

Welche Workload gehört wohin?

Die Entscheidungsmatrix für
souveräne Cloud-Architekturen
im Mittelstand

PERSÖNLICH.
STARK.
SICHER.
KLUG.
RICHTIG GUT.

Welche Workload gehört wohin?

Die Entscheidungsmatrix für souveräne Cloud-Architekturen im Mittelstand

Datensoeveränität ist im Unternehmensalltag angekommen – doch zwischen strategischem Anspruch und technischer Umsetzung klafft weiterhin eine deutliche Lücke. Dieser Leitfaden liefert kein pauschales Urteil für oder gegen Cloud, sondern eine praxisnahe Methode: eine Entscheidungsmatrix, mit der Sie für jede einzelne Workload begründet festlegen, welches Betriebsmodell zu ihr passt.

Inhalt

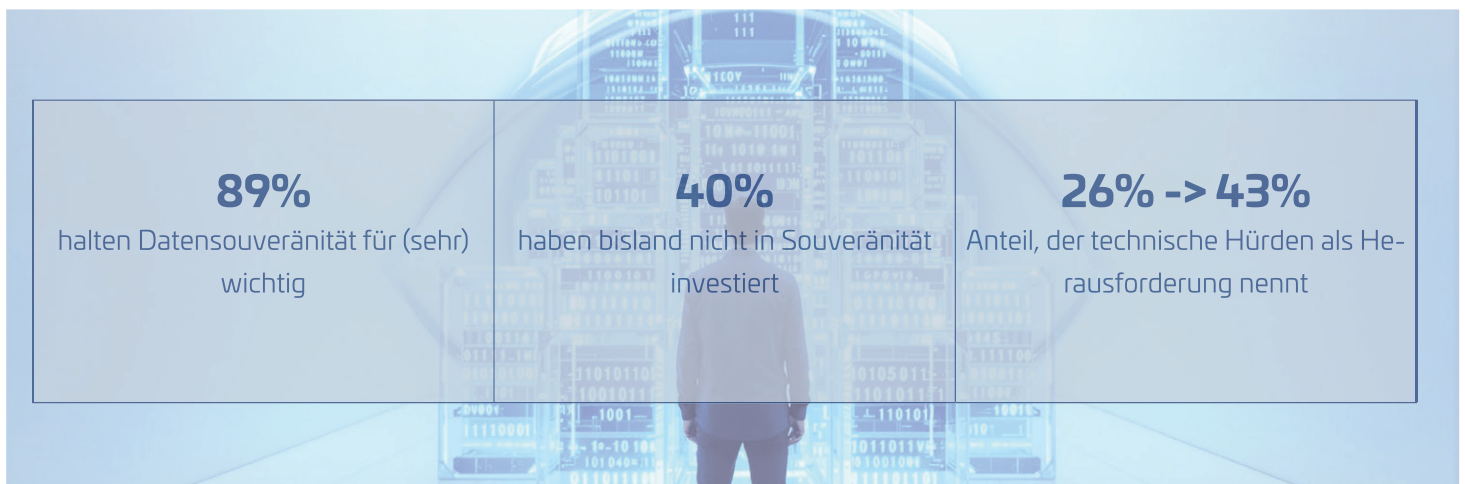
Welche Workload gehört wohin?.....	2
Management Summary.....	4
1. Die falsche Frage: „Cloud oder On-Premises?“	5
2. Die vier Betriebsmodelle im Überblick.....	7
3. Die sechs Bewertungsdimensionen der Entscheidungsmatrix	9
4. Die Matrix in der Praxis: Schritt für Schritt	12
5. Checkliste: Vier Bausteine der operativen Souveränität	14
6. Praxisbeispiele: Zwei Workload-Typen im Vergleich	15
7. Beispiel-Zielarchitektur für einen mittelständischen IT-Mix	16
8. Fazit und nächste Schritte	18
Über diesen Leitfaden.....	18

Management Summary

Souveränität ist kein Ort. Sie ist die Fähigkeit, für jede Workload bewusst zu entscheiden, wem Sie vertrauen – und wie Sie handlungsfähig bleiben, wenn sich diese Entscheidung als falsch erweist.

Die von SpaceNet in Auftrag gegebene Studie „Data Sovereignty 2026“ zeigt: Für 89 Prozent der Unternehmen ist Datensouveränität heute wichtig oder sehr wichtig – Tendenz weiter steigend. Gleichzeitig investiert ein erheblicher Teil der Unternehmen nicht systematisch in entsprechende Programme, und die technischen Hürden bei der Umsetzung haben sich innerhalb eines Jahres deutlich verschärft. Zwischen Anspruch und Umsetzung besteht also eine reale, messbare Lücke.

Dieser Leitfaden schließt die Lücke zwischen Anspruch und Umsetzung mit einer praktischen Methode statt mit weiteren



Grundsatzdebatten. Er hilft Ihnen dabei:

- > die vier grundlegenden Betriebsmodelle – On-Premises, Private Cloud, regionale/lokale Cloud-Anbieter und Hyperscaler – anhand ihrer jeweiligen Stärken und Grenzen einzuordnen
- > jede Workload anhand von sechs klar definierten Dimensionen zu bewerten (Datenschutz, Kritikalität, Integration, Performance, Kosten, Portabilität)
- > diese Bewertung in eine konkrete, dokumentierbare Entscheidung für ein Betriebsmodell zu überführen
- > mit einer Checkliste die vier operativen Bausteine echter Souveränität – Datenhoheit, Schlüsselmanagement, Logging und Exit-Strategie – abzusichern.

Das Ergebnis ist kein Dogma für oder gegen Cloud, sondern ein begründbarer, wiederholbarer Entscheidungsprozess, der sich auf jede neue Workload anwenden lässt – und der sich, anders als eine einmalige Grundsatzentscheidung, mit veränderten Rahmenbedingungen mitentwickelt.

1. Die falsche Frage: „Cloud oder On-Premises?“

Kaum eine IT-Entscheidung wird in den vergangenen Jahren so intensiv diskutiert wie die nach dem „richtigen“ Betriebsmodell für Unternehmensdaten. Häufig wird die Debatte dabei auf eine binäre Frage verkürzt: Cloud oder On-Premises, Hyperscaler oder Rückkehr zum eigenen Rechenzentrum. Diese Zuspitzung mag für Schlagzeilen taugen, an der betrieblichen Realität geht sie jedoch vorbei. Die Studie „Data Sovereignty 2026“ zeichnet ein differenzierteres Bild. Datensouveränität hat sich von einem reinen Compliance-Thema zu einer strategischen Voraussetzung für den verlässlichen Betrieb daten- und KI-getriebener Kernprozesse entwickelt. Gleichzeitig zeigt die Studie, dass die treibenden Kräfte hinter dieser Entwicklung vielfältiger geworden sind: Zwar bleiben gesetzliche und regulatorische Anforderungen mit 61 Prozent der Nennungen der wichtigste externe Treiber, ihr Anteil ist gegenüber dem Vorjahr aber leicht gesunken.

Im Gegenzug haben andere, risikobezogene Treiber spürbar an Gewicht gewonnen: politische Entwicklungen in den USA (von 46 auf 54 Prozent), Cybersicherheitsvorfälle (von 42 auf 49 Prozent) und die Sorge vor Abhängigkeit von einzelnen Public-Cloud-Anbietern (von 40 auf 46 Prozent). Mit anderen Worten: Souveränität wird zunehmend als Risikomanagement verstanden, nicht mehr nur als Pflichterfüllung. Das verändert, wie Unternehmen die Frage stellen sollten. Statt „Wo dürfen unsere Daten grundsätzlich liegen?“ lautet die relevante Frage: „Welche Anwendung und welche Daten gehören unter welchen Bedingungen in welches Betriebsmodell – und wie behalten wir die Fähigkeit, diese Entscheidung bei Bedarf zu revidieren?“

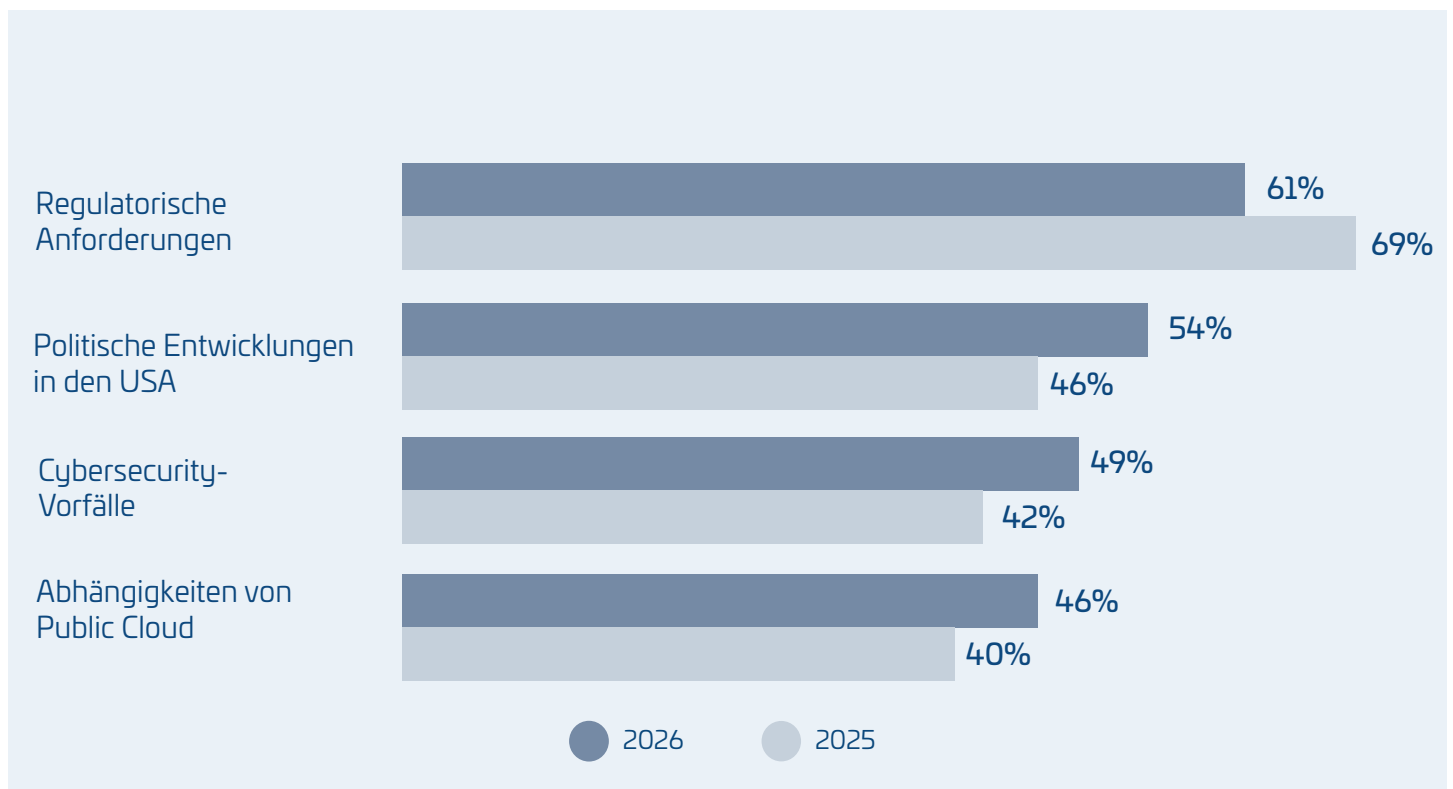


Abbildung 1: Externe Treiber der Datensouveränität im Jahresvergleich. Quelle: BARC, Data Sovereignty 2026.

Die Lücke zwischen Anspruch und Umsetzung

Dass diese differenzierte Sichtweise noch nicht überall angekommen ist, zeigt ein Blick auf die Umsetzungspraxis. Zwar hat knapp ein Drittel der Unternehmen Datensouveränität bereits als festen Bestandteil ihrer Daten- oder Digitalstrategie verankert, ein weiteres Drittel adressiert das Thema selektiv in einzelnen Initiativen. Bei der Finanzierung zeigt sich jedoch ein deutlicheres Bild der Zurückhaltung: 40 Prozent aller Unternehmen haben bislang keinerlei Investitionen in Souveränitätsinitiativen getätigt, nur 10 Prozent verfügen über ein dediziertes Budget. Auch beim technischen Reifegrad zeigt sich Luft nach oben: Während 44 Prozent eine gut entwickelte strategische Verankerung berichten, sind es bei der praktisch angewendeten Governance nur 38 Prozent.

Diese Lücke ist kein Grund zur Beunruhigung, sondern der Ausgangspunkt für diesen Leitfaden. Sie entsteht meist nicht aus mangelndem Willen, sondern aus fehlender Methode: Ohne ein nachvollziehbares Raster, anhand dessen sich Workload-Entscheidungen treffen und dokumentieren lassen, bleibt Souveränität eine Absichtserklärung. Genau dieses Raster liefert die Entscheidungsmatrix in den folgenden Kapiteln.

Was dieser Leitfaden nicht ist

Dieser Leitfaden ist kein Plädoyer für die pauschale Rückkehr zu On-Premises-Infrastruktur, und ebenso wenig ein grundsätzliches Misstrauensvotum gegenüber Hyperscalern. Beide Positionen greifen zu kurz.

Bezeichnenderweise berichten 46 Prozent der befragten Unternehmen, dass sich ihre Souveränitätsinitiativen positiv auf die eigene Innovationsfähigkeit auswirken – nur 9 Prozent sehen einen negativen Effekt. Klare Kontrollen, wiederverwendbare Architekturmuster und definierte Verantwortlichkeiten beschleunigen Entscheidungen eher, als dass sie sie verlangsamen. Souveränität und Innovationsfähigkeit stehen sich also nicht zwangsläufig entgegen – vorausgesetzt, die Entscheidung wird bewusst und pro Workload getroffen, statt einmalig und pauschal für die gesamte IT-Landschaft.



2. Die vier Betriebsmodelle im Überblick

Bevor sich einzelne Workloads bewerten lassen, lohnt ein kurzer, nüchterner Blick auf die grundsätzlichen Betriebsmodelle, zwischen denen Unternehmen heute wählen können. Hybrid- und Multi-Cloud-Strategien sind dabei keine fünfte, eigenständige Kategorie, sondern die bewusste Kombination mehrerer der folgenden vier Modelle – und in der Praxis inzwischen der Normalfall: 35 Prozent der Unternehmen stärken laut BARC-Studie gezielt ihre Hybrid-Cloud- und On-Premises-Strategie, 26 Prozent bauen ihre Multi-Cloud-Strategie aus.

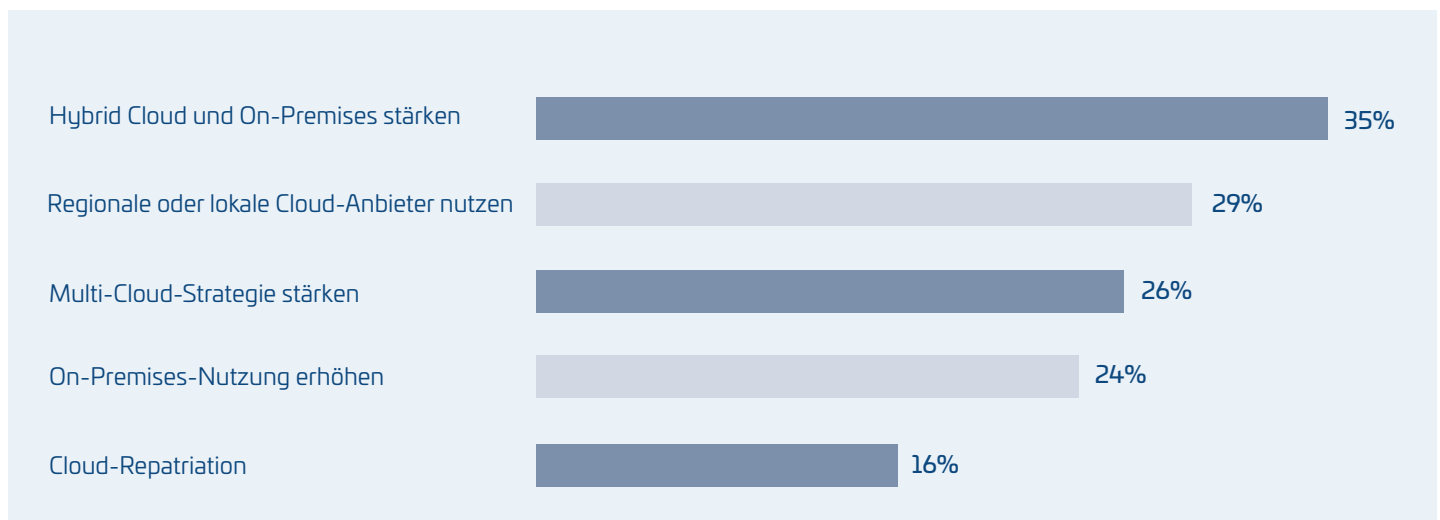


Abbildung 2: Maßnahmen zur Stärkung der Datensouveränität. Quelle: BARC, Data Sovereignty 2026.

On-Premises

Eigene Infrastruktur im eigenen oder angemieteten Rechenzentrum, vollständig unter eigener Betriebsverantwortung. Bietet maximale Kontrolle über Datenstandort, Zugriff und Konfiguration, verlangt aber hohe Investitionen, eigenes Betriebs-Know-how und begrenzt die kurzfristige Skalierbarkeit. Klassisch geeignet für hochsensible Kernsysteme mit engem regulatorischem Korsett oder sehr spezifischen Integrationsanforderungen.

Private Cloud

Dedizierte, für ein Unternehmen reservierte Cloud-Infrastruktur – häufig bei einem spezialisierten Betreiber gehostet und verwaltet. Verbindet einen Großteil der Kontrollmöglichkeiten von On-Premises mit der operativen Entlastung eines Managed-Service-Modells und besserer Planbarkeit der Skalierung. Sinnvoll für kritische Workloads, die Cloud typische Agilität benötigen, ohne auf dedizierte Kontrolle zu verzichten.

Regionale und lokale Cloud-Anbieter

Public-Cloud-ähnliche Dienste von Anbietern, deren Rechenzentren, Rechtsraum und Vertragsbeziehungen im eigenen Land oder Wirtschaftsraum liegen. Reduziert Abhängigkeit von außereuropäischem Recht und schafft Transparenz über Subunternehmer und Zugriffsketten, bei gleichzeitig guter Skalierbarkeit. Laut Studie setzen bereits 29 Prozent der Unternehmen verstärkt auf regionale oder lokale Cloud-Anbieter – Tendenz steigend.

Hyperscaler (globale Public Cloud)

Globale Cloud-Plattformen mit sehr großem Dienstleistungsportfolio, praktisch unbegrenzter Skalierbarkeit und kurzer Time-to-Value. Der Preis dafür ist eine geringere Kontrolle über Datenstandort, Subunternehmerketten und rechtliche Zugriffsmöglichkeiten Dritter – ein Aspekt, den mittlerweile 46 Prozent der Unternehmen als wachsendes Risiko einstufen. Besonders geeignet für unkritische, hochgradig skalierende oder experimentelle Workloads.

Modelle im Vergleich

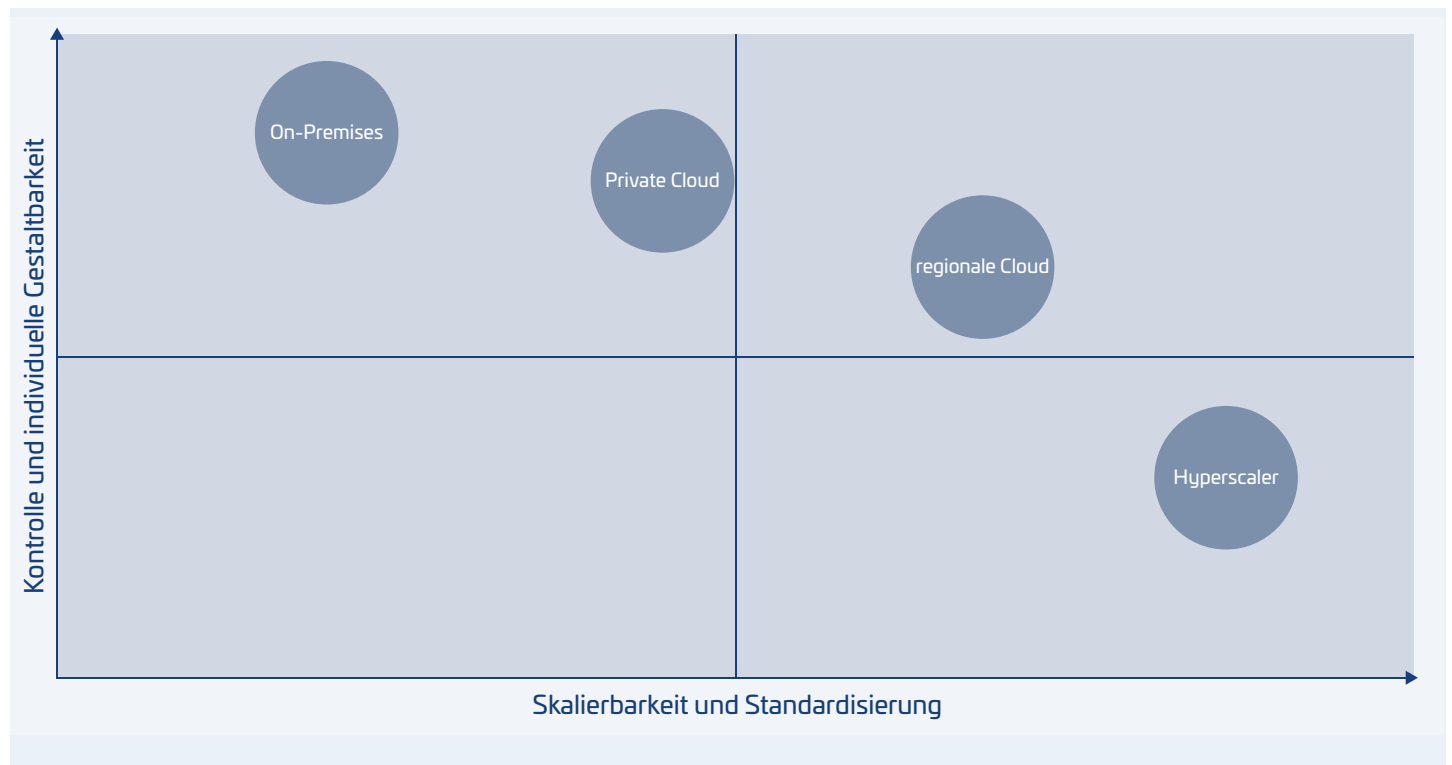


Abbildung 3: Orientierungsbild der vier Betriebsmodelle. Eigene Darstellung.

Betriebsmodell	Kontrolle/Souveränität	Skalierbarkeit	Typische Eignung
On-Premises	Sehr hoch	Begrenzt, kapital intensiv	Regulatorisch hochsensibile oder stark integrierte Kernsysteme
Private Cloud	Hoch	Gut, planbar	Kritische Workloads mit hohem Kontrollbedarf, aber Bedarf an Cloud-Agilität
Regionale/lokale Cloud	Hoch bis mittel	Gut	Sensible Daten mit Bedarf an Cloud-Flexibilität und klarem Rechtsraum
Hyperscaler	Mittel bis niedrig	Sehr hoch, global	Unkritische, skalierungsintensive oder innovationsgetriebene Workloads

3. Die sechs Bewertungsdimensionen der Entscheidungsmatrix

Die eigentliche Entscheidungsmatrix bewertet jede Workload entlang sechs Dimensionen. Diese Dimensionen sind bewusst so gewählt, dass sie sowohl regulatorische als

auch betriebswirtschaftliche und technische Realitäten abbilden – denn eine Entscheidung, die nur eine dieser Perspektiven berücksichtigt, hält der Praxis selten stand.

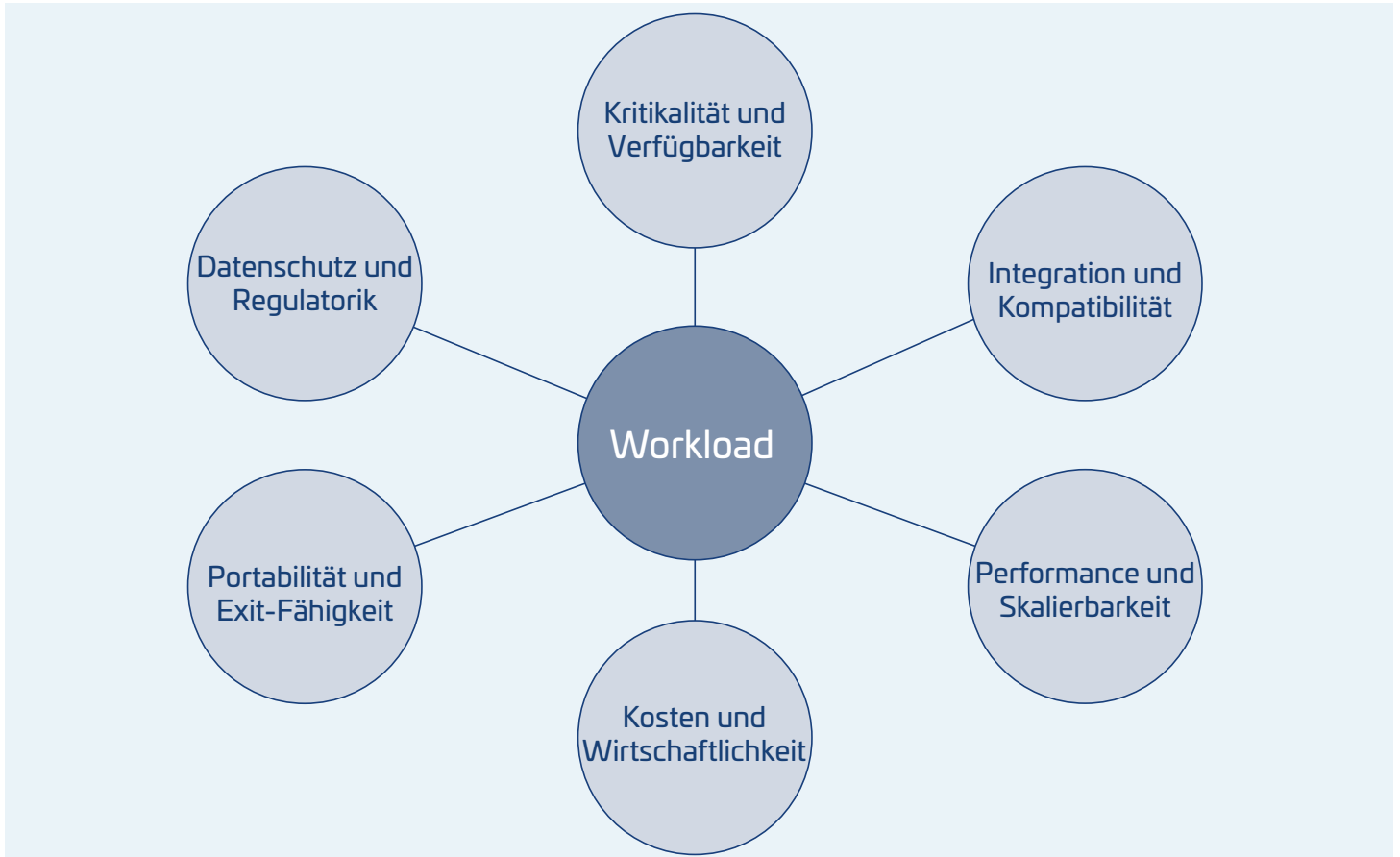


Abbildung 4: Die sechs Bewertungsdimensionen der Entscheidungsmatrix. Eigene Darstellung.

3.1 Datenschutz & Regulatorik

Diese Dimension bewertet, wie sensibel die verarbeiteten Daten sind und welchen regulatorischen Anforderungen sie unterliegen – von der DSGVO über branchenspezifische Vorgaben (etwa in Finanzdienstleistung, Gesundheitswesen oder öffentlichem Sektor) bis zu vertraglich vereinbarten Kundenanforderungen.

Je höher die Sensibilität und je strenger die Vorgaben, desto wichtiger werden Datenstandort, Zugriffsrechte und Nachweispflichten bei der Wahl des Betriebsmodells.

- > Welche Vorschriften gelten für diese Daten (DSGVO, Branchenrecht, Kundenverträge)?
- > Ist der Verarbeitungsort vertraglich oder regulatorisch festgelegt?
- > Wer außer dem eigenen Unternehmen könnte rechtlich Zugriff auf die Daten verlangen?
- > Muss die Einhaltung der Vorgaben jederzeit nachweisbar sein (Audit, Zertifizierung)?

3.2 Kritikalität & Verfügbarkeit

Hier wird bewertet, wie stark der Geschäftsbetrieb von der ununterbrochenen Verfügbarkeit der Workload abhängt und welche Folgen ein Ausfall hätte. Core-Prozesse wie Produktionssteuerung, ERP oder Auftragsabwicklung verlangen in der Regel höhere Verfügbarkeitsgarantien und mehr Kontrolle über Wartungsfenster und Notfallprozesse als Nebensysteme.

- > Was kostet eine Stunde Ausfall dieser Workload – finanziell und operativ?
- > Gibt es regulatorische oder vertragliche Verfügbarkeitsvorgaben (SLA)?
- > Wie schnell muss im Störfall reagiert werden, und wer trägt die Verantwortung?
- > Ist die Workload Teil einer kritischen Kette, die bei Ausfall weitere Systeme lahmlegt?

3.3 Integration & technische Kompatibilität

Diese Dimension erfasst, wie eng eine Workload mit bestehenden Systemen, Datenmodellen und Legacy-Anwendungen verzahnt ist. Laut der BARC-Studie „Data Sovereignty 2026“ sind technische Hürden binnen eines Jahres von 26 auf 43 Prozent aller genannten Herausforderungen gestiegen, und rund ein Drittel der Unternehmen nennt explizit die Integration bestehender Legacy-Systeme als Problem. Wer diese Dimension unterschätzt, plant oft eine Architektur, die auf dem Papier überzeugt, sich in der Praxis aber nicht wirtschaftlich anbinden lässt.

- > Mit welchen bestehenden Systemen muss die Workload Daten austauschen?
- > Existieren stabile Schnittstellen (APIs), oder ist proprietäre Integrationsarbeit nötig?
- > Wie hoch ist der Migrationsaufwand, falls das Betriebsmodell später gewechselt wird?
- > Gibt es Abhängigkeiten von Alt-Systemen, die den Betriebsmodell-Spielraum einschränken?



3.4 Performance & Skalierbarkeit

Hier geht es um Rechenleistung, Latenzanforderungen und Skalierungsbedarf – etwa bei saisonalen Lastspitzen, wachsenden Datenmengen oder rechenintensiven Anwendungen wie KI-Training. Modelle mit elastischer Skalierung bieten hier Vorteile, während stabile, vorhersehbare Lasten oft wirtschaftlicher in fest dimensionierten Umgebungen laufen.

- > Wie vorhersehbar ist die Auslastung dieser Workload über das Jahr?
- > Werden kurzfristig hohe Kapazitätsspitzen benötigt (z. B. Trainingsläufe, Kampagnen)?
- > Gibt es Latenzanforderungen, die einen bestimmten Standort nahelegen?
- > Wie wahrscheinlich ist signifikantes Wachstum in den nächsten 24 Monaten?

3.5 Kosten & Wirtschaftlichkeit

Diese Dimension vergleicht nicht nur den reinen Betriebskosten-Posten, sondern die Gesamtkosten über den Lebenszyklus – inklusive Migration, Integration, Betriebsteam, Lizenzierung und potenzieller Wechselkosten.

Ein Modell, das auf den ersten Blick günstiger wirkt, kann durch Integrationsaufwand oder eingeschränkte Verhandlungsposition langfristig teurer werden.

- > Wie unterscheiden sich CAPEX- und OPEX-Anteile zwischen den Betriebsmodellen?
- > Welche Kosten entstehen für Migration, Integration und Personalaufbau?
- > Wie transparent und vorhersehbar ist die Preisgestaltung des Anbieters?
- > Welche Kosten entstünden bei einem späteren Anbieterwechsel?



3.6 Portabilität & Exit-Fähigkeit

Die letzte Dimension bewertet, wie leicht sich eine Workload samt Daten aus einer Umgebung wieder herauslösen lässt – ein Kriterium, das in der Praxis oft erst dann auffällt, wenn es zu spät ist. Offene Standards, dokumentierte Exportformate und vertraglich fixierte Ausstiegsklauseln erhalten die Handlungsfähigkeit auch dann, wenn sich Anbieterbedingungen, Preise oder geopolitische Rahmenbedingungen ändern.

- > Lassen sich Daten und Konfigurationen in offenen, dokumentierten Formaten exportieren?
- > Wie lange dauert ein realistischer Anbieterwechsel – und wurde das je getestet?
- > Was regelt der Vertrag zu Kündigungsfristen, Löschpflichten und Unterstützung beim Exit?
- > Entstehen technische Abhängigkeiten (proprietäre Dienste), die eine Migration erschweren?

4. Die Matrix in der Praxis: Schritt für Schritt

Die sechs Dimensionen entfalten ihren Nutzen erst, wenn sie systematisch angewendet werden. Der folgende Fünf-Schritte-Prozess lässt sich sowohl für eine einzelne Workload als auch für ein vollständiges Workload-Portfolio nutzen.



Abbildung 5: Der Fünf-Schritte-Prozess für eine dokumentierte Workload-Entscheidung. Eigene Darstellung.

1. Workload-Inventar erstellen:

Listen Sie alle relevanten Anwendungen und Datenbestände auf – von Kernsystemen wie ERP oder CRM bis zu Nebensystemen wie Test- und Entwicklungsumgebungen. Ein unvollständiges Inventar ist die häufigste Ursache für spätere Kontrolllücken.

2. Je Dimension bewerten:

Vergeben Sie für jede Workload und jede der sechs Dimensionen einen Wert von 1 (geringe Relevanz/geringes Risiko) bis 5 (hohe Relevanz/hohes Risiko). Nutzen Sie dafür die Leitfragen aus Kapitel 3.

3. Gewichtung festlegen:

Nicht jede Dimension zählt für jede Workload gleich viel. Für ein Testsystem ohne Personenbezug ist Datenschutz kaum relevant, für ein CRM-System dagegen entscheidend. Legen Sie pro Workload-Kategorie eine Gewichtung fest, bevor Sie die Einzelwerte zusammenführen.

4. Gesamtbild interpretieren und Betriebsmodell ableiten:

Workloads mit hohen Werten bei Datenschutz, Kritikalität und Integration tendieren zu On-Premises oder Private Cloud. Workloads mit niedrigen Werten in diesen Dimensionen, aber hohem Skalierungsbedarf, sind meist gute Kandidaten für Hyperscaler-Umgebungen. Die meisten realen Workloads liegen dazwischen und profitieren von regionalen Cloud-Anbietern oder hybriden Konstruktionen.

5. Regelmäßig reevaluierten:

Kritikalität, Regulatorik und Integrationstiefe verändern sich – etwa wenn eine Anwendung vom Pilotprojekt zum Kernsystem wird. Planen Sie eine Reevaluierung mindestens einmal jährlich oder bei wesentlichen Änderungen des Einsatzzwecks fest ein.

Bewertungsvorlage zum Ausfüllen

Die folgende Tabelle lässt sich direkt als Arbeitsvorlage nutzen – pro Workload einmal kopieren und mit dem jeweiligen Team ausfüllen.

Dimension	Gewichtung (1-3)	Bewertung (1-5)	Kommentar
3.1 Datenschutz & Regulatorik			
3.2 Kritikalität & Verfügbarkeit			
3.3 Integration & Kompatibilität			
3.4 Performance & Skalierbarkeit			
3.5 Kosten & Wirtschaftlichkeit			
3.6 Portabilität & Exit-Fähigkeit			

Faustregel:

Je höher der gewichtete Gesamtwert bei Datenschutz, Kritikalität und Integration ausfällt, desto stärker sollte das Betriebsmodell in Richtung On-Premises oder Private Cloud tendieren. Dominieren dagegen Performance- und Skalierungsanforderungen bei gleichzeitig niedrigen Werten in den übrigen Dimensionen, spricht das für Hyperscaler-Umgebungen oder hybride Kombinationen.

5. Checkliste: Vier Bausteine der operativen Souveränität

Die Wahl des richtigen Betriebsmodells ist die strategische Ebene der Souveränität. Ob diese Entscheidung im Alltag auch trägt, entscheidet sich jedoch auf der operativen Ebene – anhand von vier Bausteinen, die sich unabhängig vom gewählten Modell prüfen lassen.

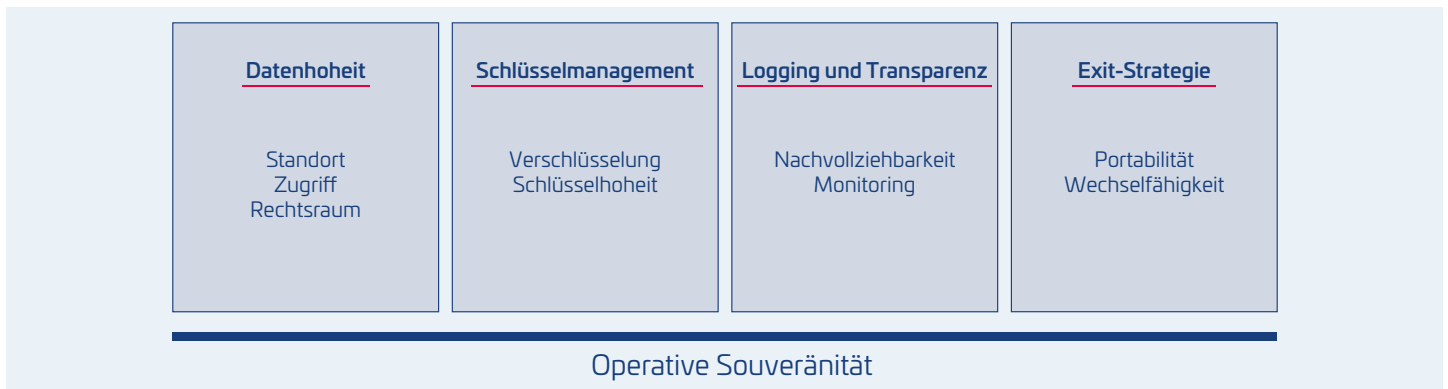


Abbildung 6: Vier Bausteine der operativen Souveränität. Eigene Darstellung.

Datenhoheit

- ☐ Speicherort und Verarbeitungsort der Daten sind dokumentiert und vertraglich fixiert.
- ☐ Die vollständige Subunternehmerkette des Anbieters ist bekannt und wird bei Änderungen gemeldet.
- ☐ Zugriffsrechte sind nach dem Prinzip der geringsten Berechtigung vergeben und regelmäßig überprüft.
- ☐ Der geltende Gerichtsstand und mögliche Zugriffsrechte ausländischer Behörden sind bekannt.

Schlüsselmanagement

- ☐ Kritische Daten sind verschlüsselt – sowohl bei der Übertragung als auch im Ruhezustand.
- ☐ Es ist geklärt, wer die Verschlüsselungsschlüssel verwaltet (Anbieter, Kunde oder Dritte – „Hold your own key“/„Bring your own key“).
- ☐ Schlüsselverwaltung und Datenspeicherung liegen, wo regulatorisch gefordert, in getrennter Verantwortung.
- ☐ Es existiert ein dokumentierter Prozess für Schlüsselrotation und -widerruf.

Logging & Transparenz

- ☐ Zugriffe auf sensible Daten und Systeme werden lückenlos protokolliert.
- ☐ Protokolle sind manipulationssicher und für einen definierten Zeitraum nachvollziehbar aufbewahrt.
- ☐ Eine Anbindung an das eigene SIEM- beziehungsweise Monitoring-System ist möglich.
- ☐ Es ist klar geregelt, wer im Ernstfall wie schnell Einblick in die Protokolle erhält.

Exit-Strategie

- ☐ Daten und Konfigurationen lassen sich in offenen, dokumentierten Formaten exportieren.
- ☐ Ein Anbieterwechsel wurde mindestens einmal exemplarisch getestet oder durchgerechnet.
- ☐ Kündigungsfristen, Übergangsunterstützung und Löschpflichten sind vertraglich klar geregelt.
- ☐ Es ist bekannt, welche proprietären Abhängigkeiten eine Migration im Ernstfall verzögern würden.

6. Praxisbeispiele: Zwei Workload-Typen im Vergleich

Zur Veranschaulichung lohnt der Blick auf zwei Workload-Typen, die in nahezu jedem Unternehmen an Bedeutung gewinnen und die Entscheidungsmatrix besonders greifbar machen: KI-Anwendungen und Collaboration-Plattformen.

6.1 KI-Anwendungen: Wo dürfen die Daten verarbeitet werden?

62 Prozent der befragten Unternehmen nennen den zunehmenden Einsatz von Daten und KI in Kernprozessen als wichtigsten internen Treiber für das Thema Datensouveränität – mehr als jeder andere interne Faktor. Das liegt daran, dass KI-Workloads die sechs Bewertungsdimensionen auf besondere Weise durchmischen: Das Training großer Modelle profitiert häufig von der Skalierbarkeit und Spezialhardware eines Hyperscalers (Dimension Performance), während die dafür verwendeten Trainings- und Inferenzdaten oft hochsensibel sind (Dimension Datenschutz) und ihre Herkunft und Verarbeitung lückenlos nachvollziehbar sein muss (Dimension Integration/Governance).

In der Praxis führt das häufig zu einer bewussten Aufteilung: rechenintensives, aber mit anonymisierten oder synthetischen Daten durchgeführtes Training in einer skalierenden Cloud-Umgebung, während produktionsnahe Inferenz mit sensiblen Kundendaten in einer stärker kontrollierten, regionalen oder privaten Umgebung erfolgt. Entscheidend ist, dass Modell-Herkunft, Trainingsdatensätze und Zugriffe während des gesamten Lebenszyklus dokumentiert bleiben – nicht nur zum Zeitpunkt der Einführung.

6.2 Collaboration-Plattformen: Wie souverän muss Zusammenarbeit sein?

E-Mail, Chat, Videokonferenzen und Dokumentenablage gehören zu den am intensivsten genutzten Workloads überhaupt – und genau das macht sie zu einem besonders anschaulichen Beispiel für die Matrix. Die Kritikalität ist hoch, da ein Ausfall die gesamte Belegschaft betrifft; gleichzeitig verarbeiten diese Plattformen durchgehend personenbezogene und oft auch strategisch sensible Daten (Verträge, Personalunterlagen, Projektpläne), was die Dimension Datenschutz deutlich anhebt.

Gleichzeitig verlangt die tägliche Nutzung durch alle Mitarbeitenden eine hohe Verfügbarkeit, gute Performance und einfache Integration mit Endgeräten und Identitätsmanagement – Anforderungen, die klassische On-Premises-Lösungen nur mit hohem Aufwand erfüllen. In der Praxis führt dies häufig zu regionalen Cloud-Lösungen oder hybriden Modellen, bei denen besonders sensible Ablagen (etwa Personalunterlagen) zusätzlich abgesichert oder separat gehalten werden, während der operative Kollaborationsalltag auf einer skalierenden, aber im eigenen Rechtsraum betriebenen Plattform läuft.



7. Beispiel-Zielarchitektur für einen mittelständischen IT-Mix

Um die Anwendung der Entscheidungsmatrix konkret zu machen, folgt ein durchgängiges – fiktives – Beispiel. Es dient ausschließlich der Veranschaulichung und bildet kein reales Unternehmen ab.

Beispielfall:

Ein mittelständisches Maschinenbauunternehmen mit rund 800 Mitarbeitenden, Produktionsstandorten in Deutschland und einer wachsenden internationalen Vertriebsorganisation. Das Unternehmen hat sein Workload-Portfolio

mithilfe der sechs Bewertungsdimensionen aus Kapitel 3 kategorisiert. Das Ergebnis ist kein einheitliches Betriebsmodell, sondern ein bewusst gestalteter, hybrider IT-Mix:



Abbildung 7: Beispielhafte Zielarchitektur für einen mittelständischen IT-Mix. Eigene Darstellung.

Workload	Kritikalität	Regulatorik	Ziel-Betriebsmodell	Begründung
ERP / Buchhaltung	Hoch	Hoch (GoBD, Compliance)	Private Cloud / Regionaler Anbieter	Hohe Kritikalität und Regulatorik verlangen maximale Kontrolle; Cloud-Betrieb reduziert Wartungsaufwand.
CRM / Kundendaten	Mittel-hoch	Hoch (DSGVO)	Regionale Cloud	Personenbezogene Daten profitieren von klarem Rechtsraum ohne auf Cloud-Vorteile zu verzichten.
Collaboration / E-Mail	Mittel	Mittel-hoch	Regionale Cloud / Hybrid	Hohe Nutzungsintensität verlangt Verfügbarkeit; Compliance-Anforderungen sprechen gegen unkontrollierte Standorte.
Entwicklung / Test	Niedrig	Niedrig	Hyperscaler	Geringe Kritikalität, hoher Bedarf an Skalierung und schnellem Provisioning.
IoT-Daten (Produktion)	Hoch	Mittel	On-Premises / Private Cloud	Niedrige Latenzanforderungen und hohe Kritikalität sprechen für Nähe zur Produktion.
Ki- / Analytics-Plattform	Mittel	Mittel (abh. vom Datensatz)	Hybrid (Training extern, sensible Daten intern)	Rechenintensives Training profitiert von Skalierung, sensible Trainingsdaten bleiben kontrolliert.
Backup & Archivierung	Hoch	Hoch	Regionaler Anbieter / On-Premises	Langfristige Aufbewahrungspflichten verlangen Rechtssicherheit und nachvollziehbare Löschprozesse.

Auffällig an diesem Beispiel ist, dass kein einzelnes Betriebsmodell dominiert. Stattdessen ergibt sich eine Architektur, in der jede Workload-Kategorie dort betrieben wird, wo ihre jeweiligen Anforderungen an Kontrolle, Skalierung und Integration am besten erfüllt werden – bei gleichzeitig dokumentierten Schnittstellen zwischen den Umgebungen. Genau dieses Muster zeigt auch die BARC-Studie auf breiter Basis: 35 Prozent der Unternehmen stärken ihre Hybrid-Cloud- und On-Premises-Strategie, ohne deshalb auf Cloud-Nutzung insgesamt zu verzichten.



8. Fazit und nächste Schritte

Datensouveränität lässt sich nicht mit einer einmaligen Grundsatzentscheidung erledigen. Sie entsteht dort, wo Unternehmen für jede Workload nachvollziehbar begründen können, warum sie einem bestimmten Anbieter und einer bestimmten Infrastruktur vertrauen – und wie sie handlungsfähig bleiben, falls sich diese Entscheidung ändern muss.

Die wichtigsten Punkte in Kürze

- > Die Frage „Cloud oder On-Premises?“ greift zu kurz. Relevant ist die Frage, welches Betriebsmodell zu welcher Workload passt.
- > Sechs Dimensionen – Datenschutz, Kritikalität, Integration, Performance, Kosten, Portabilität – liefern ein wiederholbares Bewertungsraster.
- > Strategische Verankerung allein reicht nicht: Governance und technische Architektur müssen in der gleichen Tiefe mitwachsen.
- > Souveränität und Innovationsfähigkeit schließen sich nicht aus – im Gegenteil, klare Kontrollen beschleunigen oft die sichere Skalierung.

Wie es weitergeht

Die Entscheidungsmatrix aus diesem Leitfaden lässt sich eigenständig im Unternehmen anwenden. Für Unternehmen, die den Einstieg gemeinsam mit erfahrenen Architekt:innen angehen möchten, bietet sich ein strukturierter Souveränitäts- und Architektur-Check an: eine gemeinsame Bestandsaufnahme des bestehenden Workload-Portfolios, angewendet auf die in diesem Leitfaden beschriebene Methode, mit einer konkreten Empfehlung für den weiteren IT-Mix.

Über diesen Leitfaden

Dieser Leitfaden basiert auf den Ergebnissen der Studie „Data Sovereignty 2026: Reality, Relevance, Roadmap“, einer weltweiten Online-Befragung von 320 Unternehmen aus einer breiten Branchen-, Größen- und Regionenverteilung, durchgeführt von BARC im Auftrag von SpaceNet im Februar und März 2026. Alle in diesem Leitfaden verwendeten Prozentangaben stammen aus dieser Studie, sofern nicht anders vermerkt.

Die Entscheidungsmatrix, die Bewertungsdimensionen sowie die Beispielarchitektur in diesem Dokument sind eine eigenständige methodische Aufbereitung für die praktische Anwendung und gehen über die reinen Studienergebnisse hinaus.

