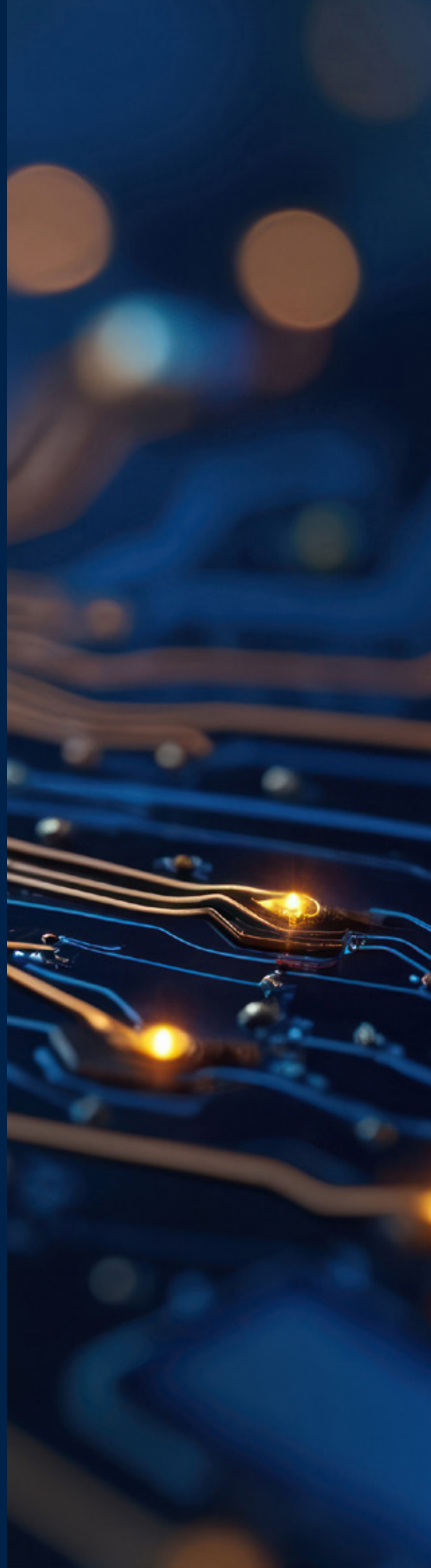


Die Handlungs-
fähigkeit sichern:
*Ein Leitfaden zur
digitalen
Souveränität*

BEST PRACTICE GUIDE

Chancen und Abhängigkeiten: Der Weg zur digitalen Souveränität	03
Sieben Maßnahmen zur digitalen Unabhängigkeit Ihres Unternehmens:	04
1. Open Source Alternativen	04
2. Technologie Made in EU	05
3. Daten in der Cloud	06
4. OnPrem statt Cloud	07
5. Partner in die Pflicht nehmen	08
6. Exit-Strategien entwickeln	09
7. Co-Management und Diversifizierung	10
Fazit und Ausblick	11
Kontakt	13



Chancen & Abhängigkeiten: Der Weg zur digitalen Souveränität

In unserer vernetzten und datengetriebenen Welt ist die digitale Souveränität für Unternehmen vom reinen Buzzword zum strategischen Erfolgsfaktor geworden. Die enge Verzahnung mit Partnerunternehmen, die Nutzung von Cloud-Diensten und datenbasierte Geschäftsmodelle bieten enorme Chancen. Diese sind allerdings auch kritisch zu hinterfragen:



Auslandsabhängigkeit

96% der deutschen Unternehmen sind auf Services aus dem Ausland angewiesen – vor allem USA und China¹



Befürworter

84,4% der IT-Entscheider befürworten EU-Digitalprodukte für kritische Systeme, aber nur 20% befinden sich im Umstieg²



Konkrete Strategie

Nur **21% der Unternehmen** haben eine konkrete Strategie zur digitalen Souveränität entwickelt³



Strategisches Ziel

87% der Unternehmen sehen digitale Unabhängigkeit als strategisches Ziel, aber 79 % befinden sich in kritischer Abhängigkeit außereuropäischer Anbieter⁴

Laut einer Studie von adesso und dem Handelsblatt Research Institute bremsen vor allem fehlende Kompetenzen, Fachkräftemangel und hohe Kosten den Ausbau der Digitalen Souveränität⁵. Gerade in Zeiten globaler Unsicherheiten, wachsender Cyberbedrohungen und komplexer regulatorischer Anforderungen gewinnt die digitale Souveränität mehr und mehr an Bedeutung.

Die Kontrolle über die eigenen Daten, Infrastruktur und Prozesse zu behalten ist entscheidend, um nicht von Plattformen oder geopolitischen Interessen abhängig zu sein. Ziel ist es, die eigene Handlungsfähigkeit zu sichern, Risiken zu minimieren und langfristig wettbewerbsfähig zu bleiben.



1 Digitale Souveränität 2025 | Studienbericht | Studie 2025 | Bitkom e. V.

2 1753185101-myra-state-of-digital-sovereignty-2025.pdf

3 Erster „Index Digitale Souveränität“ von adesso zeigt: Vier von fünf Unternehmen ohne Strategie

4 Neue Bitkom-Studie zu digitaler Souveränität als Schlüsselthema der Digitalisierung | Wirtschaft Digital BW

5 Erster „Index Digitale Souveränität“ von adesso zeigt: Vier von fünf Unternehmen ohne Strategie

Sieben Maßnahmen zur digitalen Unabhängigkeit Ihres Unternehmens:

1. Open Source Alternativen

Der Löwenanteil der im Büroalltag eingesetzten Software stammt von Großkonzernen mit teils einseitiger und/oder restriktiven Lizenzmodellen. Wer sich hier vollkommen auf einzelne Ökosysteme (Walled Gardens) verlässt, kann sehr leicht von diesen Anbietern unter Druck gesetzt werden. Dem können Sie sich entziehen, durch den Einsatz von quelloffener, kostenfreier Open Source Software:

- ✓ **Spart Lizenzkosten**
- ✓ **Vermeidet Abhängigkeiten von einzelnen Herstellern**
- ✓ **Ist sicherer, durch das konsequente Review der Codebasis und ihre bessere Nachvollziehbarkeit**
- ✓ **Bietet Unterstützung von großen Online-Communities**

PROMINENTE BEISPIELE

für erfolgreiche, professionelle Open Source Lösungen sind: Libre Office, GIMP Bildbearbeitung, Linux-OS, Mozilla Firefox Browser oder Thunderbird Mail Client.

2. Technologie Made in EU

Datensouveränität steht und fällt mit der zuständigen Jurisdiktion des Technologiepartners. Wird ein Technologiepartner von seiner Regierung gezwungen Daten herauszugeben, helfen auch keine noch so sicher formulierten vertraglichen Vereinbarungen. Hier hilft nur die Wahl des richtigen Anbieters mit Sitz in der EU. Die EU und ihre assoziierten Staaten haben hier die weltweit strengsten Regularien in Bezug auf:

- **Datenschutz**

(DSGVO, TISAX, DORA)

- **Verbraucherschutz**

(Digital Fairness Act, Digital Services Act)

- **Sorgfaltspflichten**

(EU-Data Act, EU-Lieferkettengesetz, EU-Sorgfaltspflichtengesetz)

Software und Services aus EU-Ländern sind damit grundsätzlich eine gute Investition zum Schutz der eigenen Daten und Infrastruktur, wenn es um Rechtssicherheit und Justiziabilität geht. Dies gilt in besonderem Maße bei der Wahl eines Cloudanbieters. Selbst wenn die Server der Rechenzentren in der EU beheimatet sind, ist **entscheidend, wo das Unternehmen seinen Hauptsitz hat.**



3. Daten in der Cloud

Wer seine Daten in einer Cloud speichert, darf sich nicht allein auf die Sicherung durch den Anbieter verlassen. Auch wer Cloud-services nur innerhalb der EU mit ihren strengen Datenschutzvorschriften nutzt, sollte sich Gedanken machen über:

Verschlüsselung

Datensicherheit verlangt, dass auch der Cloudanbieter keinen Zugriff auf Klartextdaten hat. Unternehmen, die Daten verschlüsseln, zeigen Verantwortung und stärken das Vertrauen in ihre digitalen Prozesse.



Löschkonzepte

Nach Beendigung des Vertrags muss sichergestellt werden, dass Ihre Daten auch wirklich gelöscht wurden.



Freigabekonzepte

Die Nutzung von Cloud-Diensten braucht zuverlässige und durchdachte Berechtigungs- und Freigabekonzepte. Hier gilt der Grundsatz „So viel wie nötig, so wenig wie möglich“.



Durch diese Maßnahmen lässt sich bereits ein gewisses Maß an Sicherheit und Unabhängigkeit erreichen.





4. OnPrem statt Cloud

Cloud-Services bestehen vor allem durch ihren Komfort und ihre Skalierbarkeit. Dennoch ist es für ihren Einsatz unumgänglich, dass Sie Ihre Daten anderen Unternehmen anvertrauen. **Wer dies nicht möchte, sollte eine Rückkehr auf On-Premises in Betracht ziehen für die folgenden Vorteile:**

- ✓ **Kein Zugriff Dritter auf sensible, digitale Ressourcen**
- ✓ **Kann langfristig günstigere Lösung sein als Cloud**
- ✓ **Schnellere Problemlösung durch die eigenen Mitarbeiterinnen und Mitarbeiter**



Damit On-Prem gelingt, müssen Unternehmen aber rechtzeitig in das nötige Know-how und die technische Ausstattung innerhalb ihrer Organisation investieren.

5. Partner in die Pflicht nehmen

Digitale Souveränität kann nur erreicht werden, wenn Unternehmen nicht nur ihre internen Prozesse und Systeme absichern, sondern auch Partnerunternehmen konsequent in die Verantwortung nehmen. Vor- und nachgelagerte Technologie- und Servicepartner spielen eine entscheidende Rolle bei der Verarbeitung sensibler Daten und der Bereitstellung digitaler Infrastruktur. Daher ist es essenziell, klare Regelungen zur Datenverarbeitung und -speicherung sowie zu Sicherheitsstandards vertraglich festzuhalten.



Transparenz

Fordern Sie von Ihren Partnern in diesem Punkt vollständige Transparenz.



Offenlegung

Bestehen Sie auf Offenlegung von Subdienstleistern und deren Standorte, um potenzielle Risiken durch ausländische Rechtszugriffe – etwa durch den CLOUD Act oder vergleichbare Regelungen – frühzeitig zu erkennen und zu bewerten.



Absicherung

Achten Sie darauf, dass vertragliche Vereinbarungen explizit den Schutz vor unautorisiertem Zugriff durch Dritte regeln und Mechanismen zur Informationssicherheit, wie Verschlüsselung und Zugriffskontrollen, verbindlich festlegen.



Überprüfung

Vereinbaren Sie vertraglich regelmäßige Audits und Zertifizierungen (z. B. ISO 27001), um die Einhaltung der zugesicherten Standards zu überprüfen.



6. Exit-Strategien entwickeln

Unternehmen entwickeln sich weiter, so kommt es vor, dass Technologie- oder Servicepartner nicht mehr zu Ihren Anforderungen hinsichtlich eines sicheren und rechtskonformen Umgangs Ihrer Daten passen. Gründe dafür sind vielfältig: veränderte Geschäftsmodelle, Sicherheitsvorfälle, mangelnde Transparenz oder auch geopolitische Entwicklungen. Um in solchen Fällen handlungsfähig zu bleiben, ist es empfehlenswert, für alle geschäftskritischen Systeme und Dienste frühzeitig Alternativen zu suchen und Exit-Strategien zu entwickeln.

In der Strategie sollten klare Prozesse und Verantwortlichkeiten enthalten sein, um einen Wechsel strukturiert und mit minimalen Unterbrechungen durchführen zu können.



Task 1

Überprüfen Sie in regelmäßigen Inventuren, an welchen Stellen im Unternehmen Sie welche Services einsetzen und welche Alternativen es dazu gibt.

Task 2

Erstellen Sie einen Prozess, in dem sowohl Abläufe bei einem Service/Technologiewechsel als auch die Verantwortlichkeiten festgelegt sind.

Task 3

Regeln Sie Fristen für die Datenlöschung beim bisherigen Partner sowie Nachweise über die vollständige Löschung.

7. Co-Management und Diversifizierung

Digitale Souveränität bedeutet auch, unabhängig von einzelnen Softwarelösungen agieren zu können. Unternehmen sollten sich daher nicht in einseitige Abhängigkeiten begeben, sondern auf Diversifizierung setzen.

Der parallele Einsatz mehrerer kompatibler Systeme erhöht die Ausfallsicherheit und ermöglicht es, bei Störungen oder Einschränkungen einer Lösung handlungsfähig zu bleiben.

Co-Management unterstützt diesen Ansatz durch:

- **Gleichzeitige Verwaltung durch unterschiedliche Plattformen**
- **Flexibilität in der IT-Infrastruktur gemäß des „Best of Breed“ Konzepts**
- **Vermeidung von Lock-in-Effekten, also die Abhängigkeit von einzelnen Herstellern**

Durch die Kombination von Diversifizierung und Co-Management behalten Unternehmen die Kontrolle über ihre digitalen Prozesse und können schneller auf Veränderungen reagieren, sowohl aus technischen, wirtschaftlichen oder regulatorischen Gründen.



Fazit und Ausblick

Digitale Souveränität ist kein einmaliges Projekt, sondern ein fortlaufender Prozess, der strategisches Denken, technologische Kompetenz und organisatorische Klarheit erfordert. Unternehmen, die heute die richtigen Weichen stellen, sichern sich für morgen die nötige Unabhängigkeit und Flexibilität, um auf veränderte Situationen souverän reagieren zu können.



Prüfen Sie Ihre bestehenden digitalen Abhängigkeiten, definieren Sie klare Ziele für mehr digitale Selbstbestimmung und setzen Sie diese konsequent um.



Jetzt ist der richtige Zeitpunkt, *aktiv zu werden.*

Über baramundi software GmbH

baramundi software entwickelt Unified Endpoint Management für die zentrale Verwaltung von PCs, mobilen Geräten und Servern. Es automatisiert die Softwareverteilung, vereinfacht das Patch-Management und schafft Transparenz im Netzwerk. baramundi leistet damit einen wesentlichen Beitrag zur IT-Sicherheit und setzt Ressourcen frei.



Noch Fragen?

Vereinbaren Sie gerne einen Termin mit uns.

In einem persönlichen Gespräch erläutern wir Ihnen, wie die baramundi software GmbH Ihnen mit ihrer Unified-Endpoint-Management-Lösung zu mehr digitaler Unabhängigkeit verhelfen kann.



Kontaktieren Sie uns.
Wir freuen uns auf Sie!



Making IT Admins Smile



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+49 821 56708-390
request@baramundi.com