Mittelstand-Digital
Zentren
Deutschlandweit

Use-Cases für Digitale Souveränität

KMU-Typen - Ausgangslage / Risiken / Kosten / Nutzen / Lösungsansatz

Gefördert durch:

Bundesministerium
für Wirtschaft
und Energie

Mittelstand-
Digital

aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-Digital
Zentren
Deutschlandweit

Use Case Vorlage

- Vorlagefolie
- Die nachfolgenden Use-Cases auf diese Formatierung hier anpassen

- Ausgangslage:
- Risiken
- Kosten
- Nutzen
- Lösungsansätze

- Je eine Folie (oder mehr nach Bedarf)

- Kevin: Maschinenbaubetrieb (3) & Handwerk/Kleinstunternehmen (1)
- Frank: Verwaltung (5) & Online Druckerei (4)
- Lavinia: Baubetrieb (2) & mittleres KMU (6)

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 1: Einzelhandwerker & Kleinstunternehmen (1–10 MA)

- Ausgangslage
  - Einzelhandwerker und Kleinstunternehmen mit 1–10 Mitarbeitern.
- Motivation für Digitale Souveränität
  - Einfachheit und Resilienz stehen im Vordergrund. Der Betrieb darf nicht stillstehen, nur weil ein Cloud-Anbieter die Preise erhöht oder das Konto sperrt.
- Tools
  - Rechnungsstellung
  - Kundenkommunikation (WhatsApp/E-Mail)
  - Einfache Terminplanung
- Anforderungen
  - „Plug & Play“-Lösungen
  - Niedrige Wartungskosten
  - Datensicherung ohne Expertenwissen
- Risiken
  - Lock-in-Effekte: Abhängigkeit von proprietärer Branchensoftware, die nur in einer bestimmten Cloud läuft.
- Nutzen
  - Unabhängigkeit von großen Plattformen
    Schutz der Kundendaten
- Kosten
  - Geringe Investitionskosten, ggf. hohe laufende Abokosten

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 1: Einzelhandwerker & Kleinstunternehmen (1–10 MA)

- Lösungsansätze
  - Rechnungsstellung: Open-Source- oder selbstgehostete Lösungen
  - Kundenkommunikation: Messenger/E-Mail-Dienst wechseln
  - Terminplanung: Kalenderanbieter wechseln
  - Datensicherung: Lokales oder souveränes Cloud-Backup
  - Lock-in-Effekte vermeiden: Offene Datenformate verwenden
  - Hardware-Infrastruktur: Eigene Server/NAS im Haus aufstellen

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 2: Kleine bis mittlere Baubetriebe

- **Ausgangslage:** Souveränität bedeutet hier **Unabhängigkeit auf der Baustelle** (Offline-Fähigkeit)
  - NIS-2:
    - in der Regel nein
    - es sein denn, sie bauen kritische Infrastruktur (z. B. spezialisierter Tiefbau für Stromnetze)
    - dennoch steigen die Anforderungen durch Versicherungen
  - IT-Sicherheit: Pragmatisch
    - Fokus auf Schutz vor Identitätsdiebstahl (Phishing)
    - Umsetzung durch externe lokale IT-Dienstleister
  - Software: kommerzielle Branchensoftware
  - Datenhaltung:
    - lokal oder "Handwerker-Cloud"
    - Wichtig: Offline-Synchronisation für Keller / Baustellen ohne Empfang
  - Mobile Geräte:
    - Rugged Devices (stoßfest)
    - Organisation via Mobile Device Management (MDM), um bei Verlust auf der Baustelle Geräte sofort aus der Ferne zu löschen (Remote Wipe)

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 2: Kleine bis mittlere Baubetriebe

- **Risiken:**
  - Phishing-Angriffe auf Mitarbeitende mit geringer IT-Affinität — hohes Eintrittspotenzial
  - Geräteverlust auf Baustellen: ohne MDM und Remote Wipe (Fernlöschung) drohen Datenschutzverstöße (DSGVO)
  - Abhängigkeit von externer IT: Supportlücken gefährden Betriebskontinuität
  - Synchronisationsfehler bei Offline-Betrieb: Konflikte zwischen Büro- und Baustellendaten möglich
  - Spezialbetriebe (krit. Infrastruktur) übersehen NIS-2-Pflicht — empfindliche Bußgelder drohen
  - Lock-in durch kommerzielle Branchensoftware: Datenmigration bei Anbieterwechsel aufwendig
- **Kosten**:
  - Rugged Devices (stoßfeste Tablets/Smartphones): deutlich höhere Anschaffungskosten als Consumer-Geräte
  - MDM-Lösung: Lizenz pro Gerät und Einrichtungsaufwand durch IT-Dienstleister
  - Branchensoftware: monatliche SaaS (software as a service)-Gebühren oder einmalige Lizenz + Wartungsvertrag
  - Phishing-Schulungen: regelmäßig, typisch als externer Kursanbieter
  - Lokaler IT-Dienstleister: laufende Betreuungspauschale
  - Offline-Sync-Infrastruktur: ggf. lokaler Server oder NAS (netzwerkgebundener Speicher) als Zwischenspeicher

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 2: Kleine bis mittlere Baubetriebe

- **Nutzen**:
  - Arbeiten ohne Mobilfunk auf Kellerbaustellen und in Funklöchern: Produktivität bleibt erhalten
  - Automatische Synchronisation beim nächsten Verbindungsaufbau: keine Datenverluste
  - Remote Wipe per MDM: verlorene oder gestohlene Rugged Devices sofort aus der Ferne löschbar
  - Schutz vor Phishing/Identitätsdiebstahl schützt Auftragsabwicklung und Zahlungsverkehr
  - Branchensoftware mit Handwerker-Cloud: niedrige Einstiegshürde, wartungsarm
  - Bessere Versicherungseinstufung durch nachweisbare IT-Sicherheitsmaßnahmen

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 2: Kleine bis mittlere Baubetriebe

- **Lösungsansatz 1**:Einstiegslösung: Handwerker-Cloud + MDM
  - für Betriebe, die schnell starten wollen
  - mit minimalem internem IT-Aufwand
  - Planbare Kosten durch monatliche SaaS-Gebühren
  - Jedoch:
    - Daten liegen beim SaaS-Anbieter ➔ begrenzte Datensouveränität
    - Abhängigkeit vom Anbieter (Lock-In, Preiserhöhungen)
    - Für kritische-Infrastruktur-Betriebe nicht ausreichend (NIS-2)

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 2: Kleine bis mittlere Baubetriebe

- **Lösungsansatz 2**:
  - Lokale Datenhaltung + MDM + Sicherheitskonzept
  - Für Betriebe mit 10+ Mitarbeitenden oder Aufträgen im sensiblen Bereich geeignet
  - Daten bleiben im eigenen Haus ➔ echte digitale Souveränität
  - Skalierbar: NAS und MDM wachsen mit dem Betrieb
  - Geringere Abhängigkeit von Drittanbietern
  - Versicherungsanforderungen und ggf. NIS-2 erfüllt
  - Jedoch:
    - Höherer Einrichtungsaufwand
    - Lokaler IT-Dienstleister mit NAS-Erfahrung nötig
    - Eigener Server = eigene Wartungsverantwortung

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 3: Kleines produzierendes KMU (Lohnfertiger, Maschinenbau; 30 MA)

- Ausgangslage
  - Produzierende KMU mit ca. 30 Mitarbeitern, oft mit einer Person für IT oder externem Dienstleister.
- Motivation für Digitale Souveränität
  - Einfachheit und Resilienz stehen im Vordergrund. Der Betrieb darf nicht stillstehen, nur weil ein Cloud-Anbieter die Preise erhöht oder das Konto sperrt.
- Tools
  - Gemeinsame Datenablage
- ERP-System
  - Vernetzung von Büro und Produktion/Baustelle
- IT-Sicherheit:
  - Fokus auf IT-Security (Absicherung der Maschinenparks)
  - Umsetzung meist durch spezialisierte IT/OT-Dienstleister
- Software:
  - Kommerziell dominiert (CAD, ERP)
  - Open Source im Bereich Infrastruktur (z. B. Monitoring mit Grafana)
- Datenhaltung:
  - Hybrid: CAD-Daten oft lokal (Latenz!), ERP zunehmend in der Cloud
  - Backup: Air-Gapped (physisch getrennt), um Ransomware zu trotzen
- Mobile Geräte:
  - Tablets in der Fertigung für Zeichnungen/Auftragsbearbeitung
  - Absicherung über MDM mit strikter App-Kontrolle

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 3: Kleines produzierendes KMU (Lohnfertiger, Maschinenbau; 30 MA)

- Anforderungen
  - Interoperabilität:
    - Daten müssen zwischen verschiedenen Programmen fließen können (Schnittstellen).
  - IP-Schutz:
    - Schutz von Intellectual Property und Verfügbarkeit der Produktion.
  - NIS-2:
    - Oft betroffen als „Wichtige Einrichtungen“ (Sektor Verarbeitendes Gewerbe), wenn >50 MA oder >10 Mio. € Umsatz.
  - Sicherheitsstufe:
    - Wichtig (bei kritischen Zulieferern für Sektoren wie Energie/Medizin evtl. sogar Wesentlich).
- Risiken
  - Abhängigkeit vom IT-Dienstleister (z. B. wenn nur dieser die Passwörter besitzt).
- Nutzen
  - Prozessstabilität: IT-Dienstleister kann gewechselt werden, ohne die Infrastruktur neu aufbauen zu müssen.
- Kosten
  - Moderat: Investitionen in eigene Hardware (z. B. NAS) oder kontrollierte Cloud-Instanzen

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 3: Kleines produzierendes KMU (Lohnfertiger, Maschinenbau; 30 MA)

- Lösungsansätze
  - Gemeinsame Datenablage: Lokale oder souverän gehostete Ablage
  - ERP-System: Open-Source-ERP-System verwenden
  - Datenexport und Lock-In-Vermeidung:
    - Regelmäßige Backups lokal speichern
    - Offene Dateistandards (z.B. .step)
  - IP-Schutz
    - Daten klassifizieren
    - Daten lokal speichern
  - IT-Sicherheit
    - Backuplösungen
    - Nur gezielte Ausgehende Verbindungen zulassen
    - Netzwerke trennen
  - Abhängigkeit von IT-Dienstleistern
    - Eigenens Passwortmanagement einführen
    - Eigene IT-Fachkraft einstellen
  - Mobile Geräte: App-Whitelisting, Containerisierung
  - NIS-2-Complience: Risikomanagement einführen und Maßnahmenkatalog erstellen

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 4: Serviceorientierte Unternehmen (Agentur, Online-Druckerei)

- **Ausgangslage:** sie haben die höchste digitale Kompetenz, aber oft die geringste infrastrukturelle Souveränität; sie tauschen Autonomie gegen Geschwindigkeit; von NIS-2 meist nicht direkt
- **Risiken:**
  - höherer Aufwand bei Auswahl und Implementierung der aufeinander abgestimmten Open-Source-Tools
  - längere Einarbeitungszeiten in Open-Source-Software, Schulung
- **Kosten:**
  - kurzfristig höher: Tool-Auswahlprozess, Implementierung, Schulung
  - Langfristige Kostenstabilität durch Open Source und selbst gehosteten Instanzen → die Kosten pro Mitarbeiter skalieren linearer und sind planbar

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 4: Serviceorientierte Unternehmen (Agentur, Online-Druckerei)

- **Nutzen:** Souveränität wird zum strategischen Differenzierungsmerkmal
  - Wettbewerbsvorteil durch "Trust & Compliance": Kunden aus dem Enterprise-Sektor, dem öffentlichen Dienst oder der Medizinbranche ist der Datenschutz das KO-Kriterium → DSGVO-Konformität "by Design"
  - Schutz des geistigen Eigentums (IP-Security): in Kreativagenturen ist das Design, das Konzept oder der Code das Kapital
  - Zugriff auf den Quellcode und die APIs der Werkzeuge → es können individuelle Workflows entstehen, die von der Konkurrenz nicht einfach kopiert werden können
- **Lösungsansatz:**
  - Open-Source-Tool-Set
  - On-Premise oder in deutscher / europäischer Cloud

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Use Case 5: Städte- / Gemeindeverwaltung

- **Ausgangslage:** für Verwaltungen ist digitale Souveränität ein politisches Ziel und rechtliche Notwendigkeit (DSGVO, NIS-2)
- **Risiken:**
  - hoher Aufwand bei Auswahl der aufeinander abgestimmten Tools für die Fachverfahren und bei Implementierung in der deutschen Verwaltungscloud
  - längere Einarbeitungszeiten in Open-Source-Software und ggf. Ablehnung durch betroffene Mitarbeiter
- **Kosten:**
  - kurzfristig höher: Implementierung, Schulung …
  - Langfristige Kosten- / Budgetstabilität → die Kosten pro Mitarbeiter skalieren linearer und sind planbar

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 5: Städte- / Gemeindeverwaltung

- **Nutzen:**
  - Rechtssicherheit und Datenschutz (Compliance) → Ziel: deutsche Verwaltungscloud und Open-Source-Software (Trend)
  - Handlungsfähigkeit und Unabhängigkeit von außereuropäischen Anbietern („Vendor Lock-in“)
  - Effizienz durch Interoperabilität (Nachnutzung, offene Standards und Schnittstellen)
  - Transparenz und Vertrauen der Bürger, da die Prozesse transparent und sicher gestaltet sind
- **Lösungsansatz:**
  - deutsche Verwaltungscloud
  - Open-Source-Tool-Set
  - **Ziel:** deutschlandweit / europaweit einheitliche oder zumindest kompatible Lösungen

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 6: Mittleres KMU (80+ MA)

- **Ausgangslage**:
  - digitale Souveränität ist keine reine IT-Frage, es ist eine **Compliance- und Strategie-Frage,** oft greift die **NIS-2-Richtlinie**
  - **Tools:** eigene Serverlandschaften (Hybrid-Cloud), komplexe Verwaltungs- und Bürosoftware und CRM-, CAD, Simulations- und andere Systeme
  - **Anforderungen:** Open Source & Kontrolle, um Spionage oder Datenabfluss zu verhindern (Möglichkeit, den Quellcode zu prüfen oder Software selbst zu hosten)
  - **NIS-2 - Betroffenheit und Sicherheitsstufen: (**mehr als 50 Mitarbeiter, Jahresumsatz über 10 Mio. € → NIS-2 gilt in der Regel automatisch)
    - **Sicherheitsstufe "Wichtig" (Important):** trifft auf die meisten Produzenten (Maschinenbau, Textil) und Baubetriebe dieser Größe zu; Risikomanagement ist erforderlich, Vorfälle müssen gemeldet werden, unterliegen *Ex-post-Aufsicht* (Kontrolle erst nach einem Vorfall)
    - **Sicherheitsstufe "Wesentlich" (Essential):** gilt für die **Gemeindeverwaltungen** (unabhängig von der Mitarbeiterzahl) und Unternehmen, die als Zulieferer für kritische Sektoren (z.B. Energie, Gesundheit) sind → *Ex-ante-Aufsicht* (regelmäßige Audits)
  - IT-Sicherheit & Umsetzung: **Hoheit über die Sicherheitsarchitektur** notwendig

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 6: Mittleres KMU (80+ MA)

- **Risiken**
  - **Supply Chain Risiko**: Angriff auf einen zentralen Dienstleister (ERP, Cloud) legt gesamten Betrieb lahm
  - **Klumpenrisiko** durch Software-Giganten (SAP, Microsoft): Lizenzänderungen oder Ausfälle treffen sofort geschäftskritische Prozesse
  - **NIS-2-Verstoß**: Bußgelder bis hin zu Haftung der Geschäftsführung
  - **Fachkräftemangel**: Qualifizierte IT-Sicherheitspersonen sind schwer zu rekrutieren und zu halten
  - **Komplexität** des Hybrid-Modells: Fehler in der Segmentierung oder im Schlüsselmanagement öffnen kritische Lücken
  - Ransomware: Ohne Immutable Backup (3-2-1-1-Regel) droht totaler **Datenverlust** oder erpressbarer Stillstand

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 6: Mittleres KMU (80+ MA)

- **Kosten**
  - Interne **IT-Stellen**: 2 – 4 Festangestellte (First / Second Level + Strategie)
  - MSSP (*Managed Security Service Provider*) / SOC (*Security Operation Center*) Betrieb: 24/7-Monitoring durch Provider (**Kosten**)
  - ISMS (*Informationssicherheits-Managementsystem*) notwendig
  - ISO-27001-Zertifizierung: einmalig hoher **Beratungs- und Auditaufwand**
  - Hybrid-Cloud-Infrastruktur: eigene Server (On-Premise) + Cloud-Dienste mit BYOK (*bring your own key*)
  - MDM-Vollausbau für 80+ Geräte: **Lizenzen**, Zero-Touch-Deployment, Kiosk-Konfiguration (nur eine oder sehr begrenzte Auswahl an Apps)
  - Penetrationstests: 1–2× jährlich durch externe Spezialisten
  - ERP-/CAD-Lizenzen: **laufende Kosten** für kommerzielle Kernsysteme (SAP, Autodesk etc.)

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 6: Mittleres KMU (80+ MA)

- **Nutzen**
  - Volle **Hoheit** über die Sicherheitsarchitektur: kein Stillstand durch Drittanbieter-Ausfall
  - IT ist ein strategischer Wettbewerbsvorteil, es gibt eigene IT-Stellen und / oder sehr enge Verträge mit Systemhäusern
  - Open-Source-Infrastruktur eliminiert **Hardware-Lock-in** und senkt Lizenzkosten
  - Zentrales Identity and Access Management (IAM): Mitarbeiteraustritt = sofortiger Entzug aller (Tool-) Zugänge per Klick
  - BYOK-Verschlüsselung in der Cloud: Anbieter kann auf Daten nicht zugreifen, auch nicht auf behördliche Anfrage
  - Zero-Touch-Deployment: alle Geräte werden automatisch konfiguriert — kein manueller Aufwand pro Gerät
  - Netzwerksegmentierung schützt Produktion: Office-Virus kann Fräsmaschine nicht erreichen
  - ISO 27001 / TISAX-Zertifizierung öffnet Türen zu größeren Auftraggeber-Netzwerken (Automotive, Energie)

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 6: Mittleres KMU (80+ MA)

- **Lösungsansatz 1:**
  - Bestehende Microsoft-Umgebung bleibt → Datenschutzvertrag mit Microsoft, vertragliche Export-Garantie für alle ERP-Daten
  - BYOK-Verschlüsselung wird nachgerüstet
  - Managed Security Service Provider (MSSP) übernimmt 24/7-Monitoring (Security Operations Center (SOC)), kein eigenes Sicherheitsteam nötig
  - ISMS nach ISO 27001 wird aufgebaut und zertifiziert
  - MDM für alle Mobilgeräte: Zero-Touch, Remote Wipe, Kiosk-Modi
  - Netzwerksegmentierung: Büro-IT wird von Produktions- / Baunetz getrennt
  - Jährlicher Penetrationstest durch externen Spezialisten
  - ➔ Geringster Migrationsaufwand, bestehende Systeme bleiben, schnell umsetzbar: 6–12 Monate bis NIS-2-Konformität
  - ➔ Mitarbeiter kennen die Tools bereits, kein Schulungsaufwand
  - Jedoch: strukturelle Abhängigkeit von Microsoft bleibt bestehen (Lock-in) und US-Cloud-Act-Risiko ist nicht eliminiert
  - **Begrenzte Datensouveränität** — Metadaten bleiben beim Anbieter

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 6: Mittleres KMU (80+ MA)

- **Lösungsansatz 2:**
  - M365 schrittweise durch Open-Source_Alternativen ersetzen: kein Metadaten-Abfluss
  - Infrastruktur: Virtualisierung auf Open Source, kein Lizenz-Lock-in
  - Hochsensible Daten (Konstruktionspläne, Bürgerdaten) auf eigenem Server oder Co-Location-RZ (*gemeinsam genutztes Rechenzentrum*) in Deutschland
  - Zentrales IAM (*Identity Access Management*): ein Login steuert alle Tools: Austritt eines MA sind sofort alle Zugänge gesperrt
  - ERP bleibt kommerziell, aber mit vertraglicher Datenexport-Garantie
  - MSSP für 24/7-SOC-Betrieb: interner IT-Leiter steuert Strategie
  - 3-2-1-1-Backup-Regel: drei Kopien, zwei Medien, eine extern, eine Immutable („*unveränderbar*“) offline gegen Ransomware
  - ISMS nach ISO 27001:
    - Kernwissen bleibt im Haus
    - externe Partner nur für Nischenthemen

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Use Case 6: Mittleres KMU (80+ MA)

- **Lösungsansatz 3:**
  - Daten und Infrastruktur zu 100% im eigenen Unternehmen und unter eigener Kontrolle ➔ **echte digitale Souveränität**
  - ➔ Kein struktureller Lock-in: Anbieterwechsel jederzeit möglich
  - ➔ Langfristig deutlich geringere Lizenzkosten (Open-Source-Infrastruktur)
  - ➔ DSGVO- und NIS-2-konform, bis hin zu "Wesentlich"-Einstufung geeignet
  - **Jedoch**:
    - Höherer Migrationsaufwand
    - Kulturwandel bei Mitarbeitenden nötig
    - Längere Umsetzungszeit: 12–24 Monate bis Vollbetrieb
    - Erfordert IT-Personal mit Open-Source-Kompetenz

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentren
Deutschlandweit

Beispiel Checkliste

	Frage	Ja	Nein	Rechtliche Relevanz
1	Wissen Sie, wo Ihre Unternehmensdaten gespeichert werden und in welchem Land sich die Server befinden?	☐	☐	DSGVO (Art. 44–49): Datenübermittlungen in Drittstaaten außerhalb der EU sind nur unter strengen Voraussetzungen zulässig. Besonders relevant bei US-amerikanischen Cloud-Anbietern (z. B. im Kontext des EU-US Data Privacy Framework).
2	Haben Sie vertraglich sichergestellt, dass Ihre Daten nicht ohne Ihre Zustimmung an Dritte weitergegeben oder für das Training von KI-Modellen genutzt werden?	☐	☐	DSGVO (Art. 28): Auftragsverarbeitungsverträge (AVV) sind bei der Nutzung externer Dienstleister Pflicht. Zudem regelt der EU AI Act den Umgang mit Trainingsdaten und deren Herkunft.
3	Sind Sie in der Lage, Ihren Betrieb für mindestens 72 Stunden aufrechtzuerhalten, wenn ein zentraler digitaler Dienst ausfällt oder gekündigt wird?	☐	☐	NIS-2-Richtlinie: Verpflichtet Unternehmen bestimmter Sektoren zu Maßnahmen der Betriebskontinuität und zum Risikomanagement. Ergänzend relevant: DORA (Digital Operational Resilience Act) für den Finanzsektor.
4	Nutzen Sie für kritische Geschäftsprozesse mindestens einen alternativen Anbieter oder eine Open-Source-Lösung, um Abhängigkeiten von einzelnen Technologieanbietern zu reduzieren?	☐	☐	Data Act (EU 2023/2854): Stärkt das Recht auf Datenzugang und Anbieterwechsel und soll Vendor-Lock-in-Effekte reduzieren. Ergänzend: Digital Markets Act (DMA) bei der Nutzung marktbeherrschender Plattformen.
5	Sind alle eingesetzten KI-Tools und -Dienste erfasst und hinsichtlich ihrer Datenschutz- und Sicherheitsanforderungen bewertet?	☐	☐	EU AI Act: Verpflichtet Unternehmen zur Risikobewertung und Dokumentation eingesetzter KI-Systeme je nach Risikoklasse. Ergänzend: DSGVO (Art. 35) – Datenschutz-Folgenabschätzung bei risikoreichen Verarbeitungen.
6	Verfügen Ihre Mitarbeitenden über ausreichende digitale Kompetenzen, um KI-generierte Inhalte kritisch zu hinterfragen und Cyberbedrohungen zu erkennen?	☐	☐	EU AI Act (Art. 4): Schreibt vor, dass Unternehmen, die KI einsetzen, für ausreichende KI-Kompetenz ihrer Mitarbeitenden sorgen müssen. Ergänzend: NIS-2-Richtlinie fordert Schulungsmaßnahmen im Bereich Cybersicherheit.
7	Haben Sie eine dokumentierte Strategie für den Umgang mit Datenverlust oder einem KI-gestützten Cyberangriff?	☐	☐	DSGVO (Art. 33–34): Datenpannen müssen innerhalb von 72 Stunden der zuständigen Aufsichtsbehörde gemeldet werden. NIS-2-Richtlinie: Fordert dokumentierte Incident-Response-Pläne und verpflichtet zur Meldung erheblicher Sicherheitsvorfälle.

Hinweis: Diese Checkliste dient der Orientierung und ersetzt keine Rechtsberatung.
Bei konkreten rechtlichen Fragen empfehlen wir die Konsultation eines spezialisierten Anwalts.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
Mittelstand-Digital
aufgrund eines Beschlusses des Deutschen Bundestages

Beispiel Checkliste: Frage zur Auswertung

„Haben Sie die Mehrheit der Aussagen mit „Nein“ beantwortet?

- Dann helfen wir Ihnen gerne weiter!
- Wir bieten regelmäßig kostenfreie Webinare und Workshops zum Thema digitale Souveränität an.
- Alle unsere Veranstaltungen sowie hilfreiche Materialien finden Sie auf unserer Webseite unter www.xxx.de“

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital