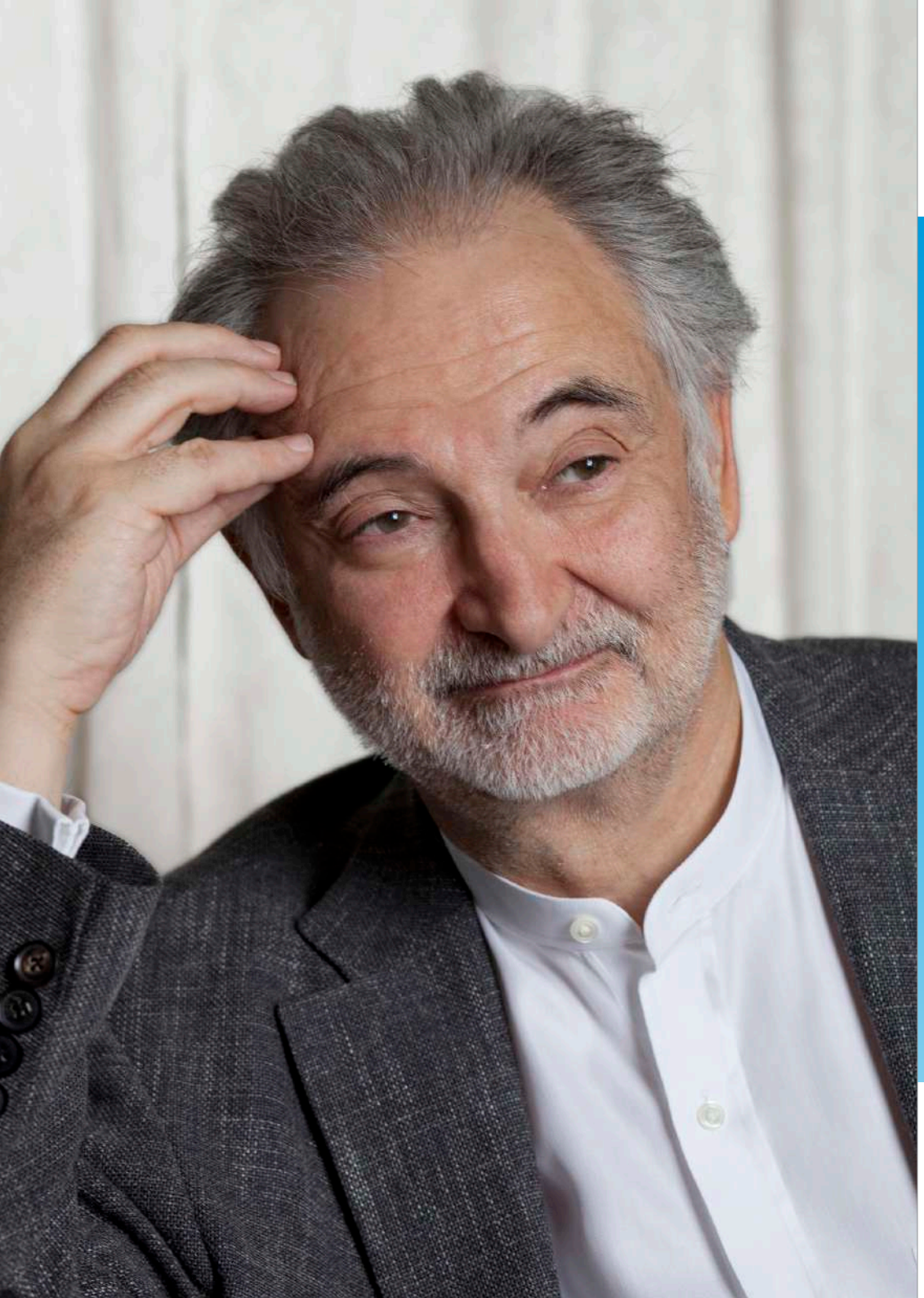
KPMG | Global Strategy Group

Der europäische Cloud-Markt: bedeutende Herausforderungen für Europa und fünf Szenarien mit großen Auswirkungen bis 2027-2030

März 2021



Die europäische Cloud in den Dienst der lebenswichtigen Wirtschaftszweige stellen

Die Virtualisierung der Datenspeicherung war bereits seit langem unweigerlich vorhersehbar. Doch leider hat Europa auch hier wiederum länger gebraucht als viele andere, um dies zu erkennen, und hat somit Microsoft, Amazon und Google einen Anteil von über 60% am globalen öffentlichen Cloud-Markt überlassen.

Dieses ist heute eine sehr gravierende Lücke in Europa, die es gilt, so schnell wie möglich zu beheben.

Erstens ist dies eine wirtschaftliche Herausforderung: Bis 2027 könnte der Cloud-Markt in Europa auf mehr als 260 Milliarden Euro anwachsen (verglichen mit 53 Milliarden Euro heute); damit würde er dieselbe Größe erreichen wie der aktuelle Telekommunikationsmarkt (mit rund 250 Milliarden Euro im Jahr 2020). Wenn Cloud-Betreiber ihre Aktivitäten und Investitionen in Europa lokalisieren würden, könnten zwischen 2021 und 2027 rund 550.000 Arbeitsplätze geschaffen und erhebliche Investitionen (in Höhe von schätzungsweise 200 Milliarden Euro im Zeitraum 2021 bis 2027) ausgelöst werden. Es wäre auch eine Gelegenheit zu einer stärkeren Unterstützung des Bereichs der Anwendungen. Denn die Cloud ist nichts ohne alle Dienste, die sie nutzen. Eine europäische Cloud könnte im wahrsten Sinne des Wortes zu einer beschleunigten Entwicklung europäischer Softwareunternehmen beitragen. Dies würde auch Entwicklungen der Bereiche der Gesundheit, Bildung, Kultur, Medien, Sicherheit, Versicherungen und Finanzen – d. h. aller zukünftig lebenswichtigen Wirtschaftszweige – in einem sicheren Kontext ermöglichen. Daher sollte dies ein wesentliches Element des europäischen Aufschwungs sein.

Es ist auch eine technologische Herausforderung: Eine Investition in die Cloud würde es Europa ermöglichen, eine führende Position auf dem Gebiet von Spitzentechnologien wie Prozessoren, 5G, Quantenverschlüsselung, Edge-Computing usw., und darüber hinaus der Biomimikry zu entwickeln. Dies sind alles grundlegende Technologien in anderen lebenswichtigen Bereichen der Wirtschaft, wie Logistik, Wasser- und Luftmanagement sowie erneuerbare Energien.

Und letztlich ist es eine strategische Herausforderung: Eine europäische Cloud würde es Europa ermöglichen, seine digitale Souveränität zu garantieren, indem sichergestellt wird, dass es die Verwaltung personenbezogener und industrieller Daten beherrscht, was im aktuellen rechtlichen und regulatorischen Kontext absolut nicht garantiert ist (DSGVO, Ungültigerklärung des Privacy Shield, Cloud Act).

In diesem Bereich, wie in vielen anderen, ist das Problem ein globales Problem, während die Lösung auf europäischer Ebene liegt; es handelt sich um ein politisches und kulturelles Problem, dessen Lösung im industriellen Bereich zu finden ist.

Jacques Attali

Haftungsausschluss

Der vorliegende Bericht („Bericht“) wurde von der KPMG SA („KPMG“) für Talan SAS, InfraNum, OVHcloud und Linkt (Tochtergesellschaft der Altitude-Gruppe) – „Beauftragte“ – gemäß dem mit ihnen am 15. Januar 2021 unterzeichneten Vertrag („der Vertrag“) und auf der Grundlage des Umfangs und der Beschränkungen, die nachfolgend dargelegt sind, erstellt.

Alleiniger Zweck des Berichts ist, wie im Vertrag angegeben, die Untersuchung der gegenwärtigen Situation und der Herausforderungen des Cloud-Markts in Europa. Er ist weder zu irgendeinem anderen Zweck noch in irgendeinem anderen Zusammenhang welcher Art auch immer zu verwenden. Für diesen Fall lehnen KPMG, ihre Tochtergesellschaften und andere Rechtsträger des KPMG-Netzwerks jegliche Haftung gegenüber jeglicher sich auf den vorliegenden Bericht stützenden Person ab.

Der Bericht ist ausschließlich zur Verwendung durch die Beauftragten unter den Vertragsbedingungen bestimmt. Die Nutzung des Berichts zu welchem Zweck auch immer ist einzig den Beauftragten erlaubt. KPMG, ihre Tochtergesellschaften und anderen verbundenen Rechtsträger lehnen jegliche Haftung oder Verpflichtung gegenüber jeglicher sich auf diesen Bericht oder seinen Inhalt stützenden Person mit Ausnahme der Beauftragten ab.

In Übereinstimmung mit den Vertragsbedingungen war der Umfang dieser Studie durch die ihr gewidmete Zeit und die KPMG zur Verfügung gestellten Informationen und Erklärungen beschränkt. KPMG hat die in dem vorliegenden Bericht enthaltenen Informationen von Quellen bei den Beauftragten und Dritten erhalten, die in den entsprechenden Abschnitten des Berichts im Einzelnen angegeben sind. KPMG hat nicht versucht, diese Informationen zu untermauern oder ihre Plausibilität zu bestätigen. Ferner wurden die Ergebnisse der in dem Bericht dargelegten Analysen auf der Grundlage der zum Zeitpunkt der Erstellung des Berichts verfügbaren Informationen erhalten und ihre Richtigkeit für spätere Zeiträume kann nicht garantiert werden.

KPMG hält sämtliche Urheber- und anderen Eigentumsrechte an dem Bericht, sofern in der vorliegenden Mitteilung oder im Vertrag nichts anderes ausdrücklich angegeben wird.

Entscheidungen für Investitionen in die, die Aufnahme von Geschäftstätigkeiten auf den, den Eintritt in die oder den Austritt aus den in dem Bericht behandelten Märkte/n sollten erst nach unabhängiger Beratung erfolgen und Dritte sollten sich in keiner Weise auf die in dem Bericht enthaltenen Informationen stützen. KPMG erbringt mit diesem Bericht keinerlei geschäftliche, finanzielle, Investitions- oder andere fachliche Dienste oder Beratungstätigkeiten. Der vorliegende Bericht stellt keinen Ersatz für solche fachlichen Beratungs- oder Dienstleistungstätigkeiten dar und sollte nicht als Grundlage für Entscheidungen oder Maßnahmen herangezogen werden, die sich auf Ihr Geschäft auswirken können. Konsultieren Sie bitte einen qualifizierten professionellen Berater, bevor Sie eine Entscheidung oder eine Maßnahme welcher Art auch immer, die sich auf Ihr Geschäft auswirken könnte, treffen. Insbesondere stellt der Bericht keine Empfehlung oder Befürwortung einer Investition in die oder einer anderen Beteiligung in den, eines Austritts aus den oder einer Nutzung in den in dem Bericht genannten Märkte/n oder Unternehmen durch KPMG dar. KPMG und die Beauftragten, ihre Tochtergesellschaften und anderen verbundenen Rechtsträger lehnen jegliche Haftung aus der Nutzung (oder Nichtnutzung) des Berichts, einschließlich jeglicher aus der Nutzung (oder Nichtnutzung) des Berichts resultierenden Maßnahmen oder Entscheidungen ab.

Der vorliegende Bericht wurde im Original auf Englisch verfasst und wurde ins Französische und Deutsche übersetzt. Bei Abweichungen zwischen der französischen, deutschen und englischen Version gilt das englische Original.

Dieses White Paper wurde auf der Grundlage verschiedener Typen von Inputs und Ressourcen verfasst

Interviews mit CxOs französischer und deutscher Unternehmen

50+ ausführliche Interviews mit französischen und deutschen **CxOs** großer und mittlerer Unternehmen (CAC40, DAX, SBF120…), sowohl **Technologie- als auch Rechtsexperten** zur Unterfütterung unserer Analyse des gegenwärtigen Markts und Hinterfragung unserer Empfehlungen

Marktstudien und öffentlich zugängliche Dokumente

Detaillierte **Marktstudien** von **Partnerunternehmen** und **Organisationen** mit Spezialisierung und Involvierung in **Herausforderungen und Fragen des Cloud-Computings**, zusammen mit **öffentlich zugänglichen und Rechtsdokumenten in Verbindung mit Fragen der Datensouveränität**

Austausch mit Cloud-Computing-Experten

Ständiger Austausch mit **Cloud-Computing-Experten**, unter anderem internen Experten (von KPMG und anderen mitwirkenden Teams), Ökonomen und öffentlichen Körperschaften zur **Hinterfragung und zum Ausfeilen unserer Empfehlungen** mit anschließender Formulierung **umsetzbarer Ansätze**

Online-Umfrage unter europäischen CxOs

Eine Online-Umfrage mit etwa 40 Fragen unter **200+ CxOs französischer und deutscher Unternehmen** (mittlerer Jahresumsatz ~ 150 Millionen €), Messung ihres Grades der Cloudifizierung, **ihres Bewusstseins für Souveränitätsbedenken bei der Auswahl eines Cloud-Anbieters** und **ihrer Wahrnehmung der Datensouveränität**

Diese Studie wurde zwischen Januar und März 2021 durch ein **eigens dazu zusammengestelltes KPMG-Team über einen Zeitraum von 8 Wochen** von KPMG GSG (Strategy) und KPMG Legal durchgeführt.

InfraNum, französischer Verband für digitale Infrastruktur, hat diesen Bericht gemeinsam mit 3 anderen Hauptbeteiligten und Interessierten auf dem Markt unterstützt und aktiv dazu beigetragen

Wichtige Informationen zum Verband InfraNum

- **Gründung 2012** zur Unterstützung von Frankreichs nationalem Plan zum Ausbau des Breitbandnetzes
- Verband mit **200+** Mitgliedern (Unternehmen mit aktivem Engagement in den **digitalen Infrastrukturmärkten**, wie Glasfaserlieferanten, IoT-Akteure, Akteure auf dem Telekommunikationsmarkt, Ausrüstungslieferanten usw.)
- **Wichtigste Ziele**:
  - Unterstützung der **digitalen Entwicklung in Frankreich**
  - Förderung der Entwicklung **digitaler Anwendungen in Frankreich** durch **Unterstützung von Unternehmen** bei der **Implementierung einer neutralen, offenen und gemeinsam genutzten digitalen Infrastruktur**
  - Entwicklung von **Partnerschaften zwischen öffentlichen und privaten Akteuren**, um es lokalen Gebietskörperschaften zu ermöglichen, die Nutzung durch Bürger zu entwickeln, den **Wert ihrer lokalen Wirtschaft zu erhöhen** und **die spezifischen Vorzüge jeder Region herauszustellen**

Wichtige Informationen über die drei anderen Mitwirkenden

Neben InfraNum trugen drei weitere Mitwirkende zu dieser von KPMG veröffentlichten Studie bei:

- **Talan**, ein auf die digitale Transformation spezialisiertes europäisches Beratungsunternehmen
- **OVHcloud**, ein europäischer Cloud-Anbieter
- **Linkt**, ein französisches B2B Telekommunikationsunternehmen

B2B-Telekommunikationsunternehmen

Die aktive Beteiligung von InfraNum und den anderen Mitwirkenden hat es uns ermöglicht, **feste Annahmen über die Zukunft des europäischen Cloud-Marktes** unter Berücksichtigung der wichtigsten damit verbundenen Risiken und Herausforderungen aufzubauen.

Der europäische Cloud-Markt: bedeutende Herausforderungen für Europa und fünf Szenarien mit großen Auswirkungen bis 2027–2030 – Zusammenfassung (1/3)

1 **Der europäische Cloud-Markt ist ein wachsender Markt (+ 27 % pro Jahr in dem Zeitraum von 2017-2019) von € 53 Mrd. im Jahr 2020, mit einem voraussichtlichen weiteren Wachstum auf ca. € 300-500 Mrd. bis 2027-2030**[1]

- **Cloud-Dienste**, die Private-, Public- und Hybrid-Clouds für IaaS-, PaaS- und SaaS- Dienste umfassen, **decken einen großen Teil der IT-Erfordernisse von Unternehmen ab, mit einigen spezifischen Vorteilen**:
  - **Pay-per-Use-Services (Zahlung für die Nutzung)**, ohne CapEx-Erfordernisse
  - **Flexible und skalierbare Kapazitäten**, mit der Fähigkeit der augenblicklichen Erhöhung oder Verringerung von gebrauchsfertiger Rechen-/ Speicherungskapazität
  - **Fokussierung auf Kerntätigkeiten**, mit komplett oder teilweise an Cloud-Anbieter ausgelagerten Tätigkeiten der Bereitstellung und Wartung
- In Europa ist **der Cloud-Computing-Markt ein starker Wachstumsmarkt**, der **enorme wirtschaftliche Vorteile für die europäische Wirtschaft darstellt**…
  - Eine zu erwartende Marktgröße von rund € 260 Mrd. bis 2027, vergleichbar mit dem derzeitigen Telco-Markt (~ € 250 Mrd. 2020)
- Ein stark von drei globalen „Hyperscalern" beherrschter Wettbewerb (z. B. 70 % der IaaS-Marktanteile), mit Sitz in den USA, die begrenzte operative Geschäfte in Europa haben
- In Europa dürften rund 550.000 mit dem Markt assoziierte Arbeitsplätze geschaffen werden und Investitionen in Höhe von rund € 200 Mrd. (über den Zeitraum von 2021 bis 2027) getätigt werden, wenn es Cloud-Anbietern gelingt, ihre operativen Geschäfte und Investitionen in Europa zu realisieren

2 **Für Cloud-Computing-Entscheidungsträger (allem voran CIOs) erscheint die Cloud-Migration als ein zwingender Weg voran, der jedoch durch gewisse Einschränkungen gekennzeichnet ist, und zwar aufgrund der begrenzten Anzahl von Cloud-Providern, die wenig übersichtliche, komplexe Angebote mit einer nicht klar definierten Datensouveränität, begrenzter Interoperabilität und ohne Datenübertragbarkeit bereitstellen, was insbesondere auf kommerzielle Praktiken wie Verbundgeschäfte zurückzuführen ist**

- Hauptsächliche **Triebfedern für den allgemeinen Übergang zu Cloud-Lösungen** sind die **betriebliche und finanzielle Optimierung**, wie eine optimierte **Kostenvariabilisierung** (OpEx anstelle von CapEx), größere **Flexibilität** bei der Erhöhung (oder Verringerung) der Speicher- und Rechenkapazitäten, agilere **Teamarbeit** (insbesondere seit der gegenwärtigen Coronavirus-Pandemie) oder ein **schnellerer Ausbau** neuer Tätigkeiten
- Die **Wahl von Cloud-Anbietern ist eine komplexe Entscheidung unter Berücksichtigung einer Reihe von Kriterien**, allem voran[1] der **Datensicherheit sowie der regulatorischen Risiken und der Compliance (einschl. Datensouveränität)** und in geringerem Maße der **Breite des Leistungsspektrums und der Kosten**
  - Datensouveränität: wird von 89 % der befragten Entscheidungsträger als wichtiges KPC genannt, obwohl das Konzept oft als unklar und mit Schwerpunkt auf zwei Hauptaspekten (DSGVO-Compliance und Standorte von Data Centern) wahrgenommen wird, und in einem Kontext, in dem die Tiefe des Serviceangebots mit Datensouveränität als zu beschränkt erachtet wird. „Während unserer letzten Qualifizierung von Cloud-Anbietern, die vor zwei Jahren durchgeführt wurde, waren europäische Angebote mit Datensouveränität nicht so ausgereift und klar definiert wie sie es heute sind. Da unser Comex in Bezug auf die Datensouveränität äußerst sensibel ist, haben wir uns entschieden, keine echte Cloud-Migration zu initiieren, doch in Anbetracht dessen, dass es jetzt mehr zuverlässige Angebote mit Datensouveränität in Europa gibt, könnten wir uns anders entscheiden" , CIO eines europäischen Logistikdienstleisters[2]

Anm.: (1). Basierend auf IDC Market Reports (2). Auszug aus über 50 ausführlichen Interviews mit französischen und deutschen CxOs

Der europäische Cloud-Markt: bedeutende Herausforderungen für Europa und fünf Szenarien mit großen Auswirkungen bis 2027–2030 – Zusammenfassung (2/3)

- Breite des Leistungsspektrums: Die Serviceangebote der Hyperscaler erscheinen breiter als die der europäischen Akteure (auf eigenständiger Basis), doch eine Reihe europäischer Akteure hat bisher mit Erfolg ein ebenso vielfältiges Cloud-Ökosystem geschaffen; durch Partnerschaften mit ihrem Ökosystem stellen die europäischen Akteure eine Fähigkeit unter Beweis, mit den Hyperscalern mithalten zu können
- Kosten: Die Preise europäischer Cloud-Provider sind mit denen der Hyperscaler vergleichbar, wenn nicht sogar günstiger; dennoch gelingt es den Hyperscalern, den Markt tendenziell mit aggressiven und unkonventionellen Kundenakquisitionspraktiken zu beherrschen; zusätzlich wird der Vertragsaustritt oder Provider-Wechsel für Cloud-Nutzer durch komplexe Austrittsbedingungen (hohe Ausstiegshürden und Anbieter-Lock-in) erschwert

„Namhafte Bürogeräteanbieter **vermarkten gebündelte IaaS- und SaaS-Produkte** zu äußerst attraktiven Preisen, **zu einem Fünftel des Preises reiner IaaS-Angebote von Konkurrenten**", europäischer Logistikdienstleister[1]

3 Aus rechtlicher und regulatorischer Sicht präsentiert der Cloud-Computing-Markt hohe Risiken und starke Diskrepanzen zwischen den US-amerikanischen und den europäischen Regelungen, wodurch die derzeitige rechtliche Lage nicht haltbar ist

- Seit 2016 sind in den USA und in der EU in dem Versuch **der Schaffung eines strengen Rechtsrahmens in Bezug auf Datenströme mehrere Datenschutzverordnungen umgesetzt worden** (DSGVO, US-EU Privacy Shield und Cloud Act); doch durch die **Außerkraftsetzung des Privacy Shield** durch den Europäischen Gerichtshof im Jahr 2020 **ist die tiefgreifende Unvereinbarkeit** der US-Regulierungen mit den Prinzipien der DSGVO, **die scheinbar nicht zu überbrücken ist**, nur noch **deutlicher hervorgetreten**
- Demzufolge verfügen **Unternehmen, die personenbezogene Daten von EU-Bürgern an die (selbst in Europa befindlichen) Server von Nicht-EU-Unternehmen transferieren**, nunmehr über **keine rechtliche Grundlage dafür** und sind **rechtlichen, aber auch industriellen Risiken** ausgesetzt, da globale Cloud-Provider Zugang zu ihren vertraulichen Daten und IP haben
- Unsere Befragungen[1] haben ergeben, dass diese Situation Anlass zu Bedenken gibt und dass sie zu finanziellen und geschäftlichen Risiken führt, wie zum Beispiel:
  - eine aufgehobene Entlassung, da die von dem Unternehmen vorgebrachten Beweise, um sie zu rechtfertigen, in nicht-konformen Data Centern von Cloud-Providern gehostet waren
  - ein europäisches Unternehmen, das nicht in der Lage ist, relevante Beweise über den Diebstahl von Kundendaten zu verwenden, da diese Daten aus einem in den USA gespeicherten und verarbeiteten Zugangsüberwachungssystem extrahiert wurden, ohne jegliche rechtliche Grundlage für eine solche Verarbeitung

4 Das derzeitige Paradigma des europäischen Cloud-Markts erscheint nicht haltbar; um die gegenwärtige festgefahrene Situation des europäischen Cloud-Markts zu beheben, wurden in unseren Expertendiskussionen fünf Szenarien betrachtet, mit sich gegenseitig ergänzenden positiven Effekten

- **Gegenwärtige europäische Marktstruktur erscheint** aufgrund zahlreicher Spannungen **unhaltbar,** darunter den vier folgenden:
  - Diskrepanz zwischen DSGVO-Compliance und extraterritorialen Regelungen; daraus ergeben sich rechtliche / geschäftliche Risiken für EU-Unternehmen, die US-Cloud-Anbieter nutzen
  - Wettbewerbswidrige Praktiken und starke kommerzielle Hindernisse für den Marktzugang, wodurch ein Wettbewerbsumfeld mit gleichen Bedingungen für alle in Europa verhindert wird
  - Markt mit einer wachsenden Nachfrage nach dem Schutz von personenbezogenen Daten und Firmendaten, wodurch ein stärkeres Bewusstsein in Bezug auf den Datenschutz und die Datensouveränität entsteht
  - Enorme und sichtbare wirtschaftliche Auswirkungen aufgrund des starken Anstiegs in der Nachfrage nach Cloud-Diensten (insbesondere SaaS) in Europa

Anm.: (1). Auszug aus über 50 ausführlichen Interviews mit französischen und deutschen CxOs

Der europäische Cloud-Markt: bedeutende Herausforderungen für Europa und fünf Szenarien mit großen Auswirkungen bis 2027–2030 – Zusammenfassung (3/3)

- **Daher könnte sich eine Reihe potenzieller Szenarien in der europäischen Cloud-Computing-Landschaft herausbilden:**
  - Cloud als Gemeingut, hauptsächlich getrieben durch freiwillige Interoperabilität von Cloud-Diensten, sektorweite Cloud-Ökosysteme und Multi-Cloud-Ausweitung, was für das Wachstum eines europäischen Ökosystems (im Einklang mit der GaiaX-Initiative) förderlich wäre und eine treibende Kraft des Wachstums europäischer Cloud-Akteure sein könnte
  - Ausbau des Leistungsangebots europäischer Provider, hauptsächlich getrieben durch bisher nicht ausreichend gedeckte, aufkommende Marktbedürfnisse (einschl. Edge-Computing, KI für industrielle Daten oder die Entwicklung von Angeboten mit Datensouveränität) und durch öffentliche Ausgaben (B2G-Vorhaben)
  - Welle starker Regulierung (ähnlich wie vor einigen Jahren auf dem Telco-Markt beobachtet), mit der Entstehung eines Cloud-Regulierers, was in strengen Auflagen für Cloud-Anbieter, insbesondere für Hyperscaler, resultieren würde: durch Hebelkräfte wie größere Preistransparenz, erzwungene Interoperabilität oder offenen Zugang zu Innovationen
  - Europäisierung von Cloud-Providern, entweder durch die Europäisierung ihrer Geschäftstätigkeiten (z. B. lokale Forschungs- und Entwicklungsausgaben) oder durch die effektive europäische Kontrolle ihrer lokalen Niederlassungen (z. B. in China, Partnerschaft zwischen Microsoft und lokalem Anbieter 21Vianet), wobei von den EU-Behörden eine effektive Wertschöpfung auf lokaler Ebene und eine strenge Angleichung an die europäischen Regelungen gewährleistet würde
  - Spaltung der Cloud-Tätigkeiten, entweder funktionale Spaltung (Trennung zwischen Cloud-Tätigkeiten und anderen Geschäftstätigkeiten) oder strukturelle Spaltung (klare Abspaltung des Cloud-Geschäfts zu einer separaten juristischen Person), was zu einem „gerechteren" Wettbewerbsumfeld zwischen europäischen und US-Providern führen würde
- Die **wirtschaftlichen Auswirkungen** (einschl. erfasster Wert, geschaffene Arbeitsplätze und Investitionen) **könnten erheblich variieren;** Europa könnte im Falle einer unzureichenden Aktivierung dieser identifizierten Hebel zwischen 20 % und 50 % der geschätzten wirtschaftlichen Auswirkungen des Cloud-Computing-Markts verlieren

5 **Kurzfristig sollte zur Minderung der Risiken einer solch ungewissen Cloud-Landschaft eine Reihe von Initiativen[1] von öffentlichen und privaten Entscheidungsträgern umgesetzt werden**

- Für CIO: Kenntnis der eigenen tatsächlichen IT-Nutzung (Daten und Auslastung), Einleitung eines kulturellen Wandels hin zu einer proaktiven Cloud-Strategie und wohlüberlegte Wahl und Verwaltung der eigenen Cloud-Plattformen (durch eine Bewertung der Cloud-Provider)
- Für CLO: Kartografierung von Datentransfers, Bewertung von Transfer-Tools, Durchführung einer Bewertung der Risiken einer Nichteinhaltung der DSGVO und Prüfung der Datenverschlüsselungsbedingungen
- Für CMO: Entwicklung eines verantwortungsbewussten und nachhaltigen Kundenversprechens im Hinblick auf den Datenschutz, Einsatz von Cloud-Zertifizierungen als greifbarer Nachweis und Unterscheidung von der Konkurrenz durch Gewährleistung der effektiven DSGVO-Compliance
- Für öffentliche Entscheidungsträger: Vereinheitlichung cloud-bezogener öffentlicher Politiken, Definition einer zweckbestimmten Ausgabenpolitik für Cloud-Computing und Information und Weiterbildung von IT-Entscheidungsträgern in lokalen Körperschaften

Anm.: (1). 50 ausführliche Interviews mit französischen und deutschen CxOs

Überblick

1.

Europäischer Cloud-Markt: ein starker Wachstumsmarkt für Europa, dessen Größe sich bis 2027 voraussichtlich vervierfachen wird

Über das letzte Jahrzehnt haben Privatpersonen und Firmen cloud-basierte Anwendungen weithin übernommen, wobei die Übernahmerate bei Unternehmen jedoch derzeit rückläufig ist

92%

unter der Bevölkerung mit Internet-Zugang **sind Cloud-Nutzer** (Weltweit, 2018)

Nur 36% der europäischen Unternehmen[1] betreiben einen Teil ihrer betrieblichen Anwendungen auf Cloud-Umgebungen, **einschließlich Public oder Private Cloud** (Europa, 2020)

Beispiele für beliebte cloud-basierte Dienste

- **Cloud-basierte Anwendungen** sind definiert als Anwendungen, die auf physischen Servern gehostet werden und **über das Internet zugänglich** sind.
- Firmen können **eine / oder alle der erforderlichen Cloud-Komponenten „as a service" mieten**[2]: Hardware / Infrastruktur (IaaS), Plattformen (PaaS) oder Software (SaaS)

Anm.: (1). Eine Umfrage mit Befragten aus ~150.000 europäischen Unternehmen (mit etwa 83 % Kleinunternehmen, 14 % mittleren Unternehmen und 3 % Großunternehmen) (2). Oder eigene für IaaS
Quellen: Eurostat; Flexera; Vision Computer Solutions; Untersuchung und Analyse von GSG;

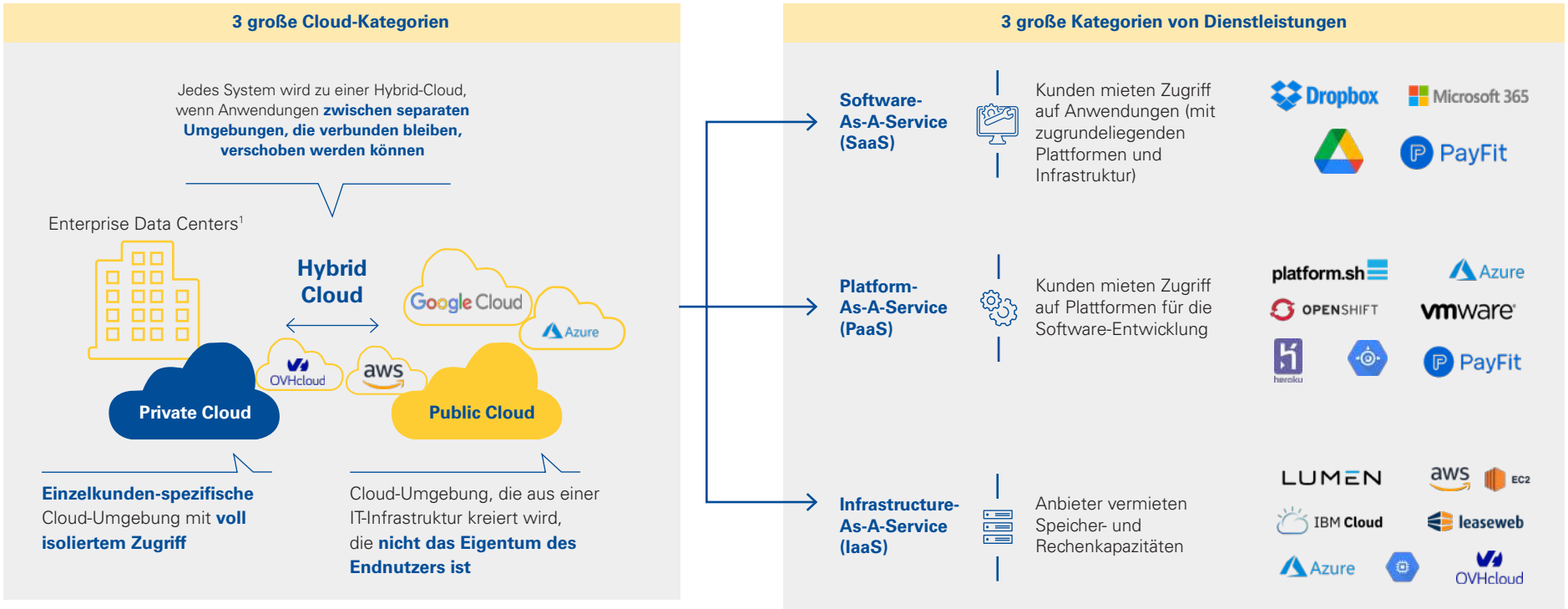
Cloud bietet Unternehmen wesentlich mehr Flexibilität und Serviceabdeckung, während der interne Investitionsaufwand im Vergleich zum herkömmlichen Modell stark reduziert wird

HERKÖMMLICH (d.h. eigene Server in eigenen Räumen oder Räumen von Drittdienstleistern)		CLOUD (d.h. gemietete Server von Drittdienstleistern)
Ausgaben für Anlagen, mit zunehmendem CapEx-Aufwand für Hardware / Server		**Zahlung für die Nutzung,** Gemietete Dienstleistungen ohne CapEx-Erfordernisse
Begrenzte, inflexible Kapazität, Langsame Anpassung der Kapazitäten (z. B. Notwendigkeit der Anschaffung, Installierung & Konfiguration von Servern, wann immer mehr Kapazität erforderlich ist)		**Flexible, „unbegrenzte" Kapazität,** Fähigkeit, gebrauchsfertige Rechen-/ Speicherkapazität sofort zu erhöhen oder zu verringern
Aufwendige interne Kapazitäten, mit der Erfordernis spezieller Teams zur Pflege und Wartung der Rechen-/ Speicherkapazität und Infrastruktur		**Begrenzte interne Kapazitäten,** Bereitstellung und / oder Wartung teilweise (IaaS und PaaS) oder komplett (SaaS) an Cloud-Anbieter ausgelagert

Quelle: Untersuchung und Analyse von GSG

Der Markt einigt sich auf sechs Cloud-Segmente, um die breite Palette an Marktangeboten zusammenzufassen

Übersicht der Cloud-Computing-Umgebung nach Art von Cloud und Art der Leistungen



Anm.: (1). Kann entweder im Unternehmen selbst („on-premise") beherbergt werden oder von einem Cloud-Anbieter gehostet werden (Hosted Private Cloud)
Quelle: Untersuchung und Analyse von GSG

NICHT ERSCHÖPFEND

Cloud-Lösungen decken einen großen Teil der IT-Lösungen von Unternehmen ab, von digitaler Zusammenarbeit bis hin zu geschäftsspezifischeren Tools

Hauptnutzungsarten in jedem Servicemodell-Typ

IaaS (hauptsächlich genutzt von CIO-Büro)

#1
Rechenkapazität
(zusätzl. Kapazität für Rechenerfordernisse)

#2
Speicherung
(Blocks, Objekte und Dateien)

#1
Virtual Private Server
(Speicher- und Rechen-umgebungen auf speziellen virtuellen Servern)

Baremetal and Hosted Private Cloud
(Physische und voll dedizierte Server)

Virtual Networking
(isoliertes und hochsicheres virtuelles Netzwerk)

Sicherheit
(Zugangsverwaltung)

PaaS (hauptsächlich genutzt von Entwicklern)

#1
Datenbankverwaltung
(Funktionen für die Datenbank-Konfiguration)

#2
AI / ML Platforms
(gebrauchsfertige Umgebung für die AI- / ML-Programmierung)

#3
Big Data & Analytics
(Opensource-Rahmen)

#4
Business Process Management
(Workflow management)

API Management Platforms
(Erstellen, Veröffentlichen & Sichern von API)

Containermanagement-Dienstleistungen
(Bereitstellung & Verwaltung containerisierter Anwend.)

SaaS (hauptsächlich genutzt von Endnutzern)

#1
Customer Relationship Management
(z. B. Salesforce CRM)

#2
Enterprise Resource Planning
(z.B. SAP ERP cloud)

#3
Collaboration-Tools
(z.B. Teams, Zoom, SharePoint)

#3
E-Mail / Messaging

Office Suite
(z.B. Office 365, Google Workspace)

Web-Hosting
(E-commerce)

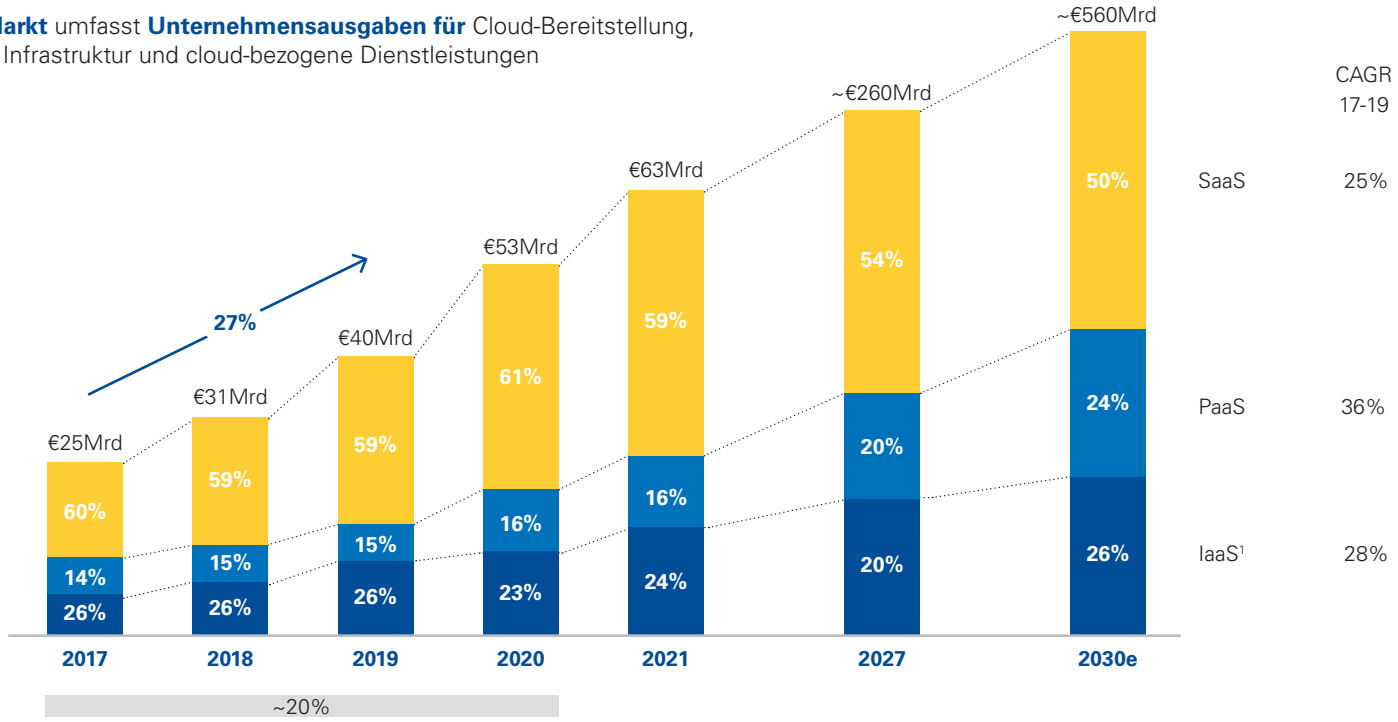
#X Rangordnung basierend auf Einnahmen aus Dienstleistungen nach Kategorie[1]

Anm.: (1) Auf der Grundlage der Umsätze des Jahres 2020 in Europa (IDC)
Quellen: Gartner; IDC IT Cloud services revenue; Untersuchung und Analyse von GSG

Der europäische Markt ist ein Wachstumsmarkt (+27 % pro Jahr während der Periode 2017-2019) von € 53 Mrd. im Jahr 2020 und voraussichtlich ca. € 300-500 Mrd. ab 2027

Entwicklung des europäischen[1] IaaS-, PaaS- und SaaS-Markts [2017-2030, € Mrd.]

Der **Cloud-Computing-Markt** umfasst **Unternehmensausgaben für** Cloud-Bereitstellung, Software, Investitionen in Infrastruktur und cloud-bezogene Dienstleistungen



Anm.: (1). IaaS-Markt umfasst Public IaaS, Hosted Private Cloud und Baremetal-Cloud (2). GSG-Prognose

Quellen: IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018–2021 (IaaS, PaaS und SaaS); IDC-Predictions-2021 European cloud predictions; IDC 2019 Forecast (Hosted Private Cloud); Untersuchung und Analyse von GSG

Die Cloud-Migration ist durch die Coronavirus-Pandemie noch wesentlich beschleunigt worden, was ihre strategische Rolle als wesentliche Infrastruktur und befähigender Faktor der „Resilienz“ zeigt

Stand der weltweiten Cloud-Migration nach Corona-Pandemie[1] [2020]

Corona-Pandemie

82%
der Befragten **erhöhten ihre Nutzung der Cloud** als direkte Reaktion auf die Pandemie

60%
verzeichneten die stetig zunehmende **Nutzung** von **Off-Premise-Technologie**

55%
erhöhten ihre Nutzung von **cloud-basierten Kollaborationstools**

zoom

+151%
aktive Nutzer
Im März 2020 im Vgl. zu 2019

+62Mio
tägliche Verbindungen
im Jahr 2020 im Vgl. zu 2019

Anm.: (1). Von den 250 befragten führenden IT-Unternehmen weltweit
Quellen: IT asset management firm Snow Software; GLG Industry Insights; Interviews mit Experten; Untersuchung und Analyse von GSG

Bis 2027 wird der Markt für EU-Cloud-Anbieter eine Größe von ~ € 260 Mrd. in Bezug auf Ausgaben, ~550.000 assoziierten Arbeitsplätzen und ~€ 200 Mrd. Investitionen (über den Zeitraum 2021-2027) erreichen

~€ 260 Mrd.

erwartete Größe des Cloud-Markts 2027

Ähnlich wie folgende europäische Märkte:

~€250Mrd. im Jahr 2020
Telekommunikationsmarkt

~€190 Mrd. im Jahr 2018
Textilmarkt

[550-600] K

geschaffene Arbeitsplätze, für einen Markt von ~€ 260 Mrd. im Jahr 2027

Viele Arbeitsplätze befinden sich in Regionen, in Data Centern oder Regionalbüros:

- Integration Developer
- Projekt- / Gebietsleiter
- Data Analysts
- Geschäftsentwickler
- Außendienstmitarbeiter
- etc.

~€ 200 Mrd.

voraussichtliche Investitionen über den Zeitraum 2021-2027

Wesentliche Bereiche der Investitionen für Cloud-Provider über die nächsten 10 Jahre werden umfassen:

- Energieeffizienzverbesserung
- Umstellung der Data Center-Architektur auf leistungsstärkere ARM-Prozessoren
- R&D in Bereichen, wie AI, Cloud-Gaming, Arzneimittelentdeckung usw.

Quellen: IDATE Digiworld; Euratex; Geschäftsberichte der Unternehmen; Untersuchung und Analyse von GSG

Auch wenn der Cloud-Markt in den nächsten zehn Jahren der Größe nach voraussichtlich mit dem Telekommunikationsmarkt vergleichbar sein wird, so ist er im Vergleich zu diesem reifen Markt noch embryonal

~€ 260 Mrd.
Cloud-Marktgröße
(Europa, 2027)

≃

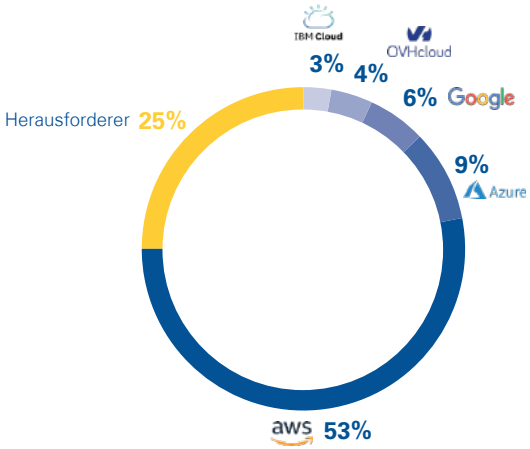
~€ 250-280 Mrd.
Telekommunikationsmarktgröße[2]
(Europa, 2027)

- Der europäische Cloud-Markt dürfte **bis 2030 der Größe nach vergleichbar** sein mit dem europäischen Telekommunikationsmarkt
- Der Cloud-Markt wird voraussichtlich der Entwicklung des Telekommunikationssektors folgen und dieselben Niveaus der Reife durch die **Eingriffe lokaler Behörden** erreichen, und sich entwickeln zu:
  - einem wettbewerbsintensiven Markt, wobei **die Lizenzen und der intensive Wettbewerb (ca. 200+ Mobilfunknetz-betreiber**[1] in Europa im Jahr 2018) eine **gute preisliche Wettbewerbsfähigkeit** und **Druck auf die Gewinnspannen ermöglichen**
  - einem hochregulierten Markt, der durch **öffentliche Behörden und Kartellbehörden** (z. B. ARCEP), **lokale Regierungsstellen** und **Telekom-Regulierungsbehörden** (z. B. BEREC, EU-Telekom-Regulierungsbehörde) **geregelt wird, was zu einer Stärkung der Innovationskraft und des Schutzes der Endverbraucher zum einen** und **zu einer Regulierung von Konsolidierungs-/ Fusionsplänen** zum anderen führt

Anm.: (1). MNOs: Mobile Network Operators (2). KPMG Estimate, unter Annahme von Stabilität / langsamem Wachstum im Vgl. zur gegenwärtigen Situation (~ € 250 Mrd.)
Quellen: Gartner 2019 Q3 (Public Cloud); IDC 2019 Forecast (Private Cloud); ETNO 2020; The Delta Perspective 2019; Untersuchung und Analyse von GSG

Der Markt ist wenig wettbewerbsintensiv, mit 3 globalen in den USA ansässigen „Hyperscalern", die den Cloud-Markt beherrschen – z. B. ~70 % der IaaS-Marktanteile

Aufteilung des europäischen Cloud-Computing-Markts (IaaS) [1H2020]



~70 % von den 3 größten „Hyperscalern" absorbiert

Landschaft der größten Akteure auf dem französischen und deutschen Cloud-Markt (IaaS, einschl. Hosted Private Cloud und PaaS) [2020]

Marktführer	aws	aws
#2	Azure	Azure
#3	OVHcloud	Google
#4	orange	T··Systems·
#5	Google	IBM Cloud
#6	IBM Cloud	ORACLE

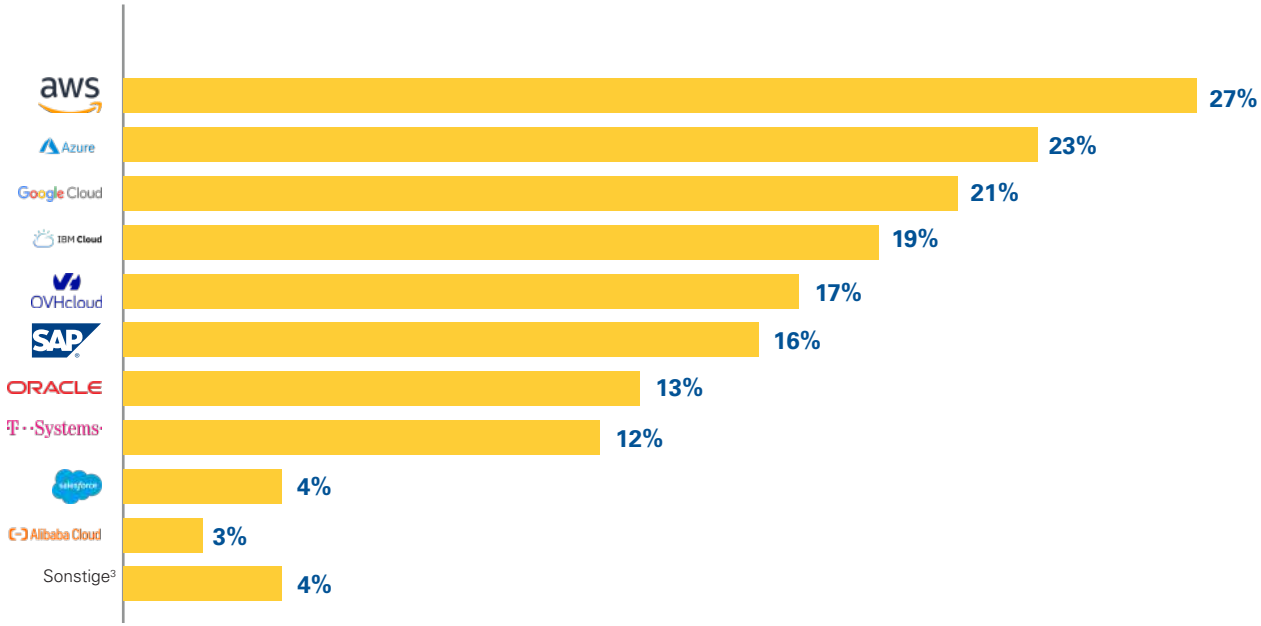
- **Der weitaus größte Anteil (~70 %) der Aufwendungen der europäischen Unternehmen für Cloud-Infrastruktur (IaaS) wird von nicht-europäischen Cloud-Anbietern absorbiert**
- Die mit der Cloud-Technologie verbundenen **Investitionen in die Infrastruktur und Technologie werden ebenfalls größtenteils außerhalb Europas getätigt, z. B.**:
  - Google Cloud investierte im Jahr 2019 über US-$ 13 Mrd. in sein Cloud-Computing-Geschäft, davon **nur 23 % außerhalb der USA**, einschließlich Europa
  - Die Investitionen von AWS werden hauptsächlich in den USA, und Indien getätigt (die für 2020-2022 geplanten Investitionen in letzterem betragen US-$ 7,8 Mrd.)
- **Europäische Cloud-Spezialisten und Telco-Betreiber erobern jedoch langsam Marktanteile** innerhalb ihrer jeweiligen nationalen Märkte (z. B. OVHcloud und Deutsche Telekom stehen jeweils an 3. und 4. Stelle auf ihren Märkten), in Bezug auf IaaS (inkl. Hosted Private Cloud) und PaaS

Quellen: Synergy Research group; IDC; Geschäftsberichte der Unternehmen; Untersuchung und Analyse von GSG

Die Beherrschung wird durch die Ergebnisse der von uns durchgeführten Umfrage bestätigt, wobei europäische Unternehmen AWS, Azure und GCP anderen Cloud-Anbietern vorziehen

Derzeitige Cloud-Dienstleistungsanbieter in den Unternehmen der Befragten[1]

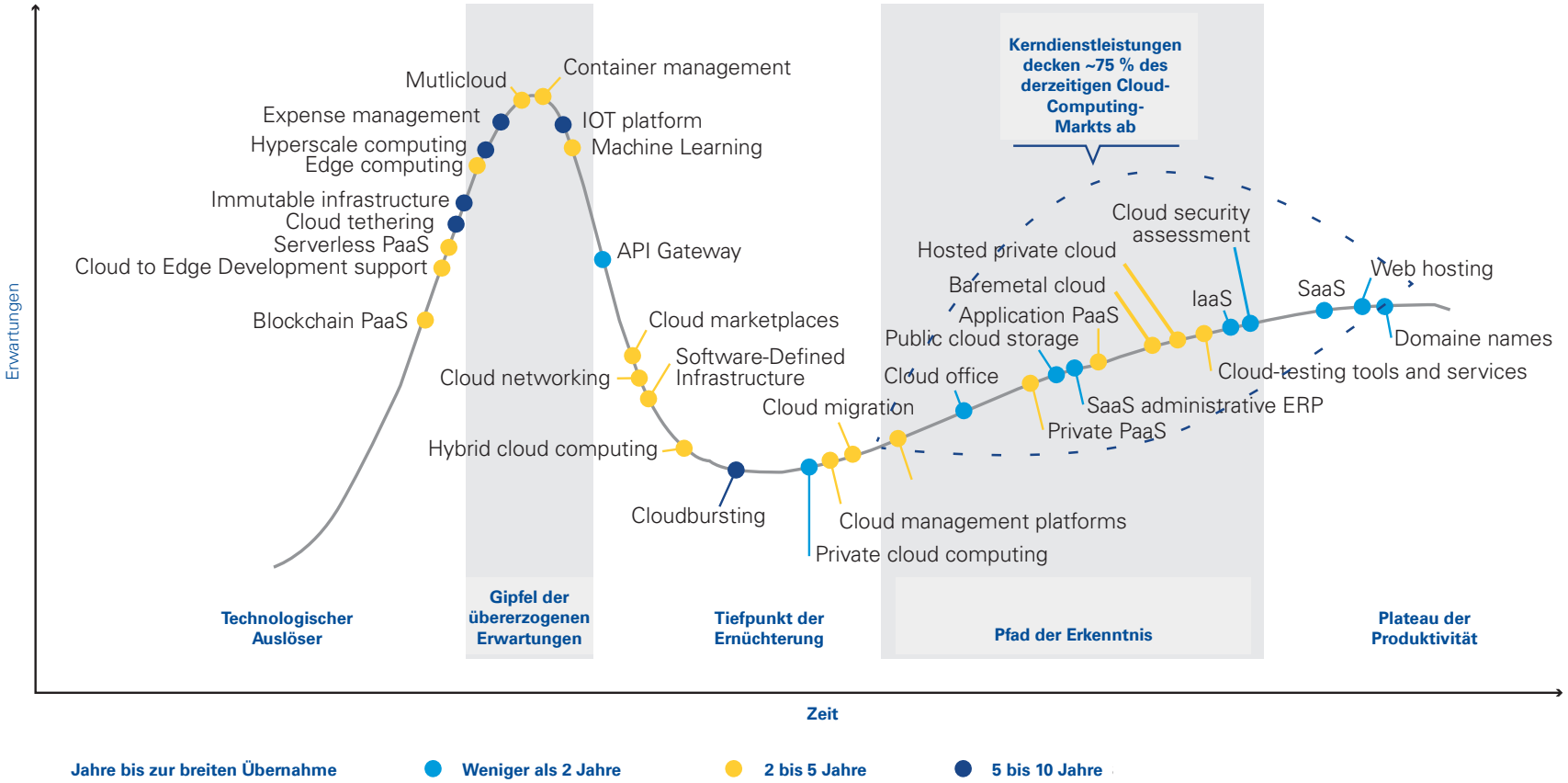
Wer sind Ihre derzeitigen **Cloud-Dienstleistungsanbieter[2],** insbesondere für **IaaS und PaaS?** (mehrere Antworten möglich)



Anm.: (1). Basierend auf 200 französischen und deutschen CxOs (2). Prozentualer Anteil basierend auf der Provider-Präsenz im Unternehmen, und nicht auf dem diesem Provider zugewiesenen IT-Budget (3). Liste anderer erwähnter Cloud-Provider: HCL, Scaleway, Veeva Systems, Huawei, TCS, QAD DynaSys Cloud
Quellen: GSG-Umfrage; GSG-Analyse

Cloud-Computing ist noch kein reifer Markt, und er wird in den kommenden Jahren zahlreiche Innovationen hervorbringen

Gartner Hype Cycle für Cloud-Computing [2018]



Anm.: (1). d. h. etwa 75 % Cloud-Marktgröße entsprechend der mit der gestrichelten ellipsenförmigen Linie umrandeten Liste von Cloud-Kerndienstleistungen
Quellen: Basierend auf der „Gartner hype cycle"-Kurve für Cloud-Computing 2018; IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018–2021 (IaaS, PaaS und SaaS);

2

Die Cloud-Migration: ein zwingender Weg, jedoch mit gewissen Einschränkungen

Triebfedern für den allgemeinen Übergang zu und die wachsende Nachfrage nach Cloud-Computing-Lösungen sind sowohl die betriebliche als auch die finanzielle Optimierung

Auswahl (nicht erschöpfend) der Hauptbeweggründe für den Cloud-Übergang

	Kosten-variabilisierung	**Flexibilität** bei der Erhöhung oder Senkung der Kapazitäten	**Teamarbeit** bei gleichzeitiger Wahrung der Datensicherheit	**Agilität & nahtloser Einsatz**	**Sicherheit** und Paradigmenwechsel hin zu mehr Resilienz	**Ermöglichung** agiler Geschäftsverlagerungen
Beispiele für Situationen	• CIO & CFO in mittelständischen Unternehmen kämpfen mit hohen Fixkosten **der On-Premise-Data Center** und erwägen Cloud-Migration… • …um aus mit Data Centern verbundenen **Fixkosten** (eigene Server) **variable Kosten** (Cloud) zu machen und somit zur Stabilisierung der Gesamtmarge des Unternehmens beizutragen	• CEO eines Start-ups, dessen neues SaaS-Produkt ein **sehr hohes Wachstum verzeichnet** und der daher benötigt: - **Flexibilität bei der Erhöhung von Speicher-/ Rechenkapazität** zur Erfüllung der Nachfrage… - …bei gleichzeitiger Wahrung der **Fähigkeit, die Kapazität nötigenfalls jederzeit zu verringern**	• Aufgrund der Covid-19-Situation können Mitarbeitende ihre Kunden nicht mehr persönlich treffen, **müssen aber online Informationen austauschen und große Dateien und vertrauliche Dokumente teilen** • Mitarbeitende verwenden daher eine cloud-basierte SaaS-Lösung als sichere Brücke zwischen Organisationen	• CIO/CTO eines Unternehmens mit dem Wunsch nach **mehr IT-Agilität bei gleichzeitiger Vermeidung der manuellen Pflege von Data Centern** (Kabel, Racks…),… • …erwägt daher eine Cloud-Migration zur **Verwaltung seiner Infrastruktur „as code" anstatt als physische Infrastruktur**	• A CIO/CTO eines Unternehmens mit dem Wunsch nach **Sicherung** der Daten des Unternehmens und **Erhöhung der Katastrophenresilienz** - Privatanwender plagt sich mit der **Speicherung großer Dateien** und erwägt das Hochladen der Dateien in die Cloud für: - **Einfachen Zugriff** für ihn und seine Familie - **Vermeidung von Datenverlust/Diebstahl**	• CxO bemüht sich sowohl um die **Verbesserung** der Leistung der bestehenden als auch um die **Entwicklung** neuer Tätigkeiten durch **Nutzung der vollen Kapazität der heutigen neuen Technologien**: - Optimierte Customer Journeys - **Einführung neuer Produkte** mit KI oder hoher Rechenkapazität - **Agiler und schneller Aufbau** neuer Tätigkeiten

Quelle: Untersuchung und Analyse von GSG

Diese verschiedenen Beweggründe spiegeln sich in den verschiedenen Interviews wider, die wir mit Entscheidungsträgern auf dem Cloud-Computing-Markt geführt haben (1/2)

Aussagen von Entscheidungsträgern auf dem europäischen Cloud-Computing-Markt

Kosten-variabilisierung

„Die Erneuerung unserer alternden Legacy-Systeme war für uns die ideale Gelegenheit, uns durch einen Cloud-Übergang unserer IT-Systeme für eine variablere Kostenstruktur zu entscheiden."

CIO, Energiewirtschaft

„Für ein kleines Start-up wie unseres, mit begrenzten finanziellen Mitteln für Investitionen in eine interne Infrastruktur und feste IT-Teams ist die Cloud als Lösung nahezu alternativlos."

CEO, französisches Start-up

Flexibilität bei der Erhöhung oder Senkung der Kapazitäten

„Cloud-Computing ist die beste Lösung, wenn es darum geht, schnell auf Stoßzeiten zu reagieren, im Gegensatz zu teuren internen Infrastrukturen, bei denen die Steigerung der Kapazitäten länger dauert."

CIO, französischer Staatsbetrieb

„Während der ersten Woche des Lockdowns im März 2020 erhöhte sich unsere Teams-Nutzung um das Zwanzigfache. Wir wären niemals in der Lage gewesen, dies in so kurzer Zeit intern zu stemmen."

CIO, Energiewirtschaft

Teamarbeit bei gleichzeitiger Wahrung der Datensicherheit

„Dank der Cloud konnten wir während des Lockdowns schnell auf Arbeit auf Distanz umstellen; so konnten unsere Teams effizient, von überall und geräteunabhängig zusammenarbeiten."

CIO, globales Consulting-Unternehmen

„Tools zur cloud-basierten Zusammenarbeit ermöglichen es uns, sensible Dateien auf sicheren und verschlüsselten Kanälen mit unseren Kunden zu teilen."

CIO, globales Consulting-Unternehmen

Quelle: Interviews mit Experten

Diese verschiedenen Beweggründe spiegeln sich in den verschiedenen Interviews wider, die wir mit Entscheidungsträgern auf dem Cloud-Computing-Markt geführt haben (2/2)

Aussagen von Entscheidungsträgern auf dem europäischen Cloud-Computing-Markt

Agilität & nahtloser Einsatz

„Die Größe und die geografische Abdeckung des Cloud-Anbieters sind sehr wichtig, da er in der Lage sein muss, sich konstant an unsere globalen Bedürfnisse anzupassen."

CIO, multinationales Chemieunternehmen

„Da wir eine Expansion auf dem nordamerikanischen Markt im Visier haben, können wir uns nicht mehr auf unsere Data Center in Frankreich stützen und erwägen auch die Nutzung der Public Cloud."

CIO, Gaming-Branche

Sicherheit und Paradigmenwechsel hin zu mehr Resilienz

„Die Kundendaten sind für uns als Unternehmen das wertvollste Gut. Unser Geschäft ist für den Katastrophenfall gewappnet, da meine Daten in Backup-Data-Centern gesichert sind, die von Cloud-Anbietern verwaltet werden."

CIO, Internationale Bank

„Durch die Migration unserer Daten zu Cloud-Umgebungen haben wir jetzt automatisch Zugang zu den Cybersicherheit-Spitzentechnologien und Sicherheits-Roadmaps unseres Cloud-Providers"

CIO, Internationale Bank

Ermöglichung agiler Geschäftsverlagerungen

„Bei der Entwicklung einer hochmodernen cloud-basierten Gaming-Plattform für unseren nationalen Markt erschien es uns sinnvoll, ihre Nutzung auch für Spieler im Ausland auf ihrem eigenen Markt zu öffnen — so haben wir uns in gewisser Weise zu einem SaaS-Provider gewandelt."

CIO, Gaming-Branche

„Wir haben uns für die Cloud-Migration entschieden, da die innovativsten Lösungen als SaaS angeboten werden"

CIO, Internationale Bank

Quelle: Interviews mit Experten

Die Wahl des Providers basiert auf einer Vielzahl von Kriterien — am wichtigsten sind Datensicherheit und Datensouveränität

Entscheidende Verkaufskriterien auf dem Cloud-Computing-Markt
(basierend auf den Antworten der Befragten[1])

KPC	Gewichtung	Begründung
Service-Resilienz & Sicherheit	●	Unser Cloud-Provider sollte in der Lage sein, **eine hohe Sicherheit der Infrastruktur und Dienste** zu gewährleisten, um **interne** und **externe Verletzungen der Datensicherheit zu verhindern**. Französischer CIO
Regulatorische Risiken und Compliance (einschl. Datensouveränität)	●	Bei der Wahl eines Cloud-Providers **sind Datensouveränität und regulatorische Compliance ebenso wichtig wie Service-Qualität.** Deutscher CIO
Zertifizierungen & Standards	◕	Da wir mit **sensiblen Gesundheitsdaten** umgehen, können wir es uns nicht leisten, **unzertifizierte Cloud-Dienste zu nutzen**. Das bestimmt die Wahl unseres Cloud-Providers. Französischer CIO
Breite und Qualität des Leistungsspektrums	◕	**Skalierbarkeit und Zuverlässigkeit sind für uns, gemeinsam mit dem Zugang zu elementaren und innovativen Spitzentechnologien die obersten Prioritäten**, wenn es darum geht, einen Cloud-Provider auszuwählen. Französischer CIO
Kosten	◑	Wir benötigen Anbieter, die **unsere Anforderungen an Funktionalität und Infrastruktur zu vernünftigen und transparenten Preisen erfüllen**. Deutscher CIO
Bekanntheit & Referenzen des Unternehmens	◑	Wir müssen uns auf einen **großen und zuverlässigen Cloud-Provider** stützen können, der in der Lage ist, uns langfristig bei der Abdeckung unserer **technologischen Anforderungen** und **geografischen Expansion zu begleiten**. Deutscher CIO

Schlüssel: ○ Niedrig — ● Hoch

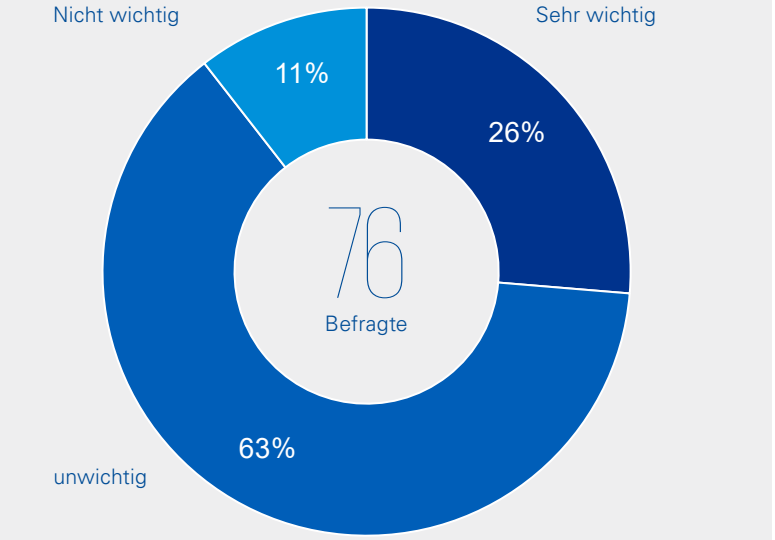
Anm.: (1). Basierend auf den Antworten von 76 befragten französischen und deutschen CIOs (quantitativ und qualitativ)
Quellen: GSG-Umfrage; GSG-Analyse

Die Befragten glauben, dass Datensouveränität wichtig ist, mit Schwerpunkt auf DSGVO-Compliance & Standort des Data Centers

Regulatorische Risiken und Compliance (einschl. Datensouveränität)

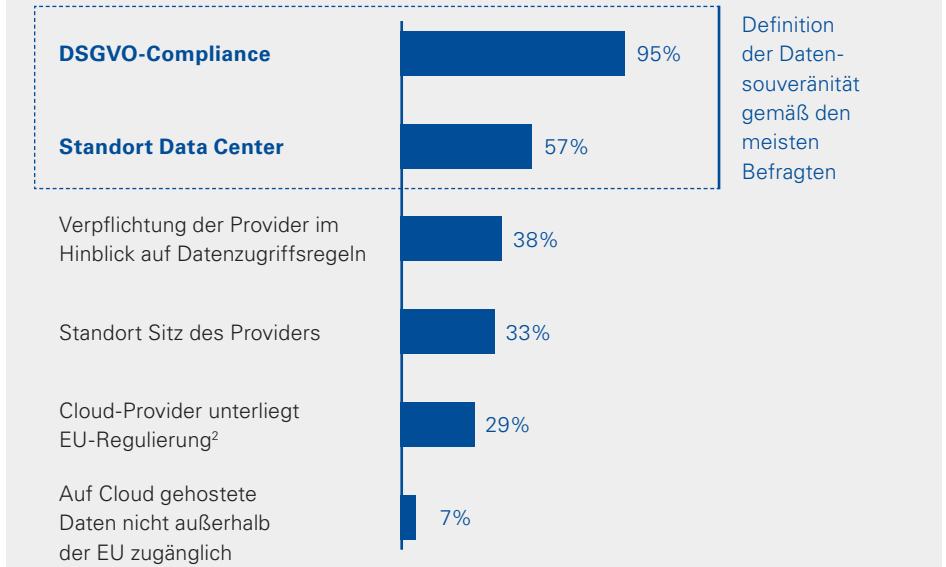
Datensouveränität wird von der großen Mehrheit der befragten Entscheidungsträger als ein **wichtiges** Kriterium i**m Entscheidungs-findungsprozess für die Wahl eines Cloud-Anbieters** genannt…

Inwieweit ist/war die Datensouveränität ein **Kriterium bei der Wahl Ihres/Ihrer Cloud Provider(s)**?[1]



…doch Datensouveränität kann mehrere Bedeutungen haben, **insbesondere zwei Hauptaspekte** (Konformität mit DSGVO-Regelungen und Standort des Data Centers)

Welche der folgenden Aspekte **beschreiben Datensouveränität Ihrer Meinung nach am besten?** (mehrere Antworten möglich)[1]



Anm.: (1). Basierend auf den Antworten von 76 französischen und deutschen CIOs (2.) Mit Ausnahme extraterritorialer Gesetzgebung (z. B. Cloud Act) der EU-Regulierung unterliegende Cloud-Provider
Quellen: GSG-Umfrage; GSG-Analyse

Trotz der Wichtigkeit der Datensouveränität bei der Wahl eines Cloud-Providers geben CxOs an, die Auswahl sei für sie begrenzt

Regulatorische Risiken und Compliance (einschl. Datensouveränität)

Kompromiss auf Kosten der Datensouveränität,das Angebot wird als zu beschränkt erachtet

„Aus Gründen der Datensouveränität **weigern wir uns, auf Unternehmensebene eine Cloud-Strategie zu implementieren**, aber bei Tätigkeitsspitzen **bleibt die Cloud die einzige schnelle und effiziente Ausweichlösung**.**"**

CIO, europäischer Logistikdienstleister

„Ich wünschte mir die **Entstehung europäischer Cloud-Provider**, dies würde uns die interne Ausrichtung auf die Cloud-Migration erleichtern und Sorgen über die Datensouveränität abnehmen. Aber wann könnte es soweit sein? Ich kann nicht noch jahrelang mit meinen alternden Systemen weitermachen…!**"**

CIO, internationaler Öl- & Gaskonzern

„Bis zum heutigen Tag gibt es kein **zufriedenstellendes Angebot für Datensouveränität bei Gesundheitsdaten**. Die Datenmigration zu einer Cloud mit Datensouveränität ist lediglich **mittelfristig denkbar, frühestens 2022**.**"**

CIO, französischer Staatsbetrieb

Akzeptanz einer unvollständigen Compliance bei der Datensouveränität

„Wir haben uns für einen US-Cloud-Provider entschieden, sobald unsere **Rechtsabteilung dem Vertrag zugestimmt hat** – dieser wurde seitdem nicht nochmals überprüft, **und das trotz großer Änderungen bei der Regulierung.**"**

CIO, internationaler Öl- & Gaskonzern

„Die Lösung für unsere **Sorgen im Hinblick auf die Datensouveränität** besteht darin, dass die Daten ausschließlich in der Europäischen Union gehalten werden, auch wenn sie sich **in den Händen von US-Providern befinden**.**"**

CIO, internationaler Öl- & Gaskonzern

„Auch wenn der Cloud-Provider das Hosting der Daten in Europa garantiert, **kommt es immer noch zu extraterritorialen Transfers**, wie beispielsweise Wartung und technischer Support.**"**

CIO, internationaler Öl- & Gaskonzern

Quelle: Interviews mit Experten

Die fehlende Kenntnis von Angeboten, die Datensouveränität sicherstellen, bremst das Wachstum des EU-Cloud-Markts, was zur Folge hat, dass einige Unternehmen die Cloud-Migration aufgeben oder verlangsamen

Regulatorische Risiken und Compliance (einschl. Datensouveränität)

Aufgabe der Cloud-Migration aufgrund von Sorgen über die Datensouveränität

„Ein Memo des französischen Innenministeriums und des Ministeriums für Kultur **verbietet die Speicherung öffentlicher Urkunden auf Data Centern, die keine Datensouveränität gewährleisten**. Solche Einschränkungen **verunmöglichen die Cloud-Migration** angesichts der **begrenzten Anzahl von Angeboten mit Datensouveränität auf dem Markt**."

CIO, französischer Staatsbetrieb

„Wir **lehnen es aus Gründen der Datensouveränität kategorisch ab**, unsere Kundendaten **auf der Cloud zu speichern**; darum haben wir uns dafür entschieden, unsere gesamte Software und Daten on-premise zu speichern."

CIO, international tätiges Unternehmen in der Gaming-Branche

„Der Vorstand hat hinsichtlich des Standorts unserer Kundendaten ein klares Wort gesprochen. **Diese müssen im Haus bleiben und dürfen auf keinen Fall bei Dritten gehostet werden**."

CIO, europäischer Logistikdienstleister

„Da wir über **keine Garantie für den Standort** der verschiedenen Komponenten der **Wertschöpfungskette des Cloud Providers** (Speicherung, Rechenleistung, Wartung) verfügen, bleibt uns **nichts anderes übrig, als für unsere sensiblen Daten intern verwaltete Data Center zu nutzen**."

CIO, Internationale Bank

„Wenn unsere Daten **on-premise gespeichert sind, lassen sich Audits zur Datensouveränität** recht einfach durchführen, was **bei der Verwendung der Einrichtungen eines Drittanbieters technisch unmöglich ist**."

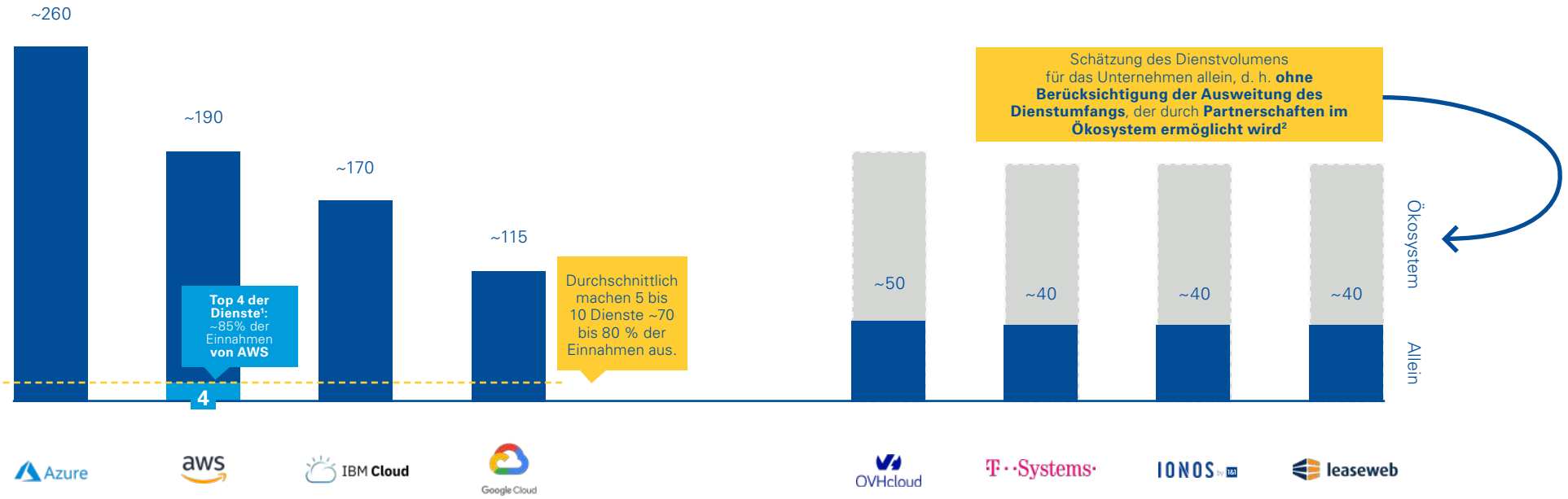
CIO, europäischer Logistikdienstleister

Quelle: Interviews mit Experten

Die Hyperscaler bieten eine große Anzahl von Diensten, erzielen aber den Großteil ihrer Einnahmen mit nur einigen wenigen davon.

Breite und Qualität des Leistungsspektrums

Anzahl von Cloud-Diensten und Produkten (in Private-, Public- und Hybrid-Clouds) **für einige große Cloud-Provider** [2020]



Anm.: (1). Grundservices: EC2 (Elastic Compute Cloud, Rechenkapazität), EBS (Elastic Block Store, Blockspeicher), RDS (Relational Database Service), S3 (Simple Storage Service, Objektspeicher) (2). Zusätzliche Informationen auf den folgenden Slides

Quellen: Untersuchung und Analyse von GSG; Websites der Unternehmen; CloudPegBoard; Cloudability State of Cloud 2018

Dennoch erscheint das europäische Cloud-Ökosystem jenseits einfacher allgemeiner Cloud-Provider dicht und vielfältig.

Breite und Qualität des Leistungsspektrums

Dichtes europäisches Ökosystem von Technologieanbietern (nicht erschöpfend)

Internet-Software & -Dienste

ROCKET.CHAT, ATEMPO, odoo, BlueMind, fastmag, Whaller, platform.sh, numen, MailOut, OVHcloud, UNIKI, HOSTING POWER, worteks, RemXcale, sugarcrm, clever cloud, paper.li

Cybersicherheit

Shadline, Acronis, CybelAngel, V6PROTECT, LINKBYNET

Cloud-Computing-Dienste

OVHcloud, T-Systems, IONOS, leaseweb, GLOBAL SWITCH, OUTSCALE, CONNECTIS, gigas, aruba CLOUD, LINKBYNET, UpCloud, ikoula, UKFAST, Scaleway, orange Business Services, alixans, iomart, HETZNER, PARTITIO

Künstliche Intelligenz

SYSTRAN, deepomatic, DIGDASH, GRAPHCORE, algolia, OVHcloud, babylon, meero, Benevolent

Internet der Dinge

claranet, sigfox, SENSEERING, INTESENS, kinéis, Actility, Neurones IT, WITHINGS

Datenverwaltung & Dienste

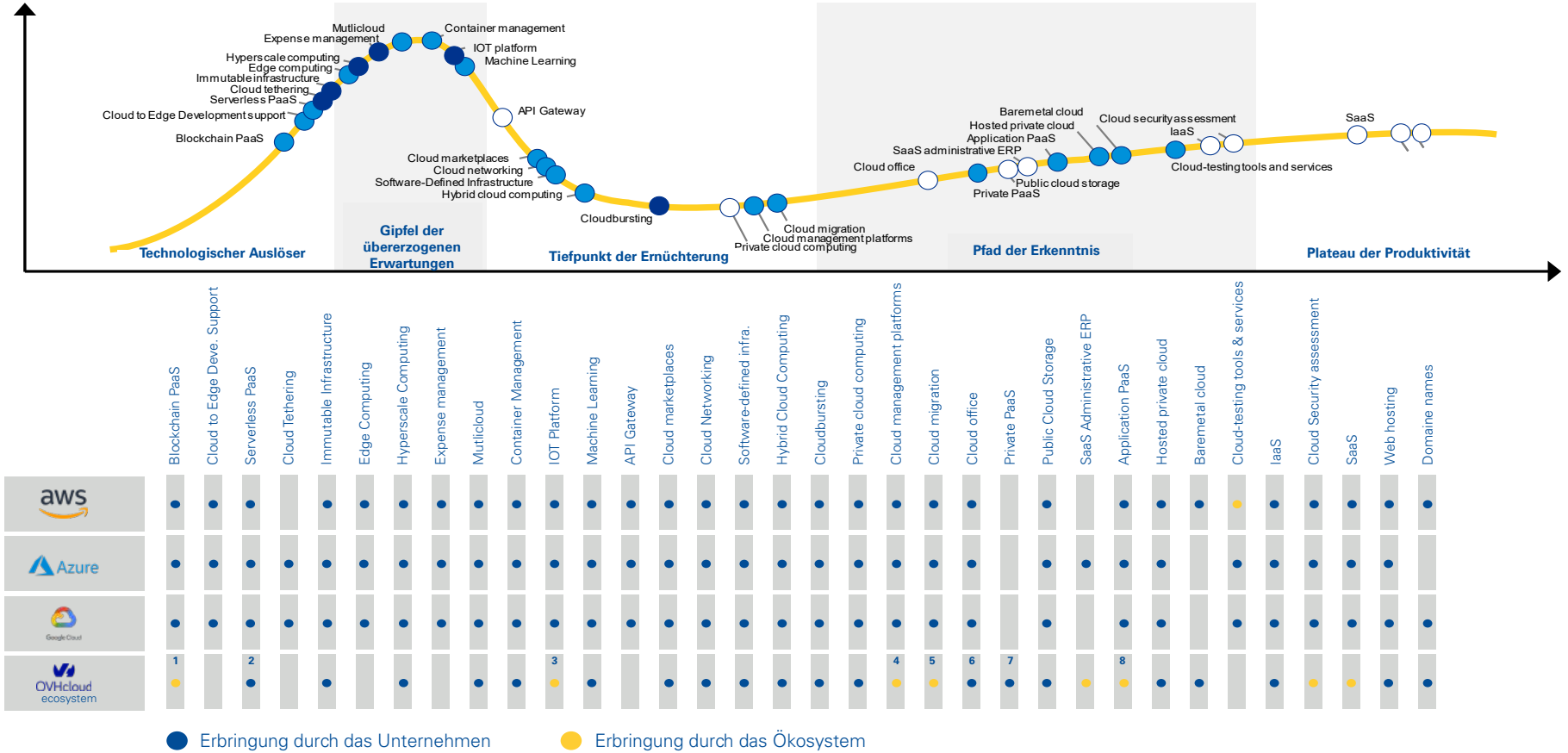
celonis, clever cloud, SIGMA, CIKLUM, OVHcloud, digitalis, N-iX

Quellen: Untersuchung und Analyse von GSG; Websites der Unternehmen; CB Insights Global Unicorn Club; Forrester

Durch wirksamen Einsatz ihres Ökosystem entfalten die europäischen Akteure ein breites Angebot mit einer Breite und Tiefe, die größtenteils mit demjenigen der Hyperscaler vergleichbar sind.

Breite und Qualität des Leistungsspektrums

Cloud-Provider - Positionierung der Angebote auf dem Gartner Hype Cycle für Cloud Computing [2018]



Anm.: (1). TON Ventures (2). Google Anthos, Clever Cloud (3). SmartHub (4) Cloudify (5). Capgemini, Atos, Sopra Steria, Partito (6). Sharepoint, Office 365 (7). Google Anthos (8). Platform.sh, Clever Cloud

Quellen: Gartner Hype-Zyklus für Cloud Computing 2018; Wipro; Websites der Unternehmen; Untersuchung und Analyse von GSG

Europäische Herausforderer, wie OVHcloud, bieten durch ihr dichtes Ökosystem ein umfassendes Leistungsspektrum, das die funktionalen Bedürfnisse der meisten Kunden abdeckt (1/3)

Breite und Qualität des Leistungsspektrums

Provider-Dienste und ihre funktionale Abdeckung[1] – Hauptangebot

		aws	Azure	Google Cloud	OVHcloud +ecosystem
↑ ~45% ↓ IaaS	**Speicher** (Block + Objekt + Datei)	Amazon S3 S3 Glacier Deep Archive	Blob Storage Archive Storage	Cloud Storage Archive storage	File, Object and Block Storage Cloud Archive
	Rechen-kapazität	Amazon EC2	Azure Virtual Machine	Compute Engine	Baremetal, Private Cloud, Public Cloud – Compute instances
	Hosted private cloud	VMware Cloud on AWS	Azure Private Cloud	Google Cloud VMware Engine	Hosted Private Cloud solutions
	Baremetal server	Amazon EC2 Bare Metal Instance	Azure Bare Metal Servers	Sole Tenant Node	Bare Metal Server
	Virtual private server	Amazon LightSail	Azure App Service Environment		VPS
	Virtual Networking	Amazon VPC	Azure VNet	Virtual Private Cloud	OVHcloud vRack
	Sicherheits-management	AWS IAM AWS Shield	Azure IAM Azure DDoS	Cloud IAM Google Cloud Armor	OVHcloud user management Atos, Thales Network protection (Anti-DDOS)

Andere EU-Akteure (nicht erschöpfend)

Orange Business Services · T-Systems · IONOS · OUTSCALE · HETZNER

X% Einnahmenanteil nach Service-Kategorie (2020 , Europa, IDC)

Nicht abgedeckte Funktionalität

Durch den Provider oder sein Ökosystem abgedeckte Funktionalität

Anm.: (1). Basierend auf kommunizierten Informationen auf Unternehmenswebsites

Quellen: Gartner; IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018–2021; Websites der Unternehmen; Untersuchung und Analyse von GSG

Europäische Herausforderer, wie OVHcloud, bieten durch ihr dichtes Ökosystem ein umfassendes Leistungsspektrum, das die funktionalen Bedürfnisse der meisten Kunden abdeckt (2/3)

Breite und Qualität des Leistungsspektrums

Provider-Dienste und ihre funktionale Abdeckung[1] – Hauptangebot

	aws	Azure	Google Cloud	OVHcloud +ecosystem
Big Data & Analytics	Amazon EMR	Azure HDInsight	Cloud DataProc	OVHcloud Big Data Cluster
Database management	Amazon RDS Amazon Aurora	Azure Managed databases	Cloud SQL Cloud Spanner	Cloud Databases Enterprises Cloud Databases MongoDB
Business process management	ECOBPM[2]	Logic Apps	Workflows	
IOT deployment platform	AWS IoT services	Azure IoT	Google Cloud IoT solutions	Claranet Actility
AI / ML platform	Amazon SageMaker	Azure Machine Learning	AI platform	ML Serving
API management platforms	Amazon API Gateway	API Apps	Apigee	
Container management services	EKS	AKS	Kubernetes Engine	Managed Kubernetes Service Anthos

~75% PaaS

Andere EU-Akteure (nicht erschöpfend)

Orange Business Services · T-Systems · IONOS · OUTSCALE · HETZNER

X% Einnahmenanteil nach Service-Kategorie (2020 , Europa, IDC)

Nicht abgedeckte Funktionalität

Durch den Provider oder sein Ökosystem abgedeckte Funktionalität

Anm.: (1). Basierend auf kommunizierten Informationen auf Unternehmenswebsites (2). Beispiele für auf dem Markt verfügbare Angebote

Quellen: Gartner; IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018–2021; Websites der Unternehmen; Untersuchung und Analyse von GSG

Europäische Herausforderer, wie OVHcloud, bieten durch ihr dichtes Ökosystem ein umfassendes Leistungsspektrum, das die funktionalen Bedürfnisse der meisten Kunden abdeckt (3/3)

Breite und Qualität des Leistungsspektrums

Provider-Dienste und ihre funktionale Abdeckung[1] – Hauptangebot

	aws	Azure	Google Cloud	OVHcloud +ecosystem	Andere EU-Akteure (nicht erschöpfend)
Emails / Messaging	Amazon SES	Outlook	Gmail	Trusted exchange Hosted Email and Trusted Collaborative Solutions[3]	
Collaboration tools	AWS Smart Business	Office 365	Google Workspace		
Office Suite	Amazon WorkDocs			Dedicated Exchange & Sharepoint	
CRM	Magento[2] Odoo	Dynamics 365	Copper[2]		
ERP	SAP[2]		SAP[2]	Odoo Dolibarr Surgarcrm (CRM)	
Web Hosting	Amazon Web hosting services	Azure Web Apps	Google Cloud web hosting	OVHcloud Web Hosting	

~80%

SaaS

X% Einnahmenanteil nach Service-Kategorie (2020 , Europa, IDC)

Nicht abgedeckte Funktionalität

Durch den Provider oder sein Ökosystem abgedeckte Funktionalität

Anm.: (1). Basierend auf kommunizierten Informationen auf Unternehmenswebsites (2). Beispiele für auf dem Markt verfügbare Angebote (3). Andere Partner: Zimba, Dropcloud und Nextcloud (nicht erschöpfend)

Quellen: Gartner; IDC Worldwide and Regional Public IT Cloud Services Forecast, 2018–2021; Websites der Unternehmen; Untersuchung und Analyse von GSG

Trotz unattraktiver Preise gelingt es globalen Anbietern, den Markt mit aggressiven und unkonventionellen Kundenakquisitionspraktiken zu beherrschen...

Kosten

Subventionen während der Kundenakquisitionsphase

„Um uns die Migration auf die Public Cloud eines internationalen Cloud-Providers zu erleichtern, wurden wir 6 Monate lang **kostenlos von 5 Vollzeitberatern unterstützt."**

CIO, französischer Staatsbetrieb

„Mir wurde von einem internationalen Cloud-Provider ein **100-Millionen-€-Gutschein** angeboten **im Austausch gegen einen 5-Jahres-Exklusivvertrag."**

CEO, deutsches Fintech-Unternehmen

„**Mein erstes Jahr** als Nutzer der Dienste eines globalen Cloud-Providers **kostete mich nicht einen Cent. Das hat uns die Entscheidung zur Cloud-Migration erleichtert"**

CIO, mittelständischer französischer Software-Provider

„Ziel einiger globaler Cloud-Provider ist es, **Kunden** so schnell wie möglich von ihrem Ökosystem abhängig zu machen. Deshalb ist der **Daten-Upload** (im Gegensatz zum Download) **kostenlos.**„

CIO, globales Consulting-Unternehmen

Verbundgeschäfte, Bündelung oder Leistungsaustausch

„Die Unterzeichnung eines großen **Liefervertrags für unser Kerngeschäft** mit einem internationalen Cloud-Anbieter **wurde von einer Hauptbedingung abhängig gemacht**: Der Migration unserer Daten auf ihre Public Cloud"

CIO, internationaler Öl- & Gaskonzern

„Anfangs wollte ich Office 365 in einer anderen Cloud-Umgebung als der Microsoft-Infrastruktur benutzen, aber mir wurde **schnell klar, dass das viel teurer ist**."

CIO, mittelständischer französischer Software-Provider

„Einer der Gründe, die die Entscheidung zum Wechsel unseres Cloud-Providers beschleunigt hat, **sind seine aggressiven Verkaufspraktiken**. Wir wurden häufig **gezwungen, für andere Cloud-Dienste zu bezahlen, die wir nicht benötigten**."

CIO, globales Consulting-Unternehmen

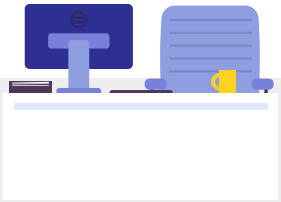
„Berüchtigte Office-Tool-Provider **vertreiben gebündelte IaaS- und SaaS-Produkte** zu extrem attraktiven Preisen, zu **einem Fünftel des Angebots von Konkurrenten, die nur IaaS anbieten."**

CIO, europäischer Logistikdienstleister

Quelle: Interviews mit Experten

...insbesondere durch Bündelung von SaaS- und IaaS-Diensten für Software-Produkte, die historisch in lokalen Umgebungen betrieben werden.

Kosten

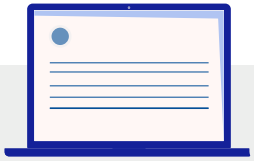


Ein großer historischer Kundenstamm, der Desktop-Software verwendet, wird nun von einigen Hyperscalern genutzt...

Von[1] **zu**

Office 365

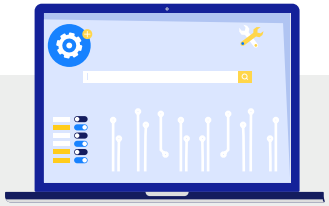
ORACLE CRM ON DEMAND



... durch Bündelung & Verbundgeschäfte mit IaaS + SaaS Angeboten, wodurch manchmal das BYOL-Prinzip („Bring Your Own License„) durch technische und finanzielle Einschränkungen missachtet wird...

"Microsoft hat sein Produkt Teams **illegal** in seine marktbeherrschende Office-Produktivitätssuite **eingebunden**, die **Installation erzwungen, seine Entfernung blockiert** und **die wahren Kosten** für Unternehmenskunden **verschleiert."**

Slack-Pressemitteilung, Juli 2020



Folglich bündeln einige historische Software-Anbieter momentan ihre Legacy-Software-Produkte (nun in SaaS) mit ihren IaaS-Produkten...

Obwohl beide Produkte historisch und technisch getrennt waren[2]

Anm.: (1). Nicht erschöpfend, Beispiele für Provider-Produkte; (2). z. B. Office 365, das gegenwärtig von Azure separat in China verkauft wird
Quellen: Unternehmenswebsites, Untersuchung und Analyse von GSG

Zusätzlich zu den unkonventionellen Kundenakquisitionspraktiken wird der Vertragsaustritt oder Provider-Wechsel für Cloud-Nutzer durch komplexe Austrittsbedingungen erschwert

Kosten

Hohe Austrittshürden & Anbieter-Lock-in

„Wenn Sie erst einmal Ihre gesamten Daten auf ihre [internationale Cloud-Provider] Cloud hochgeladen haben, **wird Ihnen klar, dass sie in der Falle sitzen, da die Kosten für den Wechsel zu einem anderen Anbieter extrem hoch sind."**

CIO, globales Consulting-Unternehmen

„Wir haben uns für die **schnelle und einfache Lösung** entschieden, proprietäre APIs von internationalen Cloud-Providern zu verwenden, anstatt unsere eigenen zu entwickeln — **wir wussten, wie teuer und schwierig** es sein würde, da wieder herauszukommen**"**

CIO, internationaler Öl- & Gaskonzern

„Bei der öffentlichen Hand müssen Cloud-Verträge **von Rechts wegen regelmäßig überprüft werden**. Daher kommen Public Cloud Provider mit ihrer **fehlenden Portabilität und ihren hohen Ausstiegskosten nicht in Frage**."

Leiter Abteilung Technische Infrastruktur, französische Behörde

„Unsere Entwickler haben sich für die Verwendung innovativer und benutzerfreundlicher **proprietärer Lösungen unseres globalen Cloud-Providers** entschieden. Wir hatten nichts dagegen, bis wir **Migrationsproblemen** gegenüberstanden und folglich unser Budget überschreiten mussten."

CIO, globales Consulting-Unternehmen

Verträge mit langer Laufzeit und Verbindlichkeiten mit unklarer Preisstellung

„Wenn Sie sich bei einigen internationalen Cloud-Providern dafür entscheiden, ihren Vertrag 3 Jahre vor Vertragsende zu kündigen, **müssen Sie den vollen Betrag für die verbleibenden 3 Jahre bezahlen"**

CIO, mittelständischer französischer Software-Provider

„Mit **den hohen Kosten einer vorzeitigen Vertragsbeendigung** und **den festgelegten Verbindlichkeiten** bei einigen globalen Cloud-Providern kann sich die Entscheidung, vorzeitig den Cloud-Provider zu wechseln, **als sehr teuer erweisen**."

CIO, französischer Staatsbetrieb

„Wir ließen uns anfangs von den **günstigen Speicherungspreisen** unseres neuen Cloud-Providers überzeugen und waren uns der zusätzlichen Kosten nicht bewusst. So kam es zu einem schnellen Anstieg **unserer Gesamtbetriebskosten und zu einer wachsenden Komplexität unserer Systeme**."

CEO, deutsches Fintech-Unternehmen

„**Aufgrund der Komplexität des Vertrags, der Schwierigkeit** eines klaren Verständnisses **des Umfangs der erbrachten Leistungen und der mangelnden Reife unserer Erfahrungen mit diesen Themen** sind wir noch heute nicht in der Lage, **unsere Cloud-Kosten vorherzusagen**."

CIO, europäischer Logistikdienstleister

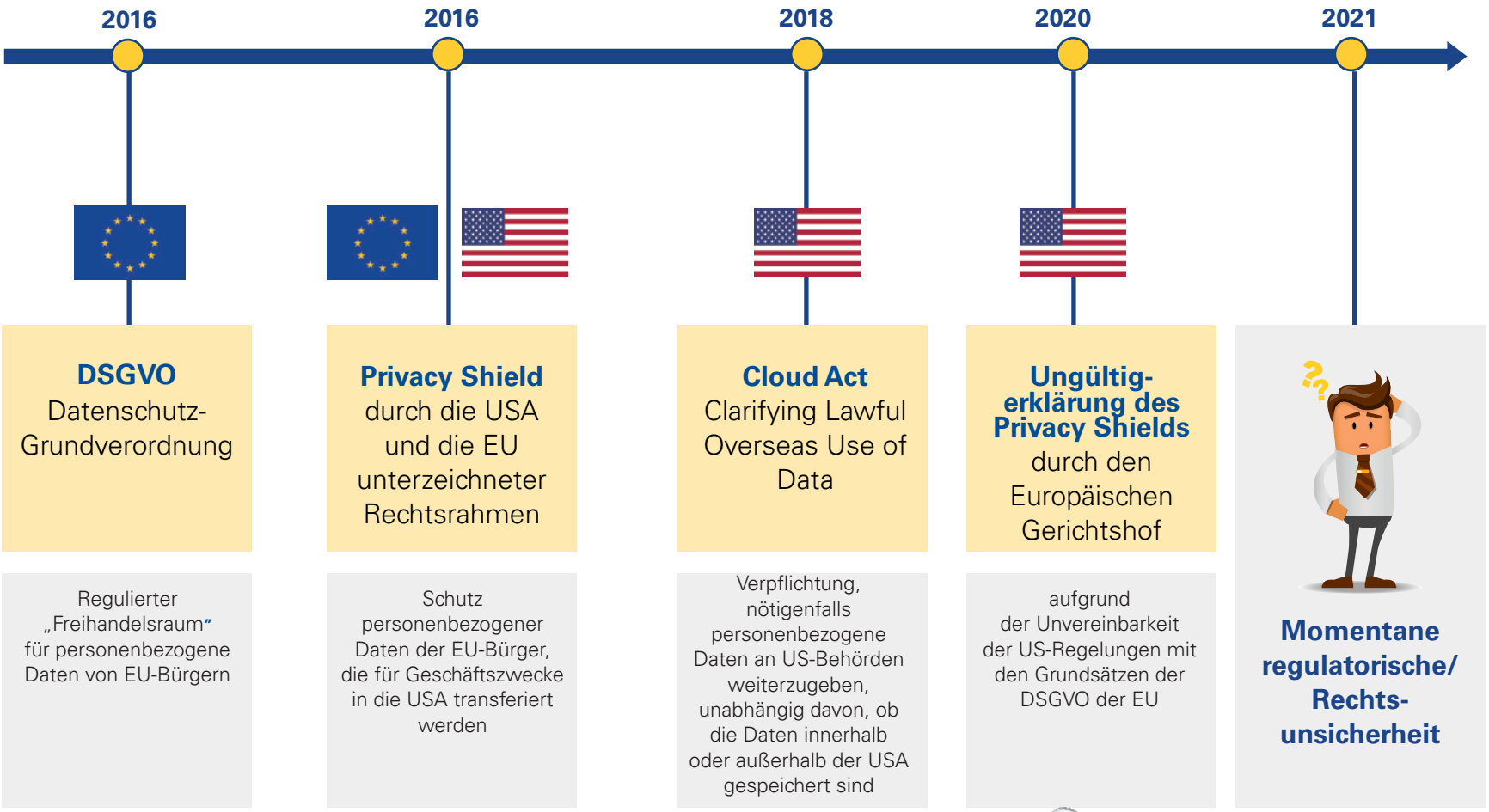
Quelle: Interviews mit Experten

3

Rechtliche Unsicherheiten in Bezug auf Daten: Was sind die Risiken für europäische Unternehmen?

Die seit 2016 eingeführten neuen Regelungen für Daten in den USA und der EU haben sich erheblich auf das Cloud-Computing ausgewirkt

Wichtigste Neuregelungen für den Cloud-Markt

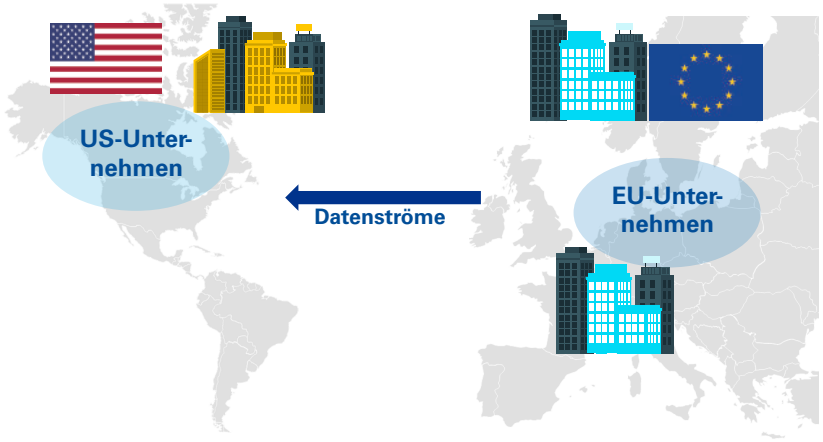


Quellen: KPMG Avocats und Untersuchung und Analyse von GSG

Zusätzliche Informationen im Anhang

Mit diesen Regelungen wurde versucht, einen engen rechtlichen Rahmen für europäische Datenströme zu schaffen, an denen US-Unternehmen (in und außerhalb der EU) beteiligt sind

Ströme mit Beteiligung von US-Unternehmen außerhalb der EU

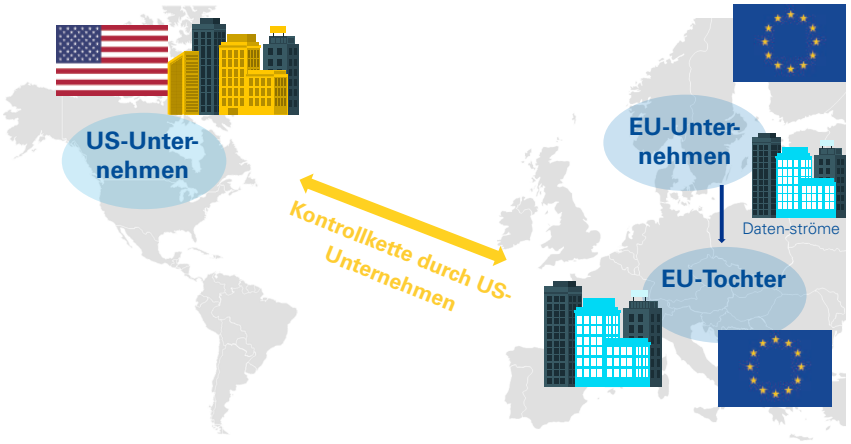


Solche Datentransfers waren erlaubt, da ein effektives und angemessenes Datenschutzniveau durch den **Privacy Shield** sichergestellt war

ABER

Am 16. Juli 2020 hat der Europäische Gerichtshof **die Privacy-Shield-Vereinbarung für ungültig erklärt**, mit der Begründung, dass die US-Überwachungsprogramme nicht mit den Grundsätzen der DSGVO vereinbar seien[1] (Schrems-II-Urteil)

Ströme mit Beteiligung von US-Unternehmen innerhalb der EU



Solche Datentransfers sind **nach DSGVO durch Verarbeitervereinbarung (in der die Standard-Vertragsklauseln enthalten sind) und Vereinbarung zwischen den gemeinsamen Verantwortlichen erlaubt**

ABER

Nationale Gesetzgebung
(wie beispielsweise Cloud Act)
hat Vorrang gegenüber Vertragsrahmen

Anm.: (1). Die US-Gesetzgebung erlaubt öffentlichen Behörden den Zugriff auf sämtliche personenbezogenen Daten, die auf US-Boden übertragen werden, insbesondere „Foreign Intelligence Surveillance Act" (FISA) und Executive Order 1233
Quellen: KPMG Avocats und Untersuchung und Analyse von GSG

Die jetzige US-Regelung scheint jedoch strukturell unvereinbar mit den Grundsätzen der europäischen DSGVO, die auf den Schutz der personenbezogenen Daten der EU-Bürger abzielen

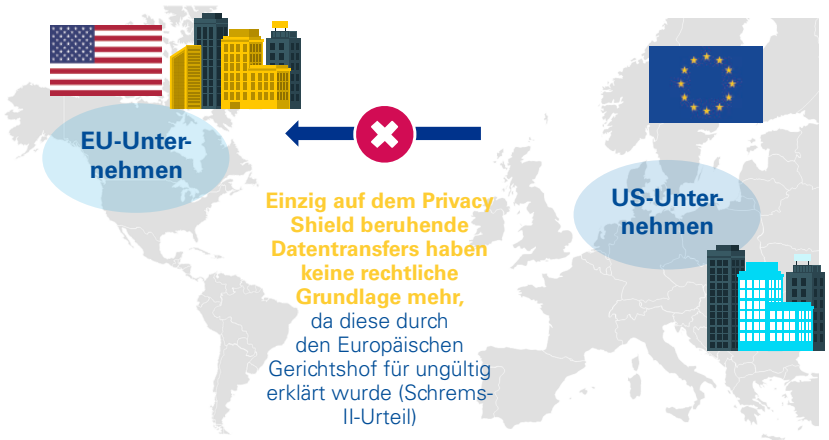
US-Gesetzgebung erlaubt US-Behörden den Zugriff auf personenbezogene Daten, unabhängig davon, ob sich diese innerhalb oder außerhalb der USA befinden		**Die europäische Gesetzgebung** schränkt den Zugriff auf personenbezogene Daten von EU-Bürgern strikt ein
Öffentliche US-Behörden **dürfen auf personenbezogene Daten zugreifen**, unabhängig davon, ob sie amerikanisch sind oder nicht		Der Zugriff öffentlicher Behörden auf personenbezogene Daten in der EU ist **streng geregelt und kontrolliert**
US-Cloud-Provider **können** den **Datenschutz** für personenbezogene Daten von EU-Nutzern gegenüber US-Behörden **nicht garantieren**…		Ein Grundsatz der DSGVO ist die **Gewährleistung der Sicherheit** und des **Schutzes personenbezogener Daten**…
…unabhängig davon, ob die Daten **sich innerhalb oder außerhalb der USA befinden**		…**innerhalb und außerhalb der Europäischen Union** (mit strengen Regeln für die Verarbeitung außerhalb der EU)

Scheinbar unüberbrückbare Unvereinbarkeit der Regulierungen

Quellen: KPMG Avocats und Untersuchung und Analyse von GSG

Unternehmen, die personenbezogene Daten von EU-Bürgern auf Server von Nicht-EU-Unternehmen transferieren, verfügen nunmehr über keine rechtliche Grundlage in Verbindung mit dem Privacy Shield und setzen sich der Gefahr der strafrechtlichen Verfolgung aus

Außerhalb der Europäischen Union



- **Der Europäische Datenschutzausschuss (EDSA)** versuchte, diese Rechtsunsicherheit aus der Außerkraftsetzung des Privacy Shield durch eine Roadmap für die Verantwortlichkeit um die Transfers zu beheben: **Know Your Transfers (KYT)** (Analyse des Datenverkehrs) mit 5 erlaubten und 2 verbotenen[1] Anwendungsfällen
- Die Erfahrung hat gezeigt, dass es sich bei den 2 verbotenen Anwendungsfällen tatsächlich um die am weitesten verbreiteten Fälle von Datentransfers handelt

Ist-Situation

Die Rechtsunsicherheit bleibt bestehen und ließe sich nur durch eine **Änderung der US-Datenschutzgesetzgebung ändern**

Innerhalb der EU

- Da die nationale Gesetzgebung Vorrang gegenüber Vertragsrahmen hat, **gilt der US Cloud Act für amerikanische Tochtergesellschaften mit Sitz in der EU:**
  - Öffentliche US-Behörden könnten auf durch EU-Töchter gehaltene personenbezogene Daten unabhängig vom Ort ihrer Speicherung zugreifen
  - Verträge zwischen einem EU-Datenverantwortlichen und europäischen Tochtergesellschaften könnten wegen Nichterfüllung der DSGVO angefochten werden

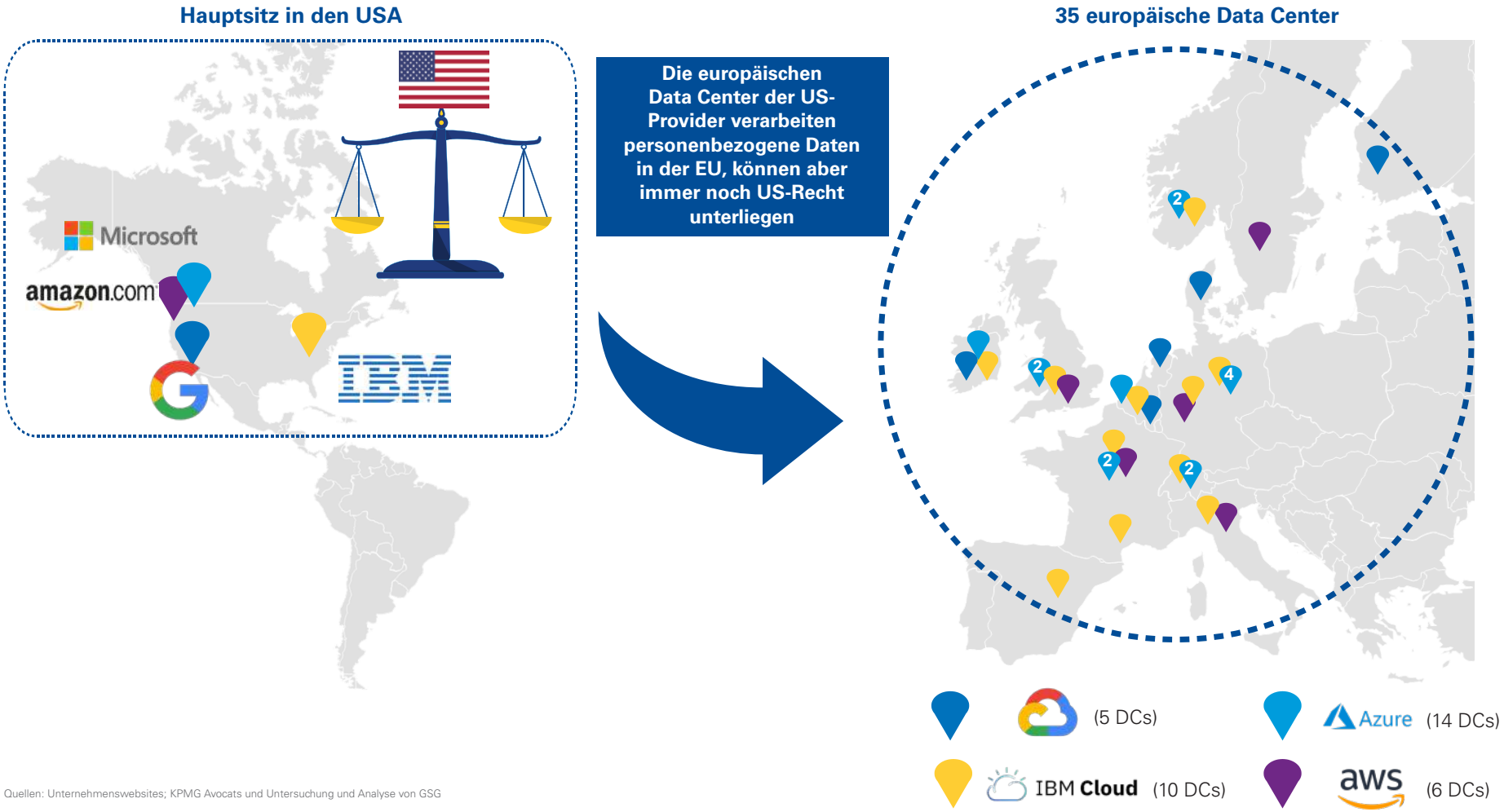
Ist-Situation

Unternehmen, die der DSGVO unterliegen, können für die Nichterfüllung von Sicherheitsmaßnahmen gegenüber Regulierungsbehörden, Kunden und Verbrauchern **haftbar gemacht werden**

Anm.: (1). „Übermittlung an Cloud-Anbieter oder sonstige Auftragsverarbeiter, die Zugriff auf Daten im Klartext" und „Fernzugriff auf Daten für Geschäftszwecke benötigen"
Quellen: KPMG Avocats und Untersuchung und Analyse von GSG

Die Speicherung personenbezogener Daten von EU-Bürgern in europäischen Data Centern von US-Providern ist noch immer keine Garantie für ihre Sicherheit, da sie immer noch US-Recht unterliegen können

Data Center von US-Cloud-Providern in der EU [2020]

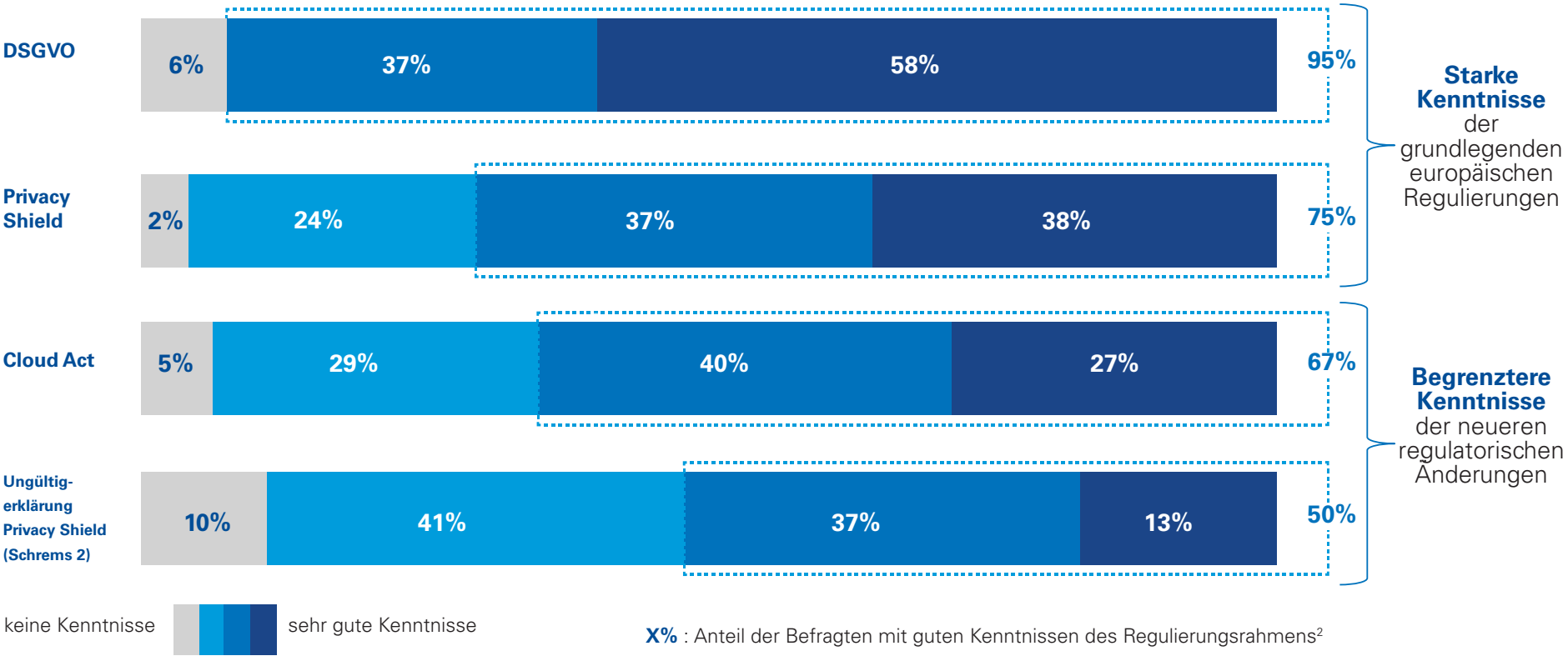


Quellen: Unternehmenswebsites; KPMG Avocats und Untersuchung und Analyse von GSG

Der Kenntnisstand der Cloud-Computing-Entscheidungsträger hinsichtlich Datenschutzregelungen ist unterschiedlich; gut, was die DSGVO betrifft, aber begrenzt im Hinblick auf den Cloud Act und Schrems 2

Kenntnis von Elementen der Datenschutzregelungen unter europäischen Befragten

Bitte geben Sie Ihren Kenntnisstand hinsichtlich dieser Regelungen an[1]



Anm.: (1). Basierend auf 200 französischen und deutschen Befragten, darunter 76 CIOs und 124 CMOs / CEOs / CLOs/ COOs. Summe beträgt möglicherweise aufgrund von Rundung nicht 100 % (2). Antworten von „gute Kenntnisse" bis „sehr gute Kenntnisse"

Quellen: GSG-Umfrage; GSG-Analyse

Der heutige Zustand der Unsicherheit birgt eine Vielzahl von Risiken für europäische Unternehmen

Hauptrisiken für europäische Unternehmen, die US/Nicht-EU-Cloud-Provider nutzen

Rechtliche Risiken

1 Von einer europäischen Behörde

- Für europäische Unternehmen besteht bei der Nutzung von US-Cloud-Diensten, die dem Cloud Act unterliegen, das Risiko der **Datenverletzung nach DSGVO**
- **Gerichtliche Schritte** können entweder von öffentlichen Behörden, Wettbewerbern für geschäftliche Zwecke oder einer Gruppe von Kunden durch Sammelklagen eingeleitet werden

2 Von einer US-Behörde

- US-Unternehmen unterliegen einer Gesetzgebung, die **es amerikanischen Behörden erlaubt, auf personenbezogene Daten zuzugreifen** die auf US-Boden transferiert/ gehostet werden
- Europäische Unternehmen, die diese Daten besitzen, können somit aufgrund dieser Daten der **extraterritorialen Verfolgung durch US-Behörden ausgesetzt sein**

Risiken für gewerbliches und geistiges Eigentum

3

- Aufgrund ihrer Allgemeinen Geschäftsbedingungen können internationale Cloud-Provider oftmals komplett oder teilweise auf wertvolle **vertrauliche gewerbliche Daten, die einen Schlüsselvorteil** bei Innovation und einen Wettbewerbsvorteil für Unternehmen (z. B. geistiges Eigentum, Preisgestaltung, Geschäftsbedingungen...) **darstellen können,** zugreifen und diese ausnutzen
- Diese Daten sind umso **wertvoller** angesichts des diversifizierten Umfangs der Tätigkeiten der größten internationalen Cloud-Provider (was sie manchmal zu potenziellen Konkurrenten für eine Vielzahl europäischer Unternehmen/Branchen[1]) macht
- Einige dieser großen Provider können auch in öffentlichen Clouds gehostete Daten (als Aggregat) einsetzen, um **einige ihrer eigenen Fähigkeiten zu verbessern** (z. B. Algorithmen)
  - Zum Beispiel beinhaltete der US 2019 National Defense Authorization Act (NDAA) ein **Verbot** der Verwendung bestimmter **chinesischer Überwachungskameras**
- Einige dieser Praktiken werden ermöglicht durch großzügige allgemeine Geschäftsbedingungen für den Verkauf, die keinen ausreichenden Schutz von Kundenrechten und geistigem Eigentum bieten und die Ausnutzung von Daten zulassen
- Im **Gauvain-Bericht**[2] werden im Übrigen die Risiken der Ausnutzung von Daten für wirtschaftlich begründete extraterritoriale Klagen hervorgehoben

Quellen: Interviews mit Experten; KPMG Avocats und Untersuchung und Analyse von GSG

Anm.: (1). So verschiedene wie Einzelhändler (z. B. Amazon), Luft- und Raumfahrt (z. B. Blue Origin), Automobil (z. B. Waymo)…)… (2) Gauvain-Bericht über den Schutz von Unternehmen vor Gesetzen und Maßnahmen mit extraterritorialer Reichweite, 26. Juni 2019

In der EU besteht für Unternehmen, die die Grundsätze der DSGVO nicht einhalten, die Gefahr empfindlicher Geldbußen, wie z. B. der von der CNIL (frz. Datenschutzbehörde) gegen Google verhängten Strafe von 50 Millionen €

Geldbußen bei Nichterfüllung der DSGVO

Von einer europäischen Behörde (1)

Art. 83 DSGVO

Allgemeine Bedingungen für die Verhängung von Geldbußen

Gemäß DSGVO-Regeln können Geldbußen von bis zu 20 Millionen € oder von bis zu 4 % des Jahresumsatzes verhängt werden, aber mangelnde Einheitlichkeit der Sanktionen in der EU

2018-2020

über 280 Millionen €

an Bußgeldern

über 160.000

Mitteilungen über Verstöße

Beispiel für gegen Google verhängte Geldbußen (2019)

Google

- Im Januar 2019 verhängte die französische Datenschutzbehörde CNIL[1] eine **Geldbuße in Höhe von 50 Millionen € gegen Google LLC** gemäß DSGVO **wegen fehlender Transparenz oder angemessener Informationen und dem Fehlen einer gültigen Zustimmung zur Anzeigenpersonalisierung**

„ Durch die festgestellten Verstöße wurden Nutzern grundlegende Garantien im Hinblick auf die Verarbeitung ihrer Daten vorenthalten, was zur Preisgabe weiter Bereiche ihrer Privatsphäre führen kann."
(CNIL-Pressemitteilung, 2019)

- Ferner hat die französische CNIL das Ende der Frist für die Einhaltung der Regeln bis 31. März 2021 angekündigt – Ab diesem Datum haben französische Unternehmen keine Ausreden mehr für die Nichteinhaltung der DSGVO.

Anm.: (1). CNIL: Commission Nationale de l'Informatique et des Libertés (französische Datenschutzbehörde)
Quellen: DLA Piper GDPR Data Breach Survey 2020; KPMG Avocats und Untersuchung und Analyse von GSG

In den USA erlaubt der Cloud Act US-Bundesbehörden den Zugriff auf im Ausland gespeicherte Daten, mit potenziellen Sanktionen bei Verstößen

Grundsätze, die Datenzugriff von US-Behörden erlauben

Von einer US-Behörde

2

Grundsatz

Daten, die außerhalb der USA bei einem Diensteanbieter gespeichert sind, der US-Recht unterliegt, können durch gerichtliche Zwangsmaßnahmen zur US-Regierung transferiert werden

Bestehende Vereinbarungen

Im Rahmen des Cloud Acts und zur Erleichterung und ordentlichen Regelung des Informationsaustauschs können Länder ein Abkommen **(Executive Agreement)** mit den Vereinigten Staaten abschließen.
In diesem Fall könnten beide Staaten die benötigten Beweisdaten direkt bei den Lieferanten anfordern, **ohne dass dazu die Beteiligung der anderen Regierung erforderlich ist.**

Potenzielle damit verbundene Bußen und Situation für europäische Unternehmen

Der Cloud Act sieht bei Nichtbefolgung von Aufforderungen an Diensteanbieter keine spezifischen Sanktionen vor, potenzielle Konsequenzen würden beinhalten:

US-Diensteanbieter mit oder ohne europäische Tochter	• Befugte Behörden können sich gegen den US-Diensteanbieter wenden. Wenn eine Tochtergesellschaft in Europa vorhanden ist, verfügt der US-Provider als Muttergesellschaft über die Kontrolle und somit über ihre Daten.
EU-Diensteanbieter mit Tochter in den USA	• Befugte Behörden können sich nur gegen die in den USA ansässige Tochtergesellschaft des europäischen Diensteanbieters wenden. Diese kann dann die US-Gerichte anrufen. Außerdem kann sie nicht zur Bereitstellung der Informationen gezwungen werden, wenn sie weder die rechtliche Kontrolle noch den technischen Zugriff auf die Daten hat.
EU-Diensteanbieter ohne Tochtergesellschaft in den USA	• Keine Einflussnahme gegen diese Diensteanbieter möglich, da • die Kommission klargestellt hat[1], dass die DSGVO Executive Agreements erfordert (sogar, wenn die geforderten Transfers sich auf Verfügungen ausländischer Gerichte stützen) - Ferner unterliegen Transfers personen-bezogener Daten mehreren zusätzlichen Bedingungen (z. B. angemessene Schutzmaßnahmen) • Wenn ein europäischer Diensteanbieter einem Urteil durch ein amerikanisches Gericht Folge leistet, obwohl keine Executive Agreements zwischen den USA und dem betreffenden Land der EU bestehen, dann verstößt der Diensteanbieter gegen europäisches Recht[2]

Anm.: (1). in ihrem Schreiben an den Obersten Gerichtshof der Vereinigten Staaten (Supreme Court) im Fall Microsoft (2). Dies wurde in Entscheidungen der Kommission jüngeren Datums bestätigt (d. h. Schrems 2)
Quellen: KPMG Avocats und Untersuchung und Analyse von GSG

Ferner sind Verträge von US-Cloud-Providern normalerweise Standardverträge, die es ihren Kunden nahezu unmöglich machen, ihre Vertragsbedingungen auszuhandeln

Beispiele für überzogene Bestimmungen, die sich in Verträgen verschiedener US-Cloud-Provider finden

3 Überzogene Bestimmungen zum geistigen Eigentum von Kunden des Cloud-Providers

Verschiedene US-Cloud-Provider implementieren **Lizenzklausen**, die vom Kunden fordern, seinem Cloud Provider für die Dauer der geistigen Eigentumsrechte des Kunden **gebührenfreie, weltweite einfache Rechte und Lizenzen** für sämtliche Technologien, Marken, Inhalte, Produktinformationen, Daten, Materialien und anderen Produkte oder Informationen des Kunden zu gewähren, die **dem Cloud Provider vom Kunden zur Verfügung gestellt werden**

Diese Art von Klausel kann sich als sehr problematisch erweisen, da eine derart breite Lizenz:

- dem Kunden durch den US-Cloud-Provider **aufgezwungen wird und nicht verhandelbar ist**,
- nicht immer auf die Erbringung des Dienstes beschränkt ist,
- es dem Cloud Provider erlaubt, **geistige Eigentumsrechte seiner Kunden zu ändern, zu kopieren und zu verteilen**, wenn solche geistigen Eigentumsrechte durch den Kunden bei der Nutzung der Cloud-Services zur Verfügung gestellt werden

Überzogene Bestimmungen für Zahlungen und zur Kündigung des Vertrags mit dem Cloud-Provider

Für die Möglichkeit für Unternehmen, ihre Hosting-Provider zu wechseln, sehen verschiedene Cloud- und Hosting-Provider **Zahlungsklauseln vor, die auch nach Vertragsende fortbestehen**. Mit anderen Worten, solche Verträge erlauben es dem Kunden nicht, den Vertrag vor seinem Ende zu kündigen, und sämtliche vertraglichen Zahlungsverpflichtungen bleiben auch nach Kündigung oder Ablauf des Vertrags bestehen.

Dabei handelt es sich um eine missbräuchliche Klausel, da:

- sie dem Kunden durch den US-Cloud-Provider **aufgezwungen wird und nicht verhandelbar ist,**
- für den Fall, dass der Kunde den Vertrag kündigen möchte, **er dem Provider immer noch sämtliche vertraglich vereinbarten Beträge schuldet**, und zwar auch für die Zeiträume, in denen keine Leistungen mehr für ihn erbracht werden, wobei angemerkt sei, dass die jährlichen Kosten sich bei einigen Verträgen auf mehrere Tausend/Millionen Euro belaufen können

Quellen: KPMG Avocats und Untersuchung und Analyse von GSG

Unsere Befragungen zeigen, dass diese Situation Befürchtungen weckt, dass sie in den nächsten Jahren zu einer Vielzahl von Klagen führen könnte und für die Unternehmen finanzielle und geschäftliche Risiken birgt (1/2)

FALLBEISPIEL 1:

Aufhebung einer Kündigung aus Gründen in Verbindung mit in einer US-Cloud gehosteten Daten

- Ein Vertriebsmanager beschafft **einem Konkurrenten sensible Daten**
- In einem Rechtsstreit in Verbindung mit seiner Entlassung verteidigt sich das Unternehmen, indem es **Daten vorlegt, die das Fehlverhalten des Vertriebsmanagers beweisen** (Protokolle, unerlaubte Zugriffe, E-Mails, Abwesenheit, Arbeitszeit usw.)
  - Diese Daten werden entweder in Data Centern von US-Cloud-Providern gehostet oder durch cloud-basierte Systeme oder Tools erzeugt, die von US-Providern angeboten werden.

- **Diese Beweise könnten,** obgleich technisch stichhaltig**, rechtlich als illegal gewonnen angefochten werden**

- Folglich könnte das Gericht entscheiden, dass die Kündigung unbegründet ist, und das Unternehmen verurteilen

FALLBEISPIEL 2:

Ein europäisches Unternehmen ist nicht in der Lage, nach einem Diebstahl von Kundendaten, die durch einen US-Provider gehostet werden, gerichtliche Schritte einzuleiten

- Ein Unternehmen ist Opfer eines **Diebstahls von Kundendaten**, die in den USA gespeichert und verarbeitet wurden
- Im Rahmen der Untersuchungen gelingt es dem Unternehmen, **die Diebe zu ermitteln**, und es erwägt **eine Klage vor Gericht**
- Das Unternehmen muss jedoch feststellen, dass **die relevanten Beweise** mit einem Zugriffsüberwachungssystem gewonnen wurden, das ohne entsprechende rechtliche Grundlage **in den USA gespeichert und verarbeitet wird**

- Das Unternehmen steht einem hohen Risiko **anfechtbarer Beweise gegenüber, die es daran hindern, einen fairen Schadensersatz zu erhalten**. Ferner könnte der Transfer möglicherweise für unzulässig erklärt werden und das Unternehmen daher gezwungen sein, die Datenströme zu ändern, und es riskiert ein Bußgeld wegen Nichterfüllung der DSGVO

Quellen: Interviews mit Experten; KPMG Avocats und Untersuchung und Analyse von GSG

Unsere Befragungen zeigen, dass diese Situation Befürchtungen weckt, dass sie in den nächsten Jahren zu einer Vielzahl von Klagen führen könnte und für die Unternehmen finanzielle und geschäftliche Risiken birgt (2/2)

FALLBEISPIEL 3:
Sogar Transfers personenbezogener Daten zwischen einem Franchisegeber und seinem Franchisenehmer müssen unter Einhaltung der DSGVO erfolgen

- Eine Gruppe von Franchisenehmern im Einzelhandel hat dem Franchisegeber die **Speicherung personenbezogener Kundendaten** anvertraut
- Dem Franchisegeber wird Zugriff auf diese Daten gewährt, mit dem Ziel der Durchführung von **Marketing-Kampagnen** (z. B. über E-Mail)
- Der Transfer personenbezogener Daten war nicht genau genug definiert oder kontrolliert, daher war es für den Franchisegeber oder den Franchisenehmer schwierig, **festzustellen, ob ein Kunde seine Einwilligung** für den Empfang von E-Mails im Rahmen von Marketing-Kampagnen **gegeben oder zurückgenommen hatte**

- **Einige Kunden klagen vor der CNIL und die CNIL verurteilt den Franchisegeber und verbietet den Datentransfer**
- Daher sind die Franchisenehmer nicht mehr in der Lage, ihre Marketing-Kampagnen durchzuführen, und **könnten** sich aufgrund ihrer finanziellen Einbußen **gegen den Franchisegeber wenden**

FALLBEISPIEL 4:
Europäische Bürger verfügen über keine Garantie mehr was die Sicherheit ihrer Gesundheitsdaten betrifft

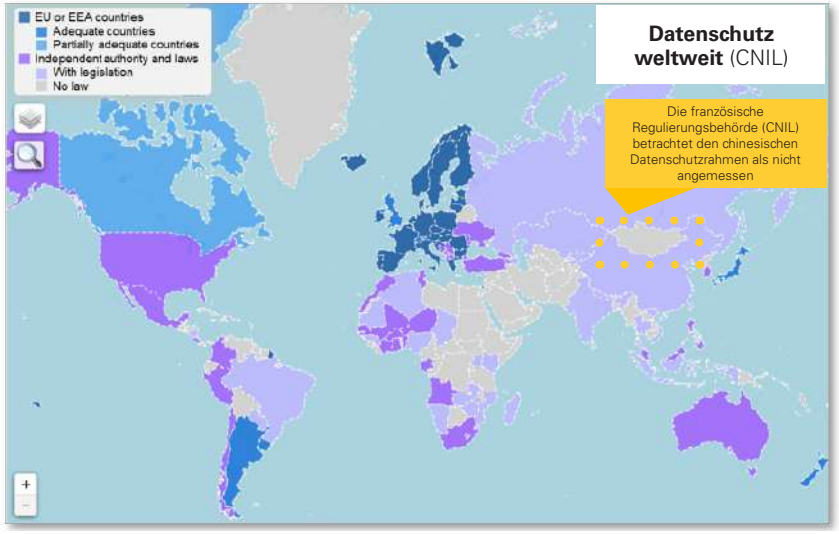
- Eine Organisation mit einer Konzession für einen öffentlichen Dienst, der die **Analyse von Gesundheitsdaten** beinhaltet**, hat für die Speicherung dieser Daten einen Vertrag mit einemUS-Dienstleister abgeschlossen**

- Die delegierende Behörde könnte aufgrund der Tatsache, dass der Transfer von Gesundheitsdaten in die USA nicht DSGVO-konform ist, den **Wechsel des Daten-Hosts** fordern oder sogar den Vertrag ohne Entschädigung **kündigen**
- Von diesem Datentransfer betroffene **Bürger könnten** gegen den Beauftragten **gerichtliche Schritte einleiten**

Quellen: Interviews mit Experten; KPMG Avocats und Untersuchung und Analyse von GSG

Neben den USA erlassen auch andere Länder, wie z. B. China, exterritoriale Regelungen, mit ähnlichen Souveränitätsproblemen für EU-Bürger

Datentransfers zwischen der Europäischen Union und China müssen mit geeigneten Sicherheitsmaßnahmen gehandhabt werden...



- Die Situation in China wird von der Europäischen Union **nicht als angemessen betrachtet**

- Folglich sind **Transfers personenbezogener Daten** zwischen China und der Europäischen Union möglich, müssen aber durch die Implementierung geeigneter **Transferinstrumente** (z. B. Standardvertragsklauseln oder verbindliche Unternehmensregeln) geregelt werden.

...bieten aber dennoch keinen vollständigen Schutz vor potenziellen extraterritorialen Handlungen der chinesischen Regierung aus Gründen der nationalen Sicherheit

Chinas Cybersicherheitsgesetz (2017)

- Liefert Richtlinien zur Wahrung von Netzwerksicherheit, zum Schutz der Rechte und Interessen von Individuen und Organisationen und zur Förderung der technologischen Entwicklung und beinhaltet:
  - **Datenspeicherung in China**
  - Organisationen und Netzwerkbetreiber, **die Sicherheits-Checks der Regierung unterzogen werden**

Datensicherheitsgesetz der Volksrepublik China[1] (2021)

- **Umfang**: gilt für sämtliche „Datenaktivitäten", darunter die Sammlung, Verarbeitung, Kontrolle und Speicherung von Daten, die die nationale Sicherheit, Geschäftsgeheimnisse und personenbezogene Daten betreffen

- **Extraterritoriale Anwendung**: Artikel 2 legt fest, dass sich die Gerichtsbarkeit auf „Organisationen und Individuen außerhalb" Chinas erstreckt, die an Datentätigkeiten beteiligt sind, die die nationale Sicherheit Chinas oder die öffentlichen Interessen des chinesischen Volkes gefährden

- Es sieht so aus, als reichten die eingerichteten **Transferinstrumente** für den Schutz der personenbezogenen Daten der EU-Bürger **nicht aus**

- Wenn es chinesischen Cloud-Providern gelingt, Marktanteile in **Europa zu gewinnen, werden europäische Unternehmen sich mit der gleichen Aufmerksamkeit mit den chinesischen Regelungen auseinandersetzen müssen** wie dies gegenwärtig für die USA der Fall ist

Siehe Details im Anhang

Quellen: CNIL-Website; KPMG Avocats und Untersuchung und Analyse von GSG

Anm.: (1). Basierend auf dem im September 2020 veröffentlichten Entwurf, erwartete Implementierung 2021

Letztendlich besteht die europäische Datensouveränität aus einer Kombination von ca. 8 Kriterien, die zur vollständigen Konformität und Vermeidung geschäftlicher Risiken als Ganzes zu betrachten sind

Was ist Datensouveränität?

Was ist eine souveräne europäische Cloud?

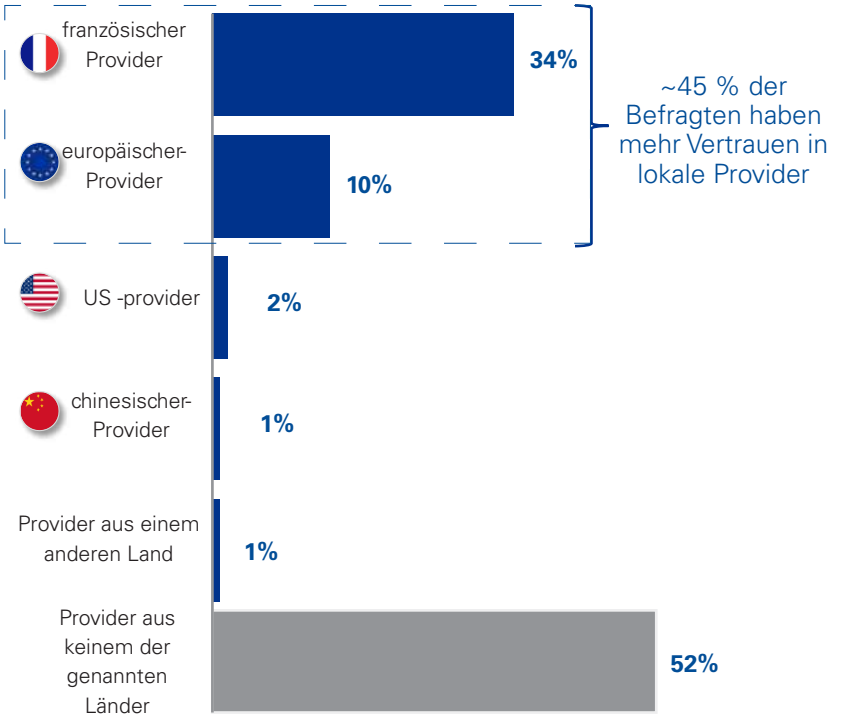
Speicherung der Daten in der EU	• Die Daten befinden sich in **Data Centern in der Europäischen Union**
Kein Zugriff auf Daten aus Ländern mit nicht angemessenen Regelungen	• Es ist technisch unmöglich, **aus Ländern mit nicht angemessenen Regelungen** (die die DSGVO nicht erfüllen) auf die **Daten des Diensteanbieters** zuzugreifen
ausschließlich EU-Gerichtsbarkeit	• Der Diensteanbieter **unterliegt ausschließlich der EU-Gerichtsbarkeit** und ist befreit von der Erfüllung extraterritorialer Gesetze
Einhaltung der DSGVO im Hinblick auf Aufforderungen ausländischer Behörden	• Richtlinien für die **Beantwortung von behördlichen Aufforderungen aus Ländern außerhalb der EU** sind angemessen und erfüllen die DSGVO
Keine Verwendung von Kundendaten	• Der Diensteanbieter verpflichtet sich (in seinen Nutzungsbedingungen), **auf die Nutzung von Kundendaten zu verzichten**, und zwar auch zur **Optimierung seiner Dienste**
Souveräne Subunternehmer	• Auch die **Subunternehmer** des Diensteanbieters müssen **souverän sein** und spezifische Souveränitätskriterien erfüllen
Europäischer Support	• **Standort des** Kunden-Supports **muss in Europa sein**
Verträge nach örtlichen Gesetzen	• Unterzeichnete **Verträge** müssen **örtlichen Gesetzen unterliegen**

Quellen: KPMG Avocats und Untersuchung und Analyse von GSG

In den kommenden Jahren wird Datensouveränität immer mehr zu einer Frage des Geschäfts, da europäische Verbraucher in dieser Hinsicht steigende Erwartungen haben

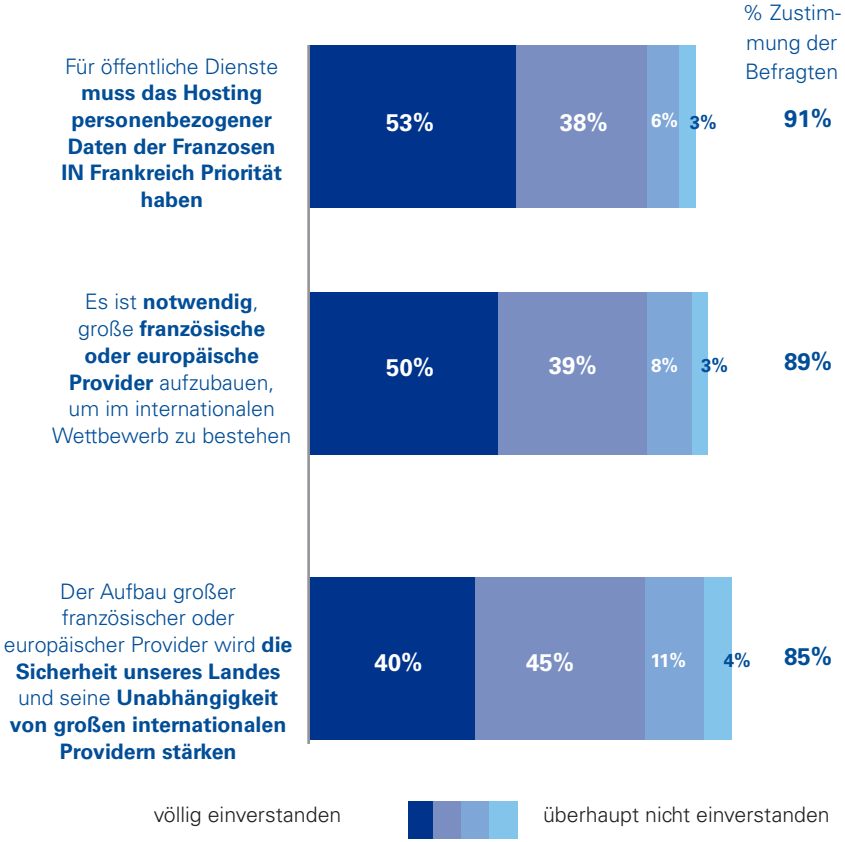
Bedenken der Befragten über ihre Datensouveränität

Welchem Provider würden **Sie mehr vertrauen,** wenn es um **den Schutz Ihrer personenbezogenen Daten** geht?



Erwartungen der Befragten an ihre Datensouveränität

Inwieweit stimmen Sie der folgenden Aussage zum Datenschutz **zu/nicht zu?**



Quelle: IFOP-Umfrage für OVHcloud Januar 2020 (selbst auszufüllende Fragebögen, repräsentative Umfrage unter 1028 über 18-Jährigen in Frankreich)

4

5 Szenarien für die Zukunft des europäischen Cloud-Markts

Derzeitiges Paradigma des europäischen Cloud-Markts erscheint aufgrund von vier Makro-Trends langfristig nicht tragfähig

Diskrepanz zwischen DS-GVO-Compliance und extraterritorialen Regelungen

- **Viele rechtliche Risiken** für europäische Unternehmen, die die Dienste von US-Cloud-Providern nutzen, aufgrund der Unvereinbarkeit zwischen dem europäischen und dem US-amerikanischen Regelungsrahmen

Wettbewerbswidrige Praktiken & kommerzielle Hindernisse, die den Zugang europäischer Provider zum Markt behindern

- Nachweislich **wettbewerbs-widrige Praktiken** durch einige Akteure (z. B. Nutzung installierter Software-Basis, Verbundgeschäfte von IaaS & SaaS, mangelnde Interoperabilität, etc.)
- …Verhinderung eines Umfeldes mit gleichen Wettbewerbs-bedingungen für alle in Europa

Wachsende Forderungen nach Datenschutz und -souveränität am Markt

- **Stärkung des Bewusstseins über den Datenschutz für B2C und B2B** (persönlich, IP, industriell, Kunden etc.)...
- …Verbunden mit zunehmendem **Bewusstsein über die Notwendigkeit des Schutzes personenbezogener Daten**, die sich derzeit in den Händen von Cloud-Anbietern befinden

Bedeutende und sichtbare Herausforderungen, die in einem starken Wachstum der Cloud-Wirtschaft resultieren

- **Stark zunehmende Nachfrage nach Cloud und SaaS insbesondere…**
- **… mit großen wirtschaftlichen und geschäftlichen Auswirkungen** (z. B. Schaffung von Arbeitsplätzen und Investitionen) und **technologischer Auslöser** (z. B. Innovationen im Zusammenhang mit KI)

Quellen: IFOP-Umfrage für OVHcloud, Januar 2020 (eigenständig auszufüllende Fragebögen, durchgeführt anhand einer repräsentativen Stichprobe von 1.028 Befragten im Alter von 18 Jahren und darüber in Frankreich); Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

In der europäischen Cloud-Computing-Landschaft könnten sich fünf potenzielle Szenarien herausbilden…

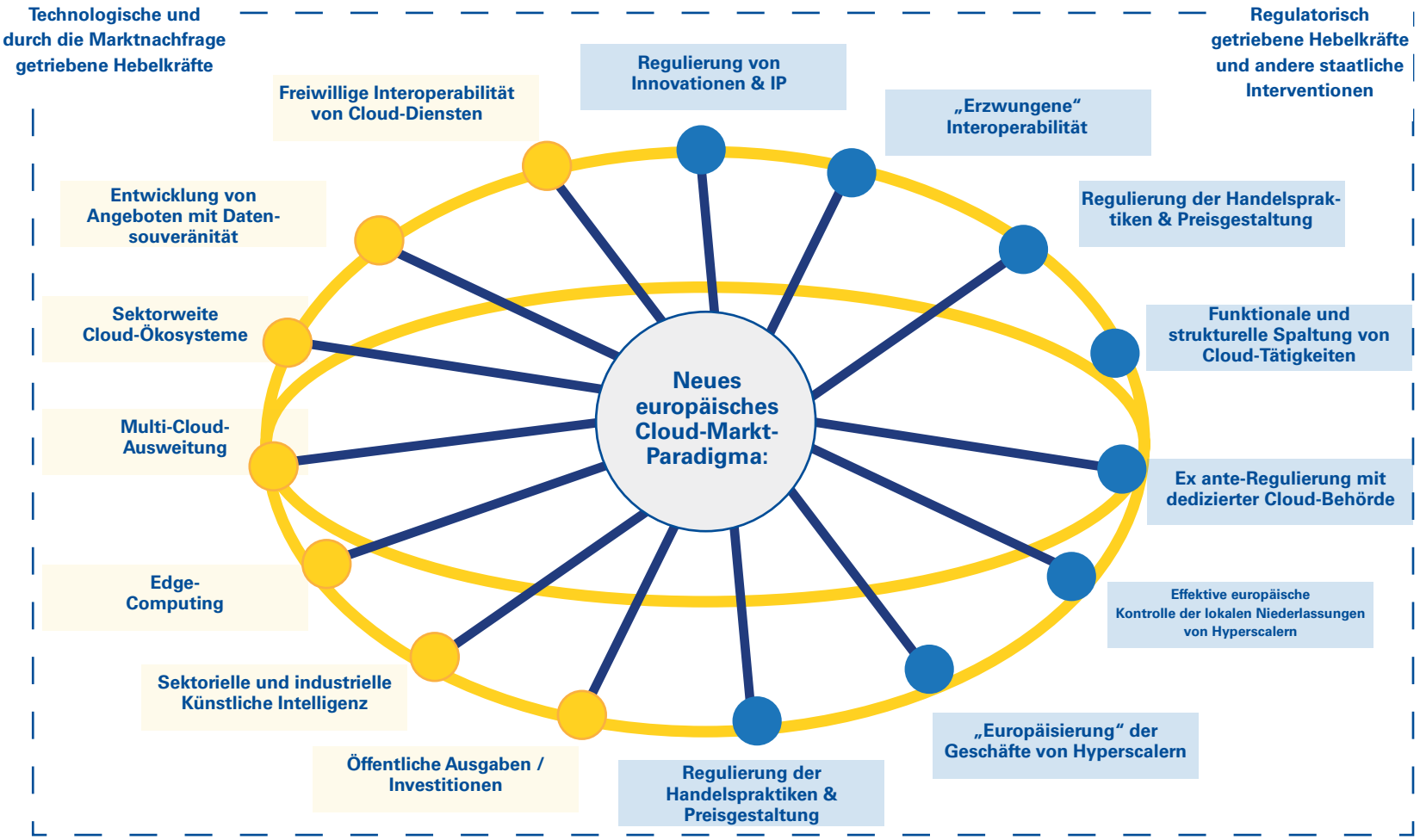
marktgetrieben ⟵ ⟶ **regulatorisch getrieben**

Ein Szenario, bei dem…	Cloud als ein Gemeingut	Ausbau der Leistungsangebote europäischer Provider	Welle starker Regulierung	Europäisierung der operativen Geschäfte von Cloud-Providern	Spaltung von Cloud-Tätigkeiten (funktional oder strukturell)
	• der Markt zur **Selbstregulierung**, tendieren würde, insbesondere durch eine **größere freiwillige Interoperabilität von Cloud-Diensten**, was in einer Steigerung der gesamtwirtschaftlichen Leistung resultieren würde • einige industrielle Akteure sogar über die Selbstregulierung hinaus gehen und **ihre Wettbewerber rund um gemeinsame sektorweite Cloud-Ökosysteme herum vereinen würden** (z. B., Finanzdienstleistungen, Energiesektor etc.), die neben „traditionellen" Cloud-Angeboten bestehen werden, dank einer **Multi-Cloud-Ausweitung**	• die **aufkommenden Bedürfnisse** von EU-Unternehmen nach nationalen Lösungen verlangen und **EU-Cloud-Providern als Sprungbrett** dienen würden, um ihre Leistungsangebote weiter auszubauen, einschließlich: - **Edge Computing**, ein aufstrebender Markt, der CapEx und lokale Partnerschaften erfordert - **Künstlicher Intelligenz für industrielle Daten**, mit Bedürfnissen, die von akkreditierten EU-Anbietern gedeckt werden könnten - **Entwicklung von Angeboten mit Datensouveränität, inkl. Cloud**-Zertifizierungen und Data Center-Standort - **Öffentlicher Ausgaben,** einer treibenden Kraft des Wachstums europäischer Provider	• die **Entstehung eines gestärkten Cloud-Regulierers** (auf europäischer und/oder nationaler Ebene) in strengen Auflagen für Cloud-Provider, insbesondere für Hyperscaler, resultieren würde: - **Größere Preistransparenz** und keine Kopplungsbedingungen - **Erzwungene Interoperabilität**, z. B. rund um eine Liste zwingender offener Kern-API - **Offener Zugang zu Innovationen,** wobei innovative Akteure gezwungen sein würden, Zugang zu bestimmten Innovationen / Dienstleistungen zu gewähren	• nicht-europäische Cloud-Provider **neuen Regelungen unterliegen würden, die sie zu einer „Europäisierung" ihrer lokalen Geschäfte zwingen würden** - analog ähnlicher Regelungen, die in China, Russland oder in den USA zu beobachten sind • Daher müssten lokale Niederlassungen globaler Cloud-Provider **effektiv im Eigentum von europäischen Partnern stehen oder von solchen betrieben werden**, zusätzlich zu nachweislichen Selbstverpflichtungen auf lokaler Ebene in Bezug auf Forschungs- und Entwicklungs-ausgaben, einer lokalen Präsenz der obersten Geschäftsführung und einer lokalen Beschaffungs- / Lieferkette	• manche nicht-europäische Cloud-Provider, wie Hyperscaler, durch Regulierer gezwungen wären, ihr **Cloud-Geschäft** von ihren restlichen Geschäftstätigkeiten (z. B. e-Commerce für Amazon) abzuspalten • **Damit würden Hyperscaler einen gewissen missbräuchlichen Wettbewerbsvorteil verlieren** (z. B. Kombination von Azure+O365) und ihre Fähigkeit verlieren, unrentable Cloud-Geschäftseinheiten finanziell zu unterstützen

Die Szenarien schließen sich nicht völlig gegenseitig aus und können sich zum Teil verbinden, wodurch die Effekte noch verstärkt würden (z. B. beschleunigtes Aufstreben europäischer Provider durch erzwungene Interoperabilität, Europäisierung von Kontrollketten, ungebündelte Cloud-Geschäfte usw.)

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

Diese Szenarien sind durch ein Zusammentreffen einer Vielzahl von marktgetriebenen und regulatorisch getriebenen Makro-Hebelkräften gekennzeichnet



Je nach der relativen Stärke dieser Makro-Hebelkräfte können mehrere Szenarien betrachtet werden

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

Szenario 1: Cloud als Gemeingut

Hebelkräfte

Freiwillige Interoperabilität von Cloud-Diensten

- **Freiwillige Interoperabilität** über Cloud-Provider hinweg (in IaaS, PaaS, SaaS) durch **offene API**, was jedem Akteur die Interaktion mit den Diensten von Cloud-Providern ermöglicht,…
- …Daher **Verlangsamung des aktuellen Trends zu proprietären / irreversiblen Cloud-Diensten**, ohne starke Eingriffe durch Regulierer, um die Interoperabilität zu „erzwingen"

Sektorweite Cloud-Ökosysteme

- **Industrielle Akteure**, die mit ähnlichen spezifischen Cloud-Computing-Bedürfnissen konfrontiert sind, ver-einen sich rund um **gemeinsame Cloud-Ökosysteme** (typischerweise sektororientiert, z. B. Finanzdienst-leistungen, Energiesektor) entsprechend ihren Erwartungen (z. B. Datensouveränität, DSGVO-Compliance)…
- …sodass diese industriellen Akteure zu **de facto-Cloud-Providern** werden können, wodurch sie internationale Cloud-Provider (einschließlich US- und chinesische) (teilweise) umgehen könnten

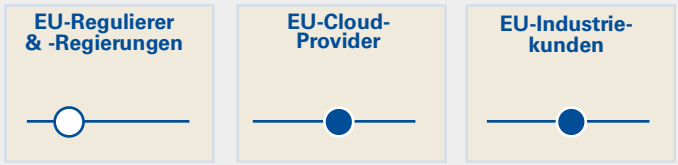
Multi-Cloud- Ausweitung

- Cloud-Architekturtrend, was die Verwendung von Cloud-Diensten von mehreren Cloud-Providern für den gleichen Zweck ermöglicht, d. h. **europäische Cloud-End-nutzer können einfacher mehrere Cloud-Provider nutzen**…
- …Erleichterung der DSGVO-Compliance (mehrere Cloud-Provider je nach verschiedenen Datentypen) und Beschränkung von Anbieter-Lock-in

Implikationen

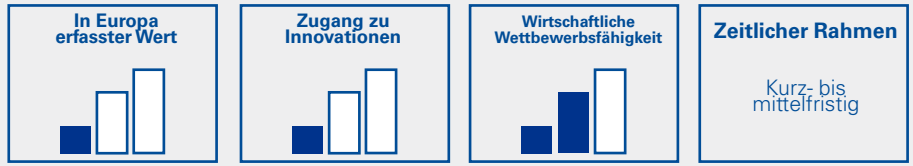
- Szenario ermöglicht **Wachstum eines europäischen Ökosystems**, im Einklang mit dem europäischen GaiaX-Projekt
  - z. B. da offene API tendenziell neue Geschäftsgelegenheiten eröffnen
- **Cloud-Endnutzer** dürften von einer Reduzierung von **Verbundgeschäften profitieren** (größere Interoperabilität & Multi-Cloud, mit Reduzierung der Kosten eines Wechsels zu anderen Anbietern)
- Letzteres kann an sich teilweise für das **relative Wachstum europäischer Cloud-Provider** im Gegensatz zu internationalen Cloud-Providern förderlich sein

Rolle im Übergang zu dem Szenario



Legende: Weniger bedeutende Rolle — Bedeutende Rolle

Szenario-Effizienz
und assoziierte Auswirkungen auf wirtschaftliche Metriken für Europäer



Legende: Begrenzte Auswirkungen — Starke Auswirkungen

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

VERANSCHAULICHEND

Dieses Szenario könnte durch die europäische Gaia-X-Initiative, die die Einrichtung eines durch europäische Gesetze geschützten interoperablen Datenaustauschs vorsieht, verwirklicht werden

#1

Gaia-X ist eine europäische Initiative, deren Ziel der Aufbau eines **sicheren und einheitlichen Cloud-Ökosystems** ist, das die höchsten **Standards der digitalen Souveränität erfüllt, bei gleichzeitiger Förderung von Innovationen**.
Es ist die Wiege eines **offenen, transparenten, interoperablen Ökosystems** (einschließlich in Bezug auf die potenzielle Anwendbarkeit extraterritorialer Gesetzgebung), in dem Daten und Dienstleistungen in einer Umgebung des Vertrauens bereitgestellt, erfasst und unter Nutzern gegenseitig ausgetauscht werden können

Jedes Cloud-Unternehmen (einschließlich nicht-europäischer Akteure) **kann sich der Gaia-X-Initiative anschließen, wobei sie jedoch an die Einhaltung der von der Initiative festgelegten Prinzipien und Leitlinien, einschließlich der folgenden, gebunden sind:**

GAIA-X

- **Europäischer Datenschutz:** Einhaltung der europäischen Gesetzgebung und Fähigkeit der Anwendung verschiedener Ebenen des Schutzes je nach Art der Daten und Anwendungsfall
- **Offene Dateninfrastruktur**, die Transparenz und einheitliche Verträge und Verfahren fördert, um Komplexität und Kosten zu reduzieren
- **Freier Marktzugang**, um Unternehmen verschiedener Branchen den Datenaustausch zu erleichtern und somit die branchenübergreifende Zusammenarbeit zu fördern
- **Modularität und Interoperabilität:** ermöglicht durch die Vernetzung und die Datenintegration von verschiedenen Cloud-Plattformen, wodurch Hindernisse für den Zugang beseitigt werden und sich auch kleinere, spezialisierte Cloud-Akteure am Wettbewerb beteiligen können

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

Szenario 2: Ausbau des Leistungsangebots europäischer Provider

Hebelkräfte

Edge-Computing

- Mit der Bereitstellung von 5G-Netzwerken, **zunehmende Notwendigkeit zur Erfassung von Billionen von Daten auf lokaler Ebene durch Edge-Computing-Technologie** und deren Verarbeitung nahe an der Datenquelle oder dem Datennutzer…
- … **woraus sich ein neuer, bisher nicht ausreichend gedeckter Markt entwickeln kann**, aufgrund hoher Anforderungen an eine lokale Infrastr., robuste Systeme sowie Datenschutz und -souveränität

Sektorielle und industrielle Künstliche Intelligenz

- Zunehmende Notwendigkeit, dass industrielle Akteure **Innovationen durch KI** und eine damit verwandte Datennutzung vorantreiben, was sie nicht einzeln erreichen können; daher **benötigen sie DSGVO-konforme Datenverarbeitungspartner…**
- …woraus sich eine interessante **Marktchance für EU-Cloud-Provider zur Implementierung eines vertrauenswürdigen Ökosystems** mit klaren Regeln für die Entwicklung und Nutzung von KI ergeben könnte

Entwicklung von Angeboten mit Datensouveränität

- **Entwicklung von Angeboten für Datensouveränität**, die den Erfordernissen von Kunden in Bezug auf die **Standorte von Data Centern**, den Schutz vor der Extraterritorialität ausländischer **Gesetze** und **Zertifizierungen**[1] gerecht werden…
- …was **europäischen Cloud-Providern eine Chance bieten kann**, solche konformen Angebote bereitzustellen und **das Niveau der Datensouveränität insgesamt zu erhöhen**

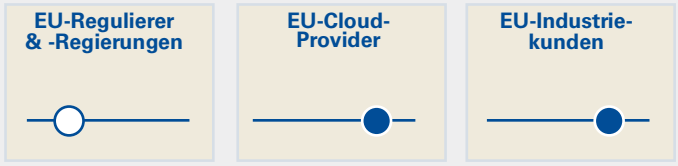
Öffentliche Ausgaben / Investitionen

- **Öffentliche Ausgaben** (durch nationale und / oder lokale Behörden) **haben in der Vergangenheit das Wachstum von US-Hyperscalern** angetrieben, und können auf ähnliche Weise in Europa unterstützt werden …
- …da viele Verwaltungen (insbesondere auf lokaler Ebene) noch eine sinnvolle Cloud-Migration vollziehen müssen; dies würde **europäischen Cloud-Providern bedeutende Entwicklungschancen bieten**

Implikationen

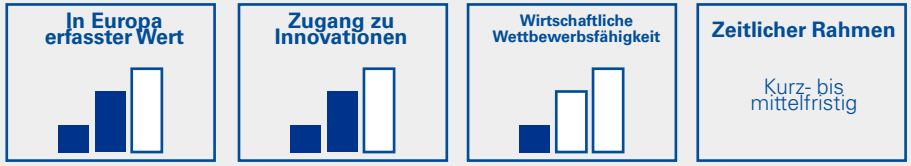
- Dieses Szenario dürfte für den **Ausbau des Angebots lokaler Akteure förderlich sein, da der Markt der industriellen Daten von internationalen Cloud-Providern (im Gegensatz zum Markt der personenbezogenen Daten) nach wie vor nicht ausreichend gedeckt wird**
- Entwicklung von **Partnerschaften zwischen Cloud-Providern & Telco-Akteuren**, um die Implementierung von Edge-Computing-Datacentern zu erleichtern
- Wachsende Bedeutung von **indirekten staatlichen Interventionen** (z. B. durch öffentliche Ausgaben) zur Förderung der europäischen Cloud-Computing-Branche

Rolle im Übergang zu dem Szenario



Legende: Weniger bedeutende Rolle — Bedeutende Rolle

Szenario-Effizienz
und assoziierte Auswirkungen auf wirtschaftliche Metriken für Europäer



Legende: Begrenzte Auswirkungen — Starke Auswirkungen

Anm.: (1). Entwurf der Regelung für eine europäische Cybersicherheitszertifizierung für Cloud-Dienste durch die ENISA, einschl. SecNumCloud in Frankreich oder des deutschen Äquivalents C5

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

VERANSCHAULICHEND

Der Ausbau der Leistungsangebote europäischer Provider könnte sich stärker auf neuen Märkten realisieren, wofür eine gesicherte lokale Cloud evtl. vorzuziehen wäre, mit spezifischen Zielvorgaben von den europäischen Behörden

#2

Überblick der Marktchancen für den Ausbau der Leistungsangebote von EU-Providern

Nicht ausreichend gedeckte Märkte…	… mit spezifischen Bedürfnissen …	… die von EU-Providern besser gedeckt werden könnten
Edge-Computing	• Lokale Datacenter mit **hoher Rechenkapazität** für die **lokale** Verarbeitung generierter Daten • **Sichere** Infrastruktur mit Datensouveränität, geeignet für das **Hosting industrieller Daten**	Für europäische Daten (einschl. kritischer industrieller Daten), könnten EU-Provider **sichere, lokale Rechen** - und **Speicherkapazitäten** innerhalb einer Umgebung mit Datensouveränität sicherstellen
Künstliche Intelligenz für industrielle Daten	• Data Center mit **hohen Rechenkapazitäten**, die in der Lage sind, **robuste KI- und ML-Algorithmen zu betreiben** • **Sicheres** Cloud-Ökosystem mit **Datensouveränität** erforderlich für kritische industrielle Daten	
Angebote mit Datensouveränität	• **Sichere** und **zertifizierte Cloud-Umgebungen mit Datensouveränität**, die europäischen Unternehmen die **Migration ihrer kritischen Daten in die Cloud** ermöglichen	

„Wir treten mit der zunehmenden Menge an **industriellen Daten** in eine neue Phase ein. Europa muss sich als der am stärksten industrialisierte Kontinent als **Marktführer auf diesem Gebiet** positionieren. Die **Zukunft der KI ist naturgemäß mit der intensiven Datennutzung verbunden, d. h.** es gibt keine KI ohne Daten.", T. Breton (Okt. 2020).

Vorgestelltes Konzept der Europäischen Kommission

Diese Marktchancen spiegeln sich in dem Ziel der **Europäischen Kommission wider, einen Daten-Binnenmarkt aufzubauen**, wobei **die europäischen Cloud-Provider** der Eckstein des Vorhabens wären.

- Die Umsetzung eines solchen Markts könnte durch folgende Maßnahmen erleichtert werden:

- **Technologische und finanzielle Unterstützung** für den Aufbau einer sicheren und souveränen europäischen Cloud-Infrastruktur, die für das **Hosting und die Verarbeitung industrieller Daten** geeignet wäre

- Schaffung einer **100 % europäischen** und souveränen **Wertschöpfungskette der Datenbearbeitung** durch die Allianz der EU-Datenverarbeiter

- Entwicklung von Selbstregulierungsnormen und -standards durch Branchenbeteiligte in Europa, nämlich des **EU-Cloud-Regelhandbuchs**, welches den **Plan für die Cybersicherheitszertifizierung, den gerechten Wettbewerb** und **einen Verhaltenskodex über die Energieeffizienz von Data Centern** abdeckt

- Zusätzliche Vorhaben, wie das „**Wichtige Vorhaben von gemeinsamem europäischem Interesse" („Important Project of Common European Interest", IPCEI)**[1] über die Cloud-Infrastruktur und -Dienstleistungen der nächsten Generation dürften zu einer effektiven Förderung der europäischen Datenführerschaft und-souveränität beitragen[2]

Anm.: (1). Innerhalb des IPCEI-Regelungsrahmens können EU-Mitgliedstaaten wichtige Vorhaben von gemeinsamem europäischem Interesse durchführen, die mittels staatlicher Förderung einen wichtigen Beitrag zu Wachstum, Beschäftigung und Wettbewerbsfähigkeit der europäischen Industrie und Wirtschaft leisten (2). Vorhaben insbesondere erwähnt in der Gemeinsamen Erklärung der Mitgliedstaaten über den Aufbau der Cloud der nächsten Generation im Oktober, 2020

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG; Sonderkommission über „Künstliche Intelligenz im digitalen Zeitalter"

Szenario 3: Welle starker Regulierung

Hebelkräfte

Ex ante-Regulierung mit dedizierter Cloud-Behörde

- Einrichtung einer **unabhängigen Cloud-Regulierungsbehörde** (auf europäischer und / oder auf nationaler Ebene), die für die Regulierung des Cloud-Markts und der Cloud-Marktteilnehmer zuständig wäre und die einen adäquaten Verbraucherschutz gewährleisten und die wirtschaftliche Wettbewerbs-fähigkeit fördern würde

Regulierung der Handelspraktiken & Preisgestaltung

- **Strengere Regulierung** in Bezug auf die Handelspraktiken der derzeitigen Hyperscaler, mit dem **Ziel einer Reduzierung der Praxis von Verbundgeschäften** (z. B. zwingende Kopplung von SaaS+IaaS)
- **Preisregulierung** zur **Verhinderung unfairer Kundenaquisitionspraktiken** (z. B. kostenlose Migration) und zur Förderung eines **gesünderen Wettbewerbs**

„Erzwungene" Interoperabilität

- **Interoperabilität** zwischen Cloud-Providern, **vom Regulierer** durch spezifische Gesetze auferlegt (im Gegensatz zur freiwilligen Verpflichtung der Marktteilnehmer), insbesondere bei PaaS / SaaS, unter anderem durch **offene und dokumentierte API**

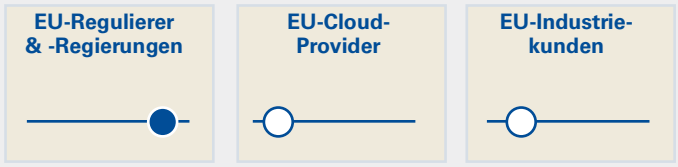
Regulierung von Innovationen & IP

- Erhöhte **Regulierung cloud-basierter oder aus der Cloud abgeleiteter Innovationen** (z. B. KI) zum Schutz verwandter europäischer Kapazitäten
- **Größerer Umfang des IP-Schutzes** für EU-Unternehmen, die ihre Daten auf Cloud-Diensten von Hyperscalern speichern (z. B. Verbot der Wiederverwendung bestimmter proprietärer Daten)

Implikationen

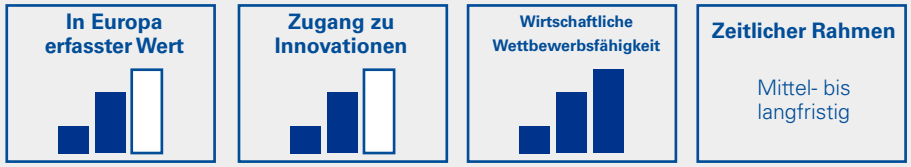
- Dieses Szenario dürfte einen **gesünderen Wettbewerb** zwischen Cloud-Providern fördern und lokalen Cloud-Akteuren somit letztlich zu größerem Wachstum verhelfen, dank:
- **Geringerer Hindernisse für den Wechsel von Anbietern** für Cloud-Nutzer, und mit Wahrscheinlichkeit einer höheren Abwanderungsquote für US-Hyperscaler aufgrund der Reduzierung der Verbundgeschäftspraktiken
- **Breiter verteilte Innovationskapazitäten**, z. B. durch Interoperabilität und Regulierung cloud-basierter Innovationen
- … sowie der **Beschleunigung der Cloud-Migration für europäische Unternehmen** dank größeren IP-Schutzes und größerer Interoperabilität
- Es wäre an das **Digitalmärkte-Gesetz („Digital Markets Act") angeglichen** (das darauf abzielt, Eigenpräferenz-Tätigkeiten ein Ende zu setzen), vorausgesetzt es behandelt sowohl B2C als auch B2B, sogenannte „Torhüter" (d.h. große Online-Plattformen)

Rolle im Übergang zu dem Szenario



Legende: Weniger bedeutende Rolle — Bedeutende Rolle

Szenario-Effizienz
und assoziierte Auswirkungen auf wirtschaftliche Metriken für Europäer



Legende: Begrenzte Auswirkungen — Starke Auswirkungen

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

VERANSCHAULICHEND

Deutschland ist eines der ersten EU-Länder, das neue DSGVO-konforme Gesetze verabschiedet hat, mit einer sogar noch strengeren Regulierung in spezifischen Bereichen (einschl. Gesundheitsdaten und digitalem Wettbewerb)

#3

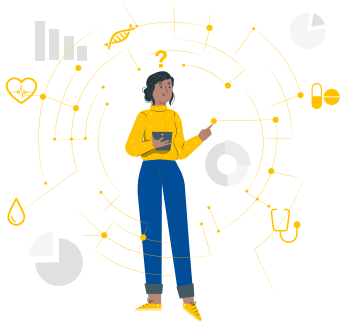
Das **Digitale-Versorgung-Gesetz (DVG)** sieht die Regulierung der Verwendung von Gesundheitsdaten vor, wobei deren Speicherung durch US-Provider verboten wird

Eine spezifische Regulierung von Gesundheitsdaten…

- In Deutschland werden digitale Gesundheits-Apps seit 2020 durch die **Digitale-Gesundheitsanwendungen-Verordnung (DiGAV)** geregelt

…mit der Festlegung spezifischer Regelungen für das Cloud-Computing

- Keine von einer Gesundheitsanwendung erfassten Gesundheitsdaten **dürfen in andere Länder außerhalb der EU transferiert werden**
- **Anwendungen, durch welche Gesundheitsdaten auf Cloud-Diensten eines US-Unternehmens gespeichert werden**, selbst mit europäischen Niederlassungen und Servern, werden vom Bundesinstitut für Arzneimittel und Medizinprodukte nicht genehmigt



Die **10. Änderung des deutschen Kartellgesetzes** sieht die Schaffung eines „Regelungsrahmens für den digitalen Wettbewerb" vor

Ein Gesetz gegen Wettbewerbsbeschränkungen…

- 2021 ist die Umsetzung der **10. Änderung des Gesetzes gegen Wettbewerbsbeschränkung** (Gesetz über Digitalen Wettbewerb) vorgesehen, wobei die Regierung die Schaffung eines „Regelungsrahmens für den digitalen Wettbewerb" beabsichtigt

…das auf die starke Beschränkung der Marktmacht digitaler Giganten abzielt

- Ein neuartiges Regulierungskonzept, **das auf** eine begrenzte Anzahl **großer „Torhüter und Vermittler" auf den digitalen Märkten abzielt**
- **Wesentliche Prinzipien**:
  - Das **Bundeskartellamt** kann eine Feststellungsentscheidung erlassen, dass die Marktposition eines Unternehmens von **„überragender marktübergreifender Bedeutung" ist** – auf der Grundlage mehrerer Faktoren (Marktbeherrschung, vertikale Integration, Finanzkraft, Zugang zu Daten oder anderen Ressourcen)
  - Das Bundeskartellamt erwirbt **die Macht, Ex-ante-Verbote für eine Reihe von in der Liste geführten Praktiken zu verhängen**, auch auf Märkten, auf denen das Unternehmen keine beherrschende Stellung hat
  - Das Unternehmen **trägt die Beweislast**, um sich zu verteidigen
- **Arten von Verhaltensweisen** solcher Unternehmen, die künftig vom Bundeskartellamt verboten werden können:
  - **Eigenpräferenz**, wenn der Zugang zum Markt der Bereitstellung und des Verkaufs gewährt wird (z. B. exklusive Vorinstallationsangebote)
  - **Behinderung der Interoperabilität** von Produkten, Dienstleistungen oder Daten

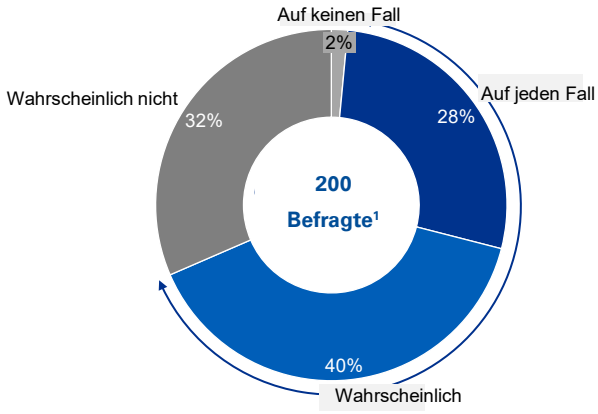
Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

Den Umfrageergebnissen zufolge erwarten Entscheidungsträger eine strengere Regulierung; infolgedessen könnte sich ihre Wahl von Cloud-Providern mehr zugunsten europäischer Provider verlagern

#3

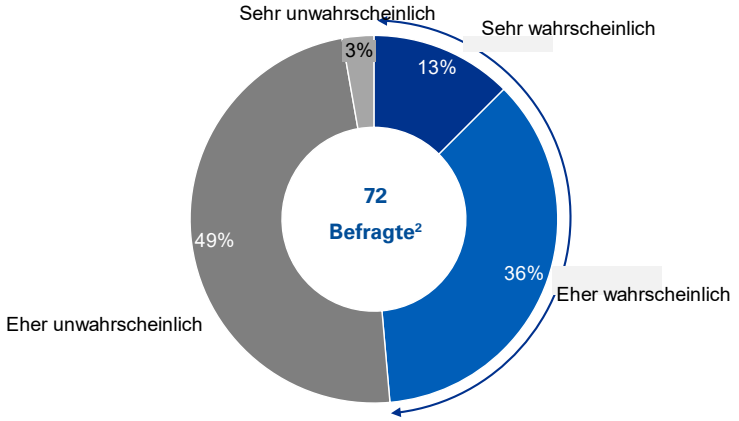
Erwartungen europäischer Cloud-Computing-Entscheidungsträger in Bezug auf die europäische Regulierung und deren Wahl von Cloud-Providern

Erwarten Sie in den nächsten 3 - 5 Jahren eine strengere europäische Regulierung?



68% der Befragten erwarten in der nahen Zukunft eine strengere europäische Regulierung

Mit welcher Wahrscheinlichkeit würde Ihr Unternehmen **seine Wahl von Cloud-Providern aus rechtlichen und/oder Marketing-Gründen in den nächsten 3** Jahren zugunsten europäischer Provider anpassen?



49% der Befragten könnten aus rechtlichen Gründen oder Marketing-Gründen einen europäischen Cloud-Provider bevorzugen

Anm.: (1). Basierend auf einer GSG-Umfrage mit 200 europäischen CxOs-Befragten (2). Basierend auf einer GSG-Umfrage mit 72 europäischen Befragten, darunter CMO, CLO, CEO und COO
Quellen: GSG-Umfrage; GSG-Analyse

Szenario 4: Europäisierung der Geschäfte von Cloud-Providern

Hebelkräfte

„Europäisierung der Geschäfte von Hyperscalern

- In diesem Szenario würden nicht-europäische Cloud-Provider einer Regulierung unterliegen, **durch die gewährleistet würde, dass ein größerer Anteil der wirtschaftlichen Vorteile des Cloud-Computing in Europa bleiben würde** (z. B. durch Investitionen, und lokale Forschungs- und Entwicklungskapazitäten), und ein **größeres Maß an Kontrolle durch europäische Akteure** ermöglicht würde…
- … dies könnte sich in Form von Verpflichtungen / Anreizen in Bezug auf **lokale Forschungs- und Entwicklungsausgaben, eine lokale Präsenz der obersten Geschäftsführungen von Hyperscalern ausgestalten** – was bereits bestehende europäische Regulierungen (z. B. für den europäischen Bankensektor) sowie **die lokale Beschaffungs-/ Lieferkette** (z. B. Bestandteile für Data Center) reflektiert, mit entsprechender Überwachung durch europäische Behörden, um eine effektive **lokale Wertschöpfung** zu gewährleisten, anstelle der „EU-Wäsche" der operativen Geschäfte von Hyperscalern

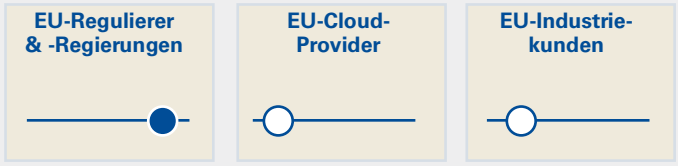
Effektive Kontrolle der lokalen Niederlassungen von Hyperscalern durch europäische Firmen

- Die europäischen Niederlassungen internationaler Cloud-Provider müssten **per Gesetz teilweise im Eigentum lokaler europäischer Unternehmen und effektiv unter deren Kontrolle stehen** (z. B. durch Joint-Ventures), insbesondere um die effektive DSGVO-Compliance zu gewährleisten...
- …**ähnlich wie die derzeitige Situation in China oder in anderen Ländern (z. B. Russland, Vereinigte Staaten)**
  - z. B. in China stellen Azure und AWS lokale Cloud-Computing-Dienste durch Joint-Ventures mit lokalen Akteuren bereit

Implikationen

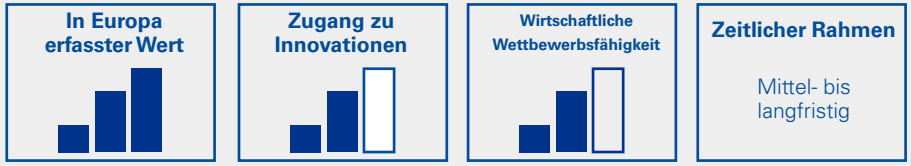
- **Mischung europäischer Investitionen durch nicht-europäische Provider entwickelt sich im Laufe der Zeit**, einschließlich eines größeren Anteils von Forschung und Entwicklung, im Gegensatz zu Kapitalausgaben von Data Centern (was den Großteil der Investitionen von Hyperscalern in einer „Ist"-Situation ausmachen würde)
- **Das europäische Cloud-Ökosystem beschleunigt seinen Ausbau** durch eine Kombination der Durchlässigkeit der lokalen Forschung und Entwicklung nicht-europäischer Provider sowie der europäischen Eigentümerschaft der operativen Geschäfte von Hyperscalern, **wodurch gewährleistet wird, dass ein bedeutendes Pool von kritischen Tech-Talenten in Verbindung mit dem Cloud-Computing in Europa bleibt und wächst**

Rolle im Übergang zu dem Szenario



Legende: Weniger bedeutende Rolle — Bedeutende Rolle

Szenario-Effizienz
und assoziierte Auswirkungen auf wirtschaftliche Metriken für Europäer



Legende: Begrenzte Auswirkungen — Starke Auswirkungen

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

VERANSCHAULICHEND

In manchen Ländern, wie China oder den USA, gilt bereits die staatliche Auflage der teilweisen Kontrolle der Tätigkeiten ausländischer Cloud-Provider durch lokale Akteure

#4

Aufgrund des chinesischen Cybersicherheitsgesetzes sind ausländische Cloud-Provider gezwungen, sich mit lokalen Unternehmen als Partnern zusammenzuschließen, um chinesische Kunden zu bedienen

- Aufgrund des im Jahr 2017 in China verabschiedeten und seitdem allmählich ausgestalteten **Cybersicherheitsgesetzes** gelten für ausländische Cloud-Provider strenge Auflagen, einschließlich:

Lokaler Datenspeicherung: Alle Unternehmen, die in China Geschäftstätigkeiten betreiben, müssen ihre Daten innerhalb der Grenzen Chinas speichern

Internet Data-Center: Ausländische Unternehmen dürfen keine direkten Anträge auf IDC-Lizenzen stellen; dies ist nur über Joint-Ventures oder Partnerschaften mit lokalen Betreibern in China zulässig

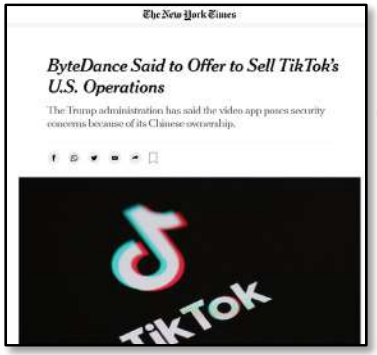
„Im Rahmen eines strategischen Partnerschaftsabkommens , **wird Microsoft seine Technologien an 21Vianet lizenzieren**, er damit zum offiziellen Dienstleistungsanbieter von Microsoft Azure, Office 365 und Dynamics 365 in China wird."365 and Dynamics 365 in China."

„Zur Einhaltung der chinesischen Gesetzgebung**, hat AWS bestimmte Bestandteile des Infrastrukturvermögens an Sinnet veräußert"**

Die USA haben in ihrer Sorge über den Umgang mit Daten durch ausländische Apps oftmals Veräußerungen zugunsten von US-Unternehmen in Betracht gezogen

- **Ausländische Anwendungen stehen** seit einiger Zeit **unter zunehmend strenger Kontrolle durch die USA in Bezug auf deren Umgang mit personenbezogenen Daten, sogar** unter Androhung von Sanktionen oder Verboten:

  - Im Jahr 2020 **drohte Präsident Trump das Verbot von TikTok an, wenn es nicht an einen US-amerikanischen Akteur veräußert würde**; als Begründung wurden Bedenken über diese App in Bezug auf die nationale Sicherheit angeführt – ByteDance (der chinesische Eigentümer von TikTok) zog demzufolge die Veräußerung seines US-Geschäfts in Betracht, doch diese wurde in der Folge mit der Wahl von J. Biden als neuen Präsident aufgehalten
  - Im Jahr 2020 **veräußerte die chinesische Gaming-Firma Beijing Kunlun Tech die Grindr-App**, eine im Jahr 2016 von ihr erworbene beliebte Dating-App., nachdem ihr vom Ausschuss für ausländische Investitionen in den Vereinigten Staaten (Committee on Foreign Investment in the United States, CFIUS) **die Auflage erteilt worden war, sie zu veräußern**



„Was ist die richtige Antwort? Die Übernahme von TikTok durch ein amerikanisches Unternehmen wie Microsoft. Das ist für beide Seiten von Vorteil. Der Wettbewerb wird aufrechterhalten, und es wird verhindert, dass die Daten in die Hände der Kommunistischen Partei Chinas gelangen." Senator L. Graham (Republikaner)

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

Szenario 5: Spaltung von Cloud-Tätigkeiten (funktional oder strukturell)

Hebelkräfte

Funktionale Spaltung von Cloud-Tätigkeiten

- „Funktionale" **Spaltung zwischen Cloud-Tätigkeiten von Hyperscalern und anderen Tätigkeiten** (z. B. GCP vs. Advertising-Kerngeschäft von Google), einschließlich mit einer klaren Spaltung in Bezug auf Personal, Büros, IP etc., wobei die Eigentümerschaft des Unternehmens unverändert bleibt…
- …als eine **regulatorische Anforderung konzipiert, bedeutet eine verbesserte Einhaltung in Bezug auf Handelspraktiken** (z. B. Verhinderung von Verbundgeschäften; oder Verhinderung der Subventionierung eines Cloud-Geschäfts durch Kerngeschäft), durch **größere Transparenz** über die Beziehungen zwischen den verschiedenen Tätigkeiten von Hyperscalern

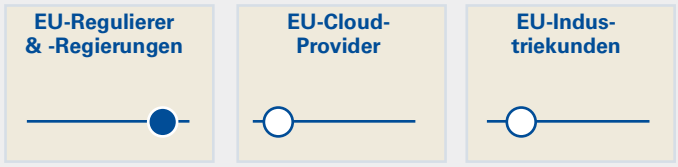
Strukturelle Spaltung von Cloud-Tätigkeiten

- Ähnlich wie die „funktionale" **Spaltung von Cloud-Tätigkeiten**, hier jedoch mit einer klaren Abspaltung des Cloud-Geschäfts zu einer **separaten juristischen Person** (entweder in Europa oder global, sollte der Hebel von einem amerikanischen Regulierer aktiviert werden), d. h. mit einer potenziellen Entwicklung der Eigentümerschaft des Cloud-Geschäfts…
  - Der Hebel insgesamt könnte evtl. im Zusammenhang mit einem Joint-Venture betrachtet werden (siehe Szenario 4)
- …Im Einklang mit einer Reihe von Vorlagen, die von politischen Kandidaten in den USA (z. B. E. Warren) ausgehen

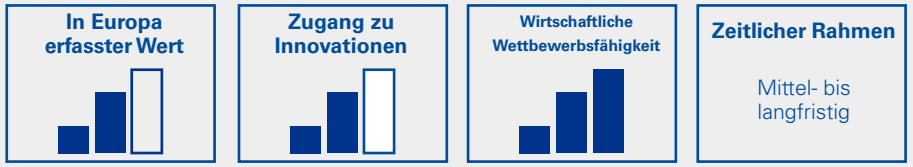
Implikationen

- **„Gerechtere" Wettbewerbsumgebung** zwischen europäischen Cloud-Providern und Hyperscalern, da letztere den vom alten Kerngeschäft geerbten Wettbewerbsvorteil verlieren würden (z. B. O365+Azure für Microsoft)
- **Cloud-Endnutzer** dürften von **einer Reduzierung von Verbundgeschäften profitieren** (verbesserte Umgebung in Bezug auf Handelspraktiken)

Rolle im Übergang zu dem Szenario



Szenario-Effizienz
und assoziierte Auswirkungen auf wirtschaftliche Metriken für Europäer



Legende: Weniger bedeutende Rolle — Bedeutende Rolle

Legende: Begrenzte Auswirkungen — Starke Auswirkungen

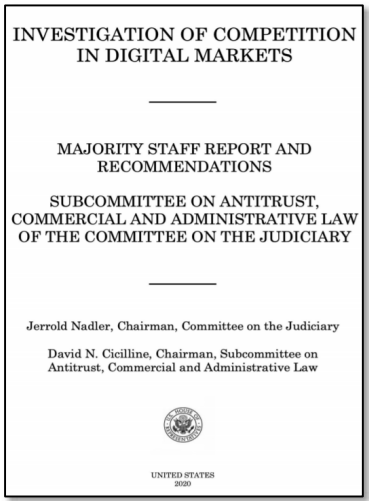
Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

VERAN-SCHAULICHEND

In den Vereinigten Staaten werden die Rufe nach dem Aufbrechen der Tech-Giganten zunehmend lauter und es besteht eine wachsende Notwendigkeit der Beschränkung ihrer Macht über Wirtschaft und Gesellschaft

#5

US-Haus berichtet über den Wettbewerb auf digitalen Märkten, mit Schwerpunkt auf der Notwendigkeit einer Reform der kartellrechtlichen Vorschriften…



INVESTIGATION OF COMPETITION IN DIGITAL MARKETS

MAJORITY STAFF REPORT AND RECOMMENDATIONS

SUBCOMMITTEE ON ANTITRUST, COMMERCIAL AND ADMINISTRATIVE LAW OF THE COMMITTEE ON THE JUDICIARY

Jerrold Nadler, Chairman, Committee on the Judiciary

David N. Cicilline, Chairman, Subcommittee on Antitrust, Commercial and Administrative Law

UNITED STATES
2020

Empfehlungen einschließlich:

- **Reduzierung von Interessenkonflikten** durch **strukturelle Spaltungen** und **Geschäftszweigbeschränkungen**
- Förderung von Innovationen durch **Interoperabilität und offenen Zugang** (Datenübertragbarkeit)
- **Reduzierung der Marktmacht** durch Fusionsvermutung

… werden von einem steigenden Anteil von Politikern und Bürgern unterstützt, die wünschen, „sie aufzubrechen"

„Diesen Unternehmen sollte der gleichzeitige **Besitz der Plattform-Dienstanbieter** und **der Teilnehmer** auf der Plattform verboten werden. Plattform-Dienstanbieter wären zur Einhaltung eines **Standards des gerechten, angemessenen und nicht-diskriminierenden Umgangs mit Nutzern verpflichtet**. Plattform-Dienstanbietern **wäre keine Übermittlung oder Weiterleitung von Daten an Dritte erlaubt**."
Senator E. Warren (März 2019)

„Slack fordert ganz einfach **einen fairen Wettbewerb mit gleichen Bedingungen für alle.** […] Slack fordert von der Europäischen Kommission, rasch **Maßnahmen zu ergreifen, um sicherzustellen, dass Microsoft seine marktbeherrschende Stellung nicht weiter unrechtmäßig** durch Bündelung oder Kopplung von Produkten **missbrauchen kann**." Auszug aus der EU-Kartellbeschwerde von Slack gegen Microsoft (Juli 2020)

„Die US-Regierung bekräftigt ganz einfach erneut eine Grundregel für alle Unternehmen: **Es geht nicht, dass sie sich einfach aus dem Wettbewerb frei kaufen**," so T. Wu, neuer Berater im Weißen Haus und erklärter Befürworter einer aggressiven Durchsetzung kartellrechtlicher Auflagen gegenüber US-amerikanischen Technologie-Giganten (März 2021)

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG; House Judiciary Committee (Interner Rechtsausschuss); „Here's how we can break up Big Tech" (E. Warren)

Fazit: Die Zukunft des europäischen Cloud-Markts könnte eine Kombination verschiedener Szenarien sein, jedes davon mit seinen Vorteilen, mit unterschiedlichen Zeitrahmen

	Rolle im Übergang zu dem Szenario				**Szenario-Effizienz** und assoziierte Auswirkungen auf wirtschaftliche Metriken für Europäer				
	EU Regul. & Reg.	**EU-Cloud-Anb.**	**EU ind-kunden**	**Rationale**	**In Europa erfasster Wert**	**Zugang zu Inno-vation**	**Wirtschaftl. Wettbewerbs fähigkeit**	**Zeitlicher Rahmen**	**Rationale**
1.Cloud als Gemein-gut	○	●	●	• Wesentliche Rolle von Cloud-Providern (einschl. EU-Providern), ein Ökosystem entsprechend der industr. Bedürfnisse zu schaffen (z. B. interoperabel)	▂▅▇	▂▅▇	▂▅▇	Kurz- bis mittelfristig	• Begrenzte lokale Werterfassung – (jeder Provider kann sich auf diese Angebote positionieren), doch mit Vorteilen in Bezug auf die EU-Wettbewerbsfähigkeit insgesamt
#2. Ausbau der Leistungsangebote europäischer Provider	○	●	●	• EU-Provider würden sich auf neuen, nicht ausreichend gedeckten Märkten positionieren, wo europäische Industriekunden hohe Anforderungen haben	▂▅▇	▂▅▇	▂▅▇	Kurz- bis mittelfristig	• Wert in Europa erfasst, da die Bedürfnisse von Industriekunden (KI, gesicherte Cloud) nur größtenteils durch EU-Provider gedeckt werden können
#3. Welle starker Regulierung	●	○	○	• Veränderungen hauptsächlich getrieben durch die Schaffung einer Regulierungsbehörde und die Umsetzung von Ex-ante-Regelungen	▂▅▇	▂▅▇	▂▅▇	Mittel- bis langfristig	• Der Markt dürfte sich zugunsten eines gesünderen Wettbewerbs öffnen (keine Verbundgeschäfte mehr, Preisregulierung), mit Vorteilen in Bezug auf die Wettbewerbsfähigkeit.
#4. Europäisierung der Geschäfte von Cloud-Providern	●	○	○	• Notwendigkeit einer strengeren Regulierung in Europa zur Verbesserung der Kontrolle der Datenspeicherungsorte (vgl. chinesische Regulierung)	▂▅▇	▂▅▇	▂▅▇	Mittel- bis langfristig	• Globale Cloud-Provider sollten EU-Gesetze einhalten, die lokale Cloud-Tätigkeiten vorsehen, sodass die Wertschöpfung in Europa bleibt
#5. Spaltung der Cloud-Tätigkeiten	●	○	○	• Durch europäischen Regulierer auferlegte funktionale und strukturelle Trennung, um ein „gerechteres" Wettbewerbsumfeld zu schaffen	▂▅▇	▂▅▇	▂▅▇	Langfristig	• Strukturelle Veränderungen dürften den Wettbewerb fördern, wodurch ein besserer Zugang zu Innovationen und mehr EU-Wertschöpfung gewährleistet wird

Legende: ○——— Weniger bedeutende Rolle ———● Bedeutende Rolle

Legende: ▂▅▇ Begrenzte Auswirkungen ▂▅▇ Starke Auswirkungen

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

Im Falle einer unzureichenden Aktivierung der identifizierten Hebel könnte Europa zwischen 20 % und 50 % der geschätzten wirtschaftlichen Auswirkungen des Cloud-Computing-Markts verlieren

Geschätzte wirtschaftliche Auswirkungen für den zukünftigen europäischen Cloud-Markt

In Europa erfasster Wert, 2027

Unveränderte aktuelle Lage, mit einer starken Beherrschung durch Hyperscaler

€ [40 - 45] Mrd.

-50%

Effiziente Aktivierung der identifizierten Hebel, resultiert in wachsenden Marktanteilen für europäische Provider in Europa

€ [60 - 70] Mrd.

In Europa geschaffene Arbeitsplätze, für den Markt im Jahr 2027

[150.000 - 175.000] Arbeitsplätze

-50%

[330.000 - 350.000] Arbeitsplätze

Investitionen, in Europa erfasst für den Zeitraum 2021-2027

€ [135 - 140]Mrd.

-20%

Verlorene Chance für Europa

€ [160 - 170] Mrd

Die wirtschaftlichen Auswirkungen der Cloud in Europa (einschl. des erfassten Wertes, der geschaffenen Arbeitsplätze und Investitionen) werden je nach dem tatsächlichen Szenario (bzw. einer potenziellen Kombination verschiedener Szenarien) oder den aktivierten Hebeln variieren

Quellen: Interviews mit Kunden und Experten; KPMG Avocats und Untersuchung und Analyse von GSG

5

Der Weg voran: bewährte Praktiken und Initiativen für öffentliche und private Beteiligte

Diese gegenwärtigen Herausforderungen bergen, gemeinsam mit der Unsicherheit im Hinblick auf die Zukunft der europäischen Cloud-Landschaft, Risiken für die Hauptbeteiligten und Interessierten des Privatsektors...

Unsicherheit im Hinblick auf die Zukunft der europäischen Cloud-Landschaft

Potenzielle Auswirkungen auf Hauptbeteiligte und Interessierte des Privatsektors

Für Chief Information, Technical & Security Officer

Risiken in Verbindung mit Informations- & Computer-Technologien:
- Abweichende IT- und Geschäftsstrategien
- Cloud-Mehrkosten, fehlender Wettbewerbsvorteil durch die Cloud
- Mangelnde Interoperabilität, Anbieter-Lock-in
- Ineffiziente Infra-Konfiguration führt zu Sicherheitslücken

Für Chief Legal Officer

Risiken in Verbindung mit dem Rechts- und Regulierungsrahmen:
- Nichteinhaltung der DSGVO-Regeln
- Geltungsbereich extraterritorialer Gesetze
- Verlust der Kontrolle über strategische

Für Chief Marketing Officer

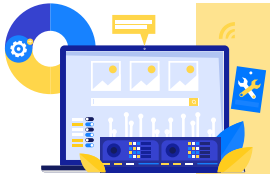
Risiken in Verbindung mit Marketing und Kunden-beziehungen:
- Nichtnutzung von Apps auf dem neuesten Stand der Technik (Verkauf & Marketing), dadurch Schädigung der Kundenerfahrung / Erosion des Ansehens
- Kundenverlust

Für öffentliche Entschei-dungsträger

Risiken in Verbindung mit der Verwaltung öffentlicher Daten:
- Verwaltung sensibler Daten mit begrenzten öffentlichen Finanzmitteln und Unterstützung
- Nichtnutzung der Vorteile des Werts der Datenaggregation

Quellen: Interviews mit Experten; Untersuchung und Analyse von GSG

...die mit einigen Initiativen durch CIOs, CLOs, CMOs und öffentliche Entscheidungsträger entschärft werden können



Chief Information, Technical & Security Officer

- Kenntnis der eigenen gegenwärtigen IT-Nutzung (Daten und Auslastung)
- Einleitung eines kulturellen Wandels hin zu einer proaktiven Cloud-Strategie
- Wohlüberlegte Wahl und Verwaltung der eigenen Cloud-Plattformen

Chief Legal Officer

- Kenntnis der eigenen Datentransfers und Transfer-Tools
- Durchführung einer Bewertung der Risiken einer Nichteinhaltung der DSGVO
- Prüfung der Daten-verschlüsselungs-bedingungen

Chief Marketing Officer

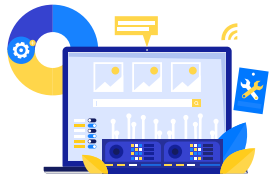
- Entwicklung eines verantwortungsbewussten und nachhaltigen Kundenversprechens
- Einsatz von Cloud-Zertifizierungen als greifbarer Nachweis
- Unterscheidung von der Konkurrenz

öffentliche Entscheidungs-träger

- Standardisierung cloud-bezogener öffentlicher Politiken
- Definition einer zweckbestimmten Ausgabenpolitik für Cloud-Computing
- Information und Weiterbildung von IT-Entscheidungsträgern bei lokalen Körperschaften

Quellen: Interviews mit Experten; Untersuchung und Analyse von GSG

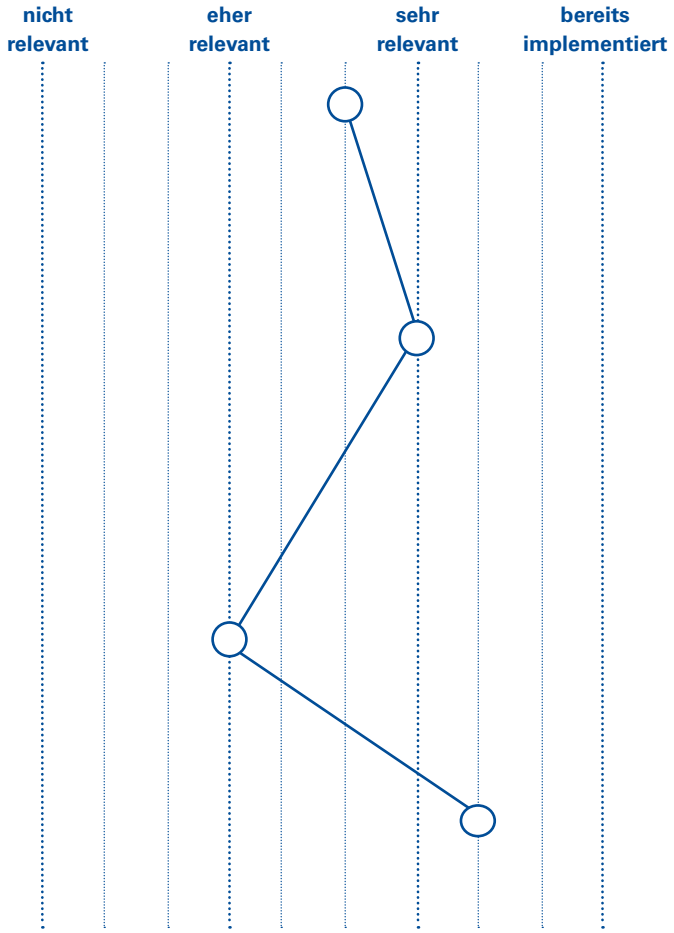
CIOs, CTOs und CISOs, die das Potenzial ihrer Cloud-Infrastruktur ausschöpfen möchten, sollten einige bewährte Praktiken für eine konforme & sichere Migration berücksichtigen



Von CIOs/CTOs/CISOs zu implementierende bewährte Praktiken und Initiativen

Bewährte Praktiken	Initiativen
Kenntnis der eigenen tatsächlichen IT-Nutzung und Daten	• **Einstufung Ihrer Daten** nach Vertraulichkeitsstufe (C1 bis C4), mit besonderer Aufmerksamkeit für personenbezogene und/oder sensible Daten • **Einrichtung der richtigen Governance** über die gesamte Lebensdauer der Daten nach Stufe und Typ (z. B. Speicherungsort & -dauer, Zugriff & Berechtigung, Zweck)
Kenntnis der eigenen tatsächlichen IT-Nutzung und Auslastung	• **Bewertung Ihrer Auslastung in enger Zusammenarbeit mit BusinessStakeholdern, dies beinhaltet:** • benötigter Rechenumfang und -typ (CPU, GPU, HPC)2 • Skalierbarkeit der Auslastung (VM, Container oder überhaupt nicht skalierbar) • Auslastungsnutzung (Häufigkeit, durch wen, Dauer, warum, mit welchen Eingangsdaten, für welche Ausgangsdaten)
Einleitung eines kulturellen Wandels hin zu einer proaktiven Cloud-Strategie	• Einleitung eines **kulturellen Wandels** auf verschiedenen Ebenen des Unternehmens: • Auf HR-Ebene mit einem Wandel beim Sourcing (von manuellen und hardwaregebundenen Jobs zu Software-Entwicklungs-Jobs) • Auf IT-Ebene, mit der Notwendigkeit der Einnahme einer proaktiven Haltung hinsichtlich Sicherheit und Cloud-Resilienz beim Infrastruktureinsatz
Wohlüberlegte Wahl und Verwaltung der eigenen Cloud-Plattformen	• **Durchführung einer Bewertung der Cloud-Provider** (z. B. hinsichtlich SLA in Krisensituationen, Datensouveränität, Datentransfers & Zugriffsgarantien) und Erwägung einer **Multicloud-Strategie** zur Vermeidung potenzieller zukünftiger Lock-in-Situationen • **Einsatz bewährter Praktiken** aus der Software-Entwicklung zur Behandlung Ihrer Infrastruktur „as code" (Devops, CI/CD)

Überblick über die Relevanz der Initiativen[1]



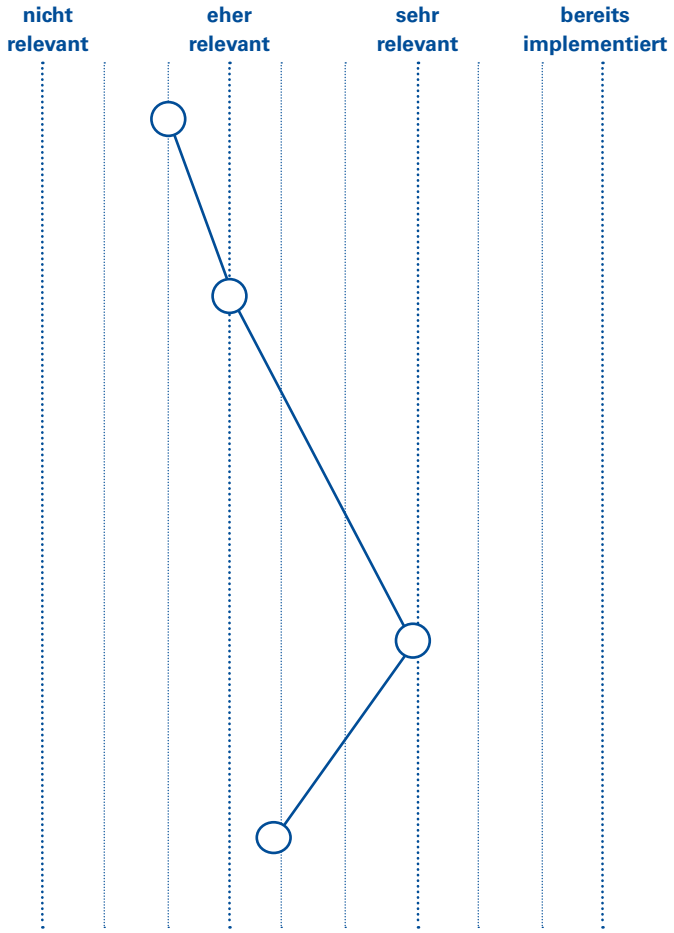
Anm.: (1) basierend auf einer GSG-Umfrage mit 76 europäischen CIOs, die die folgende Frage beantworteten: „Wie relevant wäre die Implementierung einer dieser Maßnahmen für Ihr Unternehmen?" (2). CPU: Central Processing Unit, GPU: Graphics Processing Unit, HPC: High-Performance Computing
Quellen: Interviews mit Experten; GSG-Umfrage; GSG-Analyse

Zur Anpassung an die wechselnde und komplexe Datenschutzregelung sollten CLOs ihre Datentransfers abbilden, die Datenverteilung bewerten und eine Risikobewertung durchführen

Von CLOs implementierte[2] bewährte Praktiken und Initiativen

Bewährte Praktiken	Initiativen
Abbildung Ihrer Datentransfers	• **Identifizierung von Service-Providern** mit Sitz **außerhalb der EU** oder bei denen die Wahrscheinlichkeit von Datentransfers nach außerhalb der EU besteht (Prozesse mit dem höchsten Risiko) • Identifizierung der **Verarbeitung personenbezogener Daten**, die diesen Providern anvertraut werden, und der damit verbundenen **Rechtsgrundlage** (Einwilligung, legitimes Interesse usw.)
Bewertung Ihrer Transfer-Tools	• **Identifizierung der Transfer-Tools, auf die Sie sich stützen** (Entscheidungen im Hinblick auf die Zweckmäßigkeit, verbindliche Unternehmensregeln, Verhaltenskodex, Ad-hoc-Vertragsklauseln, Zertifizierungsmechanismen usw.) • **Analyse der lokalen Gesetzgebungen** zur Bewertung, ob das DSGVO-Transfer-Tool, auf das Sie sich stützen, unter allen Umständen effektiv ist
Durchführung einer Bewertung der Risiken einer Nichteinhaltung der DSGVO	• Bei nicht konformen Transfers oder Tools, **Bewertung der damit verbundenen Risiken** (erlaubte oder unerlaubte Anwendungsfälle) und der Notwendigkeit zusätzlicher Maßnahmen • **Erlaubte Anwendungsfälle**: Stärkung Ihres Vertrags (z. B. Datenschutzklauseln, verbindliche Unternehmensregeln, Vertragsklauseln) • **Unerlaubte Anwendungsfälle** (die häufigsten): Rückführung Ihrer Daten in ein DSGVO-konformes Land (einschl. Bewertungen im Hinblick auf Kosten, erforderliche Zeit und betriebliche Hemmnisse) • **Erneute Durchführung dieser Risikobewertung in regelmäßigen Abständen**
Prüfung der Daten-verschlüsselungs-bedingungen	• **Bewertung der Datenverschlüsselungsbedingungen** (wird häufig als die schnelle und effiziente Art der Erlangung der GDPR-Konformität betrachtet), einschl. Modalitäten, Relevanz, Wirksamkeit und Volumen der verschlüsselten Daten

Überblick über die Relevanz der Initiativen[1]



Anm.: (1) basierend auf einer GSG-Umfrage mit 124 europäischen CxOs, die die folgende Frage beantworteten: „Wie relevant wäre die Implementierung einer dieser Maßnahmen für Ihr Unternehmen?“ (2) basierend auf den Empfehlungen des Europäischen Datenschutzausschusses
Quellen: Interviews mit Experten; GSG-Umfrage; GSG-Analyse

VERANSCHAULICHEND

Über die regulatorische Compliance hinaus kann Datenverschlüsselung die Datensouveränität sicherstellen, aber nur mit sehr strengen (und häufig nicht eingehaltenen) Implementierungskriterien

Während Datenverschlüsselung eine der wirksamsten Methoden für den Schutz vor dem Datenzugriff ist,...

- Verschlüsselungsverfahren – sowohl algorithmische Verfahren (TLS, Ströme, Speicherung, Datenbanken usw.) als auch Infrastrukturen (Key Management Service – KMS, KMS as a service) – sind zugänglich, um **die Daten** zusätzlich zu den robusten, von Cloud-Technologien und -Infrastruktur bereitgestellten Sicherheitsebenen **vor externen Verletzungen und böswilligen Handlungen zu schützen**

„**Der Schutz der personenbezogenen Daten unserer Nutzer ist unsere oberste Pflicht**. Bestes Beispiel dafür ist die heutige Entscheidung zur **generellen Ende-zu-Ende-Verschlüsselung** auf Doctolib. Solange Sie die **Daten mit Verschlüsselungsschlüsseln** von einem vertrauenswürdigen Dritten verschlüsseln, **ist der Hosting-Provider von geringer Bedeutung.**“
Doctolib CEO

„Die Deutsche Bahn hat ein hochmodernes und sehr **umfassendes Verschlüsselungskonzept** entwickelt, das einen vollständigen Schutz unserer Daten in der Cloud ermöglicht.“ Sprecher der Deutschen Bahn

... sollte diese richtig implementiert werden, um Schutz vor der Extraterritorialität ausländischer Regulierungen sicherzustellen

Bei der Datenverschlüsselung zu berücksichtigende Schlüsselfaktoren

Insbesondere, Sicherstellung einer **unabhängigen Speicherung und Verwaltung von Verschlüsselungsschlüsseln durch einen Dritten** (d. h. unterschiedliche Provider für Cloud-Dienste und KMS), da von Cloud-Providern angebotener KMS zwar **die Datensicherheit sicherstellen kann,** aber **normalerweise keine Garantie für** Datensouveränität liefert

Beauftragung **hochqualifizierter Spezialisten und dedizierter Teams** mit der Implementierung **der Verschlüsselungsverfahren**; diese sind für die Implementierung eines umfassenden risikobasierten Ansatzes und einer Sicherheitsrichtlinie mit Schwerpunkt auf einer Minderung der Risiken im Zusammenhang mit extraterritorialem Zugriff zuständig

Management von Datenverschlüsselung als ein **komplexes Projekt** mit einer gut durchdachten **Einsatz-Roadmap**, unter Berücksichtigung der **Spezifizitäten des gegenwärtigen IT-Systems des Unternehmens** und der **potenziell hohen anfallenden Kosten**

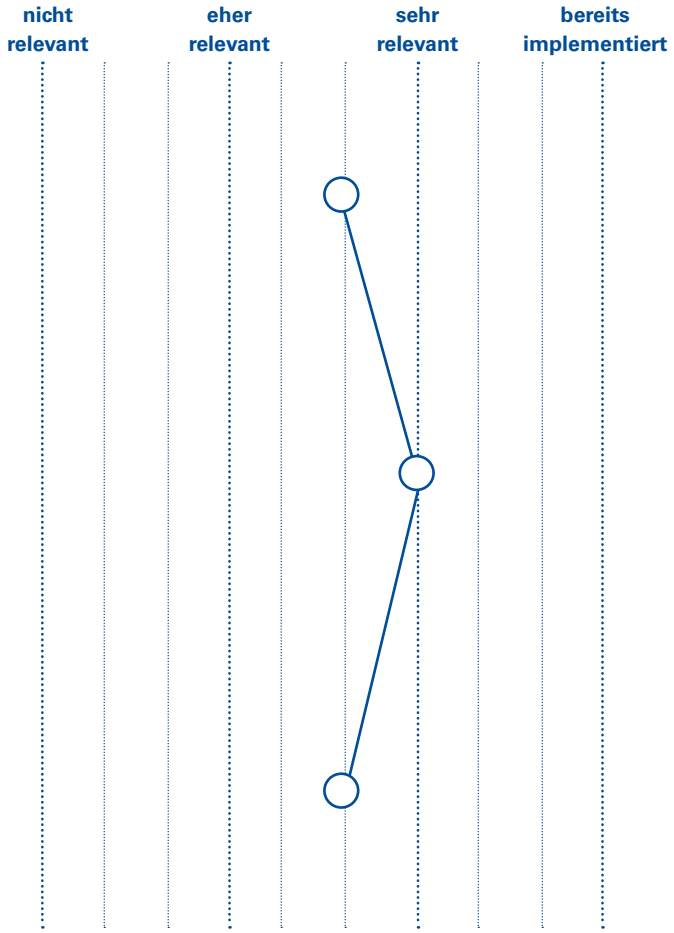
Quellen: Interviews mit Experten; Untersuchung und Analyse von GSG

Auch CMOs müssen ihrer Rolle gerecht werden und ihre Kundenwertversprechen an die IT-Entscheidungen im Hinblick auf Datenschutz & Souveränität angleichen

Von den Beteiligten und Interessierten – CMOs zu implementierende bewährte Praktiken und Initiativen

Bewährte Praktiken	Initiativen
Entwicklung eines verantwortungs-bewussten und nachhaltigen Kunden-versprechens im Hinblick auf den Datenschutz	• **Anerkennung der wachsenden Bedeutung von Datenschutz und -souveränität** für Kunden und der verbundenen Geschäftsrisiken, wenn diese nicht berücksichtigt werden (z. B. Kundenabwanderung) • Sicherstellen, dass die **Cloud-Politik des Unternehmens diese Bedeutung widerspiegelt** (z. B. Souveränitätskriterium bei der Auswahl eines Cloud-Providers, angemessene Prozesse vorhanden...) • **Verbindung der Datenschutzentscheidungen des Unternehmens mit dem Gesamtwertversprechen**, um bestehenden und potenziellen Kunden zu zeigen, wie viel Wert das Unternehmen ihren Daten beimisst… • …mit besseren Chancen der Vermeidung einer potenziellen Schädigung der Marke, z. B. Leak persönlicher Daten außerhalb von Europa
Einsatz von Cloud-Zertifizierun-gen als greifbarer Nachweis	• Sicherstellung, dass das Unternehmen sich für Provider mit relevanten Zertifizierungen entscheidet, um das Engagement des Unternehmens unter Beweis zu stellen... • …und **Zeigen dieser Zertifizierungen als Nachweis**, dass das Unternehmen das Thema Datenschutz und -souveränität ernst nimmt
Unterscheidung von der Konkurrenz	• **Die Sicherstellung der effektiven Einhaltung der DSGVO** – z. B. durch Untervertragnahme eines europäischen Cloud-Providers – ist eine Möglichkeit, sich **von der Konkurrenz zu unterscheiden** und so das Kundenwertversprechen zu bekräftigen • **Kommunizieren** der durch das Unternehmen beschlossenen Cloud-Politik und Nutzung als **Verkaufsargument** • **Identifizieren von nativen Cloud-Anwendungen auf dem neuesten Stand der Technik** für Marketing (z. B. Management von Marketing-Kampagnen) und Verkauf (z. B. CRM)

Überblick über die Relevanz der Initiativen[1]



Anm.: (1) basierend auf einer GSG-Umfrage mit 124 europäischen CxOs, die die folgende Frage beantworteten: „Wie relevant wäre die Implementierung einer dieser Maßnahmen für Ihr Unternehmen?"
Quellen: Interviews mit Experten; GSG-Umfrage; GSG-Analyse

Öffentliche Entscheidungsträger können die Digitalisierung und Cloud-Migration unterstützen, insbesondere durch Standardisierung der Cloud-Politiken und finanzielle Unterstützung öffentlicher cloud-bezogener Initiativen

Von öffentlichen Entscheidungsträgern zu implementierende bewährte Praktiken und Initiativen[1]

Bewährte Praktiken	Initiativen
Standardisierung cloud-bezogener öffentlicher Politiken	• **Definition von Richtlinien für cloud-bezogene Politiken** auf nationaler und lokaler Ebene **und Ausarbeitung einer entsprechenden Roadmap** zur: - **Unterstützung öffentlicher Entscheidungsträger** beim Identifizieren sensibler Daten anhand konkreter Beispiele (z. B. Gesundheitsdaten, personenbezogene HR-Daten usw.) - **Vergemeinschaftung lokaler Bedürfnisse** hinsichtlich der Cloud-Migration auf lokaler Ebene zur Begrenzung der Kosten und Sicherstellung eines kohärenten Ansatzes
Definition einer zweckbestimmten Ausgabenpolitik für Cloud-Computing	• **Zuweisung massiver langfristiger öffentlicher Ausgaben** zur Unterstützung der Anlaufphase bei europäischen Cloud-Providern (z. B. Migration sämtlicher digitalisierten öffentlichen Archive zu europäischen Cloud-Providern)
Information und Weiterbildung von IT-Entscheidungs-trägern bei lokalen Körperschaften	• **Information lokaler/dezentraler IT-Entscheidungsträger über souveräne und lokale Optionen** zur Cloud-Migration mit europäischen Cloud-Providern zur: - Ausräumung von Bedenken hinsichtlich der Cloud-Migration - Sicherstellung lokaler/europäischer Cloud-Migration auf souveränen öffentlichen Clouds • **Schulung lokaler IT-Entscheidungsträger** im Hinblick auf die Notwendigkeit der Einstufung ihrer Daten und der Einleitung der Cloud-Migration nicht sensibler Daten (aus Kosten-, Sicherheits- und Flexibilitätsgründen)

Anm.: (1) zum Beispiel lokale und regionale Körperschaften

Quellen: Interviews mit Experten; Untersuchung und Analyse von GSG

Beispiele: Smart Cities und öffentliche Daten

• **Daten** sind eine der wichtigsten **Voraussetzungen für die Entstehung von Smart Cities**, wobei es wichtig ist zu klären:

- **wem** die erzeugten Daten **gehören**
- **wer** darauf **zugreifen kann**

• Die größte Herausforderung von Smart Cities besteht in ihrer Fähigkeit, **Daten aus verschiedenen Quellen zu vernetzen**: verschiedene Netze (Wasser, Gas, Strom), vernetzte Geräte (IoT) in Straßeneinrichtungen, … – in diesem Kontext ist **Daten-Governance ein Schlüsselelement**

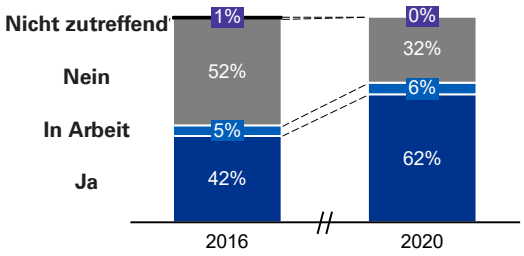
- **Offene Daten und Cloud-Computing** könnten, bei gutem Verständnis, als Ermöglicher betrachtet werden

Der relativ langsame Cloud-Übergang bei lokalen Körperschaften, auch aufgrund rechtlicher & steuerlicher Fragen, deutet auf ein höheres Potenzial für lokale Cloud-Provider und Edge Computing im breiteren Sinne hin

Immer noch langsames Tempo beim Übergang...

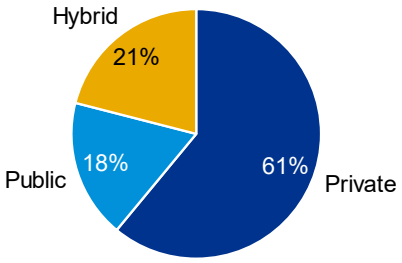
Nutzung von (mindestens 1) Cloud-Dienst durch lokale/regionale Körperschaften in Frankreich

- 2016-2020, % -



Aufteilung der von lokalen/regionalen Behörden in Frankreich genutzten Cloud-Dienste

- 2020, % -



...aufgrund verschiedener Hindernisse,...

- Die bisherigen **rechtlichen Hindernisse**, die das Hosting öffentlicher Daten in Data Centern außerhalb des französischen Territoriums verhinderten, wurden erst vor Kurzem1 aus dem Weg geräumt

- Präferenz lokaler/regionaler Körperschaften für Investition in eigene Data Center gegenüber IaaS, aufgrund von:

- **Sensibilität der Daten** (z. B. Daten der Bürger)
- **Langfristiger Horizont von Körperschaften**, zunehmende Relevanz von Investition gegenüber Cloud-Miete

„Unser gegenwärtiges Rechnungswesen bevorzugt Investitions- (CapEx) gegenüber Verwaltungshaushalten (OpEx)“,
Leiter Abteilung Technische Infrastruktur einer französischen Behörde

- Während die IaaS-Nutzung bislang sehr begrenzt war, **ist die SaaS-Nutzung mittlerweile** für Apps außerhalb ihres Kernauftrags **weit verbreitet**

...die Cloud-Provider überwinden müssen

- Obgleich lokale Körperschaften wahrscheinlich einen Anteil ihrer Infrastruktur „on-premise“ halten werden, schafft die **Beseitigung rechtlicher Hindernisse** eine natürliche **Gelegenheit für Cloud-Player, ihren Marktanteil** gegenüber „on-premise“ **zu erhöhen**.
- Ebenso wahrscheinlich ist, dass die Sensibilität der Daten auch weiterhin ein wichtiges Thema bleiben wird, das teilweise durch die Nutzung **lokaler Cloud-Provider** gelöst werden kann, die von lokalen Körperschaften als vertrauenswürdiger angesehen werden
- Es ist jedoch möglich, dass lokale Körperschaften auch weiterhin eine **Investition in eigene lokale Cloud-Einrichtungen prüfen werden, die unter mehreren lokalen Körperschaften vergemeinschaftet werden können**
- Diese Elemente liegen auf der Linie der **neuen Cloud-Strategie für die französische Verwaltung (März 2021)**, in der die Bedeutung von Datensicherheit und Souveränität, die Wichtigkeit der Auswahl kompetenter Cloud-Provider und die Notwendigkeit der Unterstützung des Cloud-Sektors durch den Staat unterstrichen werden

Anm.: (1) Ursprüngliche französische „souveräne Cloud-Strategie“, im November 2018 abgelöst durch die Cloud-Doktrin zur Schaffung von Anreizen zur Verwendung von Cloud-Lösungen durch lokale / regionale Körperschaften und 2019 die Änderungen des Code du Patrimoine, mit dem das Hosting bestimmter Arten öffentlicher Daten/Archive in Data Centern außerhalb des französischen Staatsgebiets erlaubt wurde
Quellen: Umfrage „MIPS 2020 collectivités territoriales“, Interviews mit Experten, Untersuchung und Analyse von GSG

6

Anhang

-Kapitel 1

Abkürzungen und verwendete Terminologie

Terminologie	Definition
API	Application Programme Interface (Programmierschnittstelle): eine Technologie, die die Konnektivität zwischen verschiedenen Software-Anwendungen ermöglicht.
Baremetal-cloud	Physische Server speziell für einzelne Mandanten, mit hoher Stabilität und Rechenleistung.
BYOL	Bring Your Own License: eine Praxis, die das Betreiben von SaaS-Anwendungen auf anderen Cloud-Umgebungen als denen des SaaS-Providers ermöglicht.
Cloud-computing	Das Hosting von Daten und Anwendungen auf physischen Servern, die über das Internet zugänglich sind.
Container-management	Technologie, die die Verpackung von Anwendungen und deren Abhängigkeiten in einem Block ermöglicht, wodurch zukünftige Migrationen in andere Umgebungen erleichtert werden.
CRM	Customer Relationship Management: Spezielle Software für die Verwaltung der wechselseitigen Beziehungen und Kontakte mit Kunden.
ERP	Enterprise Resource Planning: Spezielle Software für die Verwaltung der wesentlichen Geschäftsprozesse eines Unternehmens (z. B. Beschaffung, Auslieferung, Buchhaltung, Personalwesen).
Hosted Private Cloud	Vom Cloud-Provider gehostete und verwaltete private Infrastruktur.
Hybrid Cloud	Die Koordinierung von Cloud-Services über Public- und Private-Cloud-Provider hinweg, um eine weitere Cloud-Umgebung zu schaffen.
IaaS	Infrastructure-as-a-Service: Cloud-Computing-Servicemodell auf der Basis des gemieteten Zugriffs auf die Speicher- und Rechenkapazität auf physischen Servern.
IOT	Internet Of Things: materielle Objekte, die über integrierte Sensoren mit dem Internet verbunden sind.
PaaS	Platform-as-a-Service: Cloud-Computing-Servicemodell auf der Basis des gemieteten Zugriffs auf Plattformen für die Software-Entwicklung.
Private Cloud	Spezielle Cloud-Umgebungen für einen Kunden / Inhaber mit voll isoliertem Zugriff.
Public Cloud	Cloud-Umgebungen auf Servern, die das Eigentum von Cloud-Providern sind und zwischen verschiedenen Kunden / Unternehmen geteilt werden.
SaaS	Software-as-a-Service: Cloud-Computing-Servicemodell auf der Basis des gemieteten Zugriffs auf internet-basierte Anwendungen (mit zugrundeliegenden Plattformen und Infrastruktur).
Virtual Networking	Technologie, die den Aufbau einer komplexen privaten Infrastruktur durch die Verbindung einer Reihe sicherer privater Netzwerke ermöglicht.
Virtual Private Server	Virtuelle Server zur Nutzung für das Hosting von Websites und Anwendungen, wobei die Daten auf dem Nutzer gewährten virtuellen Maschinen gespeichert werden.

Quelle: GSG-Recherche

Abkürzungen und verwendete Terminologie – Gartner Hype Cycle-Kurve (1/2)

Terminologie	Definition
API Gateway	API-Zentralisierungsplattform für die Leitwegbestimmung (das Routing) von Anrufen an den entsprechenden Mikroservice mit Anfordern des Routings, Zusammensetzung und Protokollübersetzung.
Application PaaS	Cloud-Plattformservice, der Umgebungen für die Anwendungsentwicklung und -bereitstellung bietet.
Blockchain PaaS	Eine Reihe von Blockchain-Software-Plattformdiensten, die in der Cloud von einem Anbieter für Abonnenten angeboten werden.
Cloud management platforms	Plattform, die Unternehmen die Verwaltung von Private-Cloud-, Public-Cloud-, Multicloud-Services und Ressourcen ermöglicht.
Cloud marketplaces	Online-Ladenfronten, über die Kunden Cloud-Serviceangebote, einschließlich IaaS, PaaS und SaaS, finden und diese abonnieren können.
Cloud migration	Der Prozess der Planung und Ausführung der Bewegungen von Anwendungen oder Arbeitslasten von On-Premise-Infrastruktur auf externe Cloud-Dienste oder zwischen verschiedenen externen Cloud-Diensten.
Cloud Networking	Ein von Dienstleistern angebotener Service zur Verbindung zerlegter Hybrid- IT-Cloud-Umgebungen, der eine robuste Verbundfähigkeit zwischen externen Cloud-Data Centers und On-Premise-Data Centers des Kunden bietet.
Cloud office	Sammlung der meistverwendeten Suiten von SaaS-basierten Systemen für die persönliche Produktivität, die horizontale Zusammenarbeit und die Kommunikation (z. B. E-Mails, File-Sharing, Dateimanagement und -bearbeitung).
Cloud Security assessment	Formelle Sicherheitsüberprüfungen durch unabhängige Prüfstellen.
Cloud Tethering	Ein Applikationslieferungsmodell, bei dem eine gerätebasierte Anwendung mit dem Cloud-Service des Providers zur Lizenzierung verbunden ist.
Cloud to Edge Development Support	Beschreibt eine Erweiterung der Programmiermodelle des Cloud-Providers und deren Nutzung auf Edge-Geräten, wie z. B. IoT-Objekten.
Cloudbursting	Die Nutzung einer alternativen Reihe von Public- oder Private-Cloud-Diensten als Methode zur Erweiterung und Handhabung von Spitzen in IT-Systemerfordernissen beim Hochfahren oder während der Betriebszeit.
Cloud-testing tools & services	Cloud-Technologie zur Unterstützung des Testens von oder in der Cloud (einschl. Cloud-basiertem Labormanagement, Servicevirtualisierung, auf Abruf gelieferten Testwerkzeugen und Device Clouds).

Quellen: Gartner; GSG-Recherche

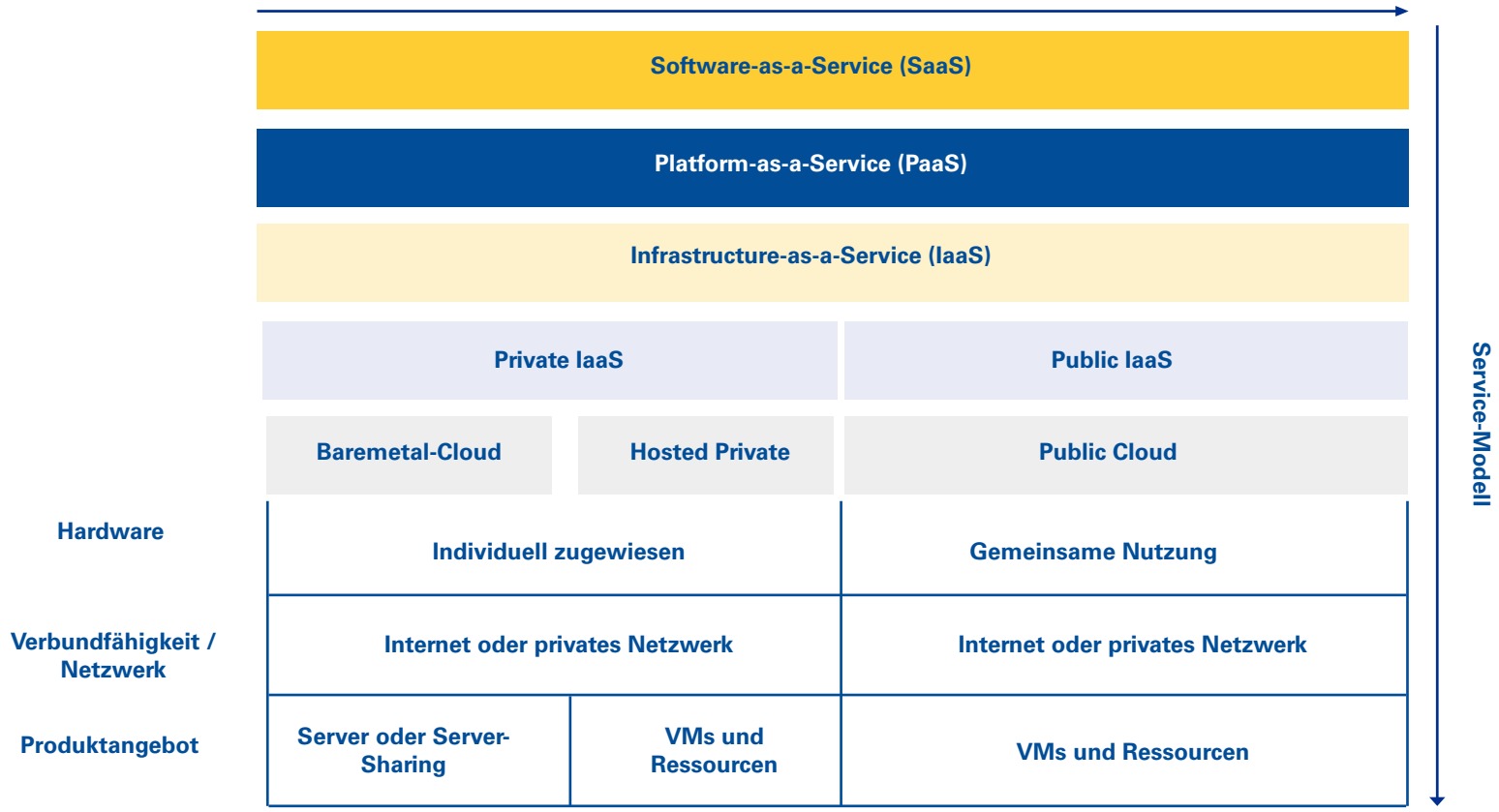
Abkürzungen und verwendete Terminologie – Gartner Hype Cycle-Kurve (2/2)

Terminologie	Definition
Container Management services	Eine Software, die das Management von Containern in großen Mengen in Produktionsumgebungen unterstützt.
Edge Computing	Eine verteilte Datenverarbeitungstopologie, bei der die Datenverarbeitung nahe an den Dingen oder Personen positioniert wird, von denen diese Daten produziert / verbraucht werden.
Expense management	Die Praxis der Prüfung und des Abgleichs der Gebühren für die von Cloud-Providern bereitgestellten Dienste mithilfe eines Überwachungssystems.
Hyperscale Computing	Eine Reihe von Architekturmustern für die Lieferung von Scale-Out-IT-Funktionen in einer enormen Größenordnung von Industriemaßstäben.
Immutable Infrastructure	Ein Architekturmuster, bei dem die Aktualisierungen des Systems und der Anwendungsinfrastruktur, wenn sie instanziiert sind, niemals am gleichen Ort vorgenommen werden.
IOT Platform	Eine Software, die die Entwicklung, Bereitstellung und Verwaltung von Lösungen, die sich mit IoT-Endpunkten verbinden lassen und aus denen Daten erfasst werden können, ermöglicht.
Machine Learning	Eine Disziplin, die auf die Lösung von Geschäftsproblemen unter Verwendung mathematischer Modelle, die in der Lage sind, Kenntnisse und Muster aus Daten zu extrahieren, abzielt.
Mutlicloud	Verwendung von Cloud-Diensten von mehreren Public-Cloud-Providern für den gleichen Zweck.
Private PaaS	Eine Art von PaaS, die den exklusiven Zugriff für das Kundenunternehmen bietet. Eine private PaaS kann von dem Kundenunternehmen (eigene Verwaltung) On-Premise eingerichtet oder auf einer öffentlichen IaaS gehostet werden.
Public Cloud Storage	IaaS, durch die Block-, Datei- und/oder Objekt-Speicherdienste, die über diverse Protokolle geliefert werden, bereitgestellt werden.
SaaS Administrative ERP	Administratives ERP mit Schwerpunkt auf dem Finanzmanagement, dem Humankapital-Management (HCM) und indirekter Beschaffung. (schließt kein Remote-Hosting, wo die eigene Verantwortung beim Kunden, oder bei der Private Cloud bleibt, mit ein).
Serverless PaaS	Mit serverlosen Eigenschaften gelieferte PaaS. Serverless ist eine Methode der Bereitstellung eines IT-Services, bei der die zugrundeliegenden Ressourcen nicht transparent sind, keine Bereitstellung vorab erforderlich ist und die durch eine Mikropreisgestaltung gekennzeichnet ist.
Software-defined infrastructure	Umfasst eine breite Reihe an Software-definierten Infrastrukturkomponenten (z. B. Software-definierte Data Center (SDDC), IP, SD Rand von randbasierten Adaptern / Monitoren / Gateways / Geräte und Maschinen).

Quellen: Gartner; GSG-Recherche

Die Cloud-Angebote auf dem Markt lassen sich nach zwei verschiedenen Dimensionen, Arten der Bereitstellung und Service-Modellen unterscheiden

Primäre Charakteristika der Cloud

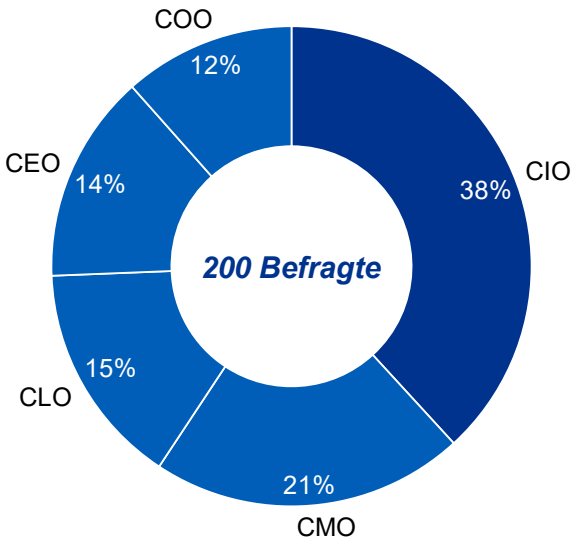


Quelle: Untersuchung und Analyse von GSG

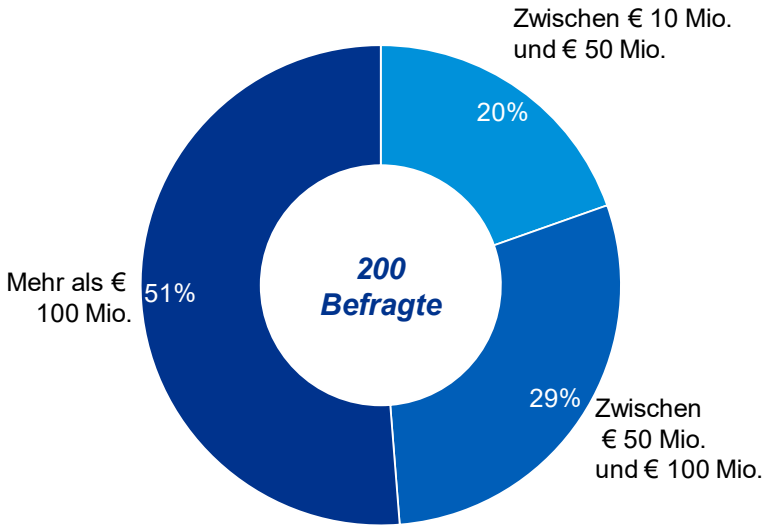
Im Verlauf der gesamten Umfrage haben wir 200 Antworten erfasst, mit einer recht ausgewogenen Gesamtanzahl von Befragten aus Unternehmen verschiedener Größenordnungen…

Profil der Befragten

Nach Position im Unternehmen



Nach Größe des Unternehmens (Jahresumsatz)



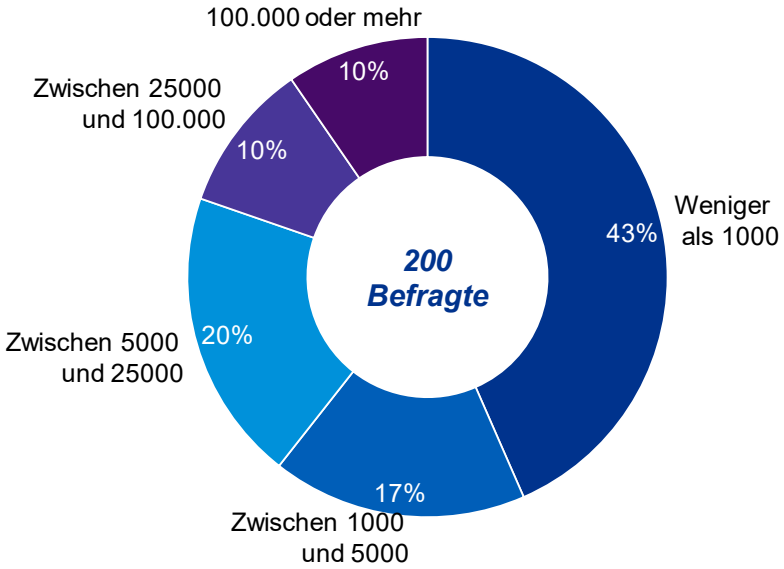
Davon  **50 % französische Umfrageteilnehmer**  **50 % deutsche Umfrageteilnehmer**

Anm.: CIOs stellen eine eigene Kategorie von Befragten für die restliche Umfrage dar, wohingegen CMO / CLO / CEO / COO als eine Kategorie von Befragten betrachtet werden
Quelle: GSG-Umfrage

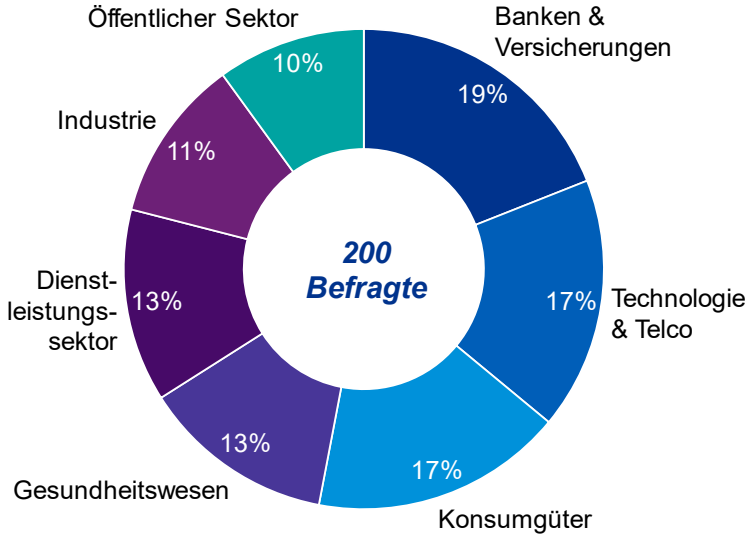
… unterschiedlich nach der Zahl der Mitarbeiter, sowie Befragte verschiedener Branchen

Profil der Befragten

Nach Anzahl Mitarbeiter



Nach Branche des Unternehmens



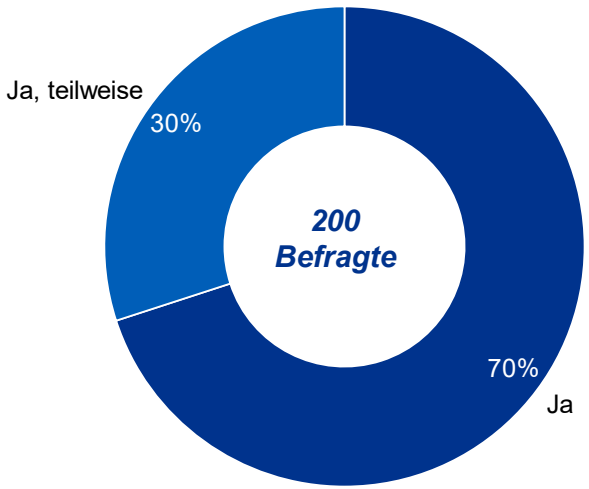
Quelle: GSG-Umfrage

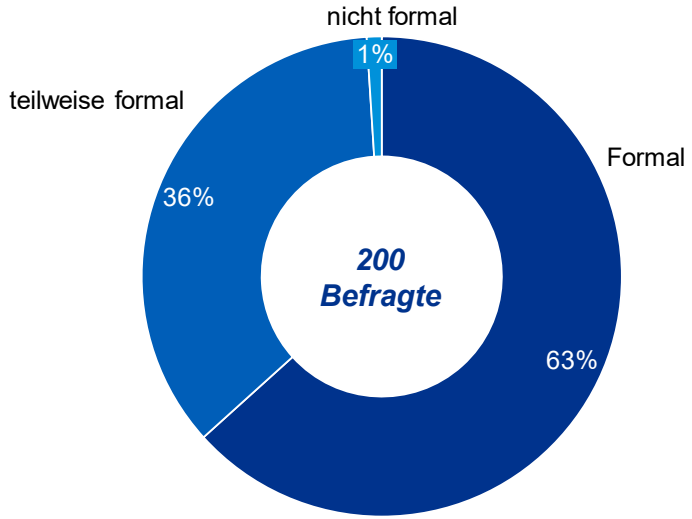
Alle Befragten sind an den Entscheidungsprozessen betreffend das Cloud-Computing beteiligt, und die Mehrheit von ihnen hat eine formale Cloud-Strategie

Profil der Umfrageteilnehmer

Sind Sie an dem **Entscheidungsprozess betreffend das Cloud-Computing** in Ihrem Unternehmen beteiligt?

Wie würden Sie Ihre Cloud-Strategie beschreiben?





Quelle: GSG-Umfrage

6

Anhang

-Kapitel 3

Mit der DSGVO ist eine regulierte „Freihandelszone“ für Daten innerhalb der Europäischen Union eingerichtet worden, und es gelten strenge Vorschriften über die Datenverarbeitung außerhalb der EU

Die Datenschutz-Grundverordnung (DSGVO) schreibt ein besonderes Niveau des Schutzes personenbezogener Daten vor und ermöglicht somit den freien Verkehr personenbezogener Daten innerhalb und außerhalb der EU.

Wer ist betroffen?

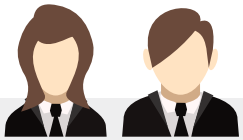
Jede öffentliche oder private Organisation, unabhängig von ihrer Größe, des Landes ihres Geschäftssitzes und ihrer Geschäftstätigkeit

Die Datenschutz-Grundverordnung

- Schafft **mehr Pflichten** für die Datenverarbeiter und die Datenverantwortlichen

- Stärkt die **Rechte derjenigen Personen**, deren Daten verarbeitet werden

- Erfordert die Umsetzung **spezifischer technischer und organisatorischer Maßnahmen**



Personenbezogene Daten

Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

Artikel 4 Abs. 1 DSGVO: „als identifizierbar wird eine natürliche Person angesehen, **die direkt oder indirekt**, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer **Kennnummer**, zu **Standortdaten**, zu einer **Online-Kennung** oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, **identifiziert werden kann**“

Datenverarbeitung

Jeder Vorgang oder jede Vorgangsreihe, im Zusammenhang mit personenbezogenen Daten

Artikel 4 Abs. 2 DSGVO: Der Ausdruck „Verarbeitung“ bezeichnet jeden **mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang** oder jede solche Vorgangsreihe **im Zusammenhang mit personenbezogenen Daten** wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;“

Quellen: Französische Datenschutzbehörde (CNIL); KPMG Avocats

Die DSGVO bietet einen einheitlichen Regelungsrahmen für den Datenschutz innerhalb der gesamten Europäischen Union, wodurch der freie interne Datenverkehr ermöglicht wird

- Um ein **gleichmäßiges und hohes Datenschutzniveau** für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten **in allen Mitgliedstaaten gleichwertig** sein(1).

Aufgrund der Tatsache, dass die DSGVO eine einheitliche Regelung in allen Mitgliedstaaten ist, kann dieser gleichmäßige Schutz in der gesamten Union gewährleistet werden.

Anm.: (1). Erwägungsgrund 10 der DSGVO
Quelle: KPMG Avocats

Datenströme aus der EU in Drittländer sind eine wirtschaftliche Notwendigkeit, und sind daher aufgrund der DSGVO unter bestimmten Bedingungen zulässig

Standard-Leitlinien

> Erwägungsgrund 101 der DSGVO
>
> Der **Fluss** personenbezogener Daten **aus** Drittländern und internationalen Organisationen und in Drittländer und internationale Organisationen **ist für die Ausweitung des internationalen Handels und der internationalen Zusammenarbeit notwendig**

- Durch die DSGVO werden internationale Datenströme nicht verboten. Die Verordnung schreibt jedoch vor, dass **das durch die Verordnung in der EU gewährleistete Schutzniveau für natürliche Personen** bei der Übermittlung personenbezogener Daten aus der Union in Drittländer oder an internationale Organisationen **nicht untergraben werden** sollte.

- Um ein **gleichmäßiges und hohes Datenschutzniveau** für natürliche Personen zu gewährleisten **und die Hemmnisse für die Übermittlung personenbezogener Daten in Drittländer und aus Drittländern zu beseitigen**, sollte das Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung dieser Daten **im Wesentlichen gleichwertig mit dem in der EU gewährleisteten Schutzniveau** sein.

Die DSGVO gewährleistet, dass unabhängig von der Herkunft des Datenverantwortlichen oder des Datenverarbeiters ein **Mindeststandard** eingehalten wird.

Quelle: KPMG Avocats

Durch die DSGVO wurden 3 wesentliche Instrumente geschaffen, um die Einhaltung des Datenschutzes in diesen Situationen des Datenverkehrs aus der EU in Drittländer zu erleichtern

Instrumentarium

Da die **Übermittlung personenbezogener Daten aus der EU in Drittländer unvermeidlich ist**, wurde mit der DSGVO ein „Instrumentarium" geschaffen, um zu gewährleisten, dass solche Datentransfers unter Einhaltung der festgelegten **Mindestanforderungen** erfolgen

1 Erstes Instrument: die Angemessenheits-entscheidung

Die Kommission darf **mit Wirkung für die gesamte Union beschließen**, dass ein bestimmtes Drittland, ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation **ein angemessenes Datenschutzniveau bietet**, und auf diese Weise in Bezug auf das Drittland oder die internationale Organisation, das bzw. die für fähig gehalten wird, ein solches Schutzniveau zu bieten, in der gesamten Union Rechtssicherheit schaffen und eine einheitliche Rechtsanwendung sicherstellen.(1)

2 Zweites Instrument: Standardvertragsklauseln

Die von der Kommission verabschiedeten Standardvertragsklauseln können zwischen Verantwortlichen und Anbietern angewandt werden, um **ausreichende Sicherheitsmaßnahmen** hinsichtlich des Datenschutzes für den internationalen Datenverkehr zu gewährleisten.

3 Drittes Instrument: Verbindliche interne Datenschutzvorschriften

Im Falle von **konzerninternen Übermittlungen** personenbezogener Daten aus der EU in Drittländer können und müssen die verbindlichen internen Datenschutzvorschriften **innerhalb derselben Unternehmensgruppe festgelegt werden**, wenn Entitäten auf der ganzen Welt beteiligt sind.

Anm.: (1). Erwägungsgrund 103 der DSGVO Quelle: KPMG Avocats
Quelle: KPMG Avocats

Der „Privacy Shield“ war ein Versuch im Jahr 2016, den Datenverkehr und - zugriff zwischen den USA und der EU zu genehmigen… doch dies wurde 2020 außer Kraft gesetzt

2016

Der „Privacy Shield“ ist ein von den USA und der EU unterzeichnetes Rahmenabkommen (Angemessenheitsentscheidung), das auf den **Schutz der Grundrechte von EU-Online-Nutzern**, deren personenbezogene Daten von US-Unternehmen und -Organisationen gehandhabt würden, abzielt. Es gestattet Verantwortlichen und Auftragsverarbeitern die **freie Übermittlung der personenbezogenen Daten** von EU-Bürgern **bei gleichzeitiger Wahrung ihrer persönlichen Rechte.**

2020

Außerkraftsetzung des „Privacy Shield“ (Schrems II)
Nach einer Beschwerte durch den Datenschutzaktivisten M. Schrems wurde das „Privacy Shield“-Abkommen vom Europäischen Gerichtshof mit der Begründung außer Kraft gesetzt, die US-amerikanischen Überwachungsprogramme seien mit den Grundsätzen der DSGVO nicht vereinbar.

Aufgrund des „Foreign Intelligence Surveillance Act” (FISA) und des Executive Orders 1233
ist US-Bundesbehörden der Zugriff auf alle personenbezogenen Daten, welche in US-amerikanisches Staatsgebiet übermittelt werden, erlaubt

Infolge der Außerkraftsetzung des Privacy Shield verfügen Unternehmen, die personenbezogene Daten an Server außerhalb der EU übermitteln, nunmehr über **keine rechtliche Grundlage** dafür und setzen sich der Gefahr der strafrechtlichen Verfolgung aus

Quellen: Französische Datenschutzbehörde (CNIL); KPMG Avocats

Der „Cloud Act“ lässt jetzt tatsächlich ein relativ hohes Maß des Zugriffs auf personenbezogene Daten durch die US-Regierung in den USA und außerhalb zu - im Widerspruch zur DSGVO

Der „Clarifying Lawful Overseas Use of Data (Cloud) Act“ US-Bundesgesetzgebung, der Anbieter von elektronischen Kommunikationsdiensten oder Remote-Computing-Services zur Offenlegung personenbezogener Nutzerdaten gegenüber der US-Regierung verpflichtet, ob die Daten in den USA oder außerhalb beherbergt sind

Wer ist betroffen?

Alle Lieferanten, die US-amerikan. Recht unterliegen, d.h. eine Entität, die Geschäfte in den USA betreibt, wie:

- **US-Unternehmen**
- Im Ausland ansässige Entitäten mit **US-Niederlassungen**

Bedingungen für die Datenoffenlegung

Behörden können Dienstleistungsanbieter nur unter Einhaltung der strengen rechtlichen Bestimmungen einer **von einem US-Gericht erlassenen Anordnung** zur Bereitstellung von Daten zwingen

Zahl der erhaltenen staatlichen Anfragen nach Nutzerdaten (2019)

81.785 Anfragen für alle Google; **282** davon an Unternehmen, **152** Daten vorgelegt für Anfragen im Zusammenhang mit Kunden von G Suite Enterprise Cloud und **0** für Anfragen im Zusammenhang mit Kunden von Google Cloud Platform Enterprise

Quellen: White Paper (US-Justizministerium); Transparenzberichte von Cloud-Anbietern; Untersuchung und Analyse von GSG; KPMG Avocats

Infolge dieser Außerkraftsetzung des Privacy Shields ist das Instrumentarium der DSGVO ebenfalls obsolet geworden, woraus sich wichtige Fragen für amerikanische und europäische Unternehmen ergeben

Ein obsoletes DSGVO-Instrumentarium

Der SCHREMS II-Fall hat zu einer **Neubetrachtung** des gesamten durch die DSGVO geschaffenen Instrumentariums geführt - in dem Maße, dass es, unabhängig von dem Instrument, nicht mehr möglich ist, ein angemessenes Niveau für den Schutz von in die USA übermittelten personenbezogenen Daten zu gewährleisten.

In Bezug auf jegliche im Rahmen der DSGVO angebotenen Mittel ist nationales Recht vorrangig, da die anderen Mittel zur Gewährleistung eines angemessenen Schutzniveaus für personenbezogene Daten, die aus der EU in Drittländer übermittelt werden, vertragliche Instrumente sind.

Aus der Neubetrachtung des Instrumentariums ergeben sich neue Fragen

- Ein **amerikanisches Hosting-Unternehmen** konnte personenbezogene Daten aus der EU nur auf der Grundlage einer Angemessenheitsentscheidung (‚Safe Harbor', dann ‚Privacy Shield') verarbeiten. Was würde geschehen, wenn eine solche Angemessenheitsentscheidung widerrufen wird?
- Was würde für ein **in der EU gegründetes Hosting-Unternehmen, dessen Tochtergesellschaften jedoch von einem amerikanischen Unternehmen kontrolliert werden**, geschehen, wenn die Angemessenheitsentscheidung, auf deren Grundlage die personenbezogenen Daten verarbeitet wurden, widerrufen wird?

Quelle: KPMG Avocats

Angesichts der Außerkraftsetzung des Privacy Shield hat der Europäische Datenschutzausschuss (EDSA) ein neues Instrumentarium mit 6 wesentlichen Schritten vorgelegt

EDSA[1] neues Instrumentarium

Angesichts der Außerkraftsetzung des Privacy Shield hat der Europäische Datenschutzausschuss ein **neues Instrumentarium** vorgelegt

ROADMAP FÜR DIE VERANTWORTLICHKEIT: beinhaltet **6 Schritte, die es für Exporteure zu befolgen gilt**, um Drittländer zu bewerten und ggf. die geeigneten zusätzlichen Maßnahmen zu identifizieren

1

Analyse des Datenverkehrs ("Know your Transfers")

2

Das Transfer-Tool, über welches der Transfer erfolgt, prüfen

3

Bewerten, ob es im Zusammenhang mit Ihrem spezifischen Transfer in dem Recht oder in der Praxis des Drittlandes irgendetwas gibt, was die Wirksamkeit der entsprechenden Sicherheits-maßnahmen der von Ihnen verwendeten Transfer-Tools beeinträchtigen kann

4

Zusätzliche Maßnahmen identifizieren und umsetzen

3 Arten möglicher Maßnahmen:

- Technische Maßnahmen
- Vertragliche Maßnahmen
- Organisatorische Maßnahmen

5

ggf. erforderliche formelle Verfahrensschritte zur Umsetzung Ihrer zusätzlichen Maßnahmen unternehmen

6

Neu bewerten und überwachen

Der EDSA hat auch **verschiedene Anwendungsfälle für zulässige und unzulässige Handlungsweisen aufgelistet**, um Unternehmen zu helfen, zu identifizieren, wo sie in Bezug auf ihre Verarbeitung personenbezogener Daten stehen

Anm.: (1). Europäischer Datenschutzausschuss
Quelle: KPMG Avocats

EDSA unterstützt durch Auflistung einer Reihe von Anwendungsfällen mit personenbezogenen Daten angesichts der Außerkraftsetzung des Privacy Shield

Anwendungsfälle für zulässige Handlungsweisen

- Anwendungsfall 1: Datenspeicherung zur Sicherung (Back-up) und für andere Zwecke, für die kein Zugriff auf unverschlüsselte Daten erforderlich ist
- Anwendungsfall 2: Übertragung pseudo-nymisierter Daten
- Anwendungsfall 3: Verschlüsselte Daten, die nur im Transit an Drittländer übermittelt werden
- Anwendungsfall 4: Geschützter Empfänger
- Anwendungsfall 5: Geteilte Verarbeitung oder Verarbeitung durch mehrere Parteien

Impliziert vertragliche Bestimmungen über technische Sicherheitsmaßnahmen im Zuammenhang mit Übermittlungen personenbezogener Daten

Der EDSA bezieht sich auf einen Datenexporteur, der personenbezogene Daten an einen Datenimporteur in ein Drittland übermittelt, welche spezifisch durch das Recht des betreffenden Landes geschützt sind, z. B. für die Zwecke der gemeinsamen Bereitstellung einer medizinischen Behandlung für einen Patienten oder einer Rechtsdienstleistung für einen Mandanten.

Ein solcher Fall ist zulässig, sofern - unter anderem - aufgrund des Rechts des Drittlandes ein dort ansässiger Datenimporteur von dem möglichen unerlaubten Zugriff auf die von dem betreffenden Empfänger gehaltenen Daten für den gegebenen Zweck (Berufsgeheimnis) ausgenommen ist und technische Maßnahmen ergriffen werden, um die Sicherheit solch vertraulicher Informationen (kryptographische Schlüssel, Passwörter usw.) zu gewährleisten.

Der EDSA bezieht sich auf einen Datenexporteur, der es beabsichtigt, personenbezogene Daten gemeinsam mit zwei oder mehr unabhängigen Datenverarbeitern, die in verschiedenen Rechtsgebieten ansässig sind, zu verarbeiten, ohne den Inhalt der Daten ihnen gegenüber offenzulegen. Vor der Übermittlung teilt der Datenexporteur die Daten in solcher Weise auf, dass kein Teil, den einer der Auftragsverarbeiter erhält, ausreichen wird, um die personenbezogenen Daten komplett oder teilweise zu rekonstruieren.

Ein solcher Anwendungsfall ist zulässig, wenn - unter anderem - personenbezogene Daten von einem Datenexporteur auf solche Weise verarbeitet werden, dass sie in zwei oder mehr Teile aufgeteilt werden, wovon keiner mehr ohne die Verwendung zusätzlicher Informationen als einem spezifischen Betroffenen eindeutig zuordnungsfähig betrachtet werden kann und wobei jeder dieser Teile an einen separaten Datenverarbeiter, der in einem anderen Rechtsgebiet ansässig ist, übermittelt wird.

Quelle: KPMG Avocats

Dennoch scheinen zwei der häufigsten Anwendungsfälle nach wie vor unzulässig - trotz der Bemühungen des EDSA zur Milderung der Folgen der Außerkraftsetzung des Privacy Shield

Anwendungsfälle für unzulässige Handlungsweisen

- Anwendungsfall 6: Transfer an Cloud-Dienstleistungsanbieter oder andere Auftragsverarbeiter, die Zugang zu unverschlüsselten Daten benötigen
- Anwendungsfall 7: Fernzugriff auf Daten für geschäftliche Zwecke

Es ist klar erkenntlich, dass die Bemühungen des EDSA zur Milderung der Auswirkungen nur teilweise wirksam sind, da die häufigsten Anwendungsfälle diejenigen sind, die unzulässig sind

Der EDSA bezieht sich auf einen Datenexporteur, der einen Cloud-Dienstleistungsanbieter oder anderen Auftrags-verarbeiter mit der Verarbeitung personenbezogener Daten gemäß seinen Anweisungen in einem Drittland beauftragt.

Ein solcher Fall ist Fall ist unzulässig, da der Cloud-Dienstleistungsanbieter oder andere Auftragsverarbeiter Zugriff auf die unverschlüsselten Daten benötigen, um die ihnen zugewiesene Aufgabe auszuführen, und sofern das Drittland der Empfänger den öffentlichen Behörden eine solche Genehmigung zum Zugriff auf die übermittelten Daten erteilt, die über das in einer demokratischen Gesellschaft als notwendig und angemessen betrachtete Maß hinausgeht.

Der EDSA bezieht sich auf einen Datenexporteur, der personenbezogene Daten an Entitäten in einem Drittland zur Verwendung für gemeinsame Geschäftszwecke zur Verfügung stellt. Das kann ein auf dem Staatsgebiet eines EU-Mitgliedstaats gegründeter Verantwortlicher oder Auftragsverarbeiter sein, der personenbezogene Daten an einen Verantwortlichen oder Auftragsverarbeiter in einem Drittland übermittelt, der derselben Unternehmensgruppe oder einer Gruppe zugehörig ist, die an einer gemeinsamen wirtschaftlichen Tätigkeit beteiligt ist.

Ein solcher Fall ist unzulässig, da der Datenexporteur dem Datenimporteur den direkten Zugriff auf Daten seiner eigenen Wahl erlaubt, indem er sie direkt durch die Nutzung eines Kommunikationsdienstes übermittelt, damit der Importeur die betreffenden unverschlüsselten Daten für seine eigenen Zwecke verwenden kann, insbesondere sofern das Drittland des Importeurs den öffentlichen Behörden eine solche Genehmigung zum Zugriff auf die übermittelten Daten erteilt, die über das in einer demokratischen Gesellschaft als notwendig und angemessen betrachtete Maß hinausgeht

In beiden Szenarien können nicht einmal die Transport-Verschlüsselung und die Data-at-Rest-Verschlüsselung zusammen eine zusätzliche Maßnahme darstellen, um ein im Wesentlichen gleichwertiges Schutzniveau für personenbezogene Daten zu gewährleisten

Quelle: KPMG Avocats

Fazit: Der Erfolg der Maßnahmen des EDSA zur Milderung der Auswirkungen der Außerkraftsetzung des ‚Privacy Shield' – durch sein Instrumentarium – scheint weitgehend relativ, da die verbotenen Anwendungsfälle die häufigsten sind

Wirksamkeit des neuen EDSA-Instrumentariums?

Die Wirksamkeit des neuen Instrumentariums des EDSA ist sehr relativ

- Dies bedeutet, dass die Problematik der Neubetrachtung des anfänglich durch die DSGVO eingeführten Instrumentariums für **alle Transfers personenbezogener Daten aus der EU in Drittländer gilt**, nicht nur in die USA, sondern auch in andere Drittländer, wie beispielsweise das Vereinigte Königreich nach dem Brexit.

Quelle: KPMG Avocats

Fazit: EU-Unternehmen, die als Datenverantwortliche der DSGVO unterliegen, können nicht mehr mit US-Unternehmen oder im Besitz von US-Gesellschaften stehenden EU-Unternehmen zusammenarbeiten

US-Unternehmen

Sie unterliegen einer nationalen Gesetzgebung, die öffentlichen US-Behörden den Zugriff auf in die USA transferierte oder auf US-Staatsgebiet gehaltene personenbezogene Daten erlaubt

Die Übertragung personenbezogener Daten an US-Unternehmen ist in Anbetracht der DSGVO rechtswidrig

EU-Unternehmen im Besitz von US-Unternehmen

Sie unterliegen der US-Gesetzgebung (Cloud Act), aufgrund der Anbieter von elektronischen Kommunikationsdiensten oder Remote-Computing-Services, die sich im Besitz einer US-Gesellschaft befinden, zur Offenlegung personenbezogener Nutzerdaten an die US-Regierung verpflichtet sind, unabhängig davon, ob die Daten sich innerhalb oder außerhalb der USA befinden

Im Besitz einer US-Gesellschaft befindliche EU-Unternehmen werden der US-Regierung mit Wahrscheinlichkeit den Zugriff auf personenbezogene Daten gewähren

In den USA ansässige Entitäten im Besitz von EU-Unternehmen

nur US-Kunden

Für US-Kunden, Besitz, Verwahrung und Kontrolle ihrer personenbezogenen Daten
Cloud Act anwendbar

EU-Datenverantwortlicher kann nicht mehr mit dieser Entität arbeiten

US- und Nicht-US-Kunden

Für Nicht-US-Kunden, Besitz, Verwahrung, Kontrolle ihrer personenbezogenen Daten nur sofern sie praktisch in der Lage sind oder das gesetzliche Recht haben, auf die Kommunikation dieser Daten zuzugreifen

EU-Unternehmen müssen Maßnahmen umsetzen, um den Zugriff auf Daten von Nicht-US-Kunden durch ihre US-Tochtergesellschaften zu verhindern

- **EU-Unternehmen, die als Datenverantwortliche der DSGVO unterliegen, können nicht mehr mit US-Unternehmen, mit im Besitz von US-Gesellschaften stehenden EU-Unternehmen oder mit in den USA ansässigen und im Besitz von EU-Unternehmen befindlichen Entitäten, die einen reinen US-Kundenstamm haben**, zusammenarbeiten, in dem Maße wie die US-Gesetzgebung mit dem DSGVO-Grundsatz des angemessenen Schutzes unvereinbar ist, unabhängig davon, ob die Daten innerhalb oder außerhalb der USA gespeichert sind.

Quelle: KPMG Avocats

Jean-Charles Ferreri

Partner

KPMG Global Strategy Group

Mobilfunk: +33 (0)6 60 07 08 99
jferreri@kpmg.fr

Bertrand Grau

Partner

KPMG Global Strategy Group

Mobilfunk: +33 (1) 55 68 25 10
bertrandgrau@kpmg.fr

Sébastien Ropartz

Partner

KPMG Technology Transformation

Mobilfunk: +33 (1) 55 68 38 83
sropartz@kpmg.fr

Patrick Amouzou

Partner

KPMG Avocats

Mobilfunk: +33 (1) 55 68 51 19
pamouzou@kpmgavocats.fr