Whitepaper

Souveräne Cloud

# Souveräne Cloud für den Mittelstand

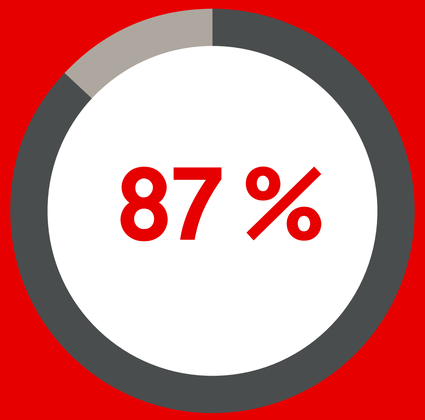
## Smarte Souveränität als Schlüssel zur Wettbewerbsfähigkeit

vodafone business

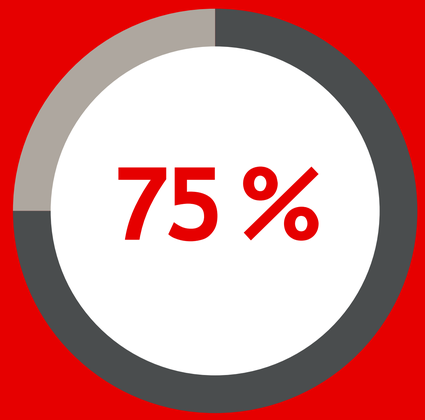
Together we can

# Großer Bedarf und großes Potenzial für souveräne Cloud-Lösungen

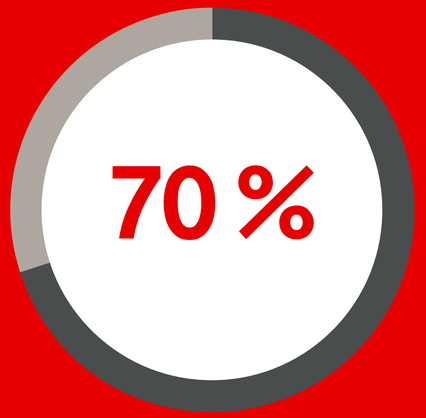

**der vom Bitkom befragten deutschen Unternehmen würden eine Cloud-Lösung von einem deutschen Anbieter bevorzugen.**
(Seite 4)




**der von deutschen Unternehmen eingesetzten digitalen Technologien und Leistungen stammen gemäß einer Bitkom-Studie aus den USA.**
(Seite 6)




**der von Kyndryl befragten Unternehmen sind besorgt über die geopolitischen Risiken, die sich aus der Speicherung und Verwaltung von Daten in globalen Clouds ergeben.**
(Seite 6)




**der in der Lünendonk-Studie 2025 befragten IT-Sourcing-Beratungen werden von ihren Kunden häufig oder sehr häufig nach souveränen Cloud-Angeboten aus Deutschland gefragt.**
(Seite 10)


**(25,6 Mrd. US-$) beträgt das von IDC prognostizierte Marktvolumen für souveräne Cloud-Lösungen in Deutschland im Jahr 2028.**
(Seite 8)

# Vorwort

**Souveränität über Unternehmens- und Kundendaten ist wichtiger denn je.** Doch was bedeutet das konkret und wie gelingt die richtige Balance zwischen Kontrolle und Wettbewerbsfähigkeit?

Die weltpolitische Lage und wirtschaftliche Krisen haben deutlich gemacht: Für Unternehmen wird Souveränität zu einem immer wichtigeren Faktor. Wie lassen sich die überzeugenden Vorteile von Cloud-Lösungen mit dem Anspruch verbinden, die volle Hoheit über Unternehmens- und Kundendaten zu behalten – technisch, rechtlich und organisatorisch?

Das Stichwort lautet „souveräne Cloud". Aber was bedeutet dies eigentlich im Detail? Was müssen speziell kleine und mittlere Unternehmen bei der Entscheidung für eine solche Lösung beachten? Wie lassen sich regulatorische Anforderungen wie die Datenschutz-Grundverordnung (DSGVO) und das Bundesdatenschutzgesetz dabei erfüllen?

Cloud-Souveränität ist für Unternehmen ein zentraler Wettbewerbsfaktor. Entscheidend ist, je nach Anwendungsfall den passenden Grad an Souveränität umzusetzen. Um Wettbewerbsfähigkeit und Cloud-Vorteile sinnvoll auszubalancieren, braucht es eine souveränitätsorientierte Strategie mit Augenmaß – abgestimmt auf das jeweilige Einsatzszenario.

Das vorliegende Whitepaper erklärt, was eine souveräne Cloud ist, welche Komponenten sie umfasst und welche aktuellen Marktentwicklungen sowie regulatorischen Rahmenbedingungen relevant sind. Darüber hinaus werden die verschiedenen Ausprägungen und konkreten Einsatzmöglichkeiten für mittelständische Unternehmen dargestellt. Abschließend erhalten Unternehmen konkrete Handlungsempfehlungen und eine Checkliste für die erfolgreiche Planung und Umsetzung.

## Inhaltsverzeichnis


**0** Zahlen, Daten und Fakten 2

**1** Was ist eine souveräne Cloud? – Definition, Dimensionen und Kernmerkmale 4

**2** Marktumfeld, Treiber und Branchenrelevanz von Cloud-Souveränität 6

**3** Regulatorische Rahmenbedingungen zur Cloud-Souveränität 9

**4** Cloud-Modelle und ihre Souveränitäts-Ausprägungen 10

**5** Einsatzmöglichkeiten und Mehrwerte für den Mittelstand 12

**6** Handlungsempfehlungen und Checkliste 13

**7** Vodafone als Partner für die Sovereign Cloud 14

**8** Glossar 15

# 1 Was ist eine souveräne Cloud? Definition und Dimensionen

Gemäß dem „Cloud Report 2025“ [1] des Branchenverbands Bitkom nutzen **74 % der deutschen Unternehmen eine Private Cloud** und **59 % zusätzlich oder alternativ eine Public Cloud**. (Definitionen siehe Glossar, S. 15). Doch zu hohe Abhängigkeit von aus dem Ausland bezogenen Diensten bereitet Unternehmen zunehmend Sorge. Alle befragten Unternehmen (n=590, 100 Prozent) würden einen **Anbieter aus Deutschland bevorzugen**, dahinter folgt mit 61 Prozent ein Anbieter aus der EU.

## Cloud-Souveränität basiert auf mehreren Säulen

Um beantworten zu können, wie sich die gewünschte Souveränität umsetzen lässt, ist zunächst eine Abgrenzung zwischen den unterschiedlichen Ausprägungen von Souveränität sinnvoll. Grundsätzlich ist **Cloud-Souveränität ein Teilaspekt von digitaler Souveränität** (siehe Kasten).

Cloud-Souveränität basiert wiederum auf mehreren Säulen:

**Datensouveränität** (wörtlich: die Hoheit über die eigenen Daten): Unternehmen oder Organisationen müssen **selbstbestimmt über ihre Daten verfügen** können. Um durchgängig **Kontrolle und Transparenz** der eigenen Daten sicherzustellen, müssen Unternehmen bestimmen können, wer Zugang dazu hat und sie nutzen kann. Zudem muss **jederzeit der eigene Zugriff** auf die Daten **sichergestellt sein**.

**Betriebliche Souveränität** beginnt bei der **Souveränität des gesamten genutzten Ökosystems** (auch Partner und Dienstleister inklusive Telekommunikations- und Cloud-Anbieter) und umfasst Aspekte wie **Ausfallsicherheit**, **Einhaltung von Sicherheits- und Governance-Vorgaben sowie aller relevanten Vorschriften und Gesetze**.

**Technische Souveränität** verlangt zudem die **Portabilität und Reversibilität** von Anwendungen und Daten sowie die **Interoperabilität** der genutzten Cloud-Lösung mit bestehenden oder zukünftigen Lösungen anderer Anbieter.

All diese Dimensionen von Cloud Souveränität basieren auf zusätzlichen Aspekten, die in der Spalte rechts aufgeführt sind.

### Begriffsabgrenzung: Digitale Souveränität versus Cloud-Souveränität

- **Digitale Souveränität** meint die Kontrolle über die eigenen Daten, Prozesse und Infrastrukturen. Digitale Systeme sollen sich unabhängig von externen Einflüssen und Zwängen nutzen lassen.
- **Cloud-Souveränität** oder englisch „Cloud Sovereignty“ ist ein Teil der digitalen Souveränität. Sie umfasst die Kontrolle über in Cloud-Diensten gespeicherte Daten und Anwendungen. Dabei gilt es, nationale Datenschutzgesetze einzuhalten und den Schutz vor unbefugtem Zugriff durch ausländische Regierungen sicherzustellen.

## Dimensionen von Cloud-Souveränität

### Daten-Souveränität

**Datenlokalisierung**: Hosting, Nutzung, Speicherung oder Verarbeitung der Cloud-Daten an einem bevorzugten Standort in einer bevorzugten Gerichtsbarkeit (meist Heimatland).

**Dateneigentum:** Die Daten unterliegen jederzeit der Kontrolle und sind Eigentum ihres Urhebers/Besitzers.

**Datenrückverfolgbarkeit:** Fokus auf Verwaltung und Transparenz der Daten über ihren gesamten Lebenszyklus.

**Datenzugriffskontrollen:** Wer kann von wo aus und zu welchem Zweck auf die Daten zugreifen?

### Betriebliche Souveränität

**Ausfallsicherheit**: Sicherstellen der Kontinuität des Cloud-Dienstes, Schutz vor ungeplanten Störungen.

**Einhaltung gesetzlicher Vorschriften:** Berücksichtigung regions-/branchenspezifischer Vorschriften und Gesetze.

**Souveränität des Ökosystems** inklusive des Telekommunikations-/Cloud-Anbieters. Umfasst auch API-Aufrufe.

**Gewährleistung von Sicherheitszielen und Governance** inklusive Erkennung von Cyberangriffen und Reaktion darauf.

### Technische Souveränität

**Portabilität und Reversibilität:** Möglichkeit, Anwendungen und Daten von einer Cloud-Umgebung in eine andere zu verschieben, wobei Unterbrechungen minimal bleiben.

**Interoperabilität:** Die Lösung entspricht gängigen Integrationsstandards und lässt sich einfach mit bestehenden und/oder zukünftigen Lösungen anderer Anbieter verbinden.

**Vendor-Lock-in vermeiden:** Anbieter lassen sich jederzeit ohne hohe Kosten, technische Hürden oder rechtliche Abhängigkeiten wechseln.

[1] Quelle: Bitkom, Cloud Report 2025, https://www.bitkom.org/Presse/Presseinformation/Wirtschaft-ruft-nach-deutscher-Cloud

# 1 Was ist eine souveräne Cloud? Merkmale im Detail

Eine **souveräne Cloud** soll sicherstellen, dass Unternehmen die volle Kontrolle über ihre Daten behalten. Doch was genau kennzeichnet solche Lösungen?

## Betriebliche und technische Kernmerkmale

- **Datenresidenz und -lokalität**: Speicherung und Verarbeitung der Daten müssen nachweislich in Deutschland beziehungsweise der EU stattfinden. Dies setzt voraus, dass für alle genutzten Services ein transparenter Nachweis von Standort und Rechtsraum vorliegt. Allerdings müssen dazu auch rechtliche Detailfragen geklärt sein, wie etwa die Debatte um die Einführung eines EU-Schemas zur Zertifizierung der Cybersicherheit von Cloud-Diensten (EUCS) deutlich macht.

- **Schlüsselhoheit:** Krypto-Schlüssel müssen allein durch das Kunden-Unternehmen kontrolliert werden („hold your own key"). Dazu kann der „Key Management Service" (KMS) von den vom Provider erbrachten IT-Diensten getrennt werden. Nach diesem Prinzip bieten einige nicht-europäische Hyperscaler einen souveränen EU-Partnerbetrieb für das Key Management an.

- **Administrative Souveränität:** Für Admin-Zugriffe müssen strenge Regeln vereinbart werden. Nur in Notfällen findet ein sogenannter „Break-Glass-Zugriff" statt (nach dem Vorbild eines Feuermelders – Zugriffe durch den Anbieter erfolgen nur im Notfall und nur auditiert bzw. durch den Kunden genehmigt), jeder Admin-Zugriff wird protokolliert.

- **Audits & Standards:** Mindeststandard in Deutschland ist die C5-Attestierung [1] durch das Bundesamt für Informationssicherheit (BSI). Ergänzend dazu können Zertifizierungen nach ISO 27001/27701, SOC 2 und weiteren, branchenspezifischen Normen stattfinden.

- **Governance und Nachweise gemäß DSGVO** (Datenschutzgrundverordnung, oder engl. GDPR, General Data Protection Regulation). Anbieter, die dem „EU Data Protection Code of Conduct for Cloud Service Providers" oder kurz „EU Cloud Code of Conduct" bzw. „EU Cloud CoC" beigetreten sind (Art. 40 DSGVO), liefern prüfbare Konformitätsebenen.

- **Portabilität und Interoperabilität:** Um Vendor-Lock-ins zu vermeiden, müssen souveräne Cloud-Lösungen API-Offenheit, Exit-Support und transparente Egress-Konditionen bieten. Auch im Zuge des „EU Data Act" gewinnt ein kostenfreier Wechsel zu einem anderen Anbieter an Bedeutung.

- **Bewertung von Rechtsraum-Risiken und Umsetzung von Schutzmaßnahmen:** Bei der Auswahl einer souveränen Cloud-Lösung gilt es, auch extraterritoriale Zugriffsrechte (zum Beispiel im Rahmen des „U.S. Cloud Acts", siehe auch S. 7) zu bewerten. Gegegebenenfalls muss es technische und vertragliche Gegenmaßnahmen geben (zum Beispiel EU-Betreibermodell, EU-Rechtswahl, Verschlüsselung, Datenteilung nach „Need-to-know"-Prinzip).

[1] „Cloud Computing Compliance Criteria Catalogue": https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

# 2 Geopolitische Risiken und Lösungs-Initiativen

In seinem „Readiness Report 2025“ [1] berichtet der IT-Infrastruktur-Zulieferer Kyndryl, dass für 86 % der befragten Unternehmen das **Herkunftsland und die regulatorischen Rahmenbedingungen von Cloud-Angeboten zunehmend wichtige Faktoren** bei der Evaluierung von Cloud-Lösungen sind. 75 % bestätigen, dass ihre Organisation zunehmend besorgt über die **geopolitischen Risiken** ist, die sich aus dem Speichern und Verwalten kritischer Daten in globalen Cloud-Umgebungen ergeben.

Im Kontrast dazu steht allerdings, aus welchen Ländern deutsche Unternehmen IT-Technologien und -Services tatsächlich beziehen. So berichtet der Digitalverband **Bitkom** [2], dass die **wichtigsten Herkunftsländer** dafür **mit 87 Prozent die USA** sind, dicht gefolgt von **China mit 78 Prozent.**

## EU-Initiative GAIA-X

Politische Weichenstellungen sollen helfen, diese Abhängigkeiten zu verringern. So will beispielsweise die **Europäische Union** mit ihrer **Initiative GAIA-X** eine leistungsfähige, sichere und vertrauenswürdige europäische Dateninfrastruktur schaffen, um Europas digitale Souveränität und Wettbewerbsfähigkeit zu stärken. Ziel ist ein **offenes, transparentes und interoperables Cloud-Ökosystem**, das europäischen Datenschutz und Selbstbestimmung garantiert. Am Projekt arbeiten Hunderte Unternehmen und Organisationen aus Wirtschaft, Wissenschaft und Politik gemeinsam daran, bestehende Lösungen zu vernetzen und nach gemeinsamen Standards auszurichten. GAIA-X setzt insbesondere auf **Open-Source-**Technologien und will eine Alternative zu US- und chinesischen Cloud-Anbietern schaffen, damit sensible Daten DSGVO-konform und unabhängig verarbeitet werden können.

## Der Sovereign Tech Fund des BMWE

Der Sovereign Tech Fund ist ein **Förderprogramm** des Bundesministeriums für Wirtschaft und Energie (**BMWE**). Es investiert gezielt in offene digitale Basistechnologien, um Wettbewerbsfähigkeit und Innovationskraft in Deutschland und Europa zu fördern. Das Programm soll insbesondere Startups und KMUs zugutekommen und die digitale Souveränität Europas stärken. Förderfähige Aktivitäten umfassen Entwicklungsarbeiten, Security Audits oder Community-Building.

## Konsequenzen geopolitischer Entwicklungen für Cloud-Lösungen

In welchem Maße stimmt Ihr Unternehmen (n=3639) folgenden Aussagen zu?

86 %

stimmen zu, dass das **Herkunftsland und die regulatorischen Rahmenbedingungen zunehmend wichtige Faktoren bei der Evaluierung von Cloud-Angeboten** sind.

75 %

stimmen zu, dass ihr Unternehmen **zunehmend besorgt über die geopolitischen Risiken ist, die sich aus der Speicherung und Verwaltung von Daten in globalen Cloud-Umgebungen** ergeben.

[1] Quelle: https://www.kyndryl.com/content/dam/kyndrylprogram/doc/en/2025/readiness-report.pdf

[2] Quelle: https://www.bitkom.org/sites/main/files/2025-02/2025-bitkom-studienbericht-digitale-souveraenitaet.pdf

# 2 Treiber für souveräne Cloud-Lösungen

## Konflikte in internationalen Rechtsrahmen

**Regulatorische Anforderungen** wie die **DSGVO** und das **Bundesdatenschutzgesetz** (BDSG, siehe auch Glossar, Seite 15) verpflichten Unternehmen bereits heute zu höchster Datensicherheit. Allerdings stehen gesetzliche Vorgaben in anderen Jurisdiktionen zum Teil im Widerspruch zu diesen Anforderungen. Daraus ergeben sich für deutsche Unternehmen unter Umständen **erhebliche Risiken**.

So unterliegen alle in den **USA ansässigen Anbieter** dem **„U.S. Cloud Act"**. Dieses Gesetz, das ausführlich den Titel „Clarifying Lawful Overseas Use of Data Act" trägt, wurde 2018 in den USA verabschiedet. Es räumt US-Behörden **weitreichenden Zugriff auf Daten von US-Unternehmen und deren Tochterfirmen** ein – unabhängig davon, ob sich diese Daten auf Servern in den USA oder im Ausland befinden. Somit sind beispielsweise auch europäische Nutzer:innen und ihre Daten bei Einsatz von US-basierten Cloud-Diensten betroffen.

US-Unternehmen sind nach dem „Cloud Act" **verpflichtet, auf behördliche Anordnung Daten herauszugeben**, selbst wenn dies gegen lokale Regelungen wie die DSGVO verstößt. Das US-Gesetz steht also in direktem Konflikt mit europäischen Datenschutzanforderungen. Zudem können zu den ohnehin für alle in der EU ansässigen Unternehmen geltenden Vorgaben wie der DSGVO zum Beispiel **explizite Datenschutz-Anforderungen in öffentlichen Ausschreibungen** hinzukommen.

## Unternehmensinterne Treiber

Solche externen Treiber können durch weitere, interne Anforderungen verstärkt werden – etwa **Compliance-Richtlinien**, aber auch das Bedürfnis, die **Kontrolle über kritische Prozesse** zu behalten sowie das **Vertrauen von Kunden, Partnern und Investoren** zu schützen. Darüber hinaus können sich technische Erfordernisse aus **IT-Sicherheitsanforderungen** ableiten. Letztlich kann eine Vielzahl unterschiedlicher Treiber die Notwendigkeit begründen, die Souveränität von Cloud-Lösungen sicherzustellen.

## Sovereign-Cloud-Lösungen als Antwort auf externe und interne Anforderungen

Für Unternehmen bietet die Sovereign Cloud erhebliche Vorteile:

- **Compliance-Faktor Sovereign Cloud:** Compliance, also die Beachtung und transparente Umsetzung von Gesetzen, Richtlinien und anderen Rechtsnormen, ist für Unternehmen nicht nur Selbstzweck. Sie minimiert außerdem viele Risiken und schützt das Image eines Unternehmens.
- **Garantierte DSGVO-Konformität:** Die Datenschutz-Grundverordnung sieht scharfe Sanktionen vor, wenn persönliche Daten von Kund:innen, Mitarbeiter:innen oder anderen natürlichen Personen gestohlen werden oder durch eine Datenpanne in den Besitz Dritter gelangen. Für Unternehmen drohen hohe Geldstrafen (bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes). Bereits die nachgewiesene Verwendung nicht mehr zeitgemäßer Verschlüsselungsverfahren kann im Einzelfall zu einer höheren Geldstrafe führen. Die Verwendung einer DSGVO-konformen Sovereign Cloud minimiert das Risiko von Datendiebstählen und Datenverlusten.
- **Schutz vor Spionage:** Durch einen Cloud-Standort innerhalb der EU oder in einem sicheren Drittland können Unternehmensdaten insgesamt besser geschützt werden. Das verhindert etwa, dass ausländische Wettbewerber oder Nachrichtendienste in den Besitz sensibler Daten gelangen.
- **Ausschreibungsbedingung Sovereign Cloud:** Behörden und Kunden aus sicherheitskritischen Sektoren verlangen bei Ausschreibungen zunehmend die Nutzung von sicheren Cloud-Produkten für die gesamte Auftragsabwicklung. Unternehmen, die bereits eine sichere Sovereign Cloud einsetzen, haben somit einen Vorteil.

# 2 Relevanz souveräner Cloud-Lösungen je nach Branche und Datenkritikalität

Das Marktforschungsunternehmen IDC [1] erwartet für souveräne Cloud-Lösungen im Jahr 2028 ein **Marktvolumen von 25,6 Milliarden US-Dollar (22 Milliarden Euro)**. Produktion und Finanzdienste haben daran die größten Anteile, das Gesundheitswesen zeigt die größten Steigerungsraten.

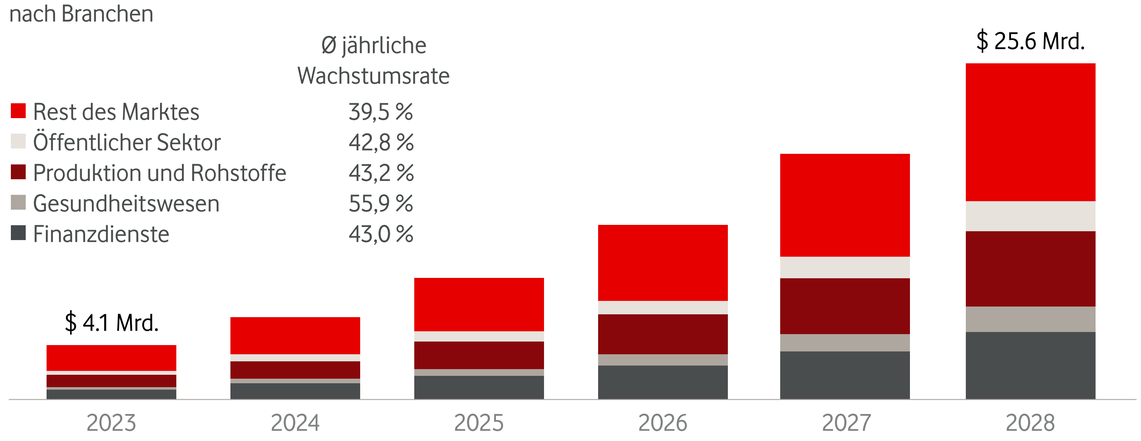
Je nach Branche bzw. Sektor bringt eine souveräne Cloud unterschiedliche Vorteile. So steht etwa im **Gesundheitswesen** der **Schutz sensibler Patientendaten** im Fokus. In **Industrie und Maschinenbau** gilt es, den **Schutz von Patenten und Innovationen auch in digitalen Lieferketten** zu gewährleisten. Im **Finanz- und Versicherungswesen** stehen **Revisionssicherheit und Bafin-Konformität** an erster Stelle.

Und im **öffentlichen Sektor** sowie im **Bildungswesen** ist die primäre Zielsetzung, **bürgernahe Dienste auf vertrauenswürdiger Infrastruktur** bereitzustellen. Allerdings ist nicht in allen Anwendungen die **Kritikalität der Daten** gleich hoch – auch innerhalb einer Branche. Es gilt also, für jede konkrete Anwendung die richtige **Balance zwischen Datenkritikalität und Souveränitäts-Anspruch** zu erreichen.

Je nach Branche spielen dabei aber auch noch regulatorische Rahmenbedingungen eine entscheidende Rolle. Diese beleuchten wir auf der nachfolgenden Seite.

## Voraussichtliche Investitionen nach Branche

Verteilung des von IDC für 2028 prognostizierten Marktvolumens für souveräne Cloud-Lösungen im Jahr 2028 nach Branchen




[1] Quelle: Vodafone und IDC

## Relevanz souveräner Cloud-Lösungen in unterschiedlichen Branchen

| Lösung | Gesundheitswesen | Industrie und Maschinenbau | Finanzen und Versicherungen | Öffentlicher Sektor und Bildung |
|---|---|---|---|---|
| Relevanz/Marktgröße | groß | sehr groß | sehr groß | groß |
| Digitalisierungsstand | mittel bis hoch | mittel bis hoch | hoch | gering bis mittel |
| Kritikalität der verarbeiteten Daten | mittel (z. B. Bettenbelegung im Krankenhaus) bis sehr hoch (z. B. elektronische Patientenakte) | hoch (z. B. Liefermanagement) bis sehr hoch (z. B. Konstruktions- und Porduktionsdaten) | mittel (z. B. Recruiting-Prozesse) bis sehr hoch (z. B. Transaktionsdaten) | mittel (z. B. Energieverbrauchserfassung) bis sehr hoch (z. B. personenbezogene Daten) |
| Potenzial souveräner Cloud-Lösungen | hoch bis sehr hoch | hoch bis sehr hoch | hoch | hoch |

# 3 Regulatorische Rahmenbedingungen zur Cloud-Souveränität

Die im Folgenden aufgeführten Rahmenbedingungen, Kriterienkataloge und Empfehlungen legen regulatorische Eckpunkte für souveräne Cloud-Lösungen fest und helfen somit auch bei der Orientierung auf dem Markt.

## Regulatorischer Kontext

Das bereits erwähnte **EU Cloud Services Scheme (EUCS)** ist ein freiwilliges Zertifizierungs-Framework, das auf dem „Cybersecurity Act" der EU (2019/881) basiert. Es ist politisch noch stark umstritten; jüngste Entwürfe lockerten die Souveränitätskriterien und fokussieren sich stärker auf technische Kriterien und Transparenz. Voraussichtlich wird die verabschiedete Fassung eine wichtige Rolle für Ausschreibungen bzw. das Labeling von Angeboten spielen.

**BSI C5:** Der Kriterienkatalog „**Cloud Computing Compliance Criteria Catalogue**" (C5) [1] des **Bundesamts für Sicherheit in der Informationstechnik (BSI)** spezifiziert Mindestanforderungen an sicheres Cloud Computing und richtet sich in erster Linie an professionelle Cloud-Anbieter, Prüfungs-Instanzen und Kunden.

Der Katalog ist die **De-facto-Baseline** für Cloud-Sicherheit, Cloud-Service-Provider können die Konformität ihrer Produkte durch eine unabhängige Prüfung nachweisen.

**EU Cloud CoC:** Der transnationale „**EU Data Protection Code of Conduct for Cloud Service Providers**" [2] harmonisiert die Vorgaben der Datenschutz-Grundverordnung (DSGVO) und gilt somit EU-weit als wichtiges Compliance-Werkzeug. Der EU Cloud COC ist eine Empfehlung des **European Data Protection Board**. Als erste europäische Behörde hat ihn die belgische Data Protection Authority genehmigt, weitere Ratifizierungen werden in Kürze erwartet.

**NIS2:** Die „**Network and Information Systems Directive 2**", (siehe auch Glossar, S. 15 und Whitepaper „Cloud Security") ist eine EU-weite Regelung zur Verbesserung der Cybersicherheit in der EU. Sie legt strenge Sicherheitsanforderungen und Meldepflichten für Unternehmen und öffentliche Einrichtungen in 18 kritischen Sektoren fest. Sie soll ein hohes Sicherheitsniveau gewährleisten, Cyberangriffe besser abwehren und die Zusammenarbeit zwischen den Mitgliedstaaten stärken.

### Sonderfall Kritische Infrastrukturen

In einigen Ländern gelten verschärfte Rechtsnormen für IT-Sicherheit und Datenschutz für bestimmte Branchen oder Sektoren.

In Deutschland gelten für Betreiber sogenannter **Kritischer Infrastrukturen (kurz: KRITIS)** besondere gesetzliche Regelungen:

- Unter anderem gilt eine **erweiterte Meldepflicht** bei IT-Störungen oder festgestellten Cyberattacken.
- Außerdem wird darüber diskutiert, für KRITIS-Organisationen **Sovereign Clouds** als einzige zulässige Cloud-Form **vorzuschreiben** – etwa über einen entsprechenden Nachtrag in der bereits bestehenden KRITIS-Verordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI-KritisV).

[1] Link: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Cloud-Computing/Kriterienkatalog-C5/kriterienkatalog-c5_node.html

[2] Link: https://eucoc.cloud/en/home

# 4 Bereitstellungsmodelle für Cloud-Lösungen

Bei der Auswahl von Cloud-Lösungen ist ein wichtiger Faktor, ob die eingesetzte Infrastruktur als **Public Cloud**, **Private Cloud** oder **Hybrid Cloud** implementiert wird (Definitionen siehe Glossar S. 15). Die Lünendonk-Studie 2025 [1] zeigt, dass hybride und souveräne Lösungen im Trend liegen.

## Wie werden Cloud-Modelle souverän?

Eine reine **Public Cloud** ermöglicht **maximale Skalierung** und bietet schnellen Zugriff auf Infrastruktur-**Innovationen**. Der Grad an Souveränität ist jedoch abhängig von den Mechanismen und Kontrollen, die der Provider anbietet. In der Regel gilt für diese Lösungen ein **globaler Rechtsrahmen**.

Wird eine Public Cloud zur **souveränen Public Cloud** erweitert, kommen Elemente wie **garantierter Betrieb innerhalb der EU**, **Kontrolle von Admin-Zugriffen**, **Schlüssel- und Datenlokalität** sowie in der EU angesiedelter Support hinzu. Diese Mechanismen müssen jedoch einer **zuverlässigen rechtlichen Kontrolle** unterliegen. Eine (rechenzentrumsgestützte) **Private Cloud** gewährleistet **höchste operative und ggf. physische Kontrolle**.

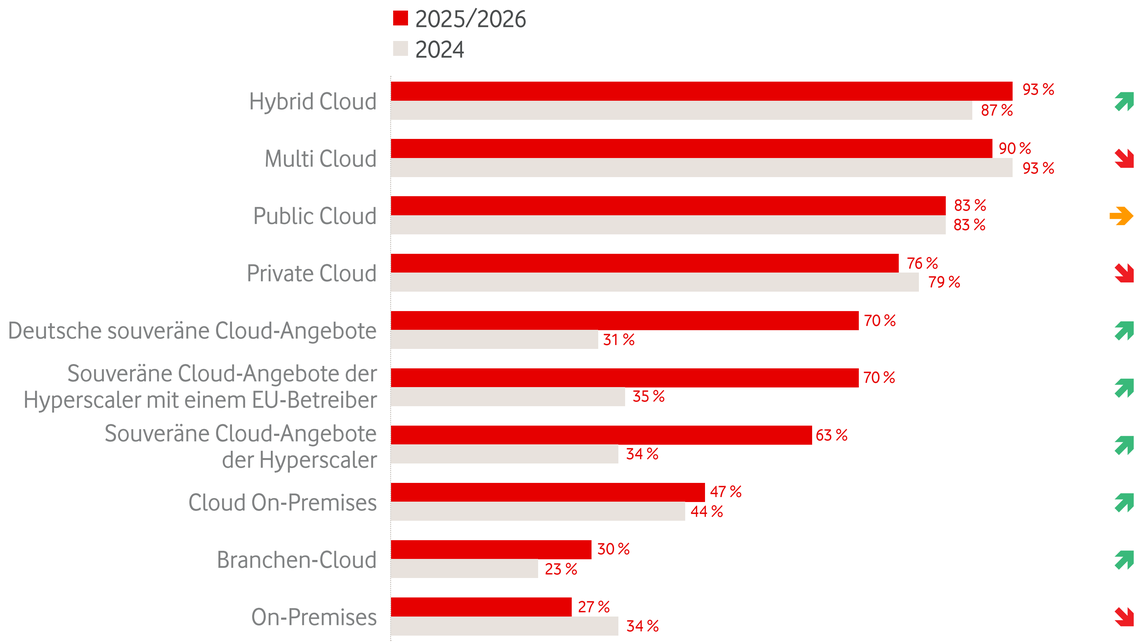
In der Regel bedingt dies ein weniger breites Angebot insbesondere an Hyperscaler-Services, ermöglicht im Gegenzug aber **maximale Daten- und Betriebs-Souveränität**. Allerdings müssen Unternehmen die geringere Skalierbarkeit solcher Lösungen ausgleichen.

In **Hybrid-Cloud**- beziehungsweise **Multicloud-Modellen** lassen sich die Workloads nach Kritikalität verteilen. Für **schützenswerte Daten** werden **souveräne Zonen** eingerichtet, während **unkritische, „elastische" Daten in Public-Cloud-Zonen** gespeichert und verarbeitet werden. In diesem Modell ist allerdings eine **Exit-/Egress-Strategie** besonders wichtig. Der „EU Data Act" definiert klare Regeln für den Wechsel von einem Cloud-Anbieter zu einem anderen – sowohl in puncto Kosten als auch im Hinblick auf die Datensouveränität.

Häufig wird die **Sovereign Cloud** als Unterkategorie der Private Cloud verstanden – das ist jedoch nicht korrekt. So bietet zum Beispiel Microsoft sowohl mit der Microsoft Sovereign Public Cloud als auch mit der Sovereign Private Cloud beide Varianten jeweils in souveräner Ausprägung an.

## Welche Bereitstellungsmodelle fragen Cloud-Kunden nach?

Umfrage unter IT-Sourcing-Beratungen; Skala von 1 = „nie" bis 4 = „sehr häufig"; dargestellte Antworten beziehen sich auf „eher häufig" und „sehr häufig"; relative Häufigkeitsverteilung; n = 29




[1] Quelle: Lünendonk-Studie 2025: IT-Sourcing-Trends 2025/2026, https://www.luenendonk.de/produkt/luenendonk-studie-2025-it-sourcing-trends-2025-2026

# 4 Entscheidungskriterien für ein souveränes Cloud-Modell

Bei der Entscheidung für ein souveränes Cloud-Modell gilt es somit, die Faktoren **Souveränität, Skalierbarkeit und Kosten auszubalancieren.** Die Zielsetzung sollte nicht sein, „Souveränität um jeden Preis" zu erlangen. Denn dies kann unter Umständen negative Auswirkungen auf die Wettbewerbsfähigkeit mit sich bringen.

Vielmehr sollten Unternehmen den erforderlichen Grad an Souveränität mit **Bedacht und Augenmaß** umsetzen – abgestimmt auf das jeweilige Einsatzszenario.

## Von Public bis Sovereign Cloud – Souveränität optimal gestalten

| | Public Cloud | Sovereign Public Cloud | Sovereign Private Cloud (Shared/Dedicated) | Sovereign Private Cloud On Premises |
|---|---|---|---|---|
| Merkmale | ✓ Multi-Tenant<br>✓ Maximale Skalierbarkeit<br>✓ Umfassendstes Angebot an Services und Applikationen | ✓ Multi-Tenant mit „Sovereign Controls"<br>✓ Hohe Skalierbarkeit<br>✓ Umfassendes Angebot an Services und Applikationen | ✓ Isolierte Umgebung von deutschem Anbieter<br>✓ Skalierbarkeit abh. von Modell<br>✓ Angepasstes Angebot an Services und Applikationen | ✓ Dedizierte Umgebung gehostet beim Unternehmen vor Ort<br>✓ Begrenzte Skalierbarkeit<br>✓ Angepasstes Angebot an Services und Applikationen |
| Daten-Kritikalität | ✓ Niedrig bis mittel<br>✓ primär öffentliche oder nicht sensible Informationen z. B. Website/eCommerce, CRM etc. | ✓ Mittel bis hoch<br>✓ geschäftsrelevant, aber nicht direkt sicherheits- oder versorgungsrelevant z. B. Kollaboration, E-Mail, ERP etc. | ✓ Hoch bis sehr hoch<br>✓ sensible personenbezogene, betriebsrelevante oder hochkritische Daten z. B. auch Kundendatenbanken mit persönlichen Daten | ✓ Sehr hoch<br>✓ hochkritische, versorgungs- oder lebensrelevante Systeme: Patienten-, Konstruktions- oder Produktions-/ Steuerungs-Daten meist OT |
| Compliance | ✓ DSGVO-konform | ✓ Verbesserte Kontrolle über die Datenhaltung und Zugriffe durch „Sovereign Controls" | ✓ Erhöhte Datenhoheit, Datenverarbeitung und -speicherung ausschließlich innerhalb Deutschlands | ✓ Volle Datenhoheit und Kontrolle über Daten, Anwendungen und Zugriffe |

**Skalierbarkeit und Preisvorteil** → **Grad der Souveränität**

Quelle: Vodafone

# 5 Einsatzmöglichkeiten und Mehrwerte für den Mittelstand

Souveräne Cloud-Lösungen werden in bestimmten Bereichen besonders häufig eingesetzt – typischerweise dort, wo **hohe Anforderungen an Datenschutz, Compliance, Datensouveränität und Betriebskontrolle** bestehen. So unter anderem in Bereichen wie Produktion und Industrie-IoT, KI-Anwendungen und CRM/Kundendatenlösungen. Einige exemplarische Beispiele zeigen, welche Vorteile und Mehrwerte eine souveräne Cloud in solchen Einsatzszenarien bietet:

## Datengetriebene Produktion & IoT

In **vernetzten Fertigungsprozessen** stellen die Trennung von OT- und IT-Umgebungen, der Schutz der Fertigungsdaten, Latenzen und die sich aus NIS2 ergebenden Pflichten besondere Anforderungen.

**Lösungs-Skizze:** Über Edge Computing oder eine Multi-Access-Edge-Cloud (etwa über ein 5G-Campusnetz) wird die Vorverarbeitung und Pseudonymisierung der Daten in den Werkshallen realisiert.
Eine souveräne Public-Cloud-Zone dient der Skalierung (Streaming/Time-Series, Data Lake, Analytics), eine souveräne Zone im Rechenzentrum für vertrauliche Daten wie Konstruktionspläne, Seriennummern etc.
Tragende Sicherheitselemente sind EU-Datenlokalität, „Bring your own key" und „Hold your own key", eine konsequente Rollentrennung (OT-Operator vs. Cloud-Ops), Zero-Trust zwischen Edge und Cloud sowie C5-kontrollierte Services. Dies stellt maximale Effektivität sicher und vermeidet ungeplante Stillstände sowie Datenabfluss-Incidents.

## DSGVO-konformes Kunden-CRM

Da **Customer Relationship Management** immer mit sensiblen Kundendaten umgeht, stehen hier Rechtmäßigkeit und Transparenz, Lösch- und Auskunftsrechte und Marketing-Einwilligungen im Fokus. Der Transfer der Daten in Drittländer würde erhebliche Risiken bergen.

**Lösungs-Skizze:** Der Kern der CRM-Anwendung wird in einer souveränen Public-Cloud-Zone gehostet (Betrieb und Support in der EU). Ein EU-CoC-konformer Identitäts- und Consent-Service dient als zentrale Policy-Engine. Eine souveräne Zone im Rechenzentrum enthält alle sensiblen Daten in einem „Sealed Data Lake". Die Zuordnung im CRM erfolgt über pseudonymisierte Schlüssel. Die wesentlichen Sicherheitselemente hier sind zur EU Cloud CoC konforme Services, Dokumentation gemäß Standard-Datenschutzklauseln und Transfer Impact Assessment (TIA). Data Processing Agreement (DPA) mit Subprozessor-Transparenz sowie Data-Retention-Policies.

## KI-Anwendungen mit sensiblen Daten

**Training und Einsatz von KI-Modellen** bergen besondere Risiken, wenn sie auf Basis sensibler, weil etwa personenbezogener Daten erfolgen. Hinzu kommen ggf. urheberrechtliche Risiken und mögliche Angriffsszenarien wie Modell-Exfiltration und Prompt-Injection.

**Lösungs-Skizze:** Die hochsensiblen Datensätze werden in einer souveränen Private Cloud im Rechenzentrum vorgehalten und in isolierten Compute-Pools verarbeitet. Die Inferenz, also die Wissens-Aufbereitung, erfolgt in einer souveränen Public Cloud, in der Computing und Storage konform zum EU CoC erfolgen.
Als Sicherheitselemente dienen ein Policy-Gateway (etwa zur Filterung von Prompts und der Moderation des Outputs) sowie eine „Hold your own key"-Schlüsselverwaltung. Das System ist nach dem Prinzip Differential Privacy aufgebaut, für Admin-Zugriffe gelten auditierte Sovereignty-Kontrollen. Zum Einsatz kommt ein Cloud-Anbieter mit C5/ISO-Nachweisen, der EU-Rechtsraum schützt vor Risiken etwa durch den „U.S. Cloud Act".

# 6 Handlungsempfehlungen und Checkliste

Wie gehen Unternehmen nun am besten vor, um abzuwägen, ob sie eine souveräne Cloud-Lösung nutzen wollen – und wenn ja, in welcher Ausprägung und mit welchen Rahmenbedingungen?

Die nebenstehende Checkliste hilft dabei, die **eigene Situation zu verstehen**, relevante **gesetzliche und regulatorische Vorgaben** zu bewerten, **technische Erfordernisse** und gegebenenfalls Abhängigkeiten zu identifizieren und aus diesen Faktoren die **Anforderungen** an die gesuchte Lösung abzuleiten.

So lässt sich letztlich erkennen, welche der zur Verfügung stehenden souveränen Cloud-Lösungen am **besten zum Business-Szenario Ihres Unternehmens** passt.

Aus den so herausgearbeiteten **Souveränitäts-Zielen** lässt sich dann ein **Schritt-für-Schritt-Fahrplan** entwickeln.

## Checkliste zur Sovereign Cloud

### Compliance-Vorgaben

- Sind die relevanten regulatorischen Anforderungen bekannt? (z.B. DSGVO, NIS2, DORA, branchenspezifische Vorgaben)
- Gibt es Vorgaben zur Datenlokation? (Nur EU/nur Deutschland/keine Einschränkung)
- Ist eine Risikobewertung bezüglich „Cloud Act" oder extraterritorialer Gesetze nötig?
- Sind interne Policies für Datenschutz und Compliance zu berücksichtigen?

### Anwendungen und Daten

- Welche Datenarten sollen in die Cloud? (Personenbezogene Daten, Betriebsgeheimnisse, kritische Systeme?)
- Wie hoch ist die Kritikalität dieser Daten bzw. der Anforderungen für den Geschäftsbetrieb?
- Gibt es Vorgaben zur Verschlüsselung? (BYOK, Customer-Managed Keys, HSM?)
- Gibt es bereits Anforderungen an Exit-Strategien? (z. B. Dartenexport bei Anbieterwechsel)

### Technische und operative Kontrolle

- Welche Anforderungen bestehen an Transparenz und Auditierbarkeit? (z. B. Zertifikate: ISO 27001, C5, EUCS)
- Soll der Provider nur Infrastruktur liefern, oder werden Managed Services erwartet? Besteht Wunsch nach Multi-Cloud/Hybrid-Cloud zur Risikoreduzierung?
- Gibt es Anforderungen an Incident Response, Monitoring und Logging? (z.B. Echtzeit-Zugriff, lntegration in SIEM)?

### Organisation und Governance

- Gibt es klare Verantwortlichkeiten für Cloud Governance? (Compliance, IT, Security, Fachbereiche)
- Existieren interne Skills zum Betrieb und zur Steuerung von Cloud-Umgebungen?
- Soll ein Partner für Managed Sovereignty Service einbezogen werden?
- Gibt es interne Awareness / Trainingsbedarf für souveräne Cloud-Nutzung?

### Strategische Aspekte

- Ist Cloud-Souveränität Teil der Unternehmensstrategie oder nur „nice to have"?
- Welche Risiken sollen konkret vermieden werden? (z. B. Abhängigkeit, Rechtsunsicherheit, fehlende Transparenz)
- Gibt es geplante Audits, Zertifizierungen oder externe Anforderungen? (z. B. von Kunden oder Behörden)
- Soll die Lösung langfristig EU-zertifizierbar sein? (z. B. EUCS, Gaia-X-Konformität)?

# 7 Vodafone als Partner für die Sovereign Cloud

Auf den vorherigen Seiten wurde die Wichtigkeit der Souveränität von Cloud-Modellen im Hinblick auf Marktbedingungen, Einsatzszenarien und relevanter Kriterien deutlich. Vor diesem Hintergrund stellt sich die Frage, worauf es bei der Anbieterauswahl in diesem Kontext ankommt.

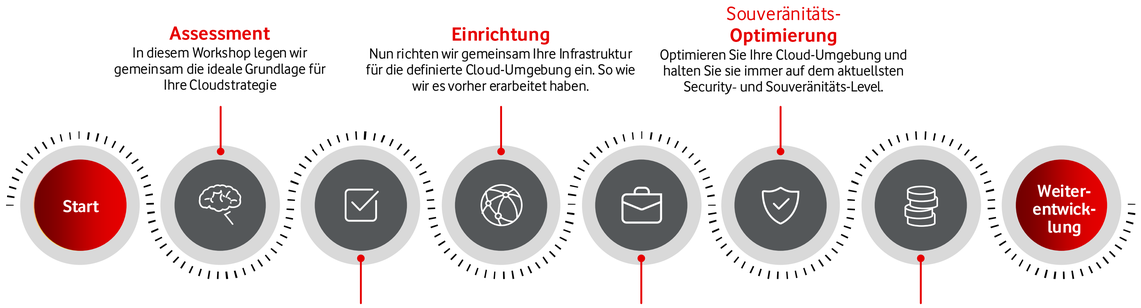
Entscheidend sind insbesondere **Ende-zu-Ende-Lösungen**, um passende Souveränität mit maximaler Wettbewerbsfähigkeit zu verbinden. Vodafone liefert dafür **smarte Cloud-Angebote**, die **speziell auf die Anforderungen unserer Kunden** zugeschnitten sind, **nahtlos integriert und individuell kombinierbar.**

Eine **Datenklassifizierung** hilft dabei, den Wert und die Kritikalität der eigenen Daten zu kennen, bevor man entscheidet, wo sie liegen und wie sie geschützt werden sollen.

**Regulatorische und Compliance-Anforderungen** sollten von Anfang an in die Lösungs-Architektur einfließen – statt sie nachträglich zu prüfen und zu berücksichtigen.

Die **Cloud-Expert:innen von Vodafone** sind zu allen diesen Themen Ihre idealen Ansprechpartner. Sichern Sie Ihre digitale Zukunft – souverän und solide.

## Ihr Weg zur souveränen Cloud




## Vodafone ist der richtige Partner für souveräne Cloud-Lösungen

### Souveränität aus eigener Erfahrung

Als KRITIS-Unternehmen muss Vodafone selbst täglich beweisen, dass es souverän agiert und bringt diese Erfahrung direkt in Kundenprojekte ein.

### Rechts- und Standortvorteil

Vodafone Deutschland ist ein eigenständiges Unternehmen, unterliegt der deutschen Rechtsprechung und arbeitet mit einer dezentralen Organisationsstruktur, um maximale Souveränität sicherzustellen.

### Komplettes Lösungsportfolio

Von Konnektivität über Cloud, SaaS bis hin zu Cyber-Sicherheit: Vodafone bietet maßgeschneiderte Komplettlösungen, die an das gewünschte Souveränitätslevel angepasst werden können und integriert bei Bedarf auch Partnerlösungen.

### Expertise und Beratung

Vodafone stellt erfahrene Cloud- und Sicherheitsexpert:innen bereit, die Unternehmen dabei unterstützen, die passende Lösung für ihre individuellen Anforderungen zu entwickeln.

### Weiterführende Informationen

Infos zur Sovereign Cloud:
**https://www.vodafone.de/business/blog/sovereign-cloud-20906**

Whitepaper Cloud Security:
**https://www.vodafone.de/business/digitale-loesungen/cloud-loesungen/whitepaper-cloud-security**

Whitepaper Migration:
**https://www.vodafone.de/business/digitale-loesungen/cloud-loesungen/whitepaper-cloud-migration**

### Individuelle unverbindliche Beratung

Kontaktieren Sie uns gerne telefonisch – kostenfrei von Montag bis Freitag, **8:00 bis 18:00 Uhr:**

**0800 505 45 13**

# 8 Glossar: Public Cloud, Private Cloud, Hybrid Cloud, BDSG, DSGVO und NIS2 – das steckt hinter den Fachbegriffen

## Bundesdatenschutz-gesetz

**Definition:** Das Bundesdatenschutzgesetz (BDSG) regelt in Deutschland den Umgang mit personenbezogenen Daten sowohl durch öffentliche Stellen wie Behörden als auch durch private Unternehmen. Es ergänzt die europaweit geltende **Datenschutz-Grundverordnung (DSGVO)** und konkretisiert deren Vorschriften dort, wo Mitgliedstaaten eigene Regelungen treffen dürfen – etwa beim Beschäftigtendatenschutz oder der Videoüberwachung. Ziel des BDSG ist es, das Recht auf informationelle Selbstbestimmung und den Schutz vor Missbrauch personenbezogener Daten sicherzustellen. Es definiert die Rechte der Betroffenen, Pflichten für Verantwortliche und Bestimmungen zur Bestellung von Datenschutzbeauftragten sowie Sanktionen bei Verstößen.

## DSGVO

**Definition:** Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der Europäischen Union, die seit dem 25. Mai 2018 unmittelbar in allen EU-Mitgliedstaaten gilt und den Schutz personenbezogener Daten natürlicher Personen regelt. Ihr Ziel ist es, einheitliche Standards für die Verarbeitung, Speicherung und Weitergabe personenbezogener Daten zu schaffen, um sowohl die Privatsphäre der Betroffenen zu schützen als auch den freien Datenverkehr im europäischen Binnenmarkt zu gewährleisten. Die DSGVO gilt für Unternehmen, Behörden und Organisationen, die personenbezogene Daten von EU-Bürger:innen verarbeiten. Bei Verstößen gegen ihre Regelungen drohen empfindliche Bußgelder.

## Hybrid Cloud

**Definition:** Eine Hybrid Cloud kombiniert **Public**- und **Private-Cloud**-Umgebungen. Dabei lassen sich Daten und Anwendungen je nach Bedarf zwischen beiden Modellen verteilen. Unternehmen können so sensible Daten in ihrer Private Cloud halten, während sie für skalierbare und weniger sensible Prozesse kostengünstige Public-Cloud-Ressourcen nutzen. Diese Architektur ermöglicht flexible Workload-Verlagerung, erhöht Ausfallsicherheit und optimiert die IT-Kosten. Häufig kommen dabei standardisierte Schnittstellen und Managementplattformen zum Einsatz, um eine nahtlose Integration der beiden Modelle und deren einheitliche Steuerung sicherzustellen.

## NIS2

**Definition:** Die „Network and Information Systems Directive 2," oder kurz NIS2-Richtlinie ist eine EU-weite Regelung zur Verbesserung der Cybersicherheit in der Europäischen Union. Sie ersetzt die erste NIS-Richtlinie von 2016 und weitet deren Anwendungsbereich deutlich aus, indem sie strengere Sicherheitsanforderungen und Meldepflichten für Unternehmen und öffentliche Einrichtungen in 18 kritischen Sektoren festlegt. Ziel ist es, ein einheitliches hohes Sicherheitsniveau für Netz- und Informationssysteme zu gewährleisten, Cyberangriffe besser abzuwehren und die Zusammenarbeit zwischen den Mitgliedstaaten zu stärken. In Deutschland gelten seit 2024 umfangreiche Umsetzungs- und Kontrollpflichten, die hohe Bußgelder bei Verstößen vorsehen.

## Private Cloud

**Definition:** Eine Private Cloud ist eine Cloud-Infrastruktur, die ausschließlich einer einzelnen Organisation zur Verfügung steht und entweder im eigenen Rechenzentrum oder durch einen dedizierten externen Anbieter betrieben wird. Sie bietet mehr Kontrolle, individuelle Sicherheitsmaßnahmen und die Möglichkeit, Infrastruktur und Anwendungen spezifisch an interne Anforderungen anzupassen. Private Clouds eignen sich besonders für Unternehmen mit hohen Datenschutz- und Compliance-Anforderungen, wie etwa im Finanz- oder Gesundheitswesen, und kombinieren Virtualisierung mit automatisierter Ressourcenbereitstellung.

## Public Cloud

**Definition:** Eine Public Cloud ist ein Cloud-Bereitstellungsmodell, bei dem Ressourcen wie Rechenleistung, Speicher und Anwendungen über das öffentliche Internet von einem externen Anbieter bereitgestellt und verwaltet werden. Die Nutzer teilen sich die Infrastruktur mit anderen Kunden, wobei die Betreiber strikte Mandantentrennung und Sicherheitsmaßnahmen gewährleisten. Die Public Cloud bietet hohe Skalierbarkeit, flexible Kostenmodelle und weltweiten Zugriff. Typische Beispiele sind Dienste wie Microsoft Azure, Amazon Web Services oder die Google Cloud Platform, die nach Bedarf genutzt und bezahlt werden.