Baischew, Dajan; Lundborg, Martin; Märkel, Christian; Papen, Marie-Christin; Gesmann-Nuissl, Dagmar

Research Report

Strategische Bedeutung von Cloud-Diensten für die digitale Souveränität von KMU. Teil 2 - Digitale Souveränität und Cloud-Dienste

WIK-Consult Bericht

Provided in Cooperation with:
WIK Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste GmbH, Bad Honnef

Suggested Citation: Baischew, Dajan; Lundborg, Martin; Märkel, Christian; Papen, Marie-Christin; Gesmann-Nuissl, Dagmar (2022) : Strategische Bedeutung von Cloud-Diensten für die digitale Souveränität von KMU. Teil 2 - Digitale Souveränität und Cloud-Dienste, WIK-Consult Bericht, WIK-Consult GmbH, Bad Honnef

This Version is available at:
https://hdl.handle.net/10419/268806

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.

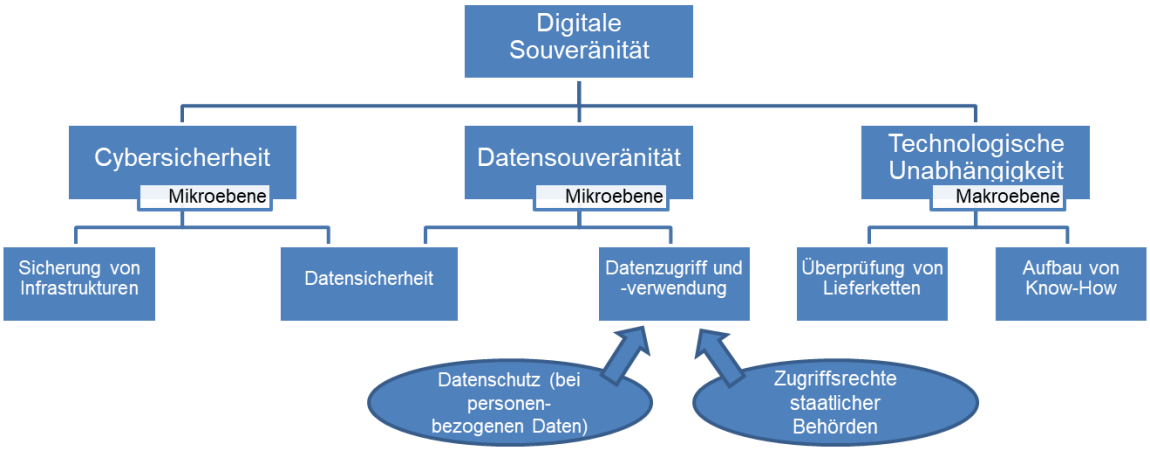
Ebenso auffallend ist, dass Begriffe wie technologische Souveränität teils als Synonym, teils als Oberbegriff und teils als Unterbegriff digitaler Souveränität verwendet werden. Datensouveränität hingegen scheint als ein Teilaspekt digitaler Souveränität verstanden zu werden. Im Zusammenhang dieser Studie 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]

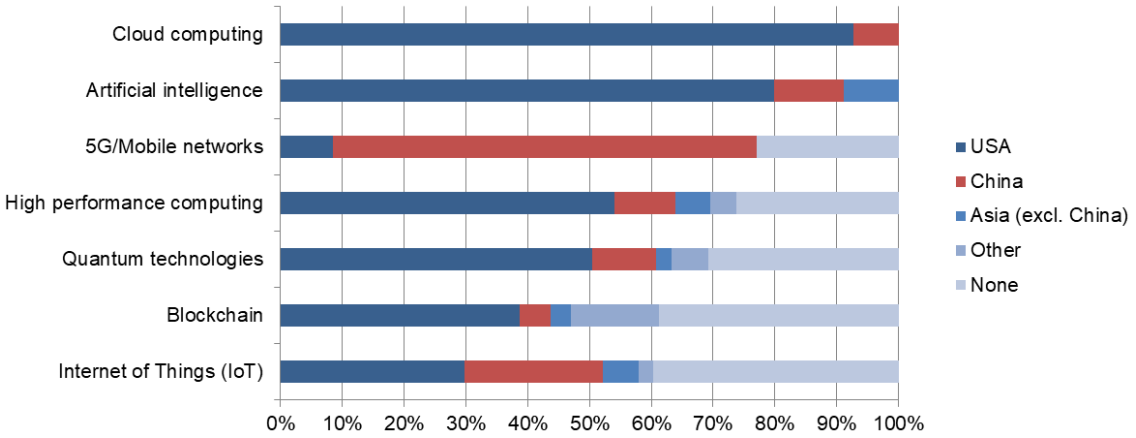
---

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.

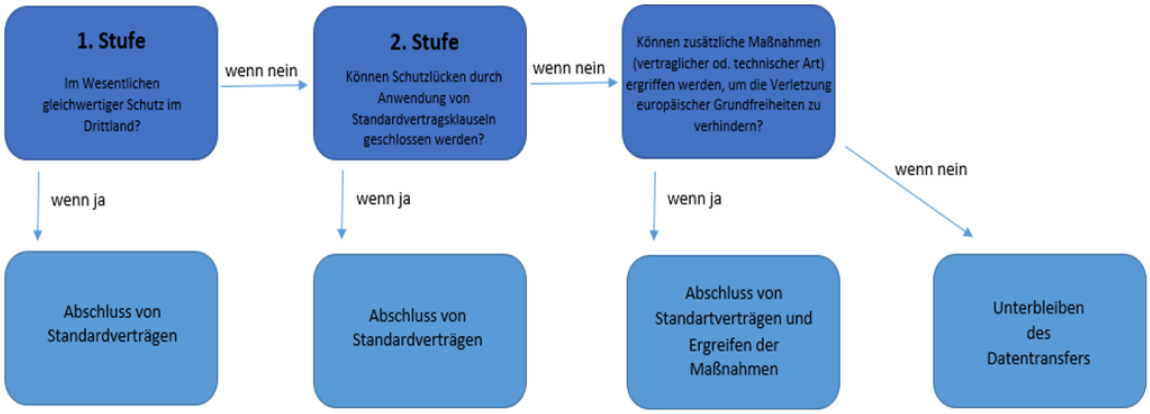
2. Stufe:

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.

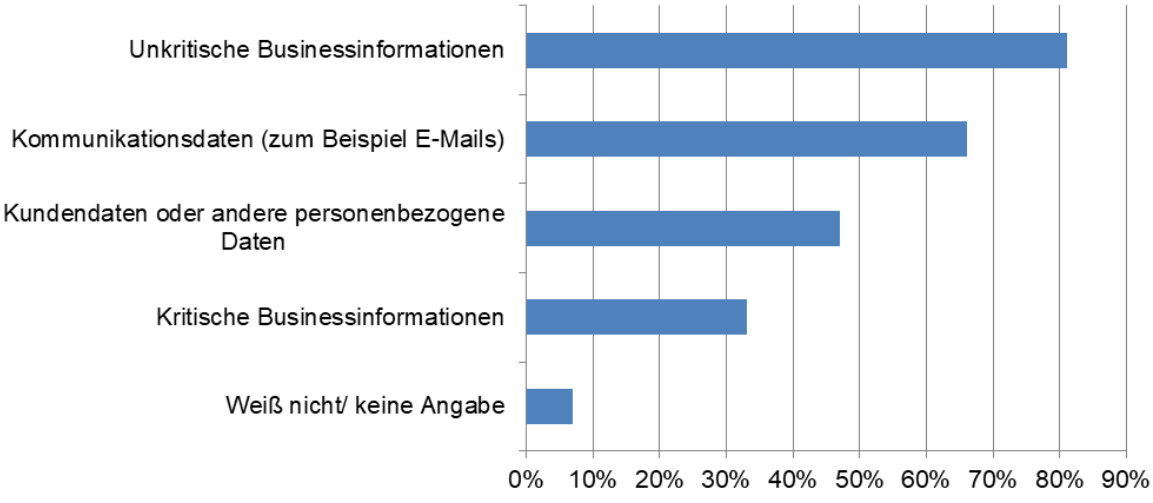
106 Bei den Befragten handelt es sich um Vertreter relevanter Verbände und Ansprechpartner aus dem Wissenstransferbereich, die sich mit Cloud-Diensten und KMU beschäftigen.

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.