des Datenschutzes nach deutschem bzw. europäischem Recht (DSGVO, BDSG)

[q24_4] Transparenz bezüglich möglicher Eingriffe bzw. Eingriffsrechte des Cloud-Providers, des Staates und anderer in Daten bzw. Informationen

[q24_5] Rechenzentren im Rechtsgebiet der EU

[q24_6] Hauptsitz im Rechtsgebiet der EU

[q24_7] Finanzielle Stabilität des Cloud-Providers

[q24_8] Reputation des Cloud-Providers

[q24_9] Cloud-Zertifizierung und / oder Provider-Zertifizierung

<1>Überhaupt nicht wichtig

<2> XXX

<3> XXX

<4> XXX

<5> Sehr wichtig

<777> Weiß nicht / keine Angabe]

Seite

#Fragentyp: Single Choice

#Anzeige-Logik: Wenn q06==1,2 [Nutzer und Planer]

[q27] Gab bzw. gibt es andere wichtige Kriterien oder Leistungen bei der Wahl des Cloud-Providers?

<1> Ja, *[Freitextfeld]*

<2>Nein

<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Multiple Choice, randomisiert

#Anzeige-Logik: Wenn q04==2 ODER q06==2 ODER q07==666[Planer & Nicht-Nutzer / -Planer, die sich gegen Cloud-Dienste entschieden haben & Nutzer, die nur vorgegebene Cloud-Dienste verwenden]

[q28] Sie haben angegeben, in Ihrem Unternehmen bisher noch keine Cloud-Dienste zu verwenden. Was sind die Gründe dafür?

<1>Bedenken hinsichtlich der Performance, Verfügbarkeit und Zuverlässigkeit des Cloud-Dienstes

<2>Bedenken hinsichtlich der IT-Sicherheit

<3>Bedenken hinsichtlich der Informations- bzw. Datensicherheit (d. h. hinsichtlich der Integrität, Verfügbarkeit und Vertraulichkeit von Daten bzw. Informationen)

<4>Bedenken hinsichtlich des Datenzugriffs und der Datenverwendung durch Zweite und Dritte

<5>Abhängigkeit vom Provider

<6>Bedenken hinsichtlich der Einhaltung von Gesetzen und Vorschriften (inkl. DSGVO, BDSG)

<7>Es besteht kein Bedarf an Cloud-Lösungen

<8>Fehlendes Wissen über Potenzial bzw. Anwendungsmöglichkeiten

<9>Unternehmen besitzt eigene Server (On-Premise Lösung)

<666> Andere: *[Freitextfeld] (fixiert)*

<777> Weiß nicht / keine Angabe *(fixiert)*

Seite

#Fragentyp: Freitext

#Anzeige-Logik: Wenn q06==1,2 ODER q04==2 ODER q07==666 [Nutzer und Planer und Nicht-Nutzer, die sich gegen eine Nutzung entschieden haben und Nutzer, die nur vorgegebene Cloud-Dienste verwenden]

[q29] Bitte benennen Sie bis zu drei Vorteile bei der Nutzung von Cloud-Diensten von großen, nicht-europäischen Cloud-Providern aus Sicht Ihres Unternehmens im Vergleich zu europäischen Cloud-Providern.

<1>*[Freitextfeld]*

<2>*[Freitextfeld]*

<3>*[Freitextfeld]*

<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Freitext

#Anzeige-Logik: Wenn q06==1,2 ODER q04==2 ODER q07==666 [Nutzer und Planer und Nicht-Nutzer, die sich gegen eine Nutzung entschieden haben und *Nutzer, die nur vorgegebene Cloud-Dienste verwenden]*

[q30] Bitte benennen Sie bis zu drei Nachteile bei der Nutzung von Cloud-Diensten von großen, nicht-europäischen Cloud-Providern aus Sicht Ihres Unternehmens im Vergleich zu europäischen Cloud-Providern.

<1>*[Freitextfeld]*

<2>*[Freitextfeld]*

<3>*[Freitextfeld]*

<777> Weiß nicht / keine Angabe

Abschnitt 4 – Kenntnisstand zu Datenschutz- und Datensicherheitsregelungen

Seite

#Fragentyp: Single Choice

#Anzeige-Logik: Alle Befragte

[q31] Wie vertraut sind Sie in Ihrem Unternehmen mit der Datenschutzgrundverordnung (DSGVO) auf einer Skala von 1=überhaupt nicht vertraut bis 5=sehr vertraut?

<1>überhaupt nicht vertraut

<2>XXX
<3>XXX
<4>XXX
<5>Sehr vertraut
<777> Weiß nicht / keine Angabe

[Anpassung der Frage für CAWI:
[q31] Wie vertraut sind Sie in Ihrem Unternehmen mit der Datenschutzgrundverordnung (DSGVO)?

<1>überhaupt nicht vertraut
<2>XXX
<3>XXX
<4>XXX
<5>Sehr vertraut
<777> Weiß nicht / keine Angabe]

Seite

#Fragentyp: Single Choice

#Anzeige-Logik: Wenn q18==1,2,3,5,8,10 ODER q18a==1 ODER q13==1,2,3,5,8,10 ODER q13a==1 [Befragte, die einen amerikanischen Provider nutzen oder planen zu nutzen]

[q32] Wie vertraut sind Sie in Ihrem Unternehmen mit dem US CLOUD Act aus dem Jahr 2018 auf einer Skala von 1=überhaupt nicht vertraut bis 5=sehr vertraut?
[Erläuterung: Beim US CLOUD Act handelt es sich um ein seit 2018 bestehendes US-amerikanisches Gesetz, welches US-Anbieter elektronischer Kommunikations- oder Remote-Computing-Dienste dazu verpflichtet, US-Behörden sämtliche in ihrem Besitz, Gewahrsam oder ihrer Kontrolle befindlichen Daten offenzulegen und zwar unabhängig davon, ob die Daten innerhalb oder außerhalb der USA gespeichert sind.].

<1>überhaupt nicht vertraut
<2>XXX
<3>XXX
<4>XXX
<5>Sehr vertraut
<777> Weiß nicht / keine Angabe

[Anpassung der Frage für CAWI:
[q32] Wie vertraut sind Sie in Ihrem Unternehmen mit dem US CLOUD Act aus dem Jahr 2018?
[Erläuterung: Beim US CLOUD Act handelt es sich um ein seit 2018 bestehendes US-amerikanisches Gesetz, welches US-Anbieter elektronischer Kommunikations- oder Remote-Computing-Dienste dazu verpflichtet, US-Behörden sämtliche in ihrem Besitz, Gewahrsam oder ihrer Kontrolle befindlichen Daten offenzulegen und zwar unabhängig davon, ob die Daten innerhalb oder außerhalb der USA gespeichert sind.].

<1>überhaupt nicht vertraut

<2>XXX

<3>XXX

<4>XXX

<5>Sehr vertraut

<777> Weiß nicht / keine Angabe]

Seite

#Fragentyp: Multiple Choice, randomisiert

#Anzeige-Logik: Wenn q13==1,2,3,5,8,10 ODER q13a==1 [Befragte, die einen amerikanischen Provider nutzen]

[Wenn q32 = 1 oder 777: Erläuterung: Beim US CLOUD Act handelt es sich um ein seit 2018 bestehendes US-amerikanisches Gesetz, welches US-Anbieter elektronischer Kommunikations- oder Remote-Computing-Dienste dazu verpflichtet, US-Behörden sämtliche in ihrem Besitz, Gewahrsam oder ihrer Kontrolle befindlichen Daten offenzulegen und zwar unabhängig davon, ob die Daten innerhalb oder außerhalb der USA gespeichert sind.].

[q33] Welche Konsequenzen hatte der US CLOUD Act aus dem Jahr 2018 auf die Nutzung von Cloud-Diensten in Ihrem Unternehmen?

<1>Anpassung der internen Regelungen zur Speicherung bzw. Verarbeitung kritischer Daten und Informationen bei dem Cloud-Provider (z.B. Verzicht auf die Speicherung bzw. Verarbeitung kritischer Daten und Informationen)

<2>Anpassung der Verträge mit dem Cloud-Provider

<3>Wechsel des Cloud-Providers

<4>Keine Konsequenzen *(fixiert)*

<666> Andere Konsequenzen: *[Freitextfeld] (fixiert)*

<777> Weiß nicht / keine Angabe *(fixiert)*

[Anpassung der Frage für CAWI:

[q33] Welche Konsequenzen hatte der US CLOUD Act aus dem Jahr 2018 auf die Nutzung von Cloud-Diensten in Ihrem Unternehmen?

<1>Anpassung der internen Regelungen zur Speicherung bzw. Verarbeitung kritischer Daten und Informationen bei dem Cloud-Provider (z.B. Verzicht auf die Speicherung bzw. Verarbeitung kritischer Daten und Informationen)

<2>Anpassung der Verträge mit dem Cloud-Provider

<3>Wechsel des Cloud-Providers

<4>Keine Konsequenzen (fixiert)

<5>Andere Konsequenzen: [Freitextfeld] (fixiert)

<777> Weiß nicht / keine Angabe (fixiert)]

Seite

#Fragentyp: Multiple Choice, randomisiert

#Anzeige-Logik: Wenn q13==1,2,3,5,8,10 ODER q13a==1 [Befragte, die einen amerikanischen Provider nutzen]

[q34] Welche Konsequenzen hatte das Urteil des Europäischen Gerichtshofs bezüglich des Privacy-Shield-Abkommens (Schrems-II-Urteil) auf die Nutzung von Cloud-Diensten in Ihrem Unternehmen?

[Erläuterung: Grundsätzlich dürfen personenbezogene Daten nur an Länder außerhalb der EU oder des Europäischen Wirtschaftsraumes (EWR) übermittelt werden, wenn in diesen Drittländern das Schutzniveau der DSVGO erreicht wird. Das Privacy Shield-Abkommen zwischen der EU und den USA aus dem Jahr 2016 hatte festgestellt, dass in den USA ein angemessenes Schutzniveau für personenbezogene Daten gewährleistet wird. Mit dem Schrems II-Urteil des EuGH vom 16. Juli 2020 wurde der Privacy-Shield für ungültig erklärt.]

<1>Anpassung der internen Regelungen zur Speicherung bzw. Verarbeitung kritischer Daten und Informationen bei dem Cloud-Provider (z.B. Verzicht auf die Speicherung bzw. Verarbeitung kritischer Daten und Informationen)

<2>Anpassung der Verträge mit dem Cloud-Provider

<3>Wechsel des Cloud-Providers

<4>Keine Konsequenzen *(fixiert)*

<666> Andere Konsequenzen: *[Freitextfeld] (fixiert)*

<777> Weiß nicht / keine Angabe *(fixiert)*

Abschnitt 5 – Digitale Souveränität

Seite

#Fragentyp: Single Choice

#Anzeige-Logik: Alle Befragte

[q35] Ist Ihnen der Begriff „Digitale Souveränität“ bekannt?

[Erläuterung: Der Begriff digitale Souveränität umfasst die unabhängige Selbstbestimmung von Unternehmen in Bezug auf die Nutzung und Gestaltung digitaler Systeme und Dienste, sowie der darin erzeugten und gespeicherten Daten.

Digitale Souveränität wird durch die technologische Unabhängigkeit von Unternehmen und durch ihre ständige Kontrolle über Infrastrukturzugriffe, Datenzugriffe und die Datenverwendung geschaffen. Dies schließt die Möglichkeit von Unternehmen ein, Dritte (z.B. Cloud-Provider, staatliche Behörden, Wettbewerber und weitere Akteure) vom Zugriff auf und der Nutzung von Daten ein- oder auszuschließen.

<1>Ja

<2>Nein

<777> Weiß nicht / keine Angabe

[Anpassung der Frage für CAWI:

[q35] Ist Ihnen der Begriff „Digitale Souveränität“ bekannt?

<1>Ja

<2>Nein

<777> Weiß nicht / keine Angabe]

Seite

#Fragentyp: Freitext

#Anzeige-Logik: Wenn q35==1 [Befragte, die angeben zu wissen, was „Digitale Souveränität“ ist]

[q36] Bitte beschreiben Sie, was Sie in Ihrem Unternehmen unter dem Begriff „Digitale Souveränität“ verstehen.

[Freitextfeld]

<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Single Choice

#Anzeige-Logik: Wenn q35==1 [Befragte, die wissen, was „Digitale Souveränität“ ist]

[q37] Wie stark wurde bzw. wird das Thema „Digitale Souveränität“ bei der Entscheidung, Cloud-Dienste zu nutzen bzw. nicht zu nutzen, berücksichtigt?

Das Thema „Digitale Souveränität“ wurde bzw. wird…

<1>…überhaupt nicht berücksichtigt.
<2>…wenig berücksichtigt.
<3>…mittelmäßig berücksichtigt.
<4>…stark berücksichtigt.
<5>…sehr stark berücksichtigt.
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Single Choice, randomisiert

#Anzeige-Logik: Wenn q35==1 [Befragte, die wissen, was „Digitale Souveränität“ ist]

[q38] Wie wichtig ist „Digitale Souveränität“ für die

-[q38_1] Wettbewerbsfähigkeit
-[q38_2] Innovationsfähigkeit

…Ihres Unternehmens auf einer Skala von 1=überhaupt nicht wichtig bis 5=sehr wichtig?

<1>Überhaupt nicht wichtig
<2>XXX
<3>XXX
<4>XXX
<5>Sehr wichtig
<777> Weiß nicht / keine Angabe

[Anpassung der Frage für CAWI:

[q38] Wie wichtig ist „Digitale Souveränität“ für die Wettbewerbs- und Innovationsfähigkeit Ihres Unternehmens?

[q38_1] Wettbewerbsfähigkeit
[q38_2] Innovationsfähigkeit

<1>Überhaupt nicht wichtig
<2>…
<3>…
<4>…
<5>Sehr wichtig
<777> Weiß nicht / keine Angabe]

Seite

#Fragentyp: Single Choice
#Anzeige-Logik: Wenn q35==1 [Befragte, die wissen, was „Digitale Souveränität“ ist]

[q39] Gefährdet die Nutzung von Cloud-Diensten die digitale Souveränität von Unternehmen? Bitte beantworten Sie die Frage aus Sicht Ihres Unternehmens.

<1>Überhaupt nicht
<2>Wenig
<3>Mittelmäßig
<4>Stark
<5>Sehr Stark
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Freitext
#Anzeige-Logik: Wenn q39==2,3,4,5 [Befragte, die die digitale Souveränität gefährdet sehen]

[q40] Warum sehen Sie die digitale Souveränität von Unternehmen durch die Nutzung von Cloud-Diensten gefährdet?

[Freitextfeld]
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Single Choice
#Anzeige-Logik: Alle Befragte

[q41] Ist Ihnen das Projekt Gaia-X bekannt?

<1>Ja
<2>Nein
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Multiple Choice, randomisiert

#Anzeige-Logik: Alle Befragte

[Wenn q41>= 1: Erläuterung: Gaia-X ist ein europäisches Projekt, welches eine europäische Dateninfrastruktur schaffen soll, die die digitale Souveränität der EU-Mitgliedstaaten und der ansässigen Unternehmen schützt und Innovationen fördert. Dafür wird ein Ökosystem aus bestehenden Server-Strukturen geschaffen, innerhalb dessen die Nutzer entscheiden, wo ihre Daten gespeichert werden, und diese frei transferieren können.

[q42] Welche Auswirkungen erhoffen Sie sich von Gaia-X auf die Anwendung von digitalen Technologien in Ihrem Unternehmen?

<1>Mehr Vertrauen in digitale Anwendungen durch erhöhte Datensouveränität und -sicherheit
<2>Schnellere Entwicklung digitaler Innovationen
<3>Höhere Datenverfügbarkeit
<4>Steigerung des Wissens- und Erfahrungsaustausches z.B. in der Cloud
<5>Wettbewerbsvorteile
<7>Neue Geschäftsmodelle, Dienstleistungen oder Produkte
<8>Keine Auswirkungen (fixiert)
<666> Andere Auswirkungen: [Freitextfeld] (fixiert)
<777> Weiß nicht / keine Angabe (fixiert)

Abschnitt 6 – Fragen zur Unternehmensstruktur

Seite

#Fragentyp: Single Choice
#Anzeige-Logik: Do not show question, extract from sampling frame

[q43] Zu welchem Wirtschaftszweig gehört Ihr Unternehmen?

<1>Bergbau und Gewinnung von Steinen und Erden
<2>Verarbeitendes Gewerbe
<3>Energieversorgung
<4>Wasserversorgung, Abwasser- / Abfallentsorgung usw.
<5>Baugewerbe
<6>Handel; Instandhaltung / Reparatur v. Kfz / Gebrauchsgütern
<7>Verkehr und Lagerei
<8>Gastgewerbe
<9>Information und Kommunikation
<10> Erbringung von Finanz- / Versicherungsdienstleistungen
<11> Grundstücks- und Wohnungswesen
<12> Freiberufl., wissenschaftl. u. techn. Dienstleistungen
<13> Sonstige wirtschaftliche Dienstleistungen
<14> Erziehung und Unterricht
<15> Gesundheits- und Sozialwesen
<16> Kunst, Unterhaltung und Erholung
<17> Erbringung von sonstigen Dienstleistungen

<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Single Choice
#Anzeige-Logik: Alle Befragte

[q43a] Ist Ihr Unternehmen Betreiber kritischer Infrastrukturen?

<1>Ja
<2>Nein
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Freitext - Jahr [keine negativen Werte erlauben]
#Anzeige-Logik: Alle Befragte

[q44] In welchem Jahr wurde Ihr Unternehmen gegründet?

[Jahr]

Seite

#Fragentyp: Single Choice
#Anzeige-Logik: Do not show question, extract from sampling frame

[q45] Wie viele Mitarbeiter hat Ihr Unternehmen?

<1>0-9 Beschäftigte
<2>10-49 Beschäftigte
<3>50-249 Beschäftigte
<4>250-499 Beschäftigte
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Single Choice
#Anzeige-Logik: Do not show question, extract from sampling frame

[q46] Wie hoch ist der Jahresumsatz Ihres Unternehmens?

<1>bis zu 2 Mio. €
<2>über 2 Mio. bis zu 10 Mio. €
<3>über 10 Mio. bis zu 50 Mio. €
<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Freitext – PLZ
#Anzeige-Logik: Alle Befragte

[q47] Wie lautet die Postleitzahl des Hauptsitzes Ihres Unternehmens?

[PLZ]

<777> Weiß nicht / keine Angabe

<778> Außerhalb Deutschlands

[Anpassung der Frage für CAWI:

[q47] Wo befindet sich der Hauptsitz Ihres Unternehmens?

[PLZ]

<777> Weiß nicht / keine Angabe

<778> Außerhalb Deutschlands]

Seite

#Fragentyp: Freitext – Anzahl

#Anzeige-Logik: Alle Befragte

[q48] Wie viele Standorte hat Ihr Unternehmen neben dem Hauptsitz?

[Anzahl]

<777> Weiß nicht / keine Angabe

<778> Keine weiteren Standorte

[Anpassung der Frage für CAWI:

[q48] Wie viele Standorte (in Deutschland und im Ausland) hat Ihr Unternehmen neben dem Hauptsitz?

[Anzahl]

<777> Weiß nicht / keine Angabe]

Seite

#Fragentyp: Freitext - Anzahl, nicht randomisiertd

#Anzeige-Logik: Wenn q48>1 [Befragte mit mehr als einem Standort]

[q49] Sie haben angegeben, dass Ihr Unternehmen über einen weiteren Standort verfügt. Wo befinden sich diese Standorte geografisch?
Bitte geben Sie die Anzahl der Standorte (ohne Hauptsitz) in den aufgeführten Regionen an.

<1>Deutschland: *[Anzahl]*

<4>Europäisches Ausland: *[Anzahl]*

<5>Nicht-europäisches Ausland: *[Anzahl]*

<777> Weiß nicht / keine Angabe

Seite

#Fragentyp: Single Choice

#Anzeige-Logik: Do not show question, extract from sampling frame

[q53] Welche Position bekleiden Sie im Unternehmen?

<1>Geschäftsführung / Vorstand

<2>Geschäftsbereichsleitung / Abteilungsleitung

<3>Teamleitung / Projektleitung

<4>Mitarbeiter / in

<666> Andere: *[Freitextfeld]*

<777> Weiß nicht / keine Angabe

Abschnitt 7 – Ende

Seite

#Fragentyp: Text

#Anzeige-Logik: Alle Befragte

Wir sind am Ende der Befragung angekommen. Gibt es abschließend noch etwas, das Sie uns mitteilen möchten?

[Freitextfeld]

Seite

#Fragentyp: Text

#Anzeige-Logik: Alle Befragte

Gerne lassen wir Ihnen exklusiv den Ergebnisbericht zukommen, sobald er erstellt ist. Möchten Sie mir hierfür eine Emailadresse geben?

[Freitextfeld]

Seite

#Fragentyp: Text

#Anzeige-Logik: Alle Befragte

Vielen Dank, dass Sie sich die Zeit genommen haben, die Befragung zu beantworten. Sollten Sie noch Rückfragen haben, können Sie sich gerne an die schon genannte Ansprechpartnerin wenden:

WIK-Consult GmbH

Frau Serpil Taş

Tel.: +49 2224 92 25-96

e-mail: s.tas@wik-consult.com