AUTONOMY TRACK · PRAXISLEITFADEN

Digitale Souveränität praktisch bewerten

25 Fragen zur Anbieterbewertung.
Mit Checklisten und Vorlagen für fundierte Entscheidungen.

Andreas Heß

Gründer von Autonomy Track

hello@autonomytrack.eu
+49 160 922 322 55
https://autonomytrack.eu

© 2026 Andreas Heß. Alle Rechte vorbehalten.

Kostenlos zum Ausdrucken, Ausfüllen und Teilen innerhalb derselben Organisation für eigene Bewertungen und Beschaffungen. Keine Weitergabe an Dritte, Weiterentwicklung oder Integration in andere Inhalte oder Systeme. Rechte an eigenen Eintragungen und zwingend gesetzlich erlaubte Nutzungen bleiben unberührt.

Es gilt die Autonomy Track Content-Lizenz:

https://autonomytrack.eu/autonomy-track-content-lizenz/

Inhalt

Wobei der Leitfaden hilft . . . 3

1. Digitale Souveränität ist keine Ja/Nein-Eigenschaft . . . 4

2. Warum Nachweise entscheidend sind . . . 5

3. Die fünf Dimensionen . . . 6

4. So nutzen Sie den Leitfaden . . . 6

5. Dimension A - Recht & Kontrolle . . . 8

6. Dimension B - Daten & Betrieb . . . 10

7. Dimension C - Technologie & Lieferkette . . . 11

8. Dimension D - Übertragbarkeit & Anbieterwechsel . . . 13

9. Dimension E - Nachweise & Verlässlichkeit . . . 14

10. Von der Feststellung zur Entscheidung . . . 16

11. Beispiel: Eine Plattform, zwei Einsatzbereiche . . . 17

12. Regulatorischer Kontext . . . 18

13. Wann sollte neu bewertet werden? . . . 19

14. Die wichtigste Regel . . . 20

Anhang A: 25-Fragen-Kurzcheckliste . . . 21

Anhang B: Nachweisliste . . . 23

Anhang C: Entscheidungsvorlage . . . 24

Quellen und weiterführende Informationen . . . 28

© 2026 Andreas Heß · Autonomy Track

Wobei der Leitfaden hilft

Digitale Souveränität lässt sich nicht zuverlässig mit einer einzigen Frage beantworten:

- Liegen die Daten in Europa?
- Ist der Anbieter europäisch?
- Gibt es eine ISO-Zertifizierung?
- Kann ich meine Daten exportieren?

Jede dieser Fragen kann relevant sein. Keine davon reicht allein aus.

Entscheidend ist, ob eine Organisation ihre technologischen Abhängigkeiten **kennt**, die wesentlichen Aussagen **belegen**, die Folgen für den konkreten Anwendungsfall **bewerten** und eine bewusste Entscheidung **treffen und umsetzen** kann.

Dieser Leitfaden hilft dabei.

Er ist kein Zertifizierungsverfahren, keine Anbieter-Rangliste und keine Rechtsberatung. Er ersetzt auch keine regulatorische oder risikobasierte Prüfung im Einzelfall. Er bietet einen strukturierten Einstieg in eine Frage, die in der Praxis häufig zu abstrakt behandelt wird:

> **Wie abhängig sind wir von einem Anbieter - und ist diese Abhängigkeit für diesen konkreten Anwendungsfall akzeptabel?**

© 2026 Andreas Heß · Autonomy Track

1. Digitale Souveränität ist keine Ja/Nein-Eigenschaft

Digitale Souveränität wird häufig über Herkunft, Rechenzentrumsstandort oder Datenschutz diskutiert. Diese Faktoren sind wichtig, bilden aber nur einen Teil des Bildes.

Eine Organisation kann ihre Daten ausschließlich in Deutschland speichern und trotzdem stark abhängig sein von:

- Proprietären APIs
- Einer nicht austauschbaren Identitätsplattform
- Globalen Administrations- oder Supportstrukturen
- Einem einzelnen Technologie- oder Lizenzlieferanten
- Proprietären Datenformaten
- Fehlendem Know-how für einen Wechsel
- Einem Vertrag ohne belastbare Regelung zum Anbieterwechsel
- Einer Architektur, die außerhalb des Anbieters nur mit hohem Aufwand reproduzierbar ist

Umgekehrt ist eine Abhängigkeit nicht automatisch ein Problem.

Ein hochintegrierter Plattformdienst kann einen großen funktionalen und wirtschaftlichen Nutzen haben. Für einen wenig kritischen Anwendungsfall kann es rational sein, eine höhere Abhängigkeit bewusst zu akzeptieren.

Die bessere Frage lautet daher nicht:

> Ist der Anbieter souverän?

Sondern:

> Welche Abhängigkeiten bestehen, welche davon sind für unseren Anwendungsfall wesentlich und welche Entscheidung treffen wir bewusst dazu?

© 2026 Andreas Heß · Autonomy Track

2. Warum Nachweise entscheidend sind

Souveränitäts- und Sicherheitsbewertungen beginnen oft mit Anbieterangaben:

- „Daten bleiben in der EU.“
- „Souveräne Cloud in der EU.“
- „Verschlüsselung unter Kontrolle des Kunden.“
- „Anbieterwechsel jederzeit möglich.“
- „Nach ISO 27001 zertifiziert.“
- „Nach C5 geprüft.“

Solche Aussagen können richtig und relevant sein. Sie sind aber zunächst **Anbieterangaben**.

Für eine belastbare Entscheidung müssen mindestens vier Ebenen getrennt werden:

Anbieterangabe	Was behauptet der Anbieter?
Nachweis	Welcher Nachweis stützt die Aussage?
Verlässlichkeit	Wie wurde der Nachweis erstellt, wie aktuell ist er und welche Aussagen lassen sich daraus belastbar ableiten?
Eignung für den Anwendungsfall	Deckt der Nachweis die relevanten Anforderungen, den betrachteten Dienst und den benötigten Zeitraum ab?

Ein Zertifikat kann beispielsweise korrekt und aktuell sein, aber nur eine bestimmte Gesellschaft, Region oder einen Teil des Dienstes abdecken.

Ein Auditbericht kann hochwertige Nachweise liefern, ohne automatisch alle Anforderungen einer Organisation abzudecken.

Ein Vertrag kann einen Datenstandort garantieren, ohne technische Portabilität sicherzustellen.

Deshalb gilt:

> **Prüfen Sie nicht nur, ob ein Nachweis vorhanden ist. Entscheidend sind seine Aussagekraft, Aktualität und sein Geltungsbereich für den betrachteten Dienst.**

© 2026 Andreas Heß · Autonomy Track

3. Die fünf Dimensionen

Der Leitfaden strukturiert die Bewertung in fünf Dimensionen:

1. **Recht & Kontrolle**
2. **Daten & Betrieb**
3. **Technologie & Lieferkette**
4. **Übertragbarkeit & Anbieterwechsel**
5. **Nachweise & Verlässlichkeit**

Diese fünf Dimensionen sind bewusst pragmatisch gehalten.

Sie ersetzen keine regulatorischen Rahmenwerke. Das Cloud Sovereignty Framework der Europäischen Kommission arbeitet beispielsweise mit 48 Kriterien in acht Souveränitätsbereichen. Der hier verwendete Ansatz gibt Organisationen einen verständlichen Einstieg und bereitet eine fundierte Technologieentscheidung vor.

4. So nutzen Sie den Leitfaden

Schritt 1 - Betrachtungsbereich festlegen

Bewerten Sie nicht „den Anbieter“ abstrakt.

Definieren Sie zuerst:

- Welchen Dienst oder welches Produkt Sie betrachten
- Welche Gesellschaft Vertragspartner ist
- Welche internen Prozesse davon abhängen
- Wie kritisch der Anwendungsfall ist
- Welche Daten verarbeitet werden
- Welche Länder/Rechtsordnungen relevant sind
- Welche regulatorischen oder internen Anforderungen gelten
- Wann der Vertrag verlängert oder neu entschieden wird

Der gleiche Anbieter kann für zwei unterschiedliche Anwendungsfälle zu unterschiedlichen Entscheidungen führen.

Schritt 2 - Fragen beantworten

Bearbeiten Sie die 25 Fragen dieses Leitfadens.

© 2026 Andreas Heß · Autonomy Track

Schritt 3 - Nachweise zuordnen

Bewerten Sie zu jeder relevanten Frage nicht nur die Antwort, sondern den Nachweis.

Verwenden Sie vier Statusangaben für Nachweise:

- **Verifiziert** - ausreichende, aktuelle Nachweise liegen vor.
- **Teilweise verifiziert** - Nachweise sind vorhanden, aber unvollständig, zu alt oder nicht vollständig passend.
- **Unbekannt** - es liegen keine ausreichenden Nachweise vor.
- **Nicht anwendbar** - die Frage ist für den definierten Betrachtungsbereich nachvollziehbar irrelevant.

Fehlt ein belastbarer Nachweis, bleibt die betreffende Aussage unbestätigt. Dokumentieren Sie die offene Frage, den benötigten Nachweis, eine verantwortliche Person und einen Termin zur Klärung.

Eine Nachweislücke belegt weder, dass eine Anforderung erfüllt ist, noch automatisch einen Verstoß. Für kritische Anforderungen kann sie dennoch ein Grund sein, eine Entscheidung zurückzustellen oder vorläufige Schutzmaßnahmen festzulegen.

„Verifiziert“ beschreibt die Beleglage einer Aussage. Auch eine nachgewiesene Schwachstelle kann verifiziert sein. Ob die festgestellte Situation akzeptabel ist, wird anschließend getrennt bewertet.

Schritt 4 - Bedeutung der Auswirkungen bewerten

Fragen Sie:

> Welche Folge hätte dieser Befund für genau diesen Anwendungsfall?

Beschreiben Sie zuerst die konkreten Folgen, etwa Betriebsunterbrechung, Datenverlust oder zusätzliche Wechselkosten. Ordnen Sie deren Schwere anschließend als **niedrig, mittel, hoch oder kritisch** ein und begründen Sie die Einstufung. Sie ersetzt keine vollständige Risikobewertung, die auch Eintrittswahrscheinlichkeit und bestehende Schutzmaßnahmen berücksichtigt.

Schritt 5 - Entscheidung treffen

Halten Sie die Entscheidung und ihre Begründung fest. Mehrere Handlungsoptionen können kombiniert werden:

- Tolerieren
- Reduzieren
- Folgen begrenzen
- Alternativen aufbauen
- Neu verhandeln
- Migrieren
- Ersetzen
- Aufgaben selbst übernehmen

© 2026 Andreas Heß · Autonomy Track

5. Dimension A - Recht & Kontrolle

A1 - Vertragspartner und Eigentums-/Kontrollstruktur

Frage: Können wir die vertragschließende Gesellschaft, kontrollierende Unternehmen und relevante Eigentums- oder Kontrollbeziehungen identifizieren?

Warum das wichtig ist

Nicht nur der Markenname ist relevant. Gesellschaftsstruktur und Kontrolle beeinflussen beispielsweise:

- Anwendbares Recht
- Offenlegungs- und Herausgabepflichten
- Vertragsdurchsetzung
- Strategische Abhängigkeit
- Risiken bei einem Eigentümerwechsel

Mögliche Nachweise

Vertrag / Bestellformular · Handels- oder Unternehmensregister · Konzernstruktur · Anbieter-Impressum · Eigentümerinformationen

A2 - Relevante Rechtsordnungen

Frage: Welche Rechtsordnungen können Anbieter, Dienst, administrativen Zugriff oder Offenlegungspflichten wesentlich beeinflussen?

Warum das wichtig ist

Der Speicherort von Daten beantwortet nicht automatisch, welche rechtlichen Regime auf Vertragspartner, Muttergesellschaften, Supportorganisationen, Betreiber oder Subunternehmer einwirken können.

Mögliche Nachweise

Vertragsbedingungen · Datenschutzvereinbarung · Rechts- und Transparenzinformationen · Unternehmensstruktur · Richtlinien zu Behördenanfragen

A3 - Vertragliche Kontroll- und Änderungsrechte

Frage: Geben uns die Verträge ausreichende Rechte bei Prüfungen, wesentlichen Änderungen, dem Einsatz von Unterauftragnehmern, Kündigung, Datenrückgabe und einem Anbieterwechsel?

Warum das wichtig ist

Eine technisch vorhandene Option ist für kritische Anforderungen weniger belastbar, wenn sie nur als Marketingaussage existiert oder vertraglich nicht abgesichert ist.

Mögliche Nachweise

Rahmenvertrag · Auftragsverarbeitungsvertrag · Leistungsvereinbarung · Audit-Klauseln · Unterauftragnehmer-Klauseln · Klauseln zu Anbieterwechsel und Übergang

© 2026 Andreas Heß · Autonomy Track

A4 - Kritische Dritte und Unterauftragnehmer

Frage: Kennen wir die Dritten und Unterauftragnehmer, ohne die der Dienst nicht in der benötigten Form betrieben werden könnte?

Warum das wichtig ist

Ein Anbieter kann selbst abhängig sein von Hyperscalern, Netzwerkdiensten, Identitätsdiensten, proprietärer Software, Sicherheitsdiensten oder externen Betriebsleistungen.

Mögliche Nachweise

Liste der Unterauftragnehmer · Architektur · Dokumentation der Lieferkette · Liste kritischer Unterauftragnehmer

A5 - Änderung von Kontrolle oder Geschäftsmodell

Frage: Was passiert, wenn sich Eigentümer, Kontrolle, kritische Subunternehmer oder die strategische Ausrichtung des Anbieters ändern?

Warum das wichtig ist

Eine heute akzeptable Konstellation kann sich durch Übernahme, Restrukturierung, Outsourcing oder Änderung des Hostingmodells wesentlich verändern.

Mögliche Nachweise

Vertragsklauseln zum Eigentümerwechsel · Benachrichtigungsrechte · Sonderkündigungsrechte · Dokumentation der Steuerung und Verantwortlichkeiten

© 2026 Andreas Heß · Autonomy Track

6. Dimension B - Daten & Betrieb

B1 - Speicher- und Verarbeitungsorte

Frage: Wissen wir, wo Primärdaten, Sicherungskopien, Protokolle, Metadaten und Kopien für die Notfallwiederherstellung gespeichert oder verarbeitet werden?

Warum das wichtig ist

„In Deutschland betrieben“ oder „Datenspeicherung in der EU“ kann sich nur auf einen Teil des Dienstes beziehen.

Zu prüfen sind insbesondere:

- Produktivdaten
- Sicherungskopien
- Telemetrie
- Protokolle
- Supportdaten
- Metadaten
- Notfallkopien

Mögliche Nachweise

Datenflussdiagramm · Architektur · Regionsdokumentation · Sicherungs- und Notfall-Dokumentation · Vertragliche Zusagen

B2 - Privilegierter Zugriff und Support

Frage: Wer kann privilegiert oder im Supportfall auf Kundenumgebungen oder Daten zugreifen, von wo aus und unter welchen Kontrollen?

Warum das wichtig ist

Operativer Zugriff kann für eine Souveränitätsentscheidung ebenso relevant sein wie der Speicherort.

Mögliche Nachweise

Konzept für Identitäten und privilegierte Zugriffe · Supportmodell · Rollenbeschreibungen · Zugriffsprotokolle · Notfallzugriffsverfahren

B3 - Kryptografische Kontrolle

Frage: Wer kontrolliert die Schlüssel, und kann der Anbieter oder eine vorgelagerte Partei technisch auf Klartext zugreifen?

Warum das wichtig ist

„Verschlüsselung gespeicherter Daten“ beantwortet nicht die Frage, wer die Schlüssel kontrolliert.

Mögliche Nachweise

Architektur zur Schlüsselverwaltung und sicheren Schlüsselaufbewahrung · Modell zur Schlüsselverwaltung · Technische Dokumentation · Vertragszusagen · Zugriffskonzept

© 2026 Andreas Heß · Autonomy Track

B4 - Operative Autonomie und Wiederherstellung

Frage: Welche Personen, technischen Steuerungsebenen, externen Dienste und Standorte sind erforderlich, um den Dienst zu betreiben und wiederherzustellen?

Warum das wichtig ist

Ein Dienst kann Daten in Europa speichern, aber für Betrieb oder Wiederherstellung abhängig sein von globalen technischen Steuerungsebenen, zentralen Supportteams, nicht austauschbaren Drittdiensten oder externen Lizenzservern.

Mögliche Nachweise

Betriebsmodell · Dienstarchitektur · Supportstandorte · Dokumentation zu Betriebsfortführung und Notfallwiederherstellung · Abhängigkeitsübersicht

B5 - Löschung, Aufbewahrung und operative Nachweise

Frage: Kann der Anbieter Aufbewahrung und Löschung nachvollziehbar belegen und ausreichende operative Nachweise für wesentliche Zusagen liefern?

Mögliche Nachweise

Aufbewahrungsrichtlinie · Löschprozess · Löschbestätigung · Prüfprotokolle · Änderungsnachweise · Dokumentation von Sicherheitsvorfällen

7. Dimension C - Technologie & Lieferkette

C1 - Proprietäre Abhängigkeiten

Frage: Welche proprietären Technologien, Schnittstellen, Datenformate oder betreuten Dienste sind erforderlich, damit die Anwendung funktioniert?

Warum das wichtig ist

Proprietäre Funktionen sind nicht automatisch schlecht. Sie können Entwicklungszeit reduzieren, Sicherheit verbessern, Skalierbarkeit erhöhen oder Betrieb vereinfachen. Gleichzeitig können sie Wechselkosten erhöhen.

Ziel ist daher nicht „kein Lock-in“, sondern **bewusst gewählter Lock-in**.

Mögliche Nachweise

Architekturdiagramm · API-Inventar · Leistungskatalog · Abhängigkeitsübersicht

C2 - Standards und Interoperabilität

Frage: Welche offenen, dokumentierten oder breit unterstützten Standards und Schnittstellen ermöglichen Zusammenarbeit mit anderen Systemen oder den Austausch einer Lösung?

Mögliche Nachweise

API-Dokumentation · Protokoll-/Formatdokumentation · Konformitätsangaben · Technische Tests

© 2026 Andreas Heß · Autonomy Track

C3 - Vorgelagerte Technologieabhängigkeiten

Frage: Welche Technologieanbieter benötigt der Anbieter für Betrieb, Updates, Patches oder Weiterentwicklung des Dienstes?

Warum das wichtig ist

Eine europäische Gesellschaft kann technologisch stark von einzelnen externen Plattformen oder Softwarelieferanten abhängig sein.

Mögliche Nachweise

Technologiearchitektur · Lizenzabhängigkeiten · Plattformbeschreibung · Dokumentation der Softwarelieferkette

C4 - Portabilität von Konfiguration und Automatisierung

Frage: Können Konfigurationen, Infrastrukturdefinitionen, Richtlinien und Automatisierungen außerhalb des Anbieters reproduziert werden?

Warum das wichtig ist

Ein vollständiger Datenexport hilft nur begrenzt, wenn Rollenmodelle, Arbeitsabläufe, Infrastruktur, Richtlinien und Integrationen komplett neu aufgebaut werden müssen.

Mögliche Nachweise

Infrastruktur als Code · Richtlinienexport · Konfigurations-API · Automatisierte Bereitstellungsabläufe · Betriebsanleitungen

C5 - Kenntnisse und Ökosystem

Frage: Haben wir oder bekommen wir realistisch die Fähigkeiten und Partner, um eine Alternative zu betreiben?

Warum das wichtig ist

Auch fehlende Kenntnisse, Personal oder geeignete Dienstleister können einen Wechsel erschweren. Eine technisch verfügbare Alternative ist erst nutzbar, wenn Betrieb und Übergang organisatorisch abgesichert sind.

Mögliche Nachweise

Übersicht der vorhandenen Kenntnisse · Partner-/Dienstleistermarkt · Schulungsbedarf · Betriebsmodell · Bewertung der Kenntnisse für Alternativen

© 2026 Andreas Heß · Autonomy Track

8. Dimension D - Übertragbarkeit & Anbieterwechsel

D1 - Vollständiger Export

Frage: Können alle benötigten Daten, Metadaten, Konfigurationen und relevanten Artefakte in nutzbarer maschinenlesbarer Form exportiert werden?

Warum das wichtig ist

Ein Export kann auf den ersten Blick vorhanden sein und trotzdem Beziehungen, Versionen, Auditdaten, Berechtigungen, Metadaten oder Konfiguration auslassen.

Mögliche Nachweise

Exportdokumentation · Testexport · Formatspezifikation · APIs · Migrationstools

D2 - Wechselprozess und Unterstützung

Frage: Gibt es einen dokumentierten Wechselprozess mit Fristen, Verantwortlichkeiten, Support, Datenaufbewahrung und bekannten Kosten?

Mögliche Nachweise

Vertrag · Wechselplan · Klauseln zur Unterstützung beim Wechsel · Aufbewahrungs- und Löschregeln · Preislisten

D3 - Realistische Zieloption

Frage: Gibt es mindestens einen realistischen alternativen Anbieter, eine alternative Architektur oder eine Lösung im eigenen Betrieb?

Warum das wichtig ist

Ein vertragliches Recht auf Wechsel ist wenig wert, wenn technisch oder organisatorisch kein realistisches Ziel existiert.

Mögliche Nachweise

Zielarchitektur · Vergleich alternativer Anbieter · Machbarkeitstest · Kompatibilitätsanalyse

D4 - Aufwand und Auswirkungen auf den Betrieb eines Anbieterwechsels

Frage: Kennen wir voraussichtliche Dauer, Kosten, Kenntnisse, Betriebsunterbrechungen, Datenübertragungsaufwand und Betriebsrisiken eines Anbieterwechsels?

Warum das wichtig ist

Wesentliche Abhängigkeit zeigt sich häufig in den tatsächlichen Wechselkosten.

Mögliche Nachweise

Aufwandsschätzung · Kostenmodell · Datenvolumen-/Netzwerkberechnung · Ressourcenplan · Migrationsanleitung

© 2026 Andreas Heß · Autonomy Track

D5 - Getesteter Anbieterwechsel

Frage: Wurden Export, Wiederherstellung, Umschaltung auf Ersatzsysteme oder Migration in einem für den Anbieterwechsel relevanten Szenario getestet und dokumentiert?

Warum das wichtig ist

Dokumentation oder eine Exportfunktion allein belegen noch keinen erfolgreichen Wechsel. Halten Sie fest, welcher Teil des Übergangs tatsächlich getestet wurde, mit welchem Ergebnis und welche Schritte noch offen sind.

Mögliche Nachweise

Testbericht · Auswertung und Verbesserungen · Betriebsanleitung · Migrationsprotokoll · Maßnahmenliste

9. Dimension E - Nachweise & Verlässlichkeit

E1 - Nachweise für kritische Aussagen

Frage: Gibt es für jede Aussage, die unsere Entscheidung wesentlich beeinflusst, einen aktuellen Nachweis?

Warum das wichtig ist

Ein beantworteter Fragebogen ist noch kein verifizierter Sachverhalt.

Ordnen Sie wesentliche Aussagen ein als:

- Anbieterangabe
- Vertragszusage
- Technische Nachweise
- Unabhängige Prüfungen
- Eigener Test

E2 - Geltungsbereich unabhängiger Prüfungen

Frage: Welche Audits, Testate oder Zertifizierungen bestehen und passen Gesellschaft, Dienst, Region, Zeitraum und Geltungsbereich zu unserem Anwendungsfall?

Mögliche Nachweise

Zertifikat einschließlich Geltungsbereich · C5-Bericht/Testat · SOC-Bericht · Erklärung der Prüfstelle · Akkreditierungsinformationen

E3 - Vertrag und Marketing

Frage: Sind wesentliche Zusagen zu Standort, Zugriff, Portabilität, Übergang und Kontrolle vertraglich ausreichend abgebildet?

Warum das wichtig ist

Eine Produktseite kann geändert werden. Kritische Anforderungen sollten belastbarer abgesichert werden.

© 2026 Andreas Heß · Autonomy Track

E4 - Aktualität und Benachrichtigung bei Änderungen

Frage: Wissen wir, wie alt die Nachweise sind, wann sie erneuert werden und wie wir von wesentlichen Änderungen erfahren?

Mögliche Nachweise

Berichtszeitraum · Zertifikatsgültigkeit · Änderungsprotokoll · Benachrichtigungsklausel · Prüfprotokoll

E5 - Nachweislücken und Verantwortlichkeit

Frage: Sind unbekannte Punkte mit einer verantwortlichen Person, einem nächsten Schritt und einem Überprüfungstermin dokumentiert?

Warum das wichtig ist

Offene Nachweisfragen brauchen eine Zuständigkeit und einen nächsten Schritt. Sonst kann eine vorläufige Annahme unbemerkt zur Entscheidungsgrundlage werden.

© 2026 Andreas Heß · Autonomy Track

10. Von der Feststellung zur Entscheidung

Wählen Sie die Handlungsoption passend zu den festgestellten Abhängigkeiten, den Folgen und den verfügbaren Alternativen. Dokumentieren Sie die Begründung, verbleibende Risiken, Zuständigkeiten und einen Termin zur Überprüfung. Mehrere Optionen lassen sich kombinieren.

Tolerieren	Eine bekannte Abhängigkeit bewusst akzeptieren, wenn Nutzen und Aufwand dafür sprechen und verbindliche Anforderungen erfüllt bleiben. Die Entscheidung wird begründet und regelmäßig überprüft.
Reduzieren	Die Abhängigkeit gezielt verringern, etwa durch offene Schnittstellen, exportierbare Konfigurationen oder den Aufbau eigener Kenntnisse.
Folgen begrenzen	Die Abhängigkeit bleibt bestehen. Sicherungskopien, Wiederanlaufverfahren oder zusätzliche Kontrollen begrenzen mögliche Schäden.
Alternativen aufbauen	Weitere Anbieter, verfügbare Kapazitäten oder eigenes Wissen schaffen Handlungsmöglichkeiten. Prüfen Sie, ob Alternativen tatsächlich unterschiedliche Abhängigkeiten haben.
Neu verhandeln	Vertragliche Rechte und Leistungen verbessern, beispielsweise bei Datenrückgabe, Unterstützung beim Wechsel oder Benachrichtigungen über Änderungen.
Migrieren	Anwendung und Daten in eine andere Umgebung überführen. Vorher prüfen, ob die Zielumgebung die maßgeblichen Anforderungen erfüllt und welche neuen Abhängigkeiten entstehen.
Ersetzen	Ein Produkt oder einen Anbieter austauschen. Funktionsumfang, Übergang, Datenübernahme und laufenden Betrieb der neuen Lösung berücksichtigen.
Aufgaben selbst übernehmen	Eine bislang ausgelagerte Aufgabe selbst betreiben oder kontrollieren. Dafür müssen Kenntnisse, Personal, Ressourcen und Verantwortlichkeiten dauerhaft gesichert sein.

Die Entscheidungsvorlage im Anhang des PDFs hält Bewertung, Begründung und Maßnahmen zusammen.

© 2026 Andreas Heß · Autonomy Track

11. Beispiel: Eine Plattform, zwei Einsatzbereiche

Das fiktive Beispiel zeigt, wie derselbe technische Befund je nach Nutzung zu unterschiedlichen Entscheidungen führen kann. Es bewertet keinen konkreten Anbieter.

Ausgangslage

Eine Organisation nutzt eine Cloud-Anwendung für die Zusammenarbeit. Bei der Prüfung werden folgende Punkte festgestellt:

- Vertragspartner ist eine europäische Gesellschaft. Kundendaten liegen laut Vertrag in einer EU-Region.
- Betrieb und technische Steuerung hängen teilweise von weiteren Anbietern außerhalb der EU ab.
- Kundenseitig verwaltete Schlüssel sind verfügbar. Sie schließen einen technischen Zugriff des Anbieters nicht in allen Verarbeitungsschritten aus.
- Primärdaten sind exportierbar. Einige Protokolle, Berechtigungsinformationen und Konfigurationen lassen sich nicht vollständig übertragen.
- Unterstützung beim Anbieterwechsel ist vertraglich geregelt. Ein vollständiger Wechsel wurde bisher nicht getestet.
- Unabhängige Prüfberichte liegen vor. Ob sie den aktuellen Dienst und die heutige Nutzung abdecken, ist noch zu klären.

Einsatz A: Allgemeine interne Zusammenarbeit

Bewertung: Die Anwendung unterstützt alltägliche Abläufe mit moderater Kritikalität. Besonders vertrauliche Daten werden in diesem Einsatzbereich nicht verarbeitet.

Mögliche Entscheidung: Die bekannten Abhängigkeiten vorläufig akzeptieren und ihre Folgen begrenzen, sofern die verbindlichen Anforderungen erfüllt sind. Offene Nachweisfragen werden fristgebunden geklärt.

Nächste Schritte:

- Regelmäßige Exporte und deren Wiederverwendbarkeit prüfen.
- Aktuelle Nachweise zum tatsächlich genutzten Dienst anfordern.
- Einen Wechseltest vor der nächsten Vertragsverlängerung durchführen.

Einsatz B: Kritische Prozesse mit vertraulichen Daten

Bewertung: Ein längerer Ausfall oder unberechtigter Zugriff hätte erhebliche Folgen. Die offenen Fragen zu Zugriffsmöglichkeiten und Wiederanlauf sind für diese Nutzung entscheidend.

Mögliche Entscheidung: Die Nutzung für diesen Einsatzbereich erst freigeben, wenn die festgelegten Anforderungen nachweislich erfüllt sind. Andernfalls eine geeignete Alternative auswählen.

Nächste Schritte:

- Wirksamkeit zusätzlicher Zugriffskontrollen und Verschlüsselungsverfahren prüfen.
- Notwendige Nachweise und vertragliche Zusagen einholen.
- Eine alternative Umgebung einschließlich Übergang und Betrieb testen.

Ergebnis: Der Anbieter ist derselbe. Kritikalität, Daten und Anforderungen unterscheiden sich. Eine pauschale Anbieterbewertung kann diese Abwägung nicht ersetzen.

© 2026 Andreas Heß · Autonomy Track

12. Regulatorischer Kontext

Dieser Leitfaden bietet keine vollständige Zuordnung gesetzlicher Anforderungen zu einzelnen Prüffragen. Einige aktuelle Regelwerke zeigen jedoch, warum Anbieterabhängigkeit, Lieferkette, Nachweise und Anbieterwechsel zunehmend konkrete Managementthemen sind.

EU Cloud Sovereignty Framework

Die Europäische Kommission veröffentlichte im Juni 2026 zusätzliche Umsetzungshinweise zu ihrem Cloud Sovereignty Framework.

Der Ansatz verwendet 48 Kriterien in acht Souveränitätsbereichen und ergänzt diese um Souveränitäts-Scores bzw. Vertrauensstufen.

Für die Anbieterbewertung bedeutet das: Neben dem Datenstandort zählen unter anderem Kontrolle, Technologieabhängigkeiten und betriebliche Fähigkeiten.

DORA

Die Verordnung (EU) 2022/2554 gilt seit dem 17. Januar 2025.

Erfasste Finanzunternehmen benötigen für IKT-Dienste, die kritische oder wichtige Funktionen unterstützen, unter anderem Ausstiegsstrategien. Die zugehörigen Ausstiegspläne müssen dokumentiert, angemessen getestet und regelmäßig überprüft werden. Alternative Lösungen und Übergangspläne gehören ebenfalls zum Konzept.

DORA gilt nicht für jede Organisation. Die Grundidee ist dennoch praktisch relevant:

> Kritische Anbieterabhängigkeit sollte nicht erst bei einer Kündigung untersucht werden.

NIS2 und deutsches BSIG

NIS2 nennt Sicherheit der Lieferkette und die Beziehung zu direkten Lieferanten und Diensteanbietern ausdrücklich als Bestandteil des Cybersicherheits-Risikomanagements.

Für deutsche besonders wichtige und wichtige Einrichtungen enthält § 30 BSIG entsprechende Anforderungen.

Das ist keine allgemeine gesetzliche Pflicht für jede Organisation und keine vollständige Souveränitätsdefinition. Es zeigt aber, dass Lieferanten- und Anbieterabhängigkeiten Teil belastbarer Risikosteuerung sind.

EU Data Act

Der Data Act enthält Anforderungen zum Wechsel zwischen Datenverarbeitungsdiensten und zur Portabilität.

Für den vom Data Act geregelten Wechsel entfallen Wechselgebühren einschließlich der dabei anfallenden Gebühren für ausgehende Datenübertragungen ab **12. Januar 2027**. Das bedeutet nicht, dass jede Datenübertragung während der laufenden Nutzung kostenfrei wird.

Ein gesetzliches Recht auf Wechsel ersetzt keine technische Wechselfähigkeit.

© 2026 Andreas Heß · Autonomy Track

BSI C5

C5 bietet einen Kriterienkatalog für unabhängige Prüfungen von Cloud-Diensten.

Das BSI stellt ausdrücklich klar, dass es sich bei einem C5-Testat **nicht um eine BSI-Zertifizierung** handelt. Das BSI weist außerdem darauf hin, dass ein C5-Testat allein nicht automatisch ausreicht, um alle Anforderungen des Mindeststandards zur Nutzung externer Cloud-Dienste zu erfüllen.

Prüfen Sie beim C5-Bericht insbesondere den erfassten Dienst, den Prüfzeitraum, den Testatstyp, festgestellte Abweichungen und die vom Kunden selbst zu erfüllenden Kontrollen.

ISO/IEC 27001

ISO/IEC 27001:2022 beschreibt Anforderungen an Informationssicherheitsmanagementsysteme.

Eine passende Zertifizierung kann die Bewertung der Informationssicherheit unterstützen.

Sie ist jedoch kein automatischer Nachweis digitaler Souveränität.

13. Wann sollte neu bewertet werden?

Eine Neubewertung sollte insbesondere ausgelöst werden durch:

- Vertragsverlängerung
- Übernahme oder Eigentümerwechsel
- Wesentliche Änderung kritischer Unterauftragnehmer
- Änderung von Daten- oder Betriebsstandorten
- Neue technische Plattform/technische Steuerungsebene
- Erheblicher Sicherheitsvorfall
- Neue regulatorische Anforderungen
- Änderung der Kritikalität der Anwendungen
- Neue realistische Alternativen
- Ergebnisse eines Wechsel-Tests

© 2026 Andreas Heß · Autonomy Track

14. Die wichtigste Regel

Das Ziel ist nicht maximale Unabhängigkeit um jeden Preis.

Das Ziel ist:

> **Abhängigkeiten sichtbar machen, Nachweise von Annahmen trennen und bewusst entscheiden, welche Abhängigkeit eine Organisation für einen konkreten Zweck akzeptiert.**

Eine dokumentierte, begründete Abhängigkeit kann eine gute Entscheidung sein.

Eine tragfähige Entscheidung benennt auch Unsicherheiten und offene Nachweise. Sie legt fest, wer diese klärt und wann die Bewertung erneut geprüft wird.

© 2026 Andreas Heß · Autonomy Track

Anhang A: 25-Fragen-Kurzcheckliste

Nur abhaken, wenn die Aussage nachvollziehbar erfüllt ist. Nicht anwendbare Punkte begründen. Offene Punkte mit Zuständigkeit und Termin festhalten. Die Haken ergeben keinen Souveränitäts-Score.

Dienst / Anbieter: _____ Datum: _____

Recht & Kontrolle

- ☐ A1 Vertragspartner, kontrollierende Gesellschaften und relevante Eigentumsstrukturen sind bekannt.
- ☐ A2 Relevante Rechtsordnungen für Vertrag, Betrieb, Zugriff und Offenlegung sind identifiziert.
- ☐ A3 Rechte zu Prüfungen, Änderungen, Unterauftragnehmern, Kündigung, Datenrückgabe und Anbieterwechsel sind geprüft.
- ☐ A4 Kritische Drittanbieter und Unterauftragnehmer sind bekannt.
- ☐ A5 Eigentümerwechsel und wesentliche Änderungen des Geschäftsmodells sind berücksichtigt.

Daten & Betrieb

- ☐ B1 Speicher-/Verarbeitungsorte für Daten, Sicherungskopien, Protokolle, Metadaten und Notfallwiederherstellung sind bekannt.
- ☐ B2 Privilegierte Zugriffs- und Supportwege sind verstanden.
- ☐ B3 Schlüsselkontrolle und möglicher Klartextzugriff sind verstanden.
- ☐ B4 Kritische operative Abhängigkeiten und Wiederherstellungswege sind bekannt.
- ☐ B5 Aufbewahrung, Löschung und operative Nachweisbarkeit sind geprüft.

Technologie & Lieferkette

- ☐ C1 Proprietäre technische Abhängigkeiten sind dokumentiert.
- ☐ C2 Standards, Schnittstellen und Interoperabilität sind bewertet.
- ☐ C3 Kritische vorgelagerte Technologieabhängigkeiten sind bekannt.
- ☐ C4 Konfiguration, Richtlinien und Automatisierung sind auf Reproduzierbarkeit geprüft.
- ☐ C5 Kenntnisse und Ökosystem für mögliche Alternativen sind bewertet.

© 2026 Andreas Heß · Autonomy Track

ANHANG A · FORTSETZUNG

25-Fragen-Kurzcheckliste

Dienst / Anbieter: _____ Datum: _____

Übertragbarkeit & Anbieterwechsel

- ☐ D1 Vollständigkeit und Nutzbarkeit des Exports sind geprüft.
- ☐ D2 Wechselprozess, Unterstützung, Fristen und Kosten sind dokumentiert.
- ☐ D3 Mindestens eine realistische Zieloption ist bekannt.
- ☐ D4 Zeit, Kosten, Kenntnisse und Auswirkungen auf den Betrieb eines Anbieterwechsels sind geschätzt.
- ☐ D5 Ein für den Anbieterwechsel relevantes Szenario wurde durchgeführt und dokumentiert. Noch ungetestete Schritte sind ausdrücklich benannt.

Nachweise & Verlässlichkeit

- ☐ E1 Wesentliche Anbieterangaben besitzen nachvollziehbare Nachweise.
- ☐ E2 Geltungsbereich und Aktualität unabhängiger Prüfungen sind geprüft.
- ☐ E3 Kritische Marketingaussagen sind mit Vertragszusagen abgeglichen.
- ☐ E4 Alter der Nachweise und Benachrichtigung bei Änderungen sind berücksichtigt.
- ☐ E5 Für offene Fragen und Nachweislücken sind Verantwortliche, nächste Schritte und Überprüfungstermine festgelegt.

Offene oder nicht anwendbare Punkte

© 2026 Andreas Heß · Autonomy Track

Anhang B: Nachweisliste

Benötigte Unterlagen auswählen. Eingang und Prüfung getrennt abhaken. „Geprüft“ bedeutet: Aussagekraft, Aktualität und Geltungsbereich bewertet. Es bedeutet nicht automatisch, dass alle Anforderungen erfüllt sind.

Dienst / Anbieter: _____ Datum: _____

Unterlage / Nachweis	Erhalten	Geprüft
Vertragspartner und Konzern-/Eigentumsstruktur	☐	☐
Aktuelle Leistungsbeschreibung	☐	☐
Architektur- und Datenflussdarstellung	☐	☐
Zugesicherte Standorte für Daten, Sicherungskopien und Notfallwiederherstellung	☐	☐
Kritische Dienstleister und Unterauftragnehmer	☐	☐
Support- und privilegiertes Zugriffsmodell	☐	☐
Verschlüsselungs- und Schlüsselverwaltungsmodell	☐	☐
Modell der geteilten Verantwortung	☐	☐
API-, Export- und Portabilitätsdokumentation	☐	☐
Wechsel-/Übergangsprozess	☐	☐
Kündigungs-, Aufbewahrungs- und Löschbedingungen	☐	☐
Leistungsvereinbarung, Betriebsfortführung und Notfallwiederherstellung	☐	☐
Benachrichtigungsregeln bei wesentlichen Änderungen	☐	☐
Aktuelle Auditberichte, Testate oder Zertifikate einschließlich Geltungsbereich	☐	☐
Beispiel für einen Export oder Migrationstest, wenn relevant	☐	☐
Bekannte Kosten für Anbieterwechsel, Export und Unterstützung beim Wechsel	☐	☐

© 2026 Andreas Heß · Autonomy Track

Anhang C: Entscheidungsvorlage

1 / 4 · Betrachtungsbereich

Dienst / Anwendung und Anbieter

Fachlich verantwortlich · Datum der Bewertung

Kritikalität und Folgen eines Ausfalls

Datenarten und Schutzbedarf

Gesetzliche und interne Anforderungen

Vertragsende / nächste Verlängerung

© 2026 Andreas Heß · Autonomy Track

ANHANG C · ENTSCHEIDUNGSVORLAGE

2 / 4 · Feststellungen und offene Fragen

Recht & Kontrolle

Feststellungen und wesentliche Abhängigkeiten · Nachweis / Fundstelle

Offene Fragen · nächste Schritte · verantwortlich · Termin

Daten & Betrieb

Feststellungen und wesentliche Abhängigkeiten · Nachweis / Fundstelle

Offene Fragen · nächste Schritte · verantwortlich · Termin

Technologie & Lieferkette

Feststellungen und wesentliche Abhängigkeiten · Nachweis / Fundstelle

Offene Fragen · nächste Schritte · verantwortlich · Termin

© 2026 Andreas Heß · Autonomy Track

ANHANG C · ENTSCHEIDUNGSVORLAGE

3 / 4 · Feststellungen und offene Fragen

Übertragbarkeit & Anbieterwechsel

Feststellungen und wesentliche Abhängigkeiten · Nachweis / Fundstelle

Offene Fragen · nächste Schritte · verantwortlich · Termin

Nachweise & Verlässlichkeit

Feststellungen und wesentliche Abhängigkeiten · Nachweis / Fundstelle

Offene Fragen · nächste Schritte · verantwortlich · Termin

© 2026 Andreas Heß · Autonomy Track

ANHANG C · ENTSCHEIDUNGSVORLAGE

4 / 4 · Entscheidung und Umsetzung

Gewählte Optionen (Mehrfachauswahl möglich)

- ☐ Tolerieren
- ☐ Folgen begrenzen
- ☐ Neu verhandeln
- ☐ Ersetzen
- ☐ Reduzieren
- ☐ Alternativen aufbauen
- ☐ Migrieren
- ☐ Aufgaben selbst übernehmen

Begründung der Entscheidung

Akzeptierte Restabhängigkeiten und Risiken

Maßnahmen · verantwortlich · Zieltermin

Freigabe / verantwortlich · Datum

Nächste Überprüfung · Termin oder Anlass

© 2026 Andreas Heß · Autonomy Track

Quellen und weiterführende Informationen

Dieser Leitfaden unterstützt die strukturierte Technologie- und Anbieterbewertung. Er ersetzt keine individuelle Rechtsberatung oder verbindliche Konformitätsprüfung.

1. Europäische Kommission: Cloud Sovereignty Framework

https://commission.europa.eu/news-and-media/news/sovereign-cloud-framework-explained-2026-06-01_en

2. EUR-Lex: DORA - insbesondere Artikel 28 bis 30 und 64

https://eur-lex.europa.eu/eli/reg/2022/2554/oj

3. Europäische Kommission: Data Act erklärt

https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

4. EUR-Lex: NIS2 - Richtlinie (EU) 2022/2555

https://eur-lex.europa.eu/eli/dir/2022/2555/oj

5. EUR-Lex: Durchführungsverordnung (EU) 2024/2690 zu NIS2

https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj

6. Gesetze im Internet: § 30 BSIG

https://www.gesetze-im-internet.de/bsig_2025/__30.html

7. BSI: Kriterienkatalog C5 für Cloud-Dienste

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

8. BSI: Einordnung von C5-Testaten bei externen Cloud-Diensten

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/Externe_Cloud-Dienste/FAQ_MST_Externe_Cloud-Dienste/faq_mst_Externe_Cloud-Dienste_node.html

9. ISO: ISO/IEC 27001:2022

https://www.iso.org/standard/27001

© 2026 Andreas Heß · Autonomy Track