



Engagement Made Easy®

Auf dem Weg zur digitalen
Unabhängigkeit:

Die Bedeutung von Datensouveränität.

SOGEDES

Offizieller Content Guru Partner

Überblick

In diesem Whitepaper befassen wir uns mit dem Thema Datensouveränität:

Was Datensouveränität bedeutet, wie sie bereits heute die Entscheidungen von Führungskräften beeinflusst und wie Organisationen ihre Strategien und Systeme unter Berücksichtigung von Datensouveränität gestalten können.

Unsicherheiten verstehen

Mit der zunehmenden Aufmerksamkeit für Datensouveränität sind regulatorische Veränderungen, gerade in der EU, zu erwarten.

57%

der europäischen KMUs sind unsicher, ob ihre Daten **innerhalb der EU gespeichert werden.**²

Risiken minimieren

Stärken Sie die Grundlagen Ihrer ITArchitektur, um die Abhängigkeit von Anbietern außerhalb Ihres Rechtsraums zu reduzieren.

77%

der IT-Entscheider geben an, dass Datensouveränität **wichtiger ist denn je.**¹

Vertrauen priorisieren

Mit der zunehmenden Aufmerksamkeit für Datensouveränität sind regulatorische Veränderungen, gerade in der EU, zu erwarten.

78%

berichten von **einer wachsenden Besorgnis** hinsichtlich der Datensouveränität.²

Unsicherheit wird zur neuen Normalität

Es gibt Jahrzehnte, in denen nichts passiert, und Wochen, in denen sich Jahrzehnte verdichten.

Die Welt bewegt sich rasant; Unsicherheit ist zur Regel geworden. Organisationen, sowohl im öffentlichen als auch im privaten Sektor, müssen gezielt Resilienz aufbauen. Andernfalls laufen sie Gefahr, unter einer Vielzahl externer und beispielloser Schocks zu kollabieren. Die politischen und wirtschaftlichen Entwicklungen der 2020er-Jahre sind geprägt von einem wiedererstarken Nationalismus. Der Nationalstaat ist erneut zur dominierenden Einheit politischer und wirtschaftlicher Organisation geworden. Sein zentrales Leitmotiv ist das Konzept der „Souveränität“.

Souveränität ist ein vielschichtiger und schwer greifbarer Begriff. Im Allgemeinen beschreibt er politische Macht, Unabhängigkeit und die Fähigkeit, im Interesse des Gemeinwohls eigenständig und wirksam zu handeln. Souveränität kann geteilt, eingeschränkt oder sogar vollständig verloren gehen. Starke Staaten versuchen häufig, Souveränität über schwächere Nachbarn zu beanspruchen. Die enge Verbindung von Souveränität mit Nationalismus, Freiheit und der Angst vor Kontrollverlust macht sie zu einem emotional aufgeladenen Konzept. Individuen, Gemeinschaften und Nationen haben im Laufe der Geschichte immer wieder bewusst auf materiellen Wohlstand zugunsten immaterieller Souveränität verzichtet und es ist schwer zu sagen, dass sie damit falsch lagen.

Heute ist Politik digital. Digitale Plattformen bilden die Grundlage dafür, wie Regierungen und Unternehmen Dienstleistungen für BürgerInnen sowie KundInnen bereitstellen. All diese Akti-

vitäten basieren auf enormen Mengen personenbezogener Daten. Um effektive öffentliche Dienstleistungen zu erbringen und überzeugende Kundenerlebnisse zu schaffen, erfassen und speichern öffentliche wie private Akteure hochsensible persönliche Informationen. Diese Daten sind keineswegs politisch neutral. Daten sind ein äußerst mächtiges Instrument und bergen erhebliche Risiken für die Sicherheit und Privatsphäre des Einzelnen. Wo diese Daten gespeichert werden und wer Zugriff darauf hat, sind hochsensible politische Fragen. Genau hier setzt das Konzept der Datensouveränität an.



Was ist Datensouveränität?

Wenn Souveränität politische Macht bedeutet, dann bedeutet Datensouveränität die Kontrolle über Daten. Um als „datensouverän“ zu gelten, muss ein Staat die letztendliche Hoheit über die Daten seiner BürgerInnen haben – also darüber, wo diese Daten gespeichert werden, wie auf sie zugegriffen wird und wer berechtigt ist, sie einzusehen, zu kopieren oder zu nutzen.

Datensouveränität ist besonders herausfordernd, weil sie die Grenzen zwischen öffentlichem und privatem Sektor verwischt und sich über nationale Grenzen hinweg erstreckt. In der Cloud gespeicherte Daten liegen in Rechenzentren auf der ganzen Welt und werden von Organisationen erhoben, verwaltet und genutzt, die ihren Sitz in unterschiedlichsten Ländern haben. Politisch leben wir vielleicht in einer Welt von Nationalstaaten, das Internet jedoch ist global. Daten bewegen sich über Ländergrenzen hinweg und lassen sich nur schwer eingrenzen. Genau diese Dynamik sorgt für zunehmende Verunsicherung. 77 % der IT-Entscheidungsträger im Vereinigten Königreich geben an, dass Datensouveränität heute wichtiger ist als noch vor drei Jahren.¹ Die weltweite Unsicherheit schärft das Bewusstsein für unsere eigene Verwundbarkeit und für die unserer Daten. Mit dem wachsenden Verständnis für Cloud-Technologien steigt auch das Interesse daran, wo Daten gespeichert werden und wer Zugriff darauf hat. Immer mehr Menschen stellen kritische Fragen: In Europa sind sich 57 % der KMU unsicher, ob ihre Anbieter Daten ausschließlich innerhalb der EU speichern.²

In ganz Europa dürfte Datensouveränität zunehmend in den Fokus politischer Aufmerksamkeit rücken. Die Entwicklung fortschrittlicher KI-

Technologien verschärft die Situation zusätzlich: Durch die Verarbeitung enormer Datenmengen und ihre weitreichenden Auswirkungen rückt KI das Thema Datensouveränität noch stärker ins Zentrum der Diskussion. Verschiedenste Beispiele in Deutschland zeigen, wie konkret diese Herausforderungen sind: Selbst bewusst gewählte lokale Cloud-Anbieter können durch Übernahmen unter ausländische Kontrolle geraten. Das verdeutlicht, wie schwierig es ist, Datensouveränität langfristig sicherzustellen.



Souveränität als strategische Priorität

KI ist eine Frage der nationalen Sicherheit. Mit zunehmender Komplexität und Verbreitung wird die Kontrolle über KI-Modelle zu einer zentralen Quelle wirtschaftlicher und politischer Macht und KI-Modelle basieren auf Daten.

Wer Zugriff auf die Daten eines Landes hat, kann daraus zahlreiche strategische Vorteile ziehen. Dies wurde bereits 2018 durch den Cambridge-Analytica-Skandal deutlich: Das britische Beratungsunternehmen nutzte rechtliche Schlupflöcher, um Daten von Millionen Facebook-Nutzern zu sammeln, von denen viele nicht ausdrücklich zugestimmt hatten. Die Daten wurden für Wahlkampagnen, Wähler-Targeting und militärische Desinformationskampagnen genutzt und gelangten teils versehentlich an russische Geheimdienste.³

Wie stark diese Daten politische Ergebnisse beeinflussen haben, ist umstritten. Entscheidend ist, dass der Skandal eine strategische Schwachstelle offenbarte: Staaten hatten die Menge der von privaten Organisationen gesammelten Daten unterschätzt, waren sich der daraus gewonnenen Erkenntnisse nicht bewusst und verfügten nicht über die rechtlichen Rahmenbedingungen, um Datenlecks an unbefugte Akteure zu verhindern. Das Problem war nicht nur die illegale Nutzung der Daten (obwohl das ein Teil des Problems war), sondern das Fehlen eines Rechtsrahmens für die datengetriebene Zukunft.

Deutschland gehört zu den proaktivsten europäischen Ländern im Umgang mit dieser strategischen Schwachstelle. Schleswig-Holstein begann im März 2024, seine 30.000 Beschäftigten von

Microsoft-Produkten auf Open-Source-Lösungen wie LibreOffice, Nextcloud und Thunderbird umzustellen. Bis Mitte 2025 hatten bereits 24.000 Mitarbeitende den Wechsel vollzogen. Die Initiative hatte Vorbildcharakter: Im Juli 2025 gründeten Deutschland, Frankreich, Italien und die Niederlande das European Digital Infrastructure Consortium for Digital Commons, um souveräne digitale Werkzeuge grenzübergreifend zu entwickeln und zu skalieren. Eine Umfrage unter deutschen Führungskräften 2025 zeigte, dass 78 % Deutschland als zu abhängig von US-Cloud-Anbietern ansehen. Dies ist ein deutliches Signal, dass Datensouveränität zunehmend als strategische Priorität verstanden wird.⁴



Vertrauen, Transparenz und die Öffentlichkeit

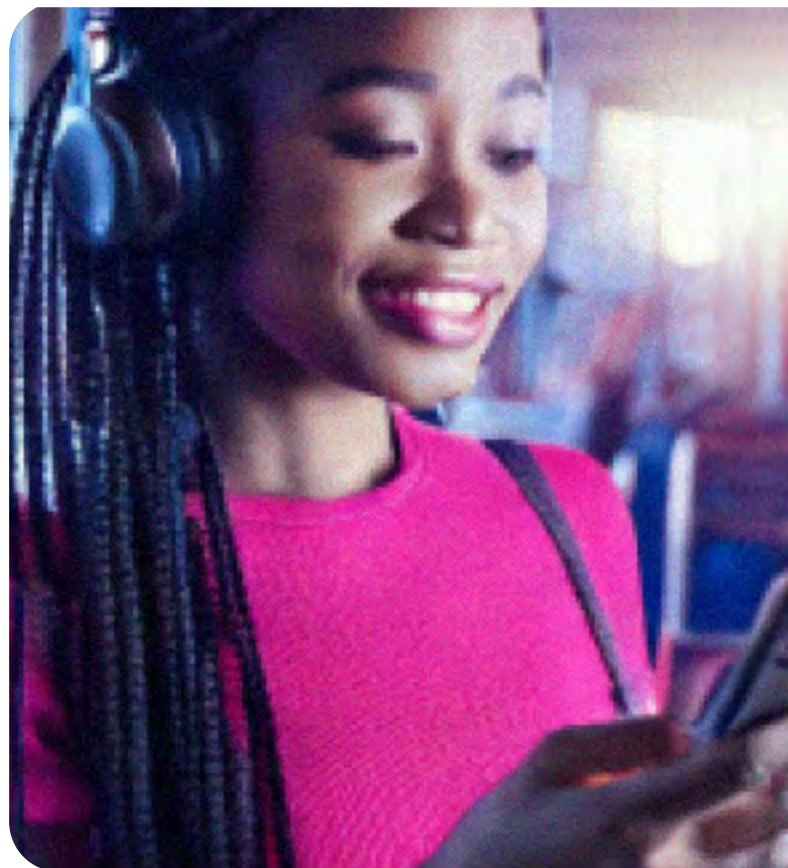
Die nahezu unbegrenzte Sammlung personenbezogener Daten durch Staaten und private Unternehmen ist zu einer bedeutenden Quelle öffentlicher Besorgnis geworden. Bürgerinnen und Bürger sorgen sich darum, wie ihre Daten genutzt werden und von wem – Datenschutzgesetze wie die DSGVO spiegeln dieses Anliegen wider.

Datenpannen ziehen häufig große öffentliche Aufmerksamkeit auf sich und können zu rechtlichen Konsequenzen führen, wie etwa beim britischen Einzelhändler Marks & Spencer im Juni 2025.⁷ Datenschutz ist ein sensibles Thema: Organisationen, die nicht sorgfältig mit persönlichen Daten umgehen, riskieren, das Vertrauen von Bürgern oder Kundinnen und Kunden zu verlieren.

Hier überschneidet sich das Thema Cybersicherheit mit Datensouveränität. Ist unklar, wo und von wem Daten gehalten werden, steigt das Risiko von Datenlecks – etwa dass Daten an Orte gelangen, an denen sie nicht sein sollten, oder in die Hände von unbefugten Akteuren fallen. Besonders kritisch wird es, wenn Daten Grenzen überschreiten und in Jurisdiktionen mit schwächeren Datenschutzvorschriften gelangen, wo ihre Sicherheit leichter gefährdet werden kann. Daten folgen dem „Pfad des geringsten rechtlichen Widerstands“ und bewegen sich schneller, wo weniger Schutz besteht. Ziel der Datensouveränität ist es, die Daten eines Landes bestmöglich abzusichern.

Dabei geht es nicht einfach um „gute“ Regierungen versus „böse“ Cyberkriminelle. Die Grenzen sind nicht klar gezogen. Manche Staaten handeln mit guten Absichten, setzen Daten aber durch

fehlende gesetzliche Rahmenbedingungen unnötigen Risiken aus. Andere handeln möglicherweise böswillig und geben Daten gezielt an geopolitische Rivalen oder kriminelle Akteure weiter. Regierungen müssen ein Mindestmaß an Datensicherheit sicherstellen – ohne Ausnahmen. Unternehmen, die in diesen Jurisdiktionen tätig sind, sollten ihre Datenlösungen so positionieren, dass sie sich in einem sich wandelnden regulatorischen Umfeld nicht angreifbar machen.



Geopolitik und die US-Cloud-Debatte

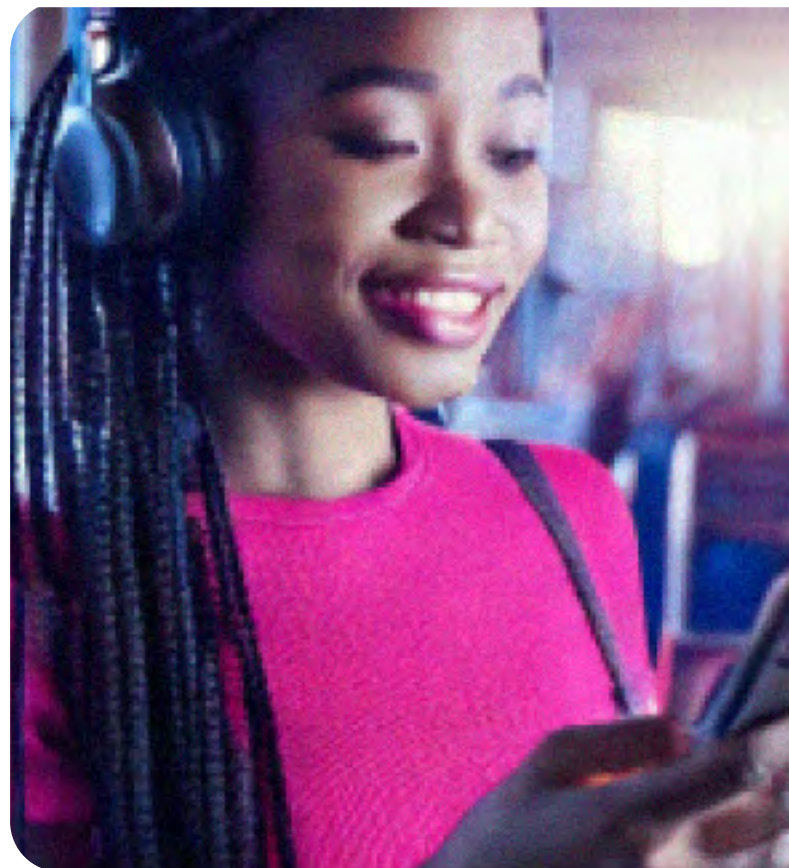
Ein anschauliches Beispiel für diese Unsicherheit kommt aus den USA. Europäische Regierungen und Unternehmen sind auf amerikanische Technologieunternehmen angewiesen, um essenzielle Dienstleistungen bereitzustellen. Dadurch vertrauen europäische Organisationen diesen Firmen sensible Bürger- und Kundendaten an. Die rechtlichen Grundlagen dieser Partnerschaft sind jedoch fragiler, als sie auf den ersten Blick erscheinen.

Der europäische Datenschutz gehört zu den strengsten der Welt, erlaubt aber Datenübertragungen an US-Unternehmen im Rahmen des Trans-Atlantic Data Privacy Framework (TADPF). Dieses Gesetz erlaubt den Transfer von Daten in Länder mit „im Wesentlichen“ gleichwertigen Datenschutzgesetzen.

2017 verabschiedete die US-Regierung den CLOUD Act, der den Behörden Zugriff auf alle Kundendaten von US-Unternehmen gewährt – auch wenn diese Daten nicht US-Bürger betreffen. Damit hat die US-Regierung theoretisch unbegrenzten Zugriff auf die Daten europäischer Bürger, sofern diese bei einem US-Unternehmen gespeichert sind. Das Ergebnis: Die Datenschutzgesetze der EU und der USA sind nicht mehr „im Wesentlichen gleichwertig“.

Das TADPF ist weiterhin gültig, beruht jedoch auf einem internationalen Abkommen. Änderungen in der US-Regierungsstruktur können direkte Auswirkungen auf dieses Abkommen haben. Um den eigenen Datenschutzgesetzen zu entsprechen, könnten europäische Organisationen gezwungen sein, sich vollständig von US-Techno-

logie zu lösen. Solange das TADPF gilt, bleibt der Datentransfer erlaubt und die EU-Kommission unterstützt das Abkommen weiterhin. Dennoch ist das Risiko für ein Worst-Case-Szenario real. Die beste Strategie für europäische Organisationen ist, sich darauf vorzubereiten und für US-Technologien oder Cloud- Dienste Notfallpläne zu entwickeln.⁵



Content Guru: Die einzige CCaaS-Lösung mit Fokus auf Souveränität.

Kunden- und Bürgerkommunikation ist datenintensiv. Sowohl öffentliche als auch private Organisationen sind auf große Mengen personenbezogener Daten angewiesen, um ihre Services zu optimieren, individuell anzupassen und Kunden effektiv zu unterstützen. Die Speicherung und Verarbeitung dieser Daten lässt sich nicht vermeiden. Organisationen haben die Pflicht, diese verantwortungsvoll zu handhaben.

Kundennahe Abläufe sollten innerhalb eines Unternehmens den Standard für Datenschutz setzen. Im Kontext von Datensouveränität bedeutet das: Rechenzentren innerhalb des eigenen Landes, die den Datenschutzgesetzen der jeweiligen rechtlichen Regularien unterliegen und nicht ausländischen Behörden verantwortlich sind.

Europa verfügt über eigene Cloud-Communications-Anbieter und umfangreiches technisches Know-how. Das Ganze ohne potenzielle rechtliche Risiken. Europäische CCaaS-Anbieter können echte Datensouveränität gewährleisten, indem sie europäische Daten „abgrenzen“ und so vor Zugriffen durch fremde Staaten schützen. Europas größter CCaaS-Anbieter, Content Guru, kann dabei höchste Sicherheits- und Souveränitätsstandards garantieren.

Quellen:

1 ITPro.com

2 MovetheNeedle.com

3 Bylinetimes.com

4 wbn.digital

5 itv.com

So werden Sie datensouverän.



Datenlandschaft prüfen – Erfassen Sie, wo die Daten Ihrer Organisation gespeichert sind, wer Zugriff darauf hat und welchen Rechtsräumen sie unterliegen.



Cloudanbieter bewerten – Prüfen Sie, ob kritische Daten bei Anbietern liegen, die ausländischen Zugriffsrechten unterliegen, etwa dem US CLOUD Act.



Inländische Datenspeicherung verifizieren – Stellen Sie sicher, dass Ihre Anbieter Daten ausschließlich innerhalb der Landesgrenzen speichern und nur dem lokalen Datenschutzrecht unterliegen.



Rechtliche Rahmenbedingungen überprüfen – Sorgen Sie dafür, dass Ihre Datenvereinbarungen aktuellen gesetzlichen Vorgaben entsprechen.



Souveränitätsorientierte Anbieter wählen – Bevorzugen Sie Anbieter, die vertraglich Datenspeicherung im eigenen Land garantieren und nicht ausländischen Behörden verpflichtet sind.



<https://www.contentguru.com/de-de/>
+ 49 8105 203 46 10



<https://www.sogedes.com>
+ 49 621 92108 300