Mittelstand-Digital
Zentrum
Smarte Kreisläufe

Trendradar Datenökonomie und digitale Souveränität

Einordnung, Erläuterung und Erkenntnisse für Ihr Unternehmen

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

INHALT

Datenökonomie und digitale Souveränität 3

— Data Governance und Data Ownership 5
— Data Sharing und Datenkooperation 5
— KI-Agenten und Semantische Daten 6
— Data Spaces, Sovereign Cloud und Infrastrukturlokalisierung 8
— Datenportabilität und Cloud-Switching 9
— DSGVO und Privacy by Design sowie Privacy by Default 10
— Grenzüberschreitende Datentransfers und Standardvertragsklauseln (SCCs) 11
— Compliance Management und Compliance Automation 11
— Branchenspezifische Standards für Datensouveränität 12

Autoren 14

Quellen 15

Über das Mittelstand-Digital Zentrum Smarte Kreisläufe 18

Kontakt und Impressum 19

DATENÖKONOMIE UND DIGITALE SOUVERÄNITÄT

Durch die zunehmende Digitalisierung steht der Wirtschaft eine neue Ressource zur Verfügung: Daten. Personenbezogene Daten, nicht-personenbezogene Daten wie Maschinen-, Produktions- oder Transaktionsdaten sind Beispiele der vielfältigen Ausprägungen. Durch die Fortschritte der Informationstechnik sind die Kosten für die Nutzung von Daten durch Erhebung, Speicherung, Analyse und Verarbeitung stark gesunken. Dies ermöglicht neuartige und vielversprechende Ansätze für die datenbasierte Wertschöpfung.

Unter dem Begriff Datenökonomie werden volks- bzw. gesamtwirtschaftliche Aspekte datenbasierter Wertschöpfung zusammengefasst, die mit dem Erheben, Speichern, Verarbeiten, Analysieren und Nutzen von Daten in Verbindung stehen. Sowohl Unternehmen als auch Einzelpersonen, öffentliche Einrichtungen oder andere Organisationen können mit Daten wirtschaften. Daten können daher auch als Wirtschaftsgut betrachtet werden. Wo Bedarf, Nachfrage und Angebot aufeinandertreffen, entstehen Märkte für die Ressource Daten.

Dies erlaubt neuartige Wertschöpfung, für die Daten eine Schlüsselrolle haben. Wird die Nutzung von Daten zur Entscheidungsfindung konsequent in den Mittelpunkt der Wertschöpfung gestellt und automatisiert, können Daten sogar zur unverzichtbaren Grundlage des wirtschaftlichen Erfolges eines Unternehmens werden. Man spricht dann von datengetriebenen Unternehmen oder datengetriebenen Geschäftsmodellen. In diesen Fällen steht vor allem die Betrachtung betriebswirtschaftlicher Aspekte datenbasierter Wertschöpfung im Mittelpunkt. Durch die effektive und effiziente Nutzung der neuen Ressource Daten lassen sich neue Geschäftsmodelle für innovative Produkte und Dienstleistungen entwickeln und betriebliche Entscheidungen und Prozesse verbessern, was unmittelbar zu Wettbewerbsvorteilen verhilft. Dem stehen Investitionen in die notwendige Infrastruktur und organisatorische Voraussetzungen gegenüber, um den notwendigen Reifegrad für effektive und effiziente Datennutzung zu erreichen.

Im Umgang mit Daten sind allerdings auch rechtliche Rahmenbedingungen wie zum Beispiel EU-Verordnungen zum Datenschutz (EU2016/679), Daten (EU2023/2854) und KI (EU2024/1689) und nationale Gesetze gewissenhaft einzuhalten, denn Daten sind neben ihrer wirtschaftlichen Bedeutung auch eine Ressource, die auf Vertrauen basiert. Die Datenökonomie bewegt sich deshalb im Spannungsfeld wirtschaftlicher Interessen, gesellschaftlicher Auswirkungen und regulatorischer Anforderungen, insbesondere, wenn es sich um personenbezogene Daten handelt. Daher ist die Datenökonomie eng mit Themen wie Datensicherheit, Datenschutz und dem sparsamen und verantwortungsbewussten Umgang mit Daten verbunden [2].

Digitale Souveränität beschreibt die Fähigkeit von Staaten, Unternehmen und Organisationen, die Kontrolle über ihre digitalen Ressourcen, Daten, Technologien und Infrastrukturen selbstbestimmt auszuüben [3,4]. Ziel ist es, digitale Systeme so zu gestalten und zu betreiben, dass Entscheidungen unabhängig von einzelnen Technologieanbietern, außereuropäischen Rechtsräumen oder geopolitischen Entwicklungen getroffen werden können [5]. Dabei geht es nicht um Abschottung, sondern um die Fähigkeit, digitale Technologien sicher, rechtskonform und im eigenen Interesse zu nutzen [4].

Die Bedeutung digitaler Souveränität hat in den vergangenen Jahren deutlich zugenommen. Geopolitische Konflikte, globale Lieferengpässe und die damit verbundene starke Abhängigkeit von wenigen internationalen Technologieanbietern, haben gezeigt, wie verwundbar digitale Wertschöpfungsketten sein können. Digitale Souveränität wird daher zunehmend zu einem strategischen Wettbewerbs- und Sicherheitsfaktor. Sie stärkt die Innovationsfähigkeit, schützt kritische Infrastrukturen und sichert die Handlungsfähigkeit von Wirtschaft, Verwaltung und Gesellschaft [4,5].

Digitale Souveränität umfasst mehrere Dimensionen: die Kontrolle über Daten und deren Nutzung, die technische Beherrschbarkeit von IT-Systemen, die Einhaltung rechtlicher Anforderungen sowie die Fähigkeit, digitale Prozesse eigenständig zu

betreiben und weiterzuentwickeln [4]. Standards, Open-Source-Technologien sowie Kooperationen spielen dabei eine zentrale Rolle [5].

Für die Datenökonomie bildet digitale Souveränität also die Voraussetzung, um Daten vertrauensvoll austauschen, gemeinsam nutzen und wirtschaftlich verwerten zu können. Die im folgenden Trendradar betrachteten Subtrends zeigen, wie Datenökonomie und digitale Souveränität beispielhaft umgesetzt werden, und welche organisatorischen, technologischen und regulatorischen Rahmenbedingungen dafür erforderlich sind.

Mithilfe von ITONICS wurden die Subtrends der Datenökonomie und der digitalen Souveränität in einem Trendradar erfasst (siehe Abbildung 1). Hierbei wurden sie nach dem Grad der Auswirkungen auf produzierende kleine und mittlere Unternehmen in sehr niedrig (very low), niedrig (low), mittel (medium), hoch (high) und sehr hoch (very high) eingeteilt.

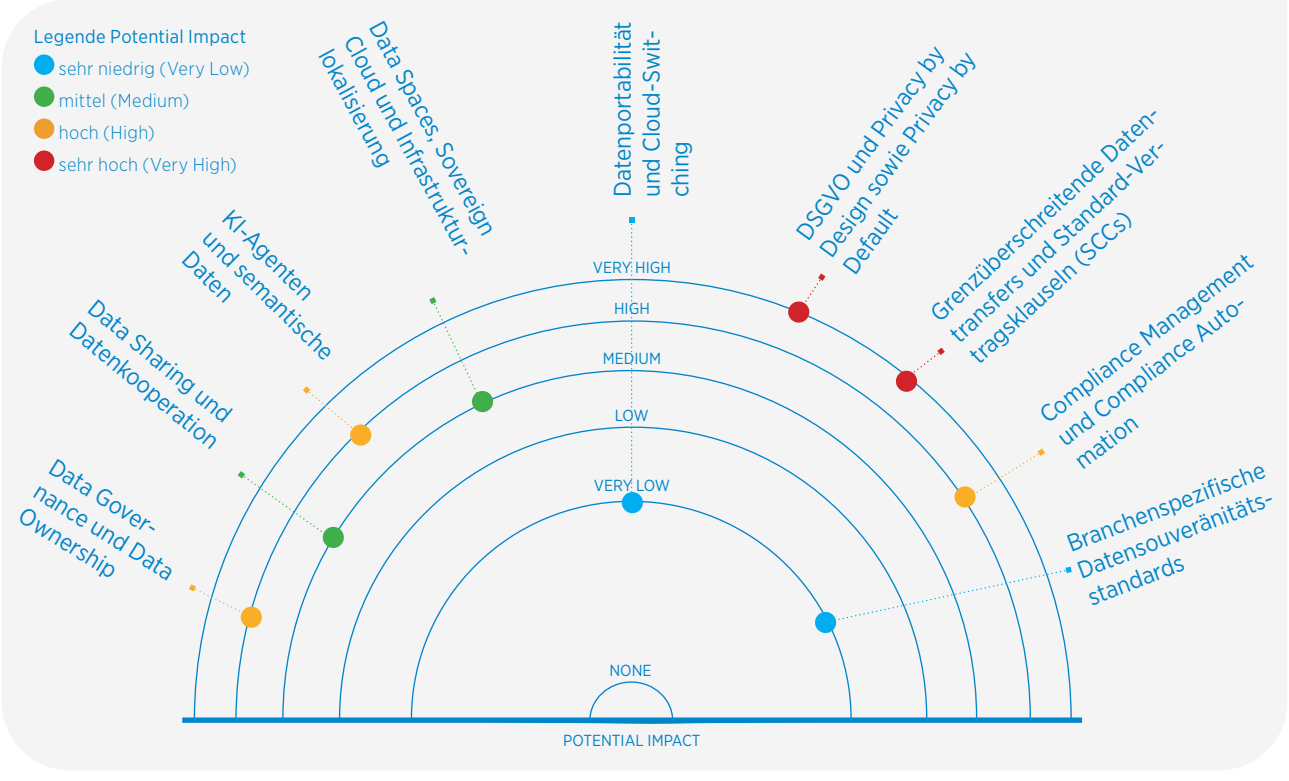


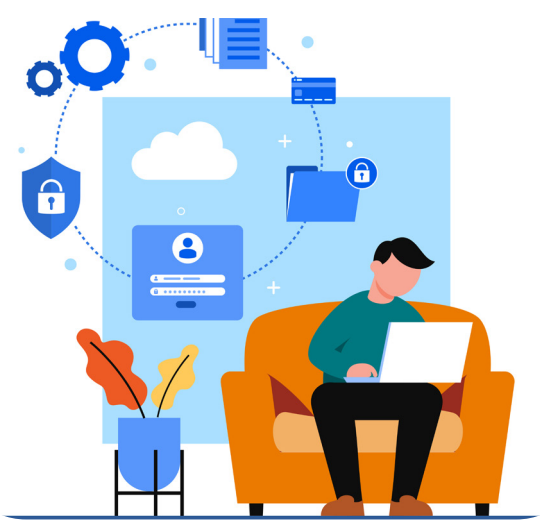
Abbildung 1: Trendradar Datenökonomie und digitale Souveränität (erstellt mit ITONICS)

Data Governance und Data Ownership

Data Governance beschreibt die organisatorischen und technischen Rahmenbedingungen, mit denen ein Unternehmen festlegt, wie Daten erfasst, gepflegt, genutzt, geschützt und gelöscht werden. Dazu gehören Richtlinien, Entscheidungsrechte, Verantwortlichkeiten und Prozesse, die eine korrekte, sichere und regelkonforme Nutzung von Daten über ihren gesamten Lebenszyklus hinweg sicherstellen. Für KMU ist Data Governance vor allem deshalb wichtig, weil sie dafür sorgt, dass alle Abteilungen mit denselben verlässlichen Daten arbeiten, Reibungsverluste sinken und Entscheidungen fundierter getroffen werden können [6,7].

Im europäischen Kontext gewinnt das Thema zusätzlich durch den Data-Governance-Rechtsakt (EU 2022/868) an Bedeutung. Diese EU-Verordnung soll den vertrauensvollen Datenaustausch fördern, klare Strukturen für die Datennutzung schaffen und die Datensouveränität stärken [8]. Für Unternehmen bedeutet das: Wer Daten wirtschaftlich nutzen oder mit Partnern teilen will, braucht nachvollziehbare Regeln und dokumentierte Zuständigkeiten.

Hier setzt das Konzept des Data Ownerships an: Data Ownership beschreibt, wer im Unternehmen die Verantwortung und Kontrolle über bestimmte Daten trägt und wer über Zugriff, Nutzung und Weitergabe entscheidet [9,10]. Dazu gehört auch die Verantwortung für Datenqualität, Integrität und Schutz. Rechtlich ist „Eigentum an Daten“ jedoch nicht immer eindeutig definiert; in der Praxis geht es daher meist weniger um klassisches Eigentum als um eine funktionale Zuordnung von Verantwortlichkeiten innerhalb der Governance-Strukturen [9].



Für die Umsetzung in KMU empfiehlt es sich, zunächst die wichtigsten Datenarten zu benennen, etwa Kundendaten, Produktdaten, Finanzdaten oder Maschinendaten. Danach sollte festgelegt werden, wer für diese Daten verantwortlich ist, wer sie ändern darf, wer sie freigibt und wann sie archiviert oder gelöscht werden. Ebenso sinnvoll sind einfache Regeln zur Datenqualität, zum Beispiel feste Pflichtfelder, regelmäßige Prüfungen und eine Dokumentation von Änderungen.

Beispiel: In einem mittelständischen Handelsunternehmen ist der Vertrieb für Kundendaten verantwortlich, der Einkauf für Lieferantendaten und die IT für Zugriffsrechte und Datensicherheit. So ist bei Fehlern oder Rückfragen schnell klar, wer zuständig ist und wer handeln muss.

Data Sharing und Datenkooperation

Data Sharing bezeichnet die strukturierte Bereitstellung, den Austausch und die gemeinsame Nutzung von Daten zwischen verschiedenen Systemen, Benutzern oder Unternehmen, um Mehrwert zu schaffen, etwa durch Analysen, bessere Prozesse oder neue Partnerschaften. Der Begriff Datenkooperation betont stärker die partnerschaftliche Zusammenarbeit mehrerer Akteure bei der Nutzung und Auswertung von Daten, auch wenn beide Begriffe in der Literatur häufig synonym verwendet werden [11,12].

Für Unternehmen ist dabei zwischen interner und externer Datennutzung zu unterscheiden. Intern werden Daten innerhalb des Unternehmens gemeinsam genutzt, extern werden sie mit Partnern, Kunden oder Dienstleistern ausgetauscht. Beide Formen setzen klare Regeln, definierte Zugriffsrechte sowie geeignete rechtliche und organisatorische Rahmenbedingungen voraus und erfordern damit eine funktionierende Data Governance [11].

Ein großer Vorteil von Data Sharing liegt darin, Datensilos aufzubrechen. Datensilos sind Informationsbestände, die nur in einzelnen Abteilungen

genutzt werden, obwohl auch andere Bereiche davon profitieren könnten. Werden solche Silos aufgelöst, kann sich die Zusammenarbeit innerhalb des Unternehmens und mit externen Partnern verbessern, gleichzeitig können auf Basis größerer und vielfältigerer Datenmengen bessere Entscheidungen getroffen sowie neue (Geschäfts-)Möglichkeiten entwickelt werden [13].

Rechtlich und organisatorisch sollten Unternehmen vor dem Datenaustausch klären, wer für die Daten verantwortlich ist (Data Ownership), welche Daten geteilt werden dürfen, zu welchem Zweck dies geschieht und wer Zugriff erhält. Gerade wenn personenbezogene oder sensible Informationen betroffen sind, müssen Datenschutzanforderungen, Vertraulichkeitsregeln und vertragliche Vereinbarungen berücksichtigt werden [14,15].

Beispiel: Ein Händler teilt Absatzdaten mit einem wichtigen Lieferanten, damit dieser seine Produktion besser planen kann. Im Gegenzug erhält der Händler frühzeitig Informationen über Lieferengpässe und kann sein Sortiment besser steuern.

Für KMU ist es sinnvoll, dafür einen einfachen Freigabeprozess einzuführen, an dem Fachbereich, IT und gegebenenfalls Datenschutz beteiligt sind.

In der Praxis kann ein Unternehmen klein anfangen, etwa mit einem gemeinsamen Datenbestand für Vertrieb, Kundenservice und Buchhaltung oder mit einem geregelten Datenaustausch mit Lieferanten. Technisch wird Data Sharing heute häufig durch Data Warehouses, APIs oder Datenaustauschplattformen unterstützt; künftig gewinnen auch Privacy Enhancing Technologies und Data Clean Rooms an Bedeutung, weil sie datenschutzkonforme Zusammenarbeit erleichtern sollen [11].

KI-Agenten und Semantische Daten

KI-Agenten sind KI-Systeme, die komplexe Aufgaben weitgehend selbstständig bearbeiten. Sie können dafür Informationen aus anderen Systemen abrufen, Werkzeuge einsetzen, einzelne Arbeitsschritte planen und ihre Ergebnisse überprüfen.

KI-Agenten implementieren dabei einen automatisierten kontinuierlichen „Denken-Handeln-Reflektieren"-Zyklus, um eine vorgegebene Zielstellung zu erreichen:

- „Denken": Analyse des aktuellen Zielerreichungsgrades und Planung notwendiger Handlungen für die Zielerreichung.
- „Handeln": Auswahl der (ggf. parallel) auszuführenden Schritte und Nutzung geeigneter Werkzeuge (z.B. Websuche, Datenbankabfragen, ökonomische Transaktionen oder Softwareanwendungen), um den Schritt auszuführen.
- „Reflektieren": Analyse der Ergebnisse des Handelns und Bewertung der Auswirkungen auf die Zielerreichung. Wiederholung des Zyklus bis zur Zielerreichung oder ggf. Zeitüberschreitung.

Für die Lösung einer Aufgabe müssen KI-Agenten nicht nur Zugriff auf die benötigten Werkzeuge, Daten und Systeme haben, sondern diese auch semantisch, d. h. in ihrem Effekt und ihrer Bedeutung verstehen und nutzen können.

Einen Lösungsansatz bietet das Model Context Protocol (MCP), über das Werkzeuge (z. B. um Datenbanken abzufragen), Ressourcen (z. B. Datenquellen) und Prompts (z. B. vorgefertigte Arbeitsabläufe) bereitgestellt werden können. Weitere Protokolle wie das Agent Payments Protocol, Agent2Agent Protocol und Universal Commerce Protocol erlauben es, typische Aktivitäten von Marktteilnehmern abzubilden.

Eine weitere wichtige Rolle spielen standardisierte Informationsmodelle, Schnittstellen und Datenformate wie die Asset Administration Shell (Verwaltungsschale) und OPC/UA. Diese sind die technologische Grundlage für den strukturierten, automatisierten Datenaustausch und ermöglichen eine reibungslose Interoperabilität und Datenintegration zwischen verschiedenen Systemen unterschiedlicher Hersteller. Die klare Definition von Struktur und Bedeutung (Semantik) der Informationen und die Erhebung von Daten mit hoher Qualität senken nicht nur die Kosten für die Integration von Systemen und die Datenerhebung, sie ermöglichen auch Data Sharing und Datenkooperation und die Nutzung durch KI-Agenten.

Ein wesentlicher ökonomischer Effekt des Einsatzes von KI-Agenten kann daher die Automatisierung typischer Transaktionen in Märkten sein [16,17]. Deren Kosten sind heute vor allem durch menschliche Tätigkeiten bestimmt, die KI-Agenten zu drastisch niedrigeren Kosten ausführen könnten: Erhebung und Bewertung von Preis- und Produktinformationen, Verhandlung von Bedingungen, Formulierung von Verträgen und Konformitätsüberwachung sind oft arbeitsintensiv und durch die Kosten menschlicher Arbeit bestimmt.

Der Markt für Internetsuche zeigt einen Ausblick auf mögliche Auswirkungen von KI-Agenten [18]: Im Jahr 2026 ist bereits mehr als die Hälfte des Internetverkehrs von Systemen statt Menschen verursacht. 52 % der Anfragen von Systemen rufen die Inhalte der Anbieter nur für KI-Training ab, 9 % für Internetsuche und 37 % für beides. Das bisherige Geschäftsmodell, die Bereitstellung von Inhalten durch Anbieter im Austausch für die Empfehlung an interessierte bzw. suchende Internetnutzer, funktioniert dadurch nicht mehr. Inhalte werden zwar weiterhin automatisiert eingesammelt und genutzt, aber wenn KI-Systeme Fragen zur Nutzung oder zu Eigenschaften von Produkten zufriedenstellend beantworten, (Markt-)Recherchen durchführen und Aufgaben ohne menschliche Interaktion lösen, verlieren Anbieter die Interaktion mit interessierten Nutzern. Es braucht daher Geschäftsmodelle, die für Anbieter neue Anreize schaffen, Inhalte bereitzustellen. Ob über Wertschätzung bzw. Monetarisierung der Inhalte, die Vermittlung „einkaufender KI-Agenten“ oder andere Mechanismen wird sich zeigen. Dies verdeutlicht: KI-Agenten können Marktmechanismen grundlegend verändern.

Beispiel: Für Unternehmen ist es wichtig zu verstehen, welchen Wert im Unternehmen verfügbare bzw. angebotene Inhalte für verschiedene Marktakteure und Partner haben. Dabei sollten die Auswirkungen von KI-Agenten auf die Nutzung dieser Inhalte und die eigenen Geschäftsmodelle verstanden werden. So können stärker als bisher eigene Inhalte für KI-Agenten effizient nutzbar gemacht werden für automatisiertes Prüfen von Identitäten, Durchsetzen von Berechtigungen, Lizenzieren von Inhalten und Durchführen kommerzieller Transaktionen.

Data Spaces, Sovereign Cloud und Infrastrukturlokalisierung

Mit der zunehmenden Nutzung von Daten stoßen zentrale Plattformmodelle, wie Data Warehouses oder Data Lakes, in vielen Fällen an Grenzen. Besonders problematisch sind dabei Abhängigkeiten von einzelnen Anbietern und der mögliche Kontrollverlust über eigene Daten. Data Spaces setzen genau hier an, indem sie einen dezentralen, vertrauenswürdigen, souveränen und interoperablen Datenaustausch ermöglichen. Im Unterschied zu klassischen zentralen Modellen verbleibt die Kontrolle über die Daten in Data Spaces grundsätzlich bei den jeweiligen Eigentümern oder Verantwortlichen. Über klare Richtlinien, semantische Modelle, Protokolle und Prozesse können Daten dennoch unter festgelegten Bedingungen für andere auffindbar und nutzbar gemacht werden [19,20].

Für KMU ist das vor allem dann interessant, wenn Daten mit Partnern geteilt werden sollen, ohne sie vollständig aus der Hand zu geben.

Ein wichtiges europäisches Beispiel ist Gaia-X, das den Aufbau eines föderierten Daten- und Infrastrukturökosystems verfolgt. Darüber hinaus werden in zahlreichen Branchen gemeinsame europäische Data Spaces aufgebaut, unter anderem in den Bereichen Gesundheit, Energie, Landwirtschaft oder Finanzwesen [21,22].

Diese Entwicklungen zeigen, dass Datenaustausch zunehmend in regulierten, interoperablen und europäischen Strukturen gedacht wird.

Eng mit diesem Thema verbunden ist die Sovereign Cloud. Darunter versteht man eine Cloud-Umgebung, die nachvollziehbare Kontrolle über Daten, Zugriffe und Betriebsprozesse innerhalb eines definierten Rechtsrahmens ermöglicht und damit die Einhaltung regionaler oder nationaler Vorschriften unterstützt. Für Unternehmen bedeutet das vor allem mehr Transparenz, bessere Compliance-Prüfbarkeit und geringere Abhängigkeit von einzelnen Anbietern [23].

Die Infrastrukturlokalisierung ergänzt diesen Ansatz. Dabei werden Daten gezielt in einem bestimmten geografischen Raum gespeichert und verarbeitet, um regulatorische Anforderungen leichter zu erfüllen und Risiken im Zusammenhang mit extraterritorialen Zugriffen zu verringern. Gerade in sensiblen Bereichen wie Gesundheitswesen, Banken oder kritischer Infrastruktur ist dies von hoher Bedeutung [23,24].

Somit bilden Data Spaces, Sovereign Cloud und

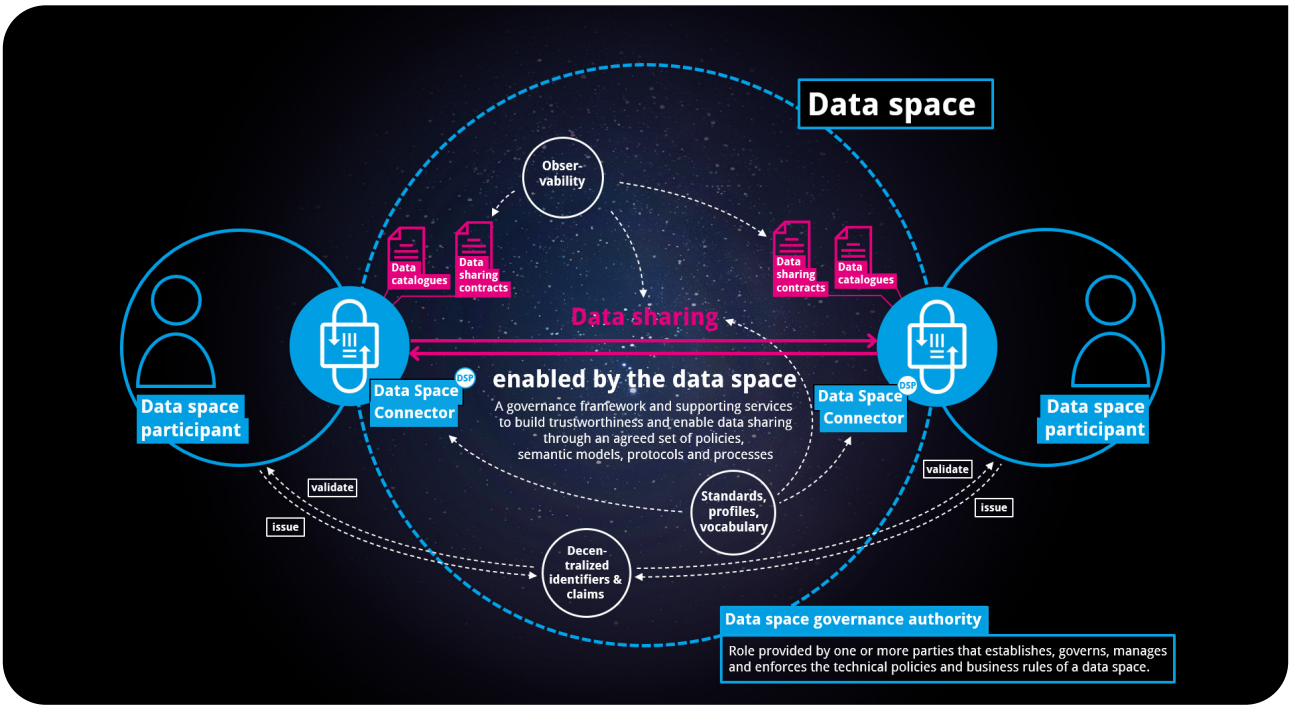


Abbildung 2: International Data Spaces Association (o.D.). DATA SPACES. Where the future of data happens

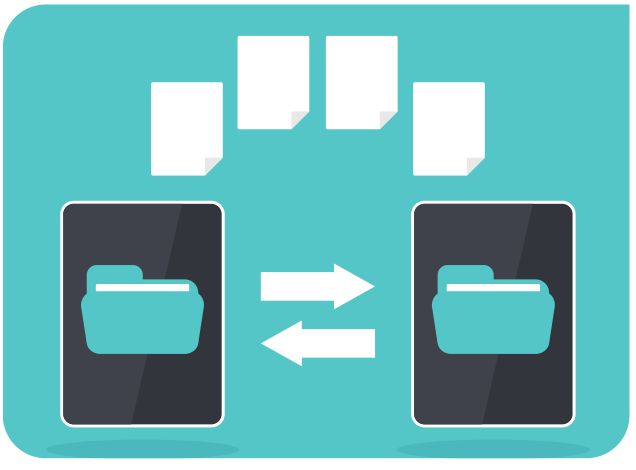
Infrastrukturlokalisierung zentrale Bausteine einer zunehmend souveränen Datenökonomie, die auf Vertrauen, Kontrolle und europäische Werte ausgerichtet ist.

Für die praktische Umsetzung sollten KMU bei der Auswahl von Cloud- und Datenplattformen nicht nur auf Preis und Funktionen achten. Wichtig sind auch Fragen wie: Wo werden die Daten gespeichert, welchem Recht unterliegt der Anbieter, wer darf auf die Daten zugreifen, wie werden Schnittstellen bereitgestellt und wie leicht ist ein späterer Wechsel zu einem anderen Anbieter? Ebenso empfiehlt es sich, Exit-Szenarien und Anforderungen an Interoperabilität bereits im Vertrag mitzudenken.

Beispiel: Ein mittelständischer Gesundheitsdienstleister wählt eine Cloud-Lösung, bei der sensible Daten ausschließlich in der EU verarbeitet werden und Zugriffe lückenlos dokumentiert sind. So lassen sich Datenschutz- und Nachweispflichten einfacher einhalten.

Datenportabilität und Cloud-Switching

Datenportabilität und Cloud-Switching bedeuten, dass Daten und Anwendungen von einem Cloud-Anbieter zu einem anderen übertragen oder kopiert werden können, ohne dass dabei wesentliche Informationen verloren gehen. Ziel ist es, den Zugang zu Daten zu erleichtern, Anbieterwechsel zu ermöglichen und Lock-in-Effekte zu vermeiden [25-27].



Für Unternehmen ist das besonders wichtig, weil viele Geschäftsprozesse heute an Cloud-Dienste gebunden sind. Wenn Daten nicht sauber exportiert und in ein anderes System übernommen werden können, entsteht schnell eine teure Abhängigkeit vom bisherigen Anbieter [26,28]. Datenportabilität stärkt deshalb nicht nur die Flexibilität, sondern auch die Verhandlungsposition von Unternehmen.

Rechtlich spielt hier insbesondere Art. 20 DSGVO eine Rolle. Danach haben betroffene Personen das Recht, personenbezogene Daten, die sie einem Verantwortlichen bereitgestellt haben, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten und an einen anderen Verantwortlichen zu übermitteln [29].

In der Praxis reicht es jedoch nicht, nur auf das gesetzliche Recht zur Datenübertragbarkeit zu verweisen. Unternehmen sollten schon vor Vertragsabschluss prüfen, ob Exportfunktionen vollständig vorhanden sind, ob neben den Daten auch Metadaten, Ordnerstrukturen oder Berechtigungen übernommen werden können und wie aufwendig eine Migration tatsächlich wäre [26,29].

Für KMU empfiehlt es sich, einen Testexport mit realistischen Datenmengen durchzuführen und Zuständigkeiten für spätere Systemwechsel früh festzulegen. Zudem ist zu beachten, dass technische Hürden die tatsächliche Nutzung der Datenportabilität bislang oft erschweren. Fehlende Kompatibilität zwischen Systemen ist einer der Gründe, warum das Recht in der Praxis noch nicht immer einfach umgesetzt werden kann [27].

Beispiel: Ein Unternehmen möchte von einem CRM-Anbieter zu einem anderen wechseln. Wenn Kontakte, Kommunikationshistorie, Dokumente und Ordnerstrukturen vollständig in offenen Formaten exportiert und wieder importiert werden können, sinken Migrationsaufwand, Kosten und Ausfallrisiken deutlich.

DSGVO und Privacy by Design sowie Privacy by Default

Die Datenschutz-Grundverordnung, kurz DSGVO, ist der zentrale europäische Rechtsrahmen für den Schutz personenbezogener Daten. Sie gilt nicht nur für Organisationen innerhalb der EU, sondern grundsätzlich auch für Unternehmen außerhalb der EU, wenn sie personenbezogene Daten von EU-Bürgern verarbeiten oder ihnen Waren und Dienstleistungen anbieten. Ziel der DSGVO ist es, den Schutz personenbezogener Daten zu stärken und zugleich einen einheitlichen Rechtsrahmen für den sicheren Datenverkehr in Europa zu schaffen [31,32].

Für Unternehmen sind besonders die Datenschutzgrundsätze relevant. Dazu gehören Rechtmäßigkeit, Fairness und Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie die Rechenschaftspflicht. Letztere bedeutet, dass Unternehmen nicht nur datenschutzkonform handeln müssen, sondern dies auch nachweisen können müssen, etwa durch Dokumentationen, Richtlinien oder Schulungen.

Hinzu kommen Anforderungen an Datensicherheit, Rechtsgrundlagen der Verarbeitung, Rechte betroffener Personen und gegebenenfalls die Benennung eines Datenschutzbeauftragten. Verstöße gegen die DSGVO können mit erheblichen Bußgeldern geahndet werden [32]. Für KMU bedeutet das: Datenschutz ist kein reines IT-Thema, sondern eine Managementaufgabe.

Besonders wichtig sind in diesem Zusammenhang Privacy by Design und Privacy by Default. Beide Konzepte sind in Art. 25 DSGVO verankert und verlangen, dass Datenschutz bereits bei der Entwicklung und Voreinstellung von Systemen, Produkten und Anwendungen berücksichtigt wird. Privacy by Design steht für Datenschutz durch Technikgestaltung, Privacy by Default für datenschutzfreundliche Voreinstellungen [31,32].

Beispiel: In einem Online-Kundenportal sind nur die nötigsten Datenfelder Pflicht, Marketingeinwilligungen sind nicht vorangekreuzt und Kundendaten sind standardmäßig nur für berechtigte Mitarbeiter sichtbar. So wird Datenschutz direkt in die Technik eingebaut.

Praktisch heißt das: Unternehmen sollten nur die Daten erheben, die für einen klaren Zweck wirklich notwendig sind, und Schutzmaßnahmen wie Pseudonymisierung, Verschlüsselung, Zugriffsbeschränkungen oder physische Sicherheitsmaßnahmen frühzeitig einplanen [31-33]. Ebenso sollten Standardeinstellungen so gewählt werden, dass personenbezogene Daten nicht automatisch umfassender verarbeitet werden als nötig [32,33].

Für KMU ist es sinnvoll, neue Prozesse systematisch zu prüfen: Welche Daten werden gebraucht, wer darf darauf zugreifen, wie lange werden sie gespeichert und welche technischen Schutzmaßnahmen sind notwendig? Auch einfache Maßnahmen wie reduzierte Pflichtfelder in Formularen, standardmäßig deaktivierte Zusatzfreigaben und klar definierte Löschfristen helfen, die Anforderungen praxisnah umzusetzen.

	Datenschutz durch Technikgestaltung (Privacy by Design)	**Datenschutz durch Voreinstellung (Privacy by Default)**
Ziel	Datenschutz in das Fundament des Systems integrieren	Benutzerdaten automatisch schützen, ohne dass manuelle Eingriffe erforderlich sind
Hauptschwerpunkt	Integration des Datenschutzes in den Entwicklungsprozess	Sicherstellen, dass standardmäßig datenschutzfreundliche Einstellungen angewendet werden
Zeitpunkt	während des gesamten Design-Lebenszyklus des Systems	während der Konfigurations- und Bereitstellungsphasen

Abbildung 3: Vergleich von Privacy by Design und Privacy by Defaul (nach Cookiebot)

Grenzüberschreitende Datentransfers und Standardvertragsklauseln (SCCs)

Sobald personenbezogene Daten den Europäischen Wirtschaftsraum verlassen, ist zu prüfen, ob die allgemeinen Anforderungen der DSGVO für die Datenübermittlung vorliegen. Unternehmen müssen sicherstellen, dass auch außerhalb des EWR ein angemessenes Datenschutzniveau gewährleistet ist [34-36].

Grundsätzlich gibt es dafür zwei zentrale Wege: Entweder liegt ein Angemessenheitsbeschluss der Europäischen Kommission vor oder es werden geeignete Garantien eingesetzt. Zu den wichtigsten geeigneten Garantien gehören die Standardvertragsklauseln, auch Standard Contractual Clauses oder SCCs genannt. Diese werden von der Europäischen Kommission vorgegeben und sollen im Wesentlichen unverändert in Verträge übernommen werden, damit ein mit der DSGVO vergleichbares Datenschutzniveau abgesichert wird [35,36].

Daneben gibt es weitere Möglichkeiten, etwa verbindliche interne Datenschutzvorschriften, genehmigte Verhaltensregeln oder Zertifizierungsmechanismen. In bestimmten Ausnahmefällen kann sich ein Datentransfer auch auf Art. 49 DSGVO stützen, etwa wenn eine betroffene Person nach Aufklärung ausdrücklich eingewilligt hat oder wenn ein Vertrag im Interesse der betroffenen Person erfüllt werden muss [36].

Für KMU ist dieses Thema besonders relevant, weil viele alltägliche Softwarelösungen, etwa für Newsletter, CRM, Support, Videokonferenzen oder Cloud-Speicher, internationale Datenübermittlungen auslösen können. Es genügt daher nicht, nur den Anbieter zu kennen; Unternehmen müssen auch wissen, wo Daten verarbeitet werden und auf welcher rechtlichen Grundlage dies geschieht.

In der praktischen Umsetzung empfiehlt es sich, zunächst alle Dienstleister zu erfassen, die personenbezogene Daten außerhalb des EWR verarbeiten. Danach sollte geprüft werden, ob ein Angemessenheitsbeschluss vorliegt oder ob SCCs beziehungsweise andere Garantien notwendig sind. Diese Prüfung sollte dokumentiert und regelmäßig aktualisiert werden, insbesondere wenn neue Tools eingeführt oder bestehende Verträge geändert werden.

> Beispiel: Ein Unternehmen nutzt einen Support-Dienstleister mit Rechenzentren außerhalb Europas. Dann muss geprüft werden, auf welcher Grundlage die Kundendaten übertragen werden, welche vertraglichen Garantien bestehen und ob zusätzliche Schutzmaßnahmen erforderlich sind.

Compliance Management und Compliance Automation

Compliance Management umfasst alle Strukturen, Maßnahmen und Prozesse, mit denen ein Unternehmen sicherstellt, dass gesetzliche Vorgaben, regulatorische Anforderungen und interne Richtlinien eingehalten werden. Im Datenkontext betrifft das unter anderem Datenschutz, IT-Sicherheit, Dokumentationspflichten, Zugriffsregelungen und Nachweispflichten [37,38].

Viele Unternehmen setzen dafür ein Compliance Management System, kurz CMS, ein. Dabei handelt es sich nicht nur um eine einzelne Software, sondern eher um ein Zusammenspiel aus Tools, Prozessen, internen Kontrollen und Verantwortlichkeiten [37]. Ziel ist es, Risiken frühzeitig zu erkennen, Verstöße zu vermeiden und Rechts-, Haftungs- und Reputationsschäden zu reduzieren [38].

Mit zunehmender Komplexität gewinnt die Compliance Automation an Bedeutung. Gemeint ist der Einsatz von Software und teilweise auch KI, um regulatorische Anforderungen automatisch zu überwachen, zu dokumentieren und in Berichten sichtbar zu machen. Dadurch können Risikoanalysen, Kontrollen und Freigaben standardisiert,

Dashboards aufgebaut und potenzielle Verstöße frühzeitig erkannt werden [39].

Für KMU ist wichtig, dass Automatisierung keine fehlende Governance ersetzt. Erst wenn klar ist, welche Regeln gelten, welche Daten betroffen sind und welche Kontrollen notwendig sind, kann Software sinnvoll unterstützen. Ein praktikabler Einstieg besteht deshalb darin, zunächst die wichtigsten Pflichten zu erfassen, diese nach Risiko zu priorisieren und anschließend zu entscheiden, welche Schritte manuell und welche automatisiert erfolgen sollen.

In der Praxis kann das zum Beispiel bedeuten, Zugriffsprüfungen, Löschfristen, Freigabeprozesse oder Audit-Nachweise softwaregestützt zu überwachen. So sinkt der manuelle Aufwand, Fehler werden reduziert und die Einhaltung von Regeln wird konsistenter [39].

Beispiel: Ein mittelständisches Unternehmen nutzt ein System, das automatisch meldet, wenn Benutzerrechte nicht mehr zur Rolle eines Mitarbeiters passen oder wenn Aufbewahrungsfristen für personenbezogene Daten ablaufen. Dadurch wird aus einer aufwendigen Listenpflege ein nachvollziehbarer, wiederholbarer Prozess.

Branchenspezifische Standards für Datensouveränität

Damit Daten in einem Ökosystem von mehreren Beteiligten gewinnbringend genutzt werden können, braucht es gemeinsame Standards. Solche Standards sorgen dafür, dass unterschiedliche Systeme Daten austauschen und trotz verschiedener technischer Grundlagen gleich interpretieren können [40]. Gleichzeitig verbessert die Standardisierung von Datenformaten die Datenqualität, erleichtert die Bearbeitbarkeit und unterstützt die Auditierung von Daten [41].

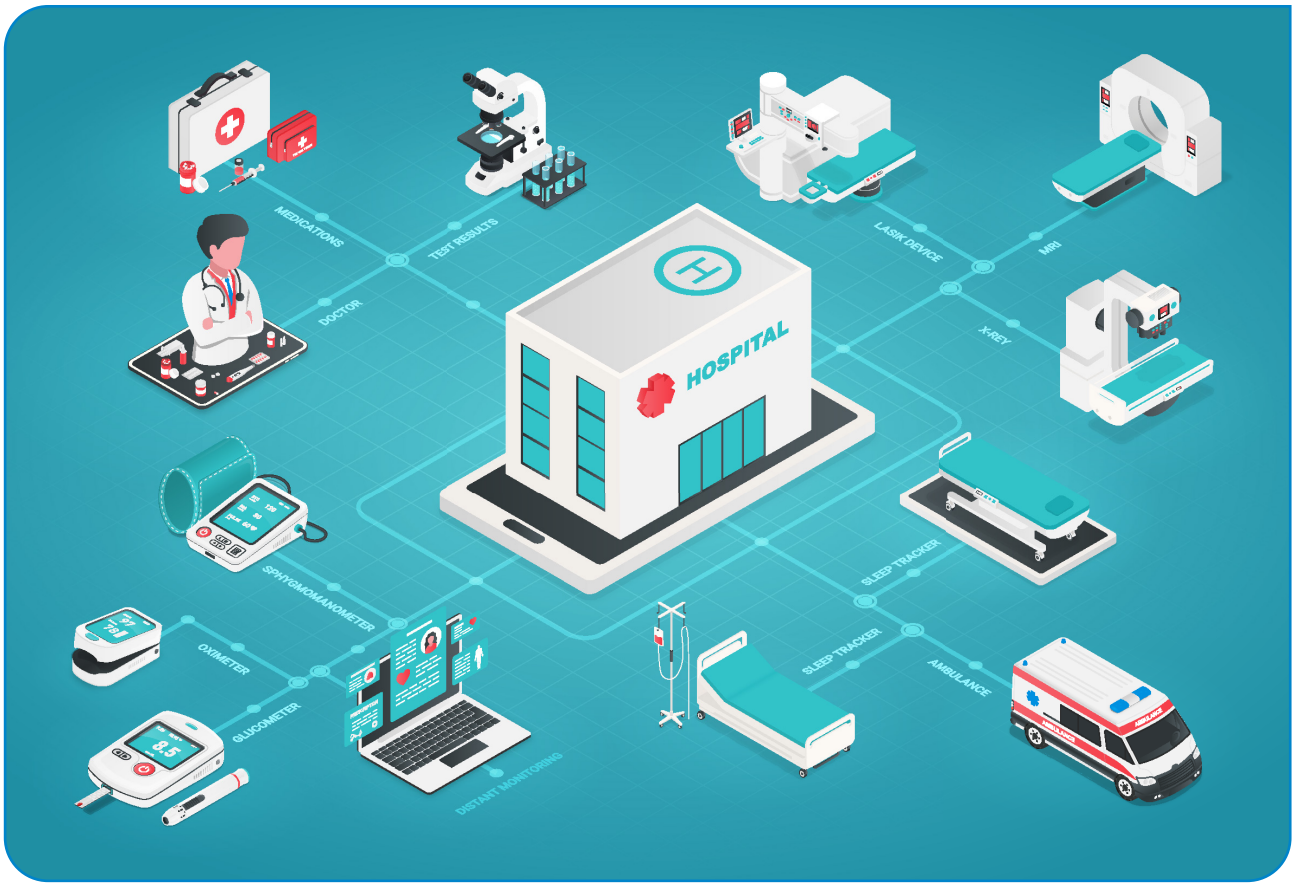
Neben der Nutzbarkeit spielt auch die Datensouveränität eine wichtige Rolle. Darunter wird unter anderem verstanden, dass Daten in einem klar definierten rechtlichen und geografischen Rahmen verarbeitet werden, damit sensible Informationen geschützt und Datenschutz- sowie Sicherheitsanforderungen eingehalten werden können [42]. Gerade in regulierten Branchen reicht technische Funktionalität allein daher nicht aus; erforderlich sind auch branchenspezifische Regeln, Sicherheitsniveaus und Nachweise.

Besonders deutlich wird das bei kritischen Infrastrukturen (KRITIS). In diesem KRITIS-Umfeld gelten zusätzliche Anforderungen an IT-Sicherheit, Meldepflichten und organisatorische Schutzmaßnahmen. Unternehmen aus Bereichen wie Energie, Gesundheit, Transport oder Telekommunikation müssen deshalb stärker als andere darauf achten, wie Daten verarbeitet, geschützt und im Störfall abgesichert werden [43].

Beispiel: Ein kleiner Gesundheitsdienstleister oder ein Zulieferer für kritische Infrastruktur kann nicht nur nach Preis und Funktionsumfang entscheiden. Er muss zusätzlich prüfen, ob ein System die geforderten Sicherheits- und Nachweisstandards der Branche tatsächlich erfüllt.

Ein anschauliches Beispiel ist die Telematikinfrastruktur im Gesundheitswesen. Sie wurde entwickelt, um medizinische Einrichtungen sicher miteinander zu vernetzen und den Austausch sensibler Gesundheitsdaten auf hohem Sicherheitsniveau zu ermöglichen. Authentifizierung, sichere Netzanbindung und klar geregelte Rollen sorgen dafür, dass nur berechtigte Akteure Zugriff erhalten [44].

Für KMU in regulierten Branchen empfiehlt es sich, frühzeitig zu prüfen, welche branchenspezifischen Standards, Meldepflichten, Sicherheitsvorgaben oder Zertifizierungsanforderungen gelten. Diese Anforderungen sollten in einer übersichtlichen Form dokumentiert und bei der Auswahl von IT-Systemen, Dienstleistern und Partnern verbindlich berücksichtigt werden. So wird vermieden, dass regulatorische Anforderungen erst im Audit, im Kundenprojekt oder im Schadensfall sichtbar werden.



AUTORINNEN & AUTOREN

Hannah Feichtner
Zentrum für Management Research
Lern- und Assistenztechnologien

Dr. Steffen Seeger
Sächsisches Textilforschungsinstitut e. V. (STFI)
Datengetriebene Geschäftsmodelle, Datenerfassung und -management, IIoT und Retrofit, Infrastrukturen für KI-Anwendungen

Gisela Stegmann
Zentrum für Management Research
Lern- und Assistenztechnologien

Dr. rer. pol. Marcus Winkler
Zentrum für Management Research
Lern- und Assistenztechnologien

Weitere Trendradare

Im Rahmen des Mittelstand-Digital Zentrums Smarte Kreisläufe wurde weitere Trendradare zu folgenden Themen veröffentlicht:

- Künstliche Intelligenz
- Kreislaufwirtschaft
- Minimalismus und Sharing Economy
- Nachhaltigkeit
- Transparente Lieferketten
- Urbane Produktion und New Work

Ein Download ist kostenfrei möglich via Website www.smarte-kreislaeufe.de oder über den Scan des QR-Codes:

QUELLEN

[1] Azjab, C., Goecke, H. und Spiekermann, M. (2020). Forschungsbereiche der Datenökonomie. Wirtschaftsdienst 2020(2), S. 124-127.

[2] Luber, S. [24.06.2025] Cloudcomputing Insider. Was ist Datenökonomie? URL: https://www.cloudcomputing-insider.de/was-ist-datenoekonomie-a-9ae8686368c4cfb22cc4374ad8145d14/

aufgerufen am 30.06.2026

[3] Fraunhofer-Institut für Offene Kommunikationssysteme (o.D.). Digitale Souveränität. URL: https://www.fokus.fraunhofer.de/de/angebot/loesungen/souveraenitaet.html

aufgerufen am 30.06.2026

[4] SAP (2026). Was ist digitale Souveränität? URL: https://www.sap.com/germany/resources/what-is-digital-sovereignty

aufgerufen am 30.06.2026

[5] Bundesministerium für Digitales und Staatsmodernisierung (o.D.). Digitale Souveränität - Eigenständigkeit sichern. URL: https://bmds.bund.de/themen/digitale-souveraenitaet

aufgerufen am 30.06.2026

[6] The Data Governance Institute (o.D.). The Data Governance Basics. URL: https://datagovernance.com/the-data-governance-basics/

aufgerufen am 30.06.2026

[7] Holdsworth, J. und Kosinski, M. (o.D.). Was ist Data Governance? URL: https://www.ibm.com/de-de/think/topics/data-governance

aufgerufen am 30.06.2026

[8] European Commission (2024). European Data Governance Act. URL: https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

aufgerufen am 30.06.2026

[9] Graux, H. (2024). What is data ownership, and does it still matter under EU data law? An exploration of traditional concepts of data ownership, and of the expected impact of the Data Act. URL: https://data.europa.eu/sites/default/files/report/What%20is%20data%20ownership%2C%20and%20does%20it%20still%20matter%20under%20EU%20data%20law.pdf

aufgerufen am 30.06.2026

[10] Deinhard, M. (2024). Was bedeutet Data Ownership. URL: https://www.it-schulungen.com/wir-ueber-uns/wissensblog/was-bedeutet-data-ownership.html

aufgerufen am 30.06.2026

[11] Mucci, T. (o.D.). Was ist gemeinsame Datennutzung? URL: https://www.ibm.com/de-de/think/topics/data-sharing

aufgerufen am 30.06.2026

[12] Koch, M. (o.D.). Kooperationssysteme. URL: https://wi-lex.de/lexikon/informations-daten-und-wissensmanagement/informationsmanagement/it-infrastruktur/informations-und-kommunikationstechnologien/computer-supported-cooperative-work-cscw/kooperationssysteme/#:~:text=Kooperation%20stellt%20schlie%C3%9Flich%20die%20Zusammenarbeit%20im%20engeren,die%20gemeinsame%20Haltung%20und%20Bearbeitung%20von%20Daten

aufgerufen am 30.06.2026

[13] Aquino, J., Badman, A. und Kosinski, M. (o.D.). What are data silos? URL: https://www.ibm.com/think/topics/data-silos

aufgerufen am 30.06.2026

[14] Kühne, M. und Meusel, D. (o.D.). Data Sharing. URL: https://tu-dresden.de/gsw/phil/iso/mes/ressourcen/dateien/prof/mitarbeit/dateien_kuehne/Arbeitspapiere/Datasharing.pdf?lang=de

aufgerufen am 30.06.2026

[15] Haller, S., Golliez, A., Hohl, L., Schwarz, D. und Fivaz, J. (2025). Data-Sharing-Initiativen und Datenräume in der Schweiz. Übersicht, Stand und Handlungsbedarf – ein Diskussionsbeitrag. URL: https://www.bfh.ch/.documents/ris/2025-746.521.714/BFHID-1292545753-2/Studie%20Data-Sharing-Initiativen%20-%20Datenraeume%202025%20final.pdf

aufgerufen am 30.06.2026

[16] Peyman, S., Gili, R., Manning, B.S., Fradkin, A. und Horton, J.J. (2026): The Coasean Singularity? Demand, Supply, and Market Design with AI Agents. In: Agrawal, A.K., Brynjolfsson, E. und Korinek, A. (Hrsg, 2026): The Economics of Transformative AI. University of Chicago Press

[17] Hanson, B. (2025): The Interline AI Report 2025. Interline and MMGNET Group. URL: https://www.theinterline.com/2025/06/16/the-ai-report-2025-available-now/

aufgerufen am 17.08.2026

[18] Weiss, A., Albertson, Z. und Lanfear, E. (2026): Content Independence Day, one year on building the business model for the agentic Internet. Cloudflare Blog 2026-07-01. URL: https://blog.cloudflare.com/agentic-internet-bot-report/

aufgerufen am 17.08.2026

[19] International Data Spaces Association (o.D.). DATA SPACES. Where the future of data happens. URL: https://internationaldataspaces.org/why/data-spaces/

aufgerufen am 30.06.2026

[20] T-Systems (o.D.). Data spaces: using data together. URL: https://www.t-systems.com/de/en/data-intelligence/solutions/data-spaces

aufgerufen am 30.06.2026

[21] Gaia-X (o.D.). About Gaia-X. URL: https://gaia-x.eu/about/

aufgerufen am 30.06.2026

[22] European Commission (2025). Common European data spaces. URL: https://digital-strategy.ec.europa.eu/en/policies/data-spaces

aufgerufen am 30.06.2026

[23] Leinweber, C. (o.D.). Sovereign cloud explained simply: control, security, and trust in the digital world. URL: https://www.maiborn-wolff.de/en/know-how/souveraene-cloud/

aufgerufen am 30.06.2026

[24] Cloudflare (o.D.). Was ist Datenlokalisierung? URL: https://www.cloudflare.com/de-de/learning/privacy/what-is-data-localization/

aufgerufen am 30.06.2026

[25] OECDpublishing [12.2021] OECD digital economy papers. Mapping data portability initiatives, opportunities and challenges. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/12/mapping-data-portability-initiatives-opportunities-and-challenges_97cd728b/a6edfab2-en.pdf

aufgerufen am 30.06.2026

[26] Ahmed, S. [21.11.2021] SSRN. Data Portability: Key to Cloud Portability and Interoperability. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1712565

aufgerufen am 30.06.2026

[27] bidt [25.10.2022] Blog. Datenportabilität lohnt sich: Eine Datenmitnahmemöglichkeit verbessert die nutzerseitige Wahrnehmung von Onlineservices. URL: https://www.bidt.digital/datenportabilitaet-lohnt-sich-eine-datenmitnahmemoeglichkeit-verbessert-die-nutzerseitige-wahrnehmung-von-onlineservices/

aufgerufen am 30.06.2026

[28] Dr. Datenschutz [o.D.] Dr. Datenschutz. Intersoft consulting services. Datenübertragbarkeit: Das Betroffenenrecht in der Praxis. URL: https://www.dr-datenschutz.de/datenuebertragbarkeit-das-betroffenenrecht-in-der-praxis/

aufgerufen am 30.06.2026

[29] Münch, S. [26.04.2026] Datenschutz.org. Datenportabilität: Das Recht auf Datenübertragbarkeit. URL: https://www.datenschutz.org/datenportabilitaet/

aufgerufen am 30.06.2026

[30] intersoft consulting [o.D.] Art. 20 DSGVO Recht auf Datenübertragbarkeit. URL: https://dsgvo-gesetz.de/art-20-dsgvo/

aufgerufen am 30.06.2026

[31] intersoft consulting (o.D.). DSGVO - Privacy by Design. URL: https://dsgvo-gesetz.de/themen/privacy-by-design/

aufgerufen am 30.06.2026

[32] Feth, D. (2018). Die DSGVO und was sie für Digitale Dienste bedeutet: Das Recht auf Datenübertragbarkeit, Privacy by Design und Privacy by Default. URL: https://www.iese.fraunhofer.de/blog/die-dsgvo-und-was-sie-fuer-digitale-dienste-bedeutet-das-recht-auf-datenuebertragbarkeit-privacy-by-design-und-privacy-by-default/

aufgerufen am 30.6.2026

[33] Industrie- und Handelskammer zu Leipzig (o.D.). Privacy by Design | Privacy by Default. URL: https://www.leipzig.ihk.de/infos-fuer-unternehmen/themen/recht-steuern/datenschutzrecht/privacy-by-design-privacy-by-default/

aufgerufen am 30.06.2026

[34] European Commission [o. D.] Rules on international data transfers. URL: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_en?prefLang=de

aufgerufen am 30.06.2026

[35] Simic, I. [31.07.2025] proliance. EU-Standardvertragsklauseln: So gelingt der internationale Datentransfer. URL: https://www.proliance.ai/blog/eu-standardvertragsklauseln-scc

aufgerufen am 30.06.2026

[36] BfDI [o. D.] Internationale Datenübermittlungen. URL: https://www.bfdi.bund.de/DE/Fachthemen/Inhalte/Europa-Internationales/Internationaler_Datentransfer.html

aufgerufen am 30.06.2026

[37] IBM (o.D.). Was ist ein Compliance-Managementsystem (CMS)? URL: https://www.ibm.com/de-de/think/topics/compliance-management-system

aufgerufen am 30.06.2026

[38] HRworks (o.D.). Definition, Maßnahmen und Prozesse - Compliance Management. URL: https://www.hrworks.de/lexikon/compliance-management/

aufgerufen am 30.06.2026

[39] Fortinet (o.D.). Was ist Compliance-Automatisierung? URL: https://www.fortinet.com/de/resources/cyberglossary/compliance-automation

aufgerufen am 30.06.2026

[40] Steinbuß, S. [17.03.2025] DIN. Standards ebnen den Weg zur Datensouveränität. URL: https://www.din.de/de/din-und-seine-partner/presse/mitteilungen/standards-ebnen-den-weg-zur-datensouveraenitaet--1211284

aufgerufen am 30.06.2026

[41] Rohde, M., Eisenträger, M., Wittenbrink, N., Straub, S. und Gabriel, P. [10.2022] Institut für Innovation und Technik (iit). Datenqualität und Qualitätsmetriken in der Datenwirtschaft. URL: https://www.iit-berlin.de/wp-content/uploads/2022/11/Datenqualitaet-und-Datenmetriken_iit-Studie_2022.pdf

aufgerufen am 30.06.2026

[42] Barbour, D. [05.10.2023] Kiteworks. Datenhoheit: Eine Best Practice oder gesetzliche Anforderung? URL: https://www.kiteworks.com/de/regulatorische-compliance/datenhoheit-eine-best-practice-oder-gesetzliche-anforderung/#Datensouveraenitaet_als_regulatorische_Anforderung

aufgerufen am 30.06.2026

[43] Leitwerk [o. D.] BSI-Kritisverordnung. URL: https://www.leitwerk.de/lexikon/bsi-kritisverordnung/

aufgerufen am 30.06.2026

[44] Bundesamt für Sicherheit in der Informationstechnik [o. D.] Telematikinfrastruktur – sichere Vernetzung medizinischer Versorgung. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/E-Health/Telematikinfrastruktur/telematikinfrastruktur.html

aufgerufen am 30.06.2026

Abbildungen

Abbildung 1: Trendradar Datenökonomie und digitale Souveränität (erstellt mit ITONICS)

Abbildung 2: International Data Spaces Association (o.D.). DATA SPACES. Where the future of data happens (https://internationaldataspaces.org/why/data-spaces/)

Abbildung 3: Vergleich von Privacy by Design und Privacy by Default (nach https://www.cookiebot.com/en/privacy-by-design/)

ÜBER DAS MITTELSTAND-DIGITAL ZENTRUM SMARTE KREISLÄUFE

Mit unseren Partnern zeigen wir passgenaue Lösungen auf, wie Sie die Digitalisierung in Ihrem Unternehmen voranbringen können. Gemeinsam mit Ihnen erstellen wir Roadmaps für die nächsten Schritte oder setzen in Praxisprojekten erste Maßnahmen um.

Das Mittelstand-Digital Zentrum Smarte Kreisläufe besteht seit März 2023 und umfasst fünf Partner:

Gesamtverband der deutschen Textil- und Modeindustrie

Als Konsortiumsführer und Transferpartner bringt der Verband seine Expertise im Bereich der sozialen Aspekte der Nachhaltigkeit, Kreislaufwirtschaft und Kooperationen mit Startups ein und managt das Netzwerk.

Deutsche Institute für Textil- und Faserforschung Denkendorf (DITF)

Die DITF sind Experten für individualisierte Produkte in den Bereichen Bekleidung, Smart Textiles und Leichtbau. Sie machen durchgehendes Engineering erlebbar: von der Idee bis zum fertigen Produkt.

Institut für Textiltechnik (ITA) der RWTH Aachen University

Das ITA zeigt, wie Smart Data dazu beitragen kann, eine nachhaltige Zukunft zu gestalten. Gäste können die Vernetzung einer vollstufigen textilen Prozesskette hautnah erleben und erfahren, welcher wirtschaftliche Nutzen sich durch die digitale Transformation ergibt.

Sächsisches Textilforschungsinstitut e. V. (STFI)

Das STFI in Chemnitz demonstriert vertikale Integration, vernetzte Produktionssysteme und Ressourceneffizienz, etwa die Selbstoptimierung von komplexen Anlagen.

Bundesverband Kooperierender Mittelstand e. V. (BKM)

Der Verband verfügt über ein breites Netzwerk aus in Verbundgruppen organisierten Unternehmen in den Bereichen Handel, Handwerk und Dienstleistungen aus 45 Branchen. Als Transferpartner erfasst er die Bedarfe der Unternehmen und bringt die Arbeitsergebnisse des Zentrums in die mittelständische Wirtschaft.

Das Mittelstand-Digital Zentrum Smarte Kreisläufe gehört zu 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

IHR DIREKTER DRAHT ZU UNS / IMPRESSUM

Schaufenster Aachen

Varqha Bagwan

bagwan@mdz-sk.de

Schaufenster Denkendorf

Dr. rer. pol. Marcus Winkler

winkler@mdz-sk.de

Schaufenster Berlin

Anja Merker

merker@mdz-sk.de

Schaufenster Köln

Tim Geier

geier@mdz-sk.de

Schaufenster Chemnitz

Dirk Zschenderlein

zschenderlein@mdz-sk.de

Mittelstand-Digital Zentrum Smarte Kreisläufe
c/o Gesamtverband textil+mode
Wallstr. 58
10179 Berlin
Telefon: 030 726220-48
E-Mail: kontakt@mdz-sk.de
www.smarte-kreislaeufe.de

Die vorliegende Broschüre ist eine Veröffentlichung des Gesamtverbandes textil+mode im Rahmen des Mittelstand-Digital Zentrums Smarte Kreisläufe.

Herausgeber:
Gesamtverband textil+mode
Wallstr. 58
10179 Berlin

Telefon: 030 726220-48
E-Mail: kontakt@mdz-sk.de

Berlin, September 2026

Vereinsregister des Amtsgerichts Berlin Charlottenburg VR 27113 B
Hauptgeschäftsführer: Dr. Uwe Mazura

Redaktion: Hannah Feichtner, DITF; Gisela Stegmann, DITF; Dr. rer. pol. Marcus Winkler, DITF; Dr. Steffen Seeger, STFI
Gestaltung: Ulrike Markert, Gesamtverband textil+mode

Bildnachweis: Titel, S. 6, 11: Magnific.com; S. 12: Adobe Stock; S. 5, 9, 12: Unsplash.com; S. 13: iStock

www.smarte-kreislaeufe.de