Mittelstand-Digital
Zentrum
Chemnitz

NACHGELESEN

Digitale Souveränität für KMU: Rechtliche und technische Grundlagen

INES TACKE & PAVLO MYKYTYN

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages

Digitale Souveränität steht spätestens seit 2020 im **Zentrum der europäischen und nationalen Debatte zur Digitalisierung** (Madiega 2020[1]). Dabei lag der Fokus bei der Digitalen Souveränität zunächst vor allem darauf, sicherzustellen, dass Staaten die Kontrolle über ihre digitalen Prozesse und Daten bewahren, um ihre Innovationskraft und Handlungsfähigkeit im digitalen Wettbewerb zu erhalten (Madiega 2020 [1]). Die Sorge, **zentrale Aspekte der digitalen Infrastruktur an externe Akteure zu verlieren**, berührt bis heute auch die Sicherung europäischer Werte bei derzeitigem digitalem Wandel (Tiedeke 2021[2]; Denga 2022[3]).

Um diese Souveränität zu stärken, wurden (bereits vor 2020) zahlreiche Gesetze und Strategien wie die DSGVO, der Digital Services Act, die Datenstrategie der Bundesregierung (BMDV und BMWK 2023[4]) und der Data Act verabschiedet oder Initiativen wie GAIA-X ins Leben gerufen (Tiedeke 2021[2]). Dennoch bleiben auch weiterhin viele Bereiche der digitalen Welt von internationalen Dienstleistern/Plattformanbietern geprägt (Europäische Kommission 2026b[5]).

Die Sicherstellung der Digitalen Souveränität ist aber nicht alleine eine Frage, die die Europäische Union und ihre Mitgliedstaaten anbetrifft. Sondern sie berührt auch kleine und mittlere Unternehmen (KMU) und wird als Thema gerade dort immer wichtiger (Grün 2024[6]).

In diesem Nachgelesen erfahren Sie,

- welche Bedeutung die Digitale Souveränität für KMU hat,
- welche rechtlichen Anforderungen an die Digitale Souveränität gestellt werden,
- welche Kontrollpunkte der Datenlebenszyklus im Unternehmen bereithält,
- welche strategischen Optionen zum Speichern von Unternehmensdaten bereitstehen und
- wie Cybersicherheit ein wesentlicher Bestandteil der Datenkontrolle darstellt.

Impressum

HERAUSGEBER
Mittelstand-Digital Zentrum Chemnitz
c/o TU Chemnitz
Erfenschlager Str. 73, 09125 Chemnitz
Tel: 0371 531 19935 Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

REDAKTION Bianca Eichler

GESTALTUNG UND PRODUKTION
PUNKT191 – Marketing und Design
www.punkt191.de

BILDNACHWEIS TITEL generiert mi KI
VERÖFFENTLICHUNG Juli 2026

Digitale Souveränität in KMU

Im Zuge der Digitalisierung und zuletzt aufgrund der steigenden Bedeutung von Künstlicher Intelligenz nimmt die Bedeutung der Digitalen Souveränität von KMU zu. Insbesondere ist zu überlegen, wie KMU den Überblick und die Kontrolle über ihren digitalen Schatz der Unternehmensdaten wahren können.

Damit ist nicht das Abschotten gemeint; natürlich sollen Unternehmensdaten künftig auch Teil der modernen Datenwirtschaft werden. Vielmehr geht es bei der Digitalen Souveränität von KMU darum, jederzeit eigenständig (souverän) über die Erhebung, Speicherung, Nutzung und die Weitergabe der eigenen Daten entscheiden zu können.

Mit einem solchen selbstbestimmten Umgang sind mehrere Dimensionen angesprochen:

- Zum einen ist der **Zugang zu Daten** relevant (Veil 2025[7]), insbesondere zu solchen, die KMU beispielsweise als Nutzende von IoT-Geräten selbst generieren oder mitgenerieren.

- Zum anderen bedarf es der Fähigkeit, **den Umgang mit den eigenen Daten zu kontrollieren und zielgerichtet zu steuern**: Wer darf auf Unternehmensdaten zugreifen? Unter welchen Bedingungen können Daten geteilt oder von Partnern genutzt werden?

Die Auseinandersetzung mit diesen Dimensionen ist zentral und notwendig, um die wirtschaftlichen Chancen, die mit der Nutzung, Weitergabe und dem Teilen der Daten verbunden sind, vollständig auszuschöpfen (Hennemann 2025[8]).

Dabei ist zu beachten, dass das Konzept der Digitalen Souveränität nicht mit einem Eigentumsrecht an Daten gleichzusetzen ist. Ein solches Dateneigentum existiert im deutschen Recht nicht (Veil 2026a[9]; Denga 2022[3]). Vielmehr geht es allein um die Entscheidungs- und Kontrollmöglichkeiten, die KMU dazu befähigen, den Wert ihrer Daten selbstbestimmt zu gestalten.

Digitale Souveränität und Rechtsrahmen

Digitale Souveränität, verstanden als ein geordneter Zugang zu den Daten sowie die anschließende Kontrolle über die Datenflüsse, schafft – wie erwähnt – die Grundlage für eine selbstbestimmte Nutzung von Daten. Dabei darf die **Erfüllung rechtlicher Anforderungen**, die sich mit Datenzugang und -fluss befassen nicht unberücksichtigt bleiben.

Bezogen auf den Datenzugang und der -nutzung ist der **Schutz von Geschäftsgeheimnissen sowie weiteren sensiblen Unternehmensinformationen** wie Produktionsdaten, Kundendaten oder strategischem Know-how zu berücksichtigen. Denn wenn Daten von Dritten eingesehen werden können oder gar über cloudbasierte KI-Anwendungen potenziell unkontrolliert verbreitet werden (Alexander 2026[10]), bedeutet das für KMU u. U. ein erhebliches wirtschaftliches Risiko; mitunter verlieren sie über die damit verbundenen unternehmensbezogenen Informationen ihre Existenzgrundlage.

Darüber hinaus bildet das **Datenschutzrecht** einen wichtigen Regulierungsrahmen (Roßnagel 2023[11]). Gerade in Europa gelten strenge Regeln dafür, wie personenbezogene Daten erhoben, gespeichert und verarbeitet werden dürfen. Digitale Souveränität bedeutet an dieser Stelle, dass Unternehmen nachvollziehen und kontrollieren können, wo Daten, für die sie die Verantwortung tragen, erhoben werden, wo sie liegen, wer darauf zugreift und wie sie genau verarbeitet werden. Aus diesem Grund umfasst Digitale Souveränität auch den verantwortungsvollen Umgang mit personenbezogenen Daten.

Digitale Souveränität erschöpft sich dabei nicht nur in der Sicherung von Geschäftsgeheimnissen oder der Abwehr von Schäden für die Privatsphäre, sondern **stellt die Grundlage für eine aktive Gestaltung und Handlungsfähigkeit von KMU in puncto Daten dar**. Denn Digitale Souveränität umfasst eine große Bandbreite ganz unterschiedlicher Daten und Informationen, von personenbezogenen über Maschinendaten und unternehmensbezogene Daten, bis hin zu Geschäftsgeheimnissen oder strategischem Know-How.

Digitale Souveränität ist also gegenüber dem Anwendungsbereich der angesprochenen rechtlichen Rahmenbedingungen – Geschäftsgeheimnisschutz und Datenschutz – wesentlich breiter zu fassen und kumuliert Anforderungen aus den diversen Rechtsgrundlagen.

So bedeutet Digitale Souveränität z.B. die rechtlichen Anforderungen aus dem Datenschutzrecht sicher zu erfüllen und zugleich die eigenen wirtschaftlichen Interessen zu schützen sowie im Hinblick auf die Datenwirtschaft handlungsfähig zu bleiben.

Dreh- und Angelpunkt einer so verstandenen Digitalen Souveränität bildet im Unternehmen daher

- das Erkennen der relevanten Daten,
- die Ausgestaltung des Zugangs zu diesen Daten sowie
- die Kontrolle über deren Nutzung.

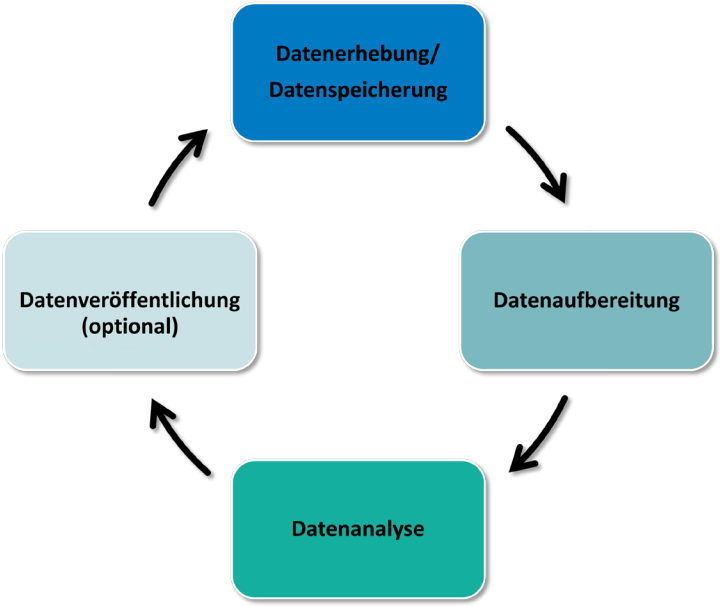

Abbildung 1: Phasen des Daten-Lebenszyklus, nach Müller-Quade, J., Houdeau, D. et al. 2023)

Der Datenlebenszyklus im Unternehmen: Kritische Kontrollpunkte für KMU

Für kleine und mittlere Unternehmen ist ein strukturierter Blick auf den Datenlebenszyklus essenziell, um die Kontrolle über Unternehmensdaten zu behalten und rechtliche Risiken zu minimieren. Gerade entlang der einzelnen Phasen des ‚Datenlebenszyklus' – von der Datenerhebung bis zur Datensekundärnutzung – offenbaren sich typische Stellen, an denen Governance, Datenschutz und unternehmerische Steuerungs- und Gestaltungsfähigkeit ineinandergreifen müssen.

1. Datenerhebung

Der Lebenszyklus beginnt mit der Entstehung von Daten, etwa über Sensoren, Maschinen, Softwareanwendungen oder digitale Interaktionen. Bereits an dieser Stelle sollten sich Unternehmen Klarheit darüber verschaffen, welche Daten konkret erhoben werden und welche Rechte und Pflichten damit verbunden sind.

DATENZUGANG NACH DEM DATA ACT

Das gilt sowohl für Daten, die unmittelbar im Unternehmen selbst vorliegen, als auch für Daten, an deren Generierung das Unternehmen lediglich als Nutzer eines Gerätes oder Dienstes beteiligt ist. Der Data Act (DA) schreibt Nutzern „ihre" Daten zu (Assion und Willecke 2023[12]). Sie haben ein Recht auf Abruf, Einsicht und Nutzung der Daten, die durch ihre Verwendung eines vernetzten Produkts, eines verbundenen Dienstes oder eines Datenverarbeitungsdienstes generiert wurden (Art. 1 Abs. 1 lit. a und Art. 3 Abs. 1 DA). Zu diesen „Nutzern" zählen nach dem DA natürliche oder juristische Personen, die ein vernetztes Produkt besitzen, denen vertraglich zeitweilige Rechte für die Nutzung eines vernetzten Produkts übertragen wurden oder die verbundenen Dienste in Anspruch nehmen (Art. 2 Nr. 12 DA).

Dazu gehören auch KMU. Der Dateninhaber, der über die rechtliche oder tatsächliche Kontrolle der Daten verfügt (z. B. ein großer internationaler Dienstleister oder der Hersteller eines vernetzten Produkts) ist verpflichtet seine Daten dem KMU als Nutzer in einem umfassenden, strukturierten, gängigen und maschinenlesbaren Format bereitzustellen (Art. 3 Abs. 1 DA). Hat beispielsweise nur der Hersteller einer Fabrikmaschine bislang den Zugriff auf die Daten, muss er diese künftig dem nutzenden KMU zur Verfügung stellen, um dort z. B. eine vorausschauende Wartung oder Reparaturen zu ermöglichen oder weitere Innovation auf Grundlage der Daten zuzulassen (ErwGr.32 S. 1 DA) (Veil 2026b[13]; Ziegler und Nagl 2023[14]).

Dabei gilt der DA sowohl für nicht-personenbezogene Industrie- oder Maschinendaten als auch für personenbezogene Daten (Art. 1 Abs. 2 DA). Im letztgenannten Fall ist das Datenschutzrecht zu beachten, weshalb die einschlägigen Rahmenbedingungen, insbesondere die datenschutzrechtliche Zweckbindung nach der DSGVO bei der Erhebung von Daten von Anfang an mitgedacht werden müssen.

ANFORDERUNGEN DER DSGVO AN DIE DATENERHEBUNG

Weisen Daten einen Personenbezug auf, weil eine natürliche Person (ein Mensch) identifiziert oder identifizierbar (der Betroffene) ist, muss das Datenschutzrecht beachtet werden (Art. 4 Nr. 1 DSGVO). Schon die Datenerhebung ist eine datenschutzrechtlich zu beachtende Datenverarbeitung. Für jede Verarbeitung personenbezogener Daten muss die verantwortliche Stelle die Einhaltung der Grundsätze aus Art. 5 DSGVO garantieren. Verantwortlich ist, wer über die Zwecke und Mittel der Datenverarbeitung entscheidet (Art. 4 Nr. 7 DSGVO), mithin bei der Nutzung von Maschinen oder Diensten in aller Regel das KMU, nicht der jeweilige Hersteller oder Anbieter. Bei diesem handelt es sich regelmäßig um einen Auftragsverarbeiten nach Art. 28 DSGVO.

- Die **Rechtmäßigkeit** ist dabei einer der zentralen Datenschutzgrundsätze. Danach muss jede Datenverarbeitung auf einer Rechtsgrundlage beruhen, welche abschließend in Art. 6 DSGVO aufgelistet sind. Hierzu zählen etwa die Einwilligung (Art. 6 Abs. 1 lit. a DSGVO), die Verarbeitung auf Grundlage eines Vertrags (Art. 6 Abs. 1 lit. b DSGVO) oder zur Wahrung der berechtigten Interessen des Verantwortlichen (Art. 6 Abs. 1 lit. f DSGVO).

- Ein weiterer datenschutzrechtlicher Grundsatz ist die **Zweckbindung**, wonach personenbezogene Daten lediglich für zuvor festgelegte, eindeutige und legitime Zwecke erhoben und verarbeitet werden dürfen (Art. 5 Abs. 1 lit. b DSGVO). Werden Daten auf Grundlage einer Einwilligung verarbeitet, ist es daher geboten, die Zweckbindung bereits vorausschauen zu adressieren. Denn ist ein solcher konkreter Verarbeitungszweck vorgesehen, muss dieser in der initialen Rechtsgrundlage für die Datenerhebung/-verarbeitung mitgeteilt werden. Eine Weiterverarbeitung zu Sekundärzwecken ist nur unter den engen Voraussetzungen des Art. 6 Abs. 4 DSGVO oder zu privilegierten Zwecken nach Art. 5 Abs. 1 lit. b DSGVO möglich.

- Neben der Rechtmäßigkeit und der Zweckbindung müssen die **Betroffenenrechte** gewahrt bleiben. Hierzu zählt, dass die Datenverarbeitung dem Betroffenen transparent, etwa im Rahmen einer Datenschutzerklärung, zu kommunizieren ist (mehr zur Datenschutzerklärung lesen Sie in unserem Beitrag: Lesbarkeit von Datenschutzerklärungen) und Anfragen auf Auskunft zeitnah beantwortet werden müssen. Hierfür gilt es, interne Strukturen und Prozesse vorzusehen. Versäumnisse in dieser frühen Phase lassen sich später nur schwer korrigieren und führen häufig zu Compliance-Risiken.

2. Datenaufbereitung

Die erhobenen Rohdaten müssen strukturiert, bereinigt und in technisch verwertbare Formate überführt werden. In dieser Phase kommt der Datenklassifikation eine zentrale Bedeutung zu: Unternehmen sollten systematisch bewerten, welche Daten besonders sensibel, geschäftskritisch oder schützenswert sind. Diese Einordnung bildet die Grundlage für angemessene technische und organisatorische Schutzmaßnahmen beispielsweise nach dem Standard-Datenschutzmodell (DSK 2024[15]) sowie für differenzierte Zugriffs- und Verarbeitungsregeln.

3. Datenanalyse

In der Analysephase wird aus Daten verwertbares Wissen generiert, etwa in Form von Statistiken, Modellen oder Reports. Zunehmend kommen hierbei auch KI-basierte Verfahren

Abbildung 2: Die datenschutzrechtlichen Gewährleistungsziele im Überblick

zum Einsatz. Gerade hier besteht jedoch ein erhöhtes Risiko für Kontrollverlust: Werden externe Analyse- oder KI-Dienste genutzt, insbesondere Cloud-basierte Angebote von Drittanbietern, ist sorgfältig zu prüfen, wo und unter welchen Bedingungen die Daten verarbeitet werden. Ohne entsprechende vertragliche und rechtliche Absicherung kann die Kontrolle über Datenflüsse und -nutzung erheblich eingeschränkt werden.

ANFORDERUNGEN DER DSGVO AN DIE DATENÜBERMITTLUNG IN EIN DRITTLAND

Datenschutzrechtlich kann die Übermittlung von Daten in ein Drittland (nicht EU-Land) brisant sein. Dabei liegt eine Übermittlung nicht nur bei zielgerichteten und absichtlichen Datentransfers vor, sondern schon, wenn eine faktische Zugriffsmöglichkeit aus dem Drittland eingeräumt wird, etwa wenn die Daten im Supportfall auf einem Bildschirm angezeigt werden (EDSA 2023[16]; DSK 2023[17]). Im Rahmen von IT-Anwendungen und -Dienstleistungen erfolgt eine Datenübertragung in Drittstaaten daher häufig unbewusst und unerkannt (Roßnagel 2023[11]).

Liegt eine Übermittlung in ein Drittland vor, sollte geprüft werden, ob ein Angemessenheitsbeschluss vorliegt, in welchem die Europäische Kommission feststellt, dass in dem betreffenden Drittland ein Datenschutzniveau herrscht, das mit dem der DSGVO vergleichbar ist (Art. 45 DSGVO) (hier finden Sie eine übersichtliche Liste der Angemessenheitsbeschlüsse). Für die USA ist dabei die Besonderheit zu beachten, dass der Angemessenheitsbeschluss lediglich für Unternehmen gilt, die sich für bestimmte Datenkategorien haben zertifizieren lassen (hier finden Sie eine Liste der zertifizierten Unternehmen) (Hessel 2023[18]). Grundsätzlich können sodann auf der Grundlage eines Angemessenheitsbeschlusses Daten in dieses, als sicher befundene Drittland übermittelt werden.

Dennoch empfehlen einige Rechtsanwälte, für den Fall, dass ein solcher Angemessenheitsbeschluss – wie in der Vergangenheit häufiger passiert – gekippt wird, zusätzlich Verträge mittels der Standardvertragsklauseln der Europäischen Union abzuschließen (Hessel 2023[18]). Auch die Standardvertragsklauseln (hier können Sie Publikationen der Kommission sowie die Standardvertragsklauseln abrufen) dienen dazu, ein angemessenes Schutzniveau für die Datenverarbeitung im Drittland sicherzustellen.

Grundsätzlich sollte die Übertragung von Daten in Drittländer jedenfalls sorgfältig geprüft, ggf. vertraglich begleitet und diese Prozesse auch dokumentiert werden (EDSA 2021[19]). Zusätzlich zur Sicherstellung der Datenschutzkonformität der Übermittlung und aller weiterer Verarbeitungsschritte, muss der Verantwortliche auch Betroffene darüber informieren, dass die Daten in das Drittland übertragen werden und ob ein Angemessenheitsbeschluss existiert (Art. 13 Abs 1 lit. f DSGVO).

4. Datenveröffentlichung (optional)

Unter bestimmten Voraussetzungen können Daten gezielt geteilt werden, etwa im Rahmen kooperativer Datenräume. Hierfür schafft der Data Governance Act (DGA) einen europäischen Rechtsrahmen. Nach ihm soll die Möglichkeit eröffnet werden, Daten kontrolliert und rechtssicher mit anderen Akteuren zu teilen, ohne die eigenen Rechte vollständig aufzugeben (ErwGr. 3 DGA). Für Branchen wie Industrie oder Gesundheitswesen könnten sich daraus erhebliche Innovationspotenziale ergeben. Allerdings besteht derzeit noch Kritik am DGA und seiner Ausgestaltung, weshalb man hier die Rechtsentwicklung weiter beobachten sollte (Dienst et al. 2026[20]; Schreiber und Schoel[21]; Gummersbach et al. 2026[22]).

5. Datenspeicherung

Die dauerhafte Ablage von Daten einschließlich Backup- und Archivierungslösungen stellt einen weiteren kritischen Schritt im Datenlebenszyklus dar. Der Speicherort und die Wahl des Cloud- oder Infrastrukturanbieters bestimmen nicht nur technische, sondern auch rechtliche Rahmenbedingungen. Werden Daten außerhalb der EU gespeichert oder von nicht-europäischen Anbietern verarbeitet, können zusätzliche Zugriffsmöglichkeiten durch ausländische Behörden entstehen.

Ein prominentes Beispiel ist der “Clarifying Lawful Overseas Use of Data Act”, bekannter unter dem Akronym CLOUD Act, der US-Anbieter unter bestimmten Voraussetzungen verpflichtet, Daten offenzulegen, unabhängig vom tatsächlichen Speicherort. Eine bewusste Standort- und Anbieterentscheidung ist daher zentral zu Erhaltung der eigenen Datensouveränität.

DATENSCHUTZGRUNDVERORDNUNG UND US CLOUD ACT

Der CLOUD Act, verpflichtet US-Telekommunikationsanbieter alle Daten elektronischer Kommunikation auf Antrag zu erfassen, zu speichern und den zuständigen US-Behörden zur Verfügung zu stellen (§ 2713 CLOUD Act). Der Begriff der US-Telekommunikationsanbieter wird dabei weit verstanden und umfasst auch Software-, Cloud und Plattformanbieter sowie Europäische Tochterunternehmen von US-Anbietern (Roßnagel 2023[11]). Da eine Übermittlung von Daten nach dem CLOUD Act unabhängig von internationalen Abkommen ist, steht die Regelung im Konflikt mit Art. 48 DSGVO zu nach dem Unionsrecht nicht zulässige Übermittlungen und Offenlegungen von personenbezogenen Daten (Meyer 2025[23]).

Der Datenlebenszyklus bedeutet mehr als eine rein technische Prozesskette: Er ist ein zentrales Steuerungsinstrument für Rechtssicherheit, Risikominimierung und Wertschöpfung. Wer die kritischen Kontrollpunkte entlang dieses Zyklus kennt und aktiv gestaltet, schafft die Grundlage für einen nachhaltigen und rechtskonformen Umgang mit Unternehmensdaten.

Daher wäre auch eine Herausgabe von Daten nicht mit der DSGVO zu vereinbaren. Der für die Datenverarbeitung Verantwortliche, i. d. R. das KMU, trägt jedoch auch die Verantwortung dafür, nur mit solchen Auftragsverarbeitern zusammenzuarbeiten, die genügend Garantien dafür bieten, dass die Datenverarbeitung im Einklang mit der DSGVO erfolgt (Art. 28 Abs. 1 DSGVO). Zwar wird durchaus vertreten, dass Tochtergesellschaften von US-Unternehmen innerhalb der Europäischen Union europäischem Recht unterliegen und nicht davon auszugehen ist, dass diese Unternehmen einen Rechtsverstoß begehen würden, indem sie sich in einer Art und Weise, die nicht mit der DSGVO zu vereinbaren ist, dem CLOUD Act unterwerfen (Hessel 2023[18]). Dennoch sollte das Risiko nicht gänzlich vernachlässigt und in die Überlegungen zum Cloudanbieter einbezogen werden.

6. Datensekundärnutzung (optional)

Am Ende des Lebenszyklus steht häufig die weitergehende Nutzung vorhandener Datenbestände. Diese sogenannte Sekundärnutzung kann erhebliche wirtschaftliche Potenziale erschließen, etwa durch die Entwicklung datenbasierter Geschäftsmodelle oder den Einsatz für das Training eigener KI-Systeme. Voraussetzung ist jedoch, dass rechtliche Grenzen wie Nutzungsrechte oder der ursprüngliche Erhebungszwecke (Einwilligung und Zweckbindung) beachtet werden.

Cloud oder eigene Infrastruktur: Strategische Optionen für KMU

Die Speicherung von Unternehmensdaten auf eigener Infrastruktur bietet zweifellos ein Höchstmaß an unmittelbarer Kontrolle. Für viele KMU ist dieses Modell jedoch angesichts steigender Anforderungen an Skalierbarkeit, Verfügbarkeit und Innovationsgeschwindigkeit nur begrenzt zu realisieren.

Cloud & cloudbasierte KI-Anwendungen: Chancen und Risiken

Cloud-Lösungen haben sich daher als Standard etabliert, auf die unternehmensseitig zugegriffen wird. Dies birgt allerdings auch Nachteile. Häufig werden Daten in **global verteilten Infrastrukturen** verarbeitet, deren rechtliche und technische Schutzmechanismen stark variieren. Insbesondere rechtliche Rahmenbedingungen außerhalb der EU können dazu führen, dass externe Akteure auf Unternehmensdaten zugreifen dürfen. Für KMU ergibt sich daraus eine strategisch relevante Abwägung zwischen technologischer Leistungsfähigkeit und rechtlicher Kontrolle.

Viele Unternehmen stehen vor der Entscheidung auf Hyperscaler mit der Fähigkeit zur flexiblen Beantwortung der Nachfrage (Powell und Smalley 2024[24]), wie Amazon Web Services, Microsoft Azure oder Google Cloud zu setzen, die durch Funktionsumfang und Skalierbarkeit überzeugen, oder auf **europäische Alternativen**. Anbieter wie

- Open Telekom Cloud
- IONOS
- STACKIT oder
- gridscale

gewinnen in diesem Kontext zunehmend an Bedeutung. Auch von Seite der Europäischen Union wird dieser Trend unterstützt. Der **‚Cloud and AI Development Act Entwurf'** (CADA-E)(Europäische Kommission 2026a[25]) soll die technologische Souveränität in der Europäischen Union bezogen auf Cloud-Lösungen und KI stärken, beispielsweise durch sogenannte „Cloud and AI Leadership Initiatives" (Art. 3 ff. CADA-E) und „Data centre acceleration zones" (Art. 10 ff. CADA-E). Ziel ist, die Rechenkapazität sowie die Entwicklung und den Einsatz von KI in der EU zu steigern und Bedenken hinsichtlich der Datenhoheit und der Betriebskontinuität von Cloud- und KI-Diensten auszuräumen (S. 2 CADA-E). Einen weiteren Baustein zur Erreichung dieses Ziels bilden die avisierten **neuen Sicherheitsvorgaben für den öffentlichen Sektor bei der Nutzung von Cloud-Diensten**. Vorgeschlagen ist die Einteilung von Diensten in vier Sicherheitsstufen (Anhang 2 CADA-E):

1. Daten werden in einer Infrastruktur innerhalb der Union verarbeitet und gespeichert.

2. Anbieter müssen ihre Unabhängigkeit von Drittländern sowie Transparenz hinsichtlich ihrer Software-Lieferkette nachweisen (kein Zugriff auf Daten durch Drittstatten).

3. Anbieter müssen sich im Besitz der EU befinden und von dieser kontrolliert werden sowie zusätzliche Kriterien erfüllen, beispielsweise hinsichtlich der Staatsangehörigkeit ihrer Mitarbeiter. (Die Kommission kann Anbieter aus Drittländern anerkennen.)

4. Anbieter verfügen über vollständige Transparenz und Kontrolle über ihre Software-Lieferkette und unterliegen keinerlei Einmischung durch ein Drittland.

Je nach Risikobewertung müssen öffentliche Stellen zukünftig einen Dienst der zuvor zugeordneten Risikostufe auswählen. Dabei ist ein Ausschluss von Anbietern aus Drittstaaten auch für den öffentlichen Bereich nicht gänzlich vorgesehen.

Cloudbasierte KI-Modelle haben sich in kurzer Zeit zu einem leicht zugänglichen und leistungsfähigen Werkzeug für Unternehmen entwickelt. Anwendungen wie ChatGPT, Gemini, Microsoft Copilot oder auch europäische Ansätze wie Mistral AI zeigen, wie niedrig die Einstiegshürden für den Einsatz generativer KI mittlerweile sind (Singh und Namin 2025[26]).

Für KMU ergeben sich daraus zunächst klare betriebliche Vorteile: Cloud-KI ist unmittelbar verfügbar, meist direkt über den Browser nutzbar und erfordert keine eigene Infrastruktur. Die zugrunde liegenden Modelle werden kontinuierlich durch die Anbieter weiterentwickelt, sodass Unternehmen automatisch von technologischen Fortschritten profitieren. Gleichzeitig greifen diese Systeme auf hochskalierte Rechenzentren zu, wodurch auch komplexe Analysen und Anwendungen ohne eigene Investitionen in Hardware möglich werden.

Diesen Vorteilen stehen jedoch strukturelle Risiken gegenüber, die insbesondere aus rechtlicher und strategischer Sicht relevant sind (Schneider 2025[27]). Generative KI-Systeme sind in hohem Maße datengetrieben. Ein zentraler Aspekt ist damit der Verlust an Kontrolle über Daten durch deren Abfluss. Sobald sensible Informationen in Cloud-KI-Systeme eingegeben werden, verlassen sie die unmittelbare Sphäre des Unternehmens und werden auf externen Servern verarbeitet.

Insbesondere bei frei zugänglichen Cloud-KI-Dienste, etwa ChatGPT, Gemini oder Microsoft Copilot gilt, dass Inhalte, die Nutzer eingeben oder hochladen, vom Anbieter zur Weiterentwicklung und zum Training der zugrunde liegenden Modelle verwendet werden (Mykytyn[28]). Auch bei kostenpflichtigen Varianten ist diese Praxis häufig zumindest teilweise vorgesehen.

Zwar bieten viele Anbieter inzwischen Einstellungsoptionen, um die Nutzung von Eingaben für Trainingszwecke zu deaktivieren, jedoch erfordert dies eine bewusste Konfiguration durch das Unternehmen. Zudem werden Nutzungsdaten und Interaktionen in der Regel zumindest temporär auf den Servern der Anbieter gespeichert. Problematisch wird es insbesondere dann, wenn keine klaren vertraglichen Regelungen zur Datennutzung bestehen. In solchen Fällen droht ein Verlust von Verwertungsrechten oder eine unkontrollierte Weiterverwendung der Daten, etwa für andere Projekte oder sogar für KI-Trainingszwecke. Geschäftsgeheimnisschutz greift nur, wenn angemessene Schutzmaßnahmen nachweisbar umgesetzt wurden (MDZC 2026[29]). Unternehmen müssen also aktiv belegen können, dass sie ihre sensiblen Informationen organisatorisch, technisch und vertraglich abgesichert haben.

Zur Stärkung der Kontrolle über Unternehmensdaten und Geschäftsgeheimnisse lassen sich mehrere zentrale Hebel identifizieren:

- Bewusste Systemauswahl: Kritische Daten sollten bevorzugt in kontrollierten Umgebungen verarbeitet werden, etwa durch lokale KI-Modelle oder vertrauenswürdige Infrastrukturen.

- Klare Vertragsgestaltung: Vereinbarungen mit Dienstleistern sollten präzise Regelungen zu Vertraulichkeit, Nutzungsrechten, Zweckbindung und Dauer der Datennutzung enthalten.

- Technische Schutzmaßnahmen: Zugriffskontrollen, Verschlüsselung und Monitoring helfen, unbefugten Zugriff und Datenabflüsse zu verhindern.

- Organisatorische Sensibilisierung: Mitarbeitende müssen verstehen, welche Daten sensibel sind und wie sie mit KI-Systemen umzugehen haben.

Hinzu kommt u. U. die datenschutzrechtliche Dimension. Auch wenn die technische Verarbeitung durch einen externen Dienstleister als Auftragsverarbeiter erfolgt (Rätze 2026[30]), liegt die datenschutzrechtliche Verantwortung weiterhin beim Unternehmen selbst (Tacke 2025[31]).

Ein weiterer kritischer Faktor ist die Abhängigkeit von einzelnen Anbietern. Cloud-KI-Dienste sind häufig tief in bestehende Prozesse integriert. Preisänderungen, Anpassungen der Nutzungsbedingungen oder Ausfälle können daher unmittelbare Auswirkungen auf betriebliche Abläufe haben (Lang et al. 2026[32]). Gleichzeitig erschweren proprietäre Systeme und fehlende Standardisierung einen späteren Wechsel des Anbieters.

Viele, auch europäische, Cloud-Plattformen basieren auf proprietären Technologien, die zu sogenannten Vendor-Lock-ins führen können (Denga 2026[33]). Das bedeutet, dass ein späterer Wechsel des Anbieters technisch aufwendig, wirtschaftlich teuer oder faktisch kaum umsetzbar ist. Für KMU entsteht dadurch ein strukturelles Risiko, insbesondere wenn sich regulatorische, wirtschaftliche oder sicherheitsrelevante Rahmenbedingungen ändern.

Ein Ansatz zur Reduzierung dieser Abhängigkeiten liegt im **Einsatz von Open-Source-Technologien** und offenen Standards (Schöttle 2026[34]). Lösungen wie

- Nextcloud
- Kopano oder
- Seafile

ermöglichen eine höhere Kontrolle über Daten und Systemarchitektur sowie eine bessere Portabilität zwischen verschiedenen Infrastrukturen. Gleichzeitig reduzieren sie die Abhängigkeit von einzelnen Anbietern.

In der Praxis zeigt sich jedoch, dass eine vollständige Migration auf selbst betriebene Open-Source-Infrastrukturen für viele KMU weder wirtschaftlich noch organisatorisch sinnvoll ist. Stattdessen setzen sich hybride Ansätze durch (Rauscher 2026[35]). Kritische oder besonders schützenswerte Daten werden lokal oder in kontrollierten Umgebungen gehalten, während weniger sensible Daten und Anwendungen in skalierbaren Cloud-Infrastrukturen betrieben werden.

Exit-Strategien als Hebel für mehr unternehmerische Flexibilität

Um das oben genannten Risiko des Vendor-Lock-ins zu adressieren, entwickelt sich die Fähigkeit, Daten zwischen Systemen und Anbietern zu übertragen sowie Cloud-Dienste im Bedarfsfall verlassen zu können, zunehmend zu einem zentralen Steuerungsfaktor für KMU.

Aktuelle Studien und Umfragen zeigen jedoch eine deutliche Diskrepanz: Während über 90 % der KMU die Kontrolle über ihre Daten als strategisch wichtig einschätzen, verfügen nur rund 20 % über eine belastbare, operationalisierte Strategie zur Sicherstellung dieser Kontrolle (Jung 2025[36]).

Für rund die Hälfte aller deutschen Cloud-Nutzer ist die Speicherung in Deutschland oder der EU entscheidend (Redaktion ZD 2025[37]).

Die tatsächliche Kontrolle über Daten zeigt sich häufig erst beim Versuch, einen Cloud-Anbieter zu wechseln. Somit sind Exit-Strategien von zentraler Bedeutung und sollten nicht als nachgelagerte Überlegungen behandelt werden, sondern als integraler Bestandteil jeder Cloud- und Datenstrategie.

Einen z**entralen rechtlichen Rahmen für Exit-Strategien schafft der europäische Data Act**, der auch darauf abzielt, die Abhängigkeit von einzelnen Anbietern zu reduzieren und die Beweglichkeit von Unternehmen im digitalen Raum zu stärken (Denga 2026[33]; Schöttle 2026[34]).

Der Anwendungsbereich des Data Act ist bewusst weit gefasst. Er greift immer dann, wenn Datenverarbeitungsdienste innerhalb der Europäischen Union angeboten werden. Damit sind nicht nur europäische Anbieter adressiert, sondern auch internationale Cloud-Anbieter, die ihre Leistungen auf dem EU-Markt bereitstellen.

Unter den viel kritisierten (Zikesch et al. 2026[38]; Siglmüller und Żdanowiecki 2025[39]) Begriff der ‚Datenverarbeitungsdienste' fällt dabei eine breite Palette digitaler Leistungen, insbesondere auch Cloud-Computing Dienste wie (ErwGr. 81 KI-VO):

- Infrastructure-as-a-Service (IaaS),
- Platform-as-a-Service (PaaS) und
- Software-as-a-Service (SaaS).

Für die beschriebenen Anwendungsfelder hält der Data Act unter anderem konkrete Verpflichtungen für Anbieter vor, bestehende Wechselbarrieren systematisch abzubauen (Kap. 6 Data Act). Dazu zählen sowohl vorkommerzielle, gewerbliche, technische, vertragliche als auch organisatorischen Hindernisse, die in der Vergangenheit häufig zu Vendor-Lock-ins geführt haben (Art. 23 Data Act). Anbieter sind unter anderem verpflichtet (Art. 23 Data Act):

- den Wechsel zwischen verschiedenen Cloud-Diensten zu erleichtern,
- die parallele Nutzung mehrerer Anbieter zu ermöglichen sowie
- den Rückzug auf eigene IT-Infrastrukturen (On-Premises) nicht unnötig zu erschweren.

Für KMU bedeutet dies eine substanzielle Stärkung ihrer Verhandlungs- und Handlungsspielräume insbesondere gegenüber marktstarken Anbietern.

Gleichzeitig bleibt aber festzuhalten: Der Data Act schafft die rechtlichen Voraussetzungen, ersetzt jedoch nicht die praktische Umsetzung im Unternehmen. Technische Architekturentscheidungen, Datenformate, Schnittstellen und vertragliche Ausgestaltungen (Sattler 2024[40]) bleiben entscheidend dafür, ob ein Anbieterwechsel tatsächlich reibungslos möglich ist. Aus diesem Grund sollten Transition-Support-Klauseln in Verträge mit Anbietern aufgenommen werden, die insbesondere weiter verarbeitbare Datenformate sowie die Definition relevanter Schnittstellen beinhalten (Schöttle 2026[34]).

Lokale KI-Modelle: Kontrolle, Flexibilität und operative Herausforderungen für KMU

Neben cloudbasierten KI-Lösungen rückt zunehmend lokal betriebene KI in den Fokus von KMU, die sich über standardisierte Schnittstellen wie das Model Context Protocol (MCP) an unternehmenseigene Werkzeuge und Datenquellen anbinden und mittels Retrieval-Augmented Generation (RAG) mit internem Wissen anreichern lassen (Romero Mateos und Zenner[41]). Dabei werden Modelle nicht über externe Anbieter genutzt, sondern direkt auf der eigenen Infrastruktur betrieben, etwa auf Unternehmensservern oder leistungsfähigen Arbeitsplatzrechnern. Technologische Fortschritte wie Quantisierungsverfahren zur Reduktion des Ressourcenbedarfs sowie effizientere Inferenz-Engines und Werkzeuge wie Llama.cpp oder Plattformen wie Ollama und LM Studio haben diese Option in den letzten Jahren deutlich zugänglicher gemacht (mehr zur Auswahl lokaler Modelle lesen Sie in dem Beitrag Cloud-KI versus lokale-KI: Leistung und Datenkontrolle) (Mykytyn[28]).

Der größte Vorteil dieses Ansatzes liegt in der **vollständigen Kontrolle über Daten**. Sämtliche Eingaben und Verarbeitungsschritte verbleiben innerhalb des Unternehmens und der eigenen IT-Infrastruktur. Hierdurch werden Risiken im Zusammenhang mit externem Zugriff oder Drittstaatentransfers erheblich reduziert, was insbesondere im Hinblick auf Datenschutz (DSK 2025 [42]) und Vertraulichkeit sensibler Unternehmensinformationen oder Geschäftsgeheimnisse von zentraler Bedeutung ist (MDZC 2026[29]; Tacke 2026[43]).

Diesen Vorteilen lokaler KI stehen jedoch nicht unerhebliche Herausforderungen gegenüber. Der Betrieb lokaler KI-Modelle erfordert technisches Know-how sowie eigene Ressourcen für Installation, Betrieb und Wartung (Schöttle 2026[34]). Insbesondere für KMU ohne ausgeprägte IT-Abteilungen kann dies eine Hürde darstellen. Hinzu kommen Hardware-Anforderungen, die je nach Modell und Anwendungsfall beträchtlich sein können (Vaziri 2026[44]). Leistungsfähige CPUs oder GPUs, ausreichend Arbeitsspeicher sowie geeignete Infrastruktur sind notwendig, um eine stabile und performante Nutzung zu gewährleisten (Mykytyn[28]).

Schließlich bestehen auch funktionale Grenzen. Lokale Modelle erreichen derzeit häufig noch nicht das Leistungsniveau großer, cloudbasierter Systeme, die auf massiv skalierter Infrastruktur trainiert und betrieben werden. Dies kann insbesondere bei komplexen oder sehr datenintensiven Anwendungen relevant sein.

Lokale KI-Modelle bieten KMU eine attraktive Möglichkeit, Kontrolle, Datenschutz und Unabhängigkeit zu stärken. Gleichzeitig erfordern sie jedoch Investitionen in Infrastruktur und Know-how. In der Praxis wird daher häufig ein hybrider Ansatz verfolgt, bei dem sensible Anwendungsfälle lokal umgesetzt werden, während weniger kritische Prozesse weiterhin über leistungsfähige Cloud-Dienste laufen (Rauscher 2026[35]).

Die Wahl zwischen Cloud und eigener Infrastruktur sowie zwischen proprietären und Open-Source-KI-Lösungen ist mehr als eine technische Entscheidung: Sie bestimmt maßgeblich den Grad an Kontrolle, Datensouveränität, Flexibilität und Abhängigkeit.

Cybersicherheit als Bestandteil der Datenkontrolle im KMU

Mit der zunehmenden Digitalisierung geraten auch KMU verstärkt ins Visier von Cyberangriffen. Cybersicherheit ist daher kein isoliertes IT-Thema, sondern ein zentraler Bestandteil jeder Strategie zur Sicherung der Kontrolle über Unternehmensdaten und damit der Digitalen Souveränität (Außendorf und Evran 2024[45]). Denn der Verlust von Datenkontrolle erfolgt nicht nur durch bewusste Weitergabe oder externe Dienstleister, sondern ebenso durch unbefugte Zugriffe von außen, etwa durch Ransomware, Phishing oder gezielte Angriffe auf IT-Systeme. **Der Schutz der eigenen Daten muss daher ganzheitlich gedacht werden und sowohl technische als auch organisatorische Maßnahmen umfassen.**

Ein zentraler Baustein ist eine **strukturierte Backup-Strategie** (Ruoff 2016[46]), insbesondere nach der sogenannten 3-2-1-Regel (Richter 2025[47]]). Unternehmen sollten mindestens drei Kopien ihrer wichtigsten Daten vorhalten, diese auf zwei unterschiedlichen Speichermedien sichern (z. B. lokale Datenträger und Cloud) und eine Kopie räumlich getrennt sowie idealerweise offline lagern. Entscheidend ist zudem, dass Backups nicht nur erstellt, sondern auch regelmäßig getestet werden. Im Ernstfall, etwa bei Ransomware-Angriffen, Hardwareausfällen oder Diebstahl, entscheidet die Funktionsfähigkeit der Backups darüber, ob ein Unternehmen handlungsfähig bleibt.

Ein weiterer kritischer Faktor ist die **Absicherung von Zugängen** (Spieker und Eichstädt 2024[48]). Schwache, mehrfach verwendete oder geteilte Passwörter zählen zu den häufigsten Einfallstoren für Angriffe. Der Einsatz von starken Passwörtern in Kombination mit Zwei-Faktor-Authentifizierung stellt hier einen grundlegenden Schutzmechanismus dar (BSI[49]).

Gleichzeitig zeigt die Praxis, dass der Mensch oft die größte Angriffsfläche ist. Ein erheblicher Teil aller Cyberangriffe beginnt mit Phishing-E-Mails oder Social-Engineering-Methoden(Weber 2024[50]). Gerade in KMU, in denen Arbeitsprozesse häufig auf Vertrauen basieren, nutzen Angreifer gezielt täuschend echte auch KI-generierte E-Mails, gefälschte Rechnungen oder vermeintliche Anweisungen von Vorgesetzten. Daher ist die **Sensibilisierung von Mitarbeitenden** ein wesentlicher Bestandteil der Sicherheitsstrategie. Schulungen und klare Verhaltensrichtlinien helfen, Risiken frühzeitig zu erkennen und Fehler zu vermeiden.

Daneben stellen eine ganze Reihe von Gesetzen wie der Cyber Resilience Act (CRA) oder die NIS2-Richtlinie (Wäsche 2025[51]) Anforderungen an die Unternehmen, um die Cybersicherheit und damit auch die effektive Souveränität zu stärken (Schöttle 2026[34]).

Cybersicherheit ist eine Grundvoraussetzung für die Kontrolle über Unternehmensdaten. Technische Maßnahmen wie Backups und Zugriffsschutz greifen nur dann effektiv, wenn sie durch organisatorische Prozesse und geschulte Mitarbeitende ergänzt werden. Datensicherheit beginnt daher nicht erst bei der IT, sondern ist eine unternehmensweite Aufgabe.

Fazit: Datensouveräne Cloud- und KI-Nutzung als strategische Aufgabe für KMU

Für KMU zeigt sich zunehmend, dass die Kontrolle über Unternehmensdaten nicht allein von der Wahl zwischen Cloud oder eigener Infrastruktur abhängt, sondern maßgeblich von der **bewussten Gestaltung der Nutzung**. Weder Cloud-Dienste noch KI-Anwendungen führen per se zum Verlust der Datenkontrolle. Entscheidend ist, wie sie eingesetzt, abgesichert und vertraglich begleitet werden. Verträge mit Cloud- und IT-Dienstleistern sind ein wesentliches Instrument zur Sicherung der eigenen Handlungsfähigkeit. Dabei ist besonders die Kernfrage der Exit-Strategien zu adressieren, d.h. es müssen klare Regelungen zur Datenlöschung, Datenrückgabe und zum Anbieterwechsel vereinbart werden.

Im Fall der Verarbeitung personenbezogener Daten liegt die Herausforderung in der **Berücksichtigung datenschutzrechtlicher Rahmenbedingungen** bei der Cloud-Nutzung. Der physische Speicherort von Daten ist nicht automatisch gleichbedeutend mit der anwendbaren Rechtsordnung. Daher empfiehlt es sich, bevorzugt Anbieter mit **Sitz in der Europäischen Union** zu wählen und gleichzeitig hybride Ansätze zu verfolgen. In lokalen KI-Anwendungen können personenbezogene Daten, sensible Unternehmensdaten oder Geschäftsgeheimnisse in kontrollierten Umgebungen verbleiben, während weniger kritische Anwendungen von der Skalierbarkeit der Cloud profitieren. Ergänzend dazu ist **Cybersicherheit** ein unverzichtbarer Bestandteil der Datenkontrolle. Maßnahmen wie starke Passwörter, Zwei-Faktor-Authentifizierung sowie regelmäßige Backups nach der 3-2-1-Regel bilden die Grundlage. Ebenso entscheidend ist die Sensibilisierung von Mitarbeitenden, da viele Angriffe auf menschliche Schwachstellen abzielen.

Insgesamt ist Datensouveränität im Unternehmen kein statischer Zustand, sondern das **Ergebnis strategischer Entscheidungen, technischer Maßnahmen und dem Befolgen klarer rechtlicher Rahmenbedingungen**. KMU, die Cloud- und KI-Nutzung bewusst gestalten, Anbieter gezielt auswählen und ihre vertraglichen sowie organisatorischen Grundlagen frühzeitig definieren, können ihre Daten nicht nur schützen, sondern auch gezielt und wirtschaftlich nutzen – sie werden digital souverän.

Literaturverzeichnis

1 Madiega, Tambiama (2020): Digital sovereignty for Europe. BRIEFING, EPRS Ideas Paper. Towards a more resilient EU. Online verfügbar unter https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf.

2 Tiedeke, Anna Sophia (2021): Die (notwendige) relativität digitaler Souveränität. Kritische Reflexionen zu einem zentralen und umstrittenen Konzept im digitalen Zeitalter. In: MMR, S. 624–628.

3 Denga, Michael (2022): Digitale Souveränität durch Datenprivatrecht. In: GRUR, 1113-1120.

4 BMDV; BMWK (Hg.) (2023): Fortschritt durch Datennutzung. Strategie für mehr und bessere Daten für neue, effektive und zukunftsweisende Datennutzung. Online verfügbar unter https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2023/datenstrategie.html, zuletzt geprüft am 12.05.2026.

5 Europäische Kommission (2026b): Supervision of the designated very large online platforms and search engines under DSA. Online verfügbar unter https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses, zuletzt geprüft am 08.05.2026.

6 Grün, Oliver (2024): Digitale Souveränität „Made in Germany" – der IT-Mittelstand als Motor für selbstbestimmte Digitalisierung. In: MMR, S. 739–740.

7 Veil, Winfried (2025): Wende in der Datenpolitik? In: ZGI, 81-82.

8 Hennemann, Moritz (2025): XIV: Datenwirtschaft. 140. Einleitung zur Datenwirtschaft. C. Datensouveränität, Datenhoheit, Datenmacht. In: Christoph Herrmann, Marian Niestedt und Patrikatrik Abel (Hg.): EU-Außenwirtschafts- und Zollrecht. München: C.H. Beck, Rn. 13 ff.

9 Veil, Winfried (2026a): DA Art. 1. In: Heinrich Amadeus Wolff, Stefan Brink und Antje v. Ungern-Sternberg: BeckOK Datenschutzrecht. DS-GVO, DA, DGA, BDSG. Datenschutz und Datennutzung, Stand: 01.02.2025. 55. Edition. München: C.H. Beck, Rn. 39–41.

10 Alexander, Christian (2026): § 2. In: Helmut Köhler und Jörn Feddersen: Gesetz gegen den unlauteren Wettbewerb. Beck'sche Kurz-Kommentare. 44. Aufl.: C.H. Beck, Rn. 88d.

11 Roßnagel, Alexander (2023): Digitale Souveränität im Datenschutz. Voraussetzungen für die Umsetzung datenschutzrechtlicher Anforderungen. In: MMR, S. 64–68.

12 Assion, Simon; Willecke, Lukas (2023): Der EU Data Act. Die neuen Regelungen zu vernetzten Produkten und Diensten. In: MMR, 805-810.

13 Veil, Winfried (2026b): DA Art. 1. In: Heinrich Amadeus Wolff, Stefan Brink und Antje v. Ungern-Sternberg: BeckOK Datenschutzrecht. DS-GVO, DA, DGA, BDSG. Datenschutz und Datennutzung. 55. Edition. München: C.H. Beck.

14 Ziegler, Nicolas; Nagl, Sebastian (2023): Zugang zu Industriedaten für KMU. Gleichzeitig eine rechtliche und technische Analyse des Entwurfs des Data Acts als KMU-Instrument. In: ZfDR, S. 57–86.

15 DSK (2024): Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewahrleistungsziele. Version 3.1. Hg. v. AK Technik der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Online verfügbar unter https://www.datenschutzkonferenz-online.de/media/ah/SDM-Methode-V31.pdf, zuletzt aktualisiert am 14.05.2024, zuletzt geprüft am 31.05.2026.

16 EDSA (2023): Leitlinien 5/2021 über das Zusammenspiel zwischen der Anwendung des Artikels 3 und der Bestimmungen über internationale Übermittlungen nach Kapitel V DSGVO. Version 2.0. Online verfügbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052021-interplay-between-application-article-3_en, zuletzt geprüft am 12.05.2026.

17 DSK (2023): Übermittlung personenbezogener Daten aus Europa an die USA. Anwendungshinweise zum Angemessenheitsbeschluss der Europäischen Kommission zum Datenschutzrahmen EU⊠USA (EU⊠US Data Privacy Framework) vom 10. Juli 2023. Hg. v. DSK. Online verfügbar unter https://www.datenschutzkonferenz-online.de/media/ah/230904_DSK_Ah_EU_US.pdf, zuletzt geprüft am 12.05.2026.

18 Hessel, Stefan (2023): Der neue Angemessenheitsbeschluss für Datenübermittlungen in die USA. In: NJW, S. 2969–2973.

19 EDSA (Hg.) (2021): Empfehlungen 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten. Online verfügbar unter https://www.edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_de.

20 Dienst, Sebastian; Hartl, Korbinian; Vogel, Paul (2026): Internationale Datentransfers im neuen Datenrecht. Vergleich der Regelungen von Data Act, DGA und DS-GVO. In: ZD, 10-16.

21 Schreiber, Kristina; Schoel, Philipp: Data Governance Act: Mehr Daten für Legal Tech-Anwendungen? In: LTZ, 3-8.

22 Gummersbach, Lina; Chan, Noemi Aguirre; Molnár-Gábor, Fruzsina (2026): Vertrauenswürdige Datentreuhänder? Datenschutzrechtliche Anforderungen für die neuen Akteure in der Netzwerkmedizin auf dem Prüfstand. In: ZfDR, 103-129.

23 Meyer, Sebastian (2025): § 51. Internationales Datenschutzrecht. In: Michael Martinek, Franz-Jörg Semler und Eckhard Flohr (Hg.): Handbuch Vertriebsrecht. 5. Aufl.: C.H. Beck; Helbing Lichtenhahn.

24 Powell, Phill; Smalley, Ian (2024): Was ist ein Hyperscale-Rechenzentrum? Hg. v. IBM Think. Online verfügbar unter https://www.ibm.com/de-de/think/topics/hyperscale-data-center.

25 Europäische Kommission (2026a): COM(2026) 502 final. 2026/0138 (COD). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing a framework of measures for strengthening Europe's cloud and AI ecosystem (Cloud and AI Development Act). Brüssel.

26 Singh, Sonali Uttam; Namin, Akbar Siami (2025): A survey on chatbots and large language models: Testing and evaluation techniques. In: Natural Language Processing Journal 10, S. 100128. DOI: 10.1016/j.nlp.2025.100128 .

27 Schneider, Udo (2025): Viele KI-Risiken sind Datenschutzrisiken. Hg. v. SpringerProfessional, zuletzt geprüft am 15.06.2026.

28 Mykytyn, Pavlo: Cloud-KI versus lokale-KI: Leistung und Datenkontrolle. Hg. v. MDZ Spreeland. Online verfügbar unter https://www.digitalzentrum-spreeland.de/Kuenstliche-Intelligenz/KI-Blog/Cloud-KI-versus-lokale-KI-Leistung-und-Datenkontrolle-.html, zuletzt geprüft am 04.06.2026.

29 MDZC (2026): Geschäftsgeheimnisschutz im KI-Zeitalter. Online verfügbar unter https://digitalzentrum-chemnitz.de/wissen/geschaeftsgeheimnisschutz-im-ki-zeitalter/, zuletzt aktualisiert am 09.04.2026, zuletzt geprüft am 09.04.2026.

30 Rätze, Michael (2026): Auftragsverarbeitung nach Art. 28 DSGVO. Hg. v. MDZC. Online verfügbar unter https://digitalzentrum-chemnitz.de/wissen/auftragsverarbeitung-nach-dsgvo/, zuletzt aktualisiert am 09.04.2026.

31 Tacke, Ines (2025): KI, Cloud & Datenschutz – wer ist verantwortlich? Online verfügbar unter https://digitalzentrum-chemnitz.de/wissen/ki-cloud-datenschutz-wer-ist-verantwortlich/, zuletzt aktualisiert am 09.04.2026.

32 Lang, Thorsten; Scheufen, Marc; Engels, Barbara (2026): Digitale Souveränität von KMU. Begleitforschung Mittelstand-Digital. Hg. v. Institut der deutschen Wirtschaft Köln e.V., Institut der deutschen Wirtschaft Köln Consult GmbH und Ramboll Management Consulting GmbH. Online verfügbar unter https://www.iwkoeln.de/studien/thorsten-lang-marc-scheufen-barbara-engels-digitale-souveraenitaet-von-kmu-begleitforschung-mittelstand-digital.html.

33 Denga, Michael (2026): Datensouveränität und Data Cloud. Binnenmarktregulierung zwischen Kontraktualisierung und Subventionierung. In: MMR, S. 91–97.

34 Schöttle, Hendrik (2026): Digitale Souveränität durch Open Source. Rechtliche Handlungsspielräume in einer vernetzten Welt. In: MMR, S. 178–183.

35 Rauscher, Alexander (2026): Die Qual der Wahl – Ein Leitfaden zur Auswahl von Large Language Models (LLM) für KMU. Nachgelesen. Hg. v. MDZC. Online verfügbar unter https://digitalzentrum-chemnitz.de/wissen/leitfaden-zur-auswahl-von-large-language-models-fuer-kmu/, zuletzt geprüft am 31.05.2026.

36 Jung, Sven (2025): Index digitale Souveränität. Die deutsche Wirtschaft zwischen Selbstbestimmung und Abhängigkeit. Hg. v. adesso SE und Handelsblatt GmbH. Online verfügbar unter https://www.adesso.de/de/impulse/digitale-souveraenitaet/souveraenitaetsindex/index.jsp, zuletzt aktualisiert am 09.04.2026.

37 Redaktion ZD (2025): Forsa-Umfrage: Cloud-Dienste und Digitale Souveränität. In: ZD-Aktuell, S. 1467.

38 Zikesch, Philipp; Sörup, Thorsten; Adrian, Maximilian (2026): Datenverarbeitungsdienst – ein Begriff sucht seine Bedeutung. Definition nach Systematik, Zielsetzung und Übertragbarkeit auf Service -Modelle. In: MMR, 171-178.

39 Siglmüller, Jonas; Żdanowiecki, Konrad (2025): Datenverarbeitungsdienste unter dem Data Act – alles Cloud, oder was? Teil III zur Data Act-Umsetzung vor dem Omnibus-Paket. In: RDi, 504-512.

40 Sattler, Andreas (2024): Anbieterwechsel nach dem Data Act – Standardvertragsklauseln für Verträge über Cloud-Computing. Was die zwingenden Vorgaben des Data Act für die künftigen nicht-verbindlichen Standardvertragsklauseln der EU-Kommission bedeuten. In: CR, S. 213–223.

41 Romero Mateos, Lucía; Zenner, Lyn Luisa: LLMs vs. SLMs: Welche Sprachmodelle eignen sich für KMU? Hg. v. MDZH. Online verfügbar unter abrufbar unter: https://digitalzentrum-hamburg.de/leitfaden/llms-vs-slms-sprachmodelle/, zuletzt geprüft am 31.05.2026.

42 DSK (2025): Orientierungshilfe zu datenschutzrechtlichen Besonderheiten generativer KI-Systeme mit RAG-Methode. Version 1.0. Online verfügbar unter https://www.datenschutzkonferenz-online.de/media/oh/DSK_OH_RAG.pdf, zuletzt aktualisiert am Oktober 2025.

43 Tacke, Ines (2026): RAG datenschutzrechtlich geprüft. Hg. v. MDZ Chemnitz. Online verfügbar unter https://digitalzentrum-chemnitz.de/wissen/rag-datenschutzrechtlich-geprueft/, zuletzt geprüft am 04.06.2026.

44 Vaziri, Daryoush Daniel (2026): Open-Source Large Language Models: Der aktuelle Stand in Wissenschaft und Praxis. In: MDZ Fokus Mensch und Denkschmiede (Hg.): Digitale Souveränität als Basis für sichere KI-Anwendungen. Kurzlehrbuch, S. 9–11.

45 Außendorf, Maik; Evran, Talha (2024): Digitale Souveränität. Was es braucht, um unabhängig, eigenständig und stark zu sein. In: KIR, S. 116–117.

46 Ruoff, Christian (2016): Mehr Schutz vor Cyberkriminalität durch geschickte Backup-Strategie. In: DSB, 108-109.

47 Richter, Benjamin (2025): Cybersicherheit für KMU. In: Andreas Kohne und Dan Bauer (Hg.): Die Mittelstandstransformation. Wissen, Impulse und Handlungsempfehlungen für den überfälligen Wandel. Wiesbaden: Springer Fachmedien Wiesbaden; Imprint Springer Gabler, S. 419–439. Online verfügbar unter https://link.springer.com/chapter/10.1007/978-3-658-48184-1_16#Sec11.

48 Spieker, Stefan; Eichstädt, Timm (2024): Authentifizierung. In: Timm Eichstädt und Stefan Spieker (Hg.): 52 Stunden Informatik. Was jeder über Informatik wissen sollte. 2. Auflage. Wiesbaden, Heidelberg: Springer Vieweg (Lehrbuch), S. 93–98.

49 BSI: Sichere Passwörter erstellen. Online verfügbar unter https://www.bsi.bund.de/dok/6596574, zuletzt geprüft am 05.06.2026.

50 Weber, Kristin (2024): Mensch und Informationssicherheit. Verhalten verstehen, Awareness fördern, Human Hacking verstehen. München: Carl Hanser.

51 Wäsche, Mike (2025): NIS-2-Richtlinie – was Unternehmen wissen müssen. Nachgelesen. Hg. v. MDZC. Online verfügbar unter https://digitalzentrum-chemnitz.de/wissen/nis-2-richtlinie-was-unternehmen-wissen-muessen/, zuletzt geprüft am 31.05.2026.

Verfasst von

INES TACKE ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Privatrecht und Recht des geistigen Eigentums der Technischen Universität Chemnitz. Im Mittelstand-Digital Zentrum Chemnitz ist sie als KI-Trainerin tätig und beschäftigt sie sich mit Innovations- und Technikrecht.
ines-maria.tacke@digitalzentrum-chemnitz.de

PAVLO MYKYTYN ist wissenschaftlicher Mitarbeiter an der Brandenburgischen Technischen Universität Cottbus-Senftenberg. Im Mittelstand-Digital Zentrum Spreeland ist er Experte im Bereich Cybersicherheit im Industrial Internet of Things.
mykytyn@b-tu.de

Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Energie die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

WAS IST MITTELSTAND-DIGITAL?

Das Mittelstand-Digital Netzwerk bietet mit den *Mittelstand-Digital Zentren* und der Initiative *IT-Sicherheit in der Wirtschaft* umfassende Unterstützung bei der Digitalisierung mit dem Schwerpunkt Künstliche Intelligenz. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung der Angebote von Mittelstand-Digital. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Mittelstand-Digital
Zentrum
Chemnitz

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages