Digitale Souveränität

Titel: Digitale Souveränität

Autor: Stephan Krausenegger, KDI GmbH - Gesellschaft für Kommunikation, Datentechnik und Informationssysteme

Kontakt: stephan.krausenegger@kdit.de

Version 1.0
München, 27.05.2026

1. Abstract

Im Rahmen des vom Bundesministerium für Digitales und Staatsmodernisierung (BMDS) initiierten Consultingprozesses für eine Nationale Rechenzentrumsstrategie wurde als eines der zentralen Ziele das Thema Digitale Souveränität herausgestellt.

Der Begriff Digitale Souveränität wird aktuell sehr inflationär verwendet und immer auf eine bestimmte Bedarfslage zugeschnitten.

Dieser Artikel versucht den Begriff Digitale Souveränität umfassend, nicht situationsbezogen, zu beschreiben und einzuordnen. Darüber hinaus wird auf Schwierigkeiten und Hindernisse Bezug genommen, die das Auflösen von Abhängigkeiten und damit das Erreichen einer Digitalen Souveränität erschweren.
Ein konkretes Anliegen ist es Lösungen aufzuzeigen, die aus Abhängigkeiten herausführen und in Richtung digitale Unabhängigkeit gehen.

2. Was sollten wir unter Digitale Souveränität verstehen

Digitale Souveränität ist die Fähigkeit von Staaten, Organisationen, Unternehmen und Individuen, die digitale Infrastruktur, die Datennutzung und die digitalen Entscheidungsprozesse selbstbestimmt zu kontrollieren und zu gestalten. Sie umfasst die Kontrolle über Daten,

Software, Hardware, Netzwerke und die Regeln ihrer Nutzung, so dass Abhängigkeiten reduziert und Handlungsfähigkeit erhalten bleiben.

Kernelemente

- **Selbstbestimmung:** Nutzung und Gestaltung digitaler Technologien, Prozesse und Regeln nach eigenen Vorstellungen.
- **Kontrolle:** Governance über Infrastruktur, Daten, Algorithmen und Anwendungen.
- **Sicherheit:** Schutz vor unbefugtem Zugriff, Cyberangriffen und digitaler Fremdbestimmung.
- **Gestaltungsfreiheit:** Möglichkeit, technologische und rechtliche Rahmenbedingungen aktiv zu formen.
- **Kompetenz:** Digitale Bildung und informierte Nutzung als Voraussetzung für wirksame Souveränität.

Zentrale Dimensionen

- **Technologisch:** Kontrolle über Systeme, Software, Hardware und technische Standards.
- **Politisch:** Fähigkeit zur Regulierung, Gesetzgebung und Durchsetzung digitaler Normen.
- **Ökonomisch:** Reduzierung Abhängigkeiten von globalen Plattformen und Märkten; wirtschaftliche Resilienz.
- **Gesellschaftlich:** Schutz der Privatsphäre, demokratische Teilhabe und Chancengleichheit im digitalen Raum.
- **Individuell:** Schutz persönlicher Daten, informierte Nutzung digitaler Dienste und digitale Bildung.

Relevanz nach Ebene

- **Individuen:** Schutz der Privatsphäre, Kontrolle über persönliche Daten und digitale Selbstbestimmung.
- **Organisationen und Unternehmen:** Souveränität über IT-Infrastruktur, Schutz vor Cyberangriffen und Unabhängigkeit von Drittanbietern.
- **Staaten/Gesellschaft:** Fähigkeit zur digitalen Gesetzgebung, Schutz kritischer Infrastrukturen, Stärkung demokratischer Prozesse und Abwehr digitaler Fremdbestimmung.

Typische Zielkonflikte

- **Innovation vs. Kontrolle:** Förderung neuer Technologien kann Kontrollverlust mit sich bringen.
- **Offenheit vs. Sicherheit:** Offene Systeme erhöhen Innovationsspielraum, sind aber oft anfälliger für Angriffe.
- **Wirtschaftlichkeit vs. Unabhängigkeit:** Kostengünstige, fremdgeführte Lösungen können ökonomisch vorteilhaft sein, aber Abhängigkeiten schaffen.

- **Datenschutz vs. Nutzbarkeit:** Strenge Datenschutzregeln können die Praktikabilität und Funktionalität digitaler Dienste einschränken.

3. Wo liegen unsere Defizite

Aktuell befindet sich Deutschland, damit sind nicht nur die öffentlichen Bereiche, sondern auch Unternehmen, Organisationen, usw. gemeint, relativ am Anfang Ihrer Bestrebungen nach IT-technologischer Unabhängigkeit und der Digitalen Souveränität als Ergebnis daraus. Hier ist es in erster Linie erforderlich die Schwächen aufzuzeigen und Lösungsansätze zur Beseitigung zu erarbeiten.

Im Folgenden eine Aufzählung von Schwächen und Defiziten, die zum gegenwärtigen Zeitpunkt als signifikant gesehen werden.

- **Infrastrukturdefizite:** Breitbandausbau und flächendeckendes 5G sind unzureichend, insbesondere in ländlichen Regionen. Glasfaserverfügbarkeit bleibt hinter Nachbarstaaten zurück.
- **Abhängigkeit von Hyperscalern:** Starke Konzentration auf wenige US-Cloudanbieter führt zu technologischer und wirtschaftlicher Abhängigkeit. Darüber hinaus bleibt eine Reihe von Fragen offen hinsichtlich der Sicherheit der Daten.
- **Fachkräftemangel und digitale Kompetenzen:** Mangel an IT-Fachkräften in Verwaltung, Forschung und Industrie sowie unzureichende digitale Grundbildung in Teilen der Bevölkerung.
- **Langsame und fragmentierte Digitalisierung des öffentlichen Sektors:** Heterogene IT-Landschaften, fragmentierte Beschaffungsprozesse und langsame Projektumsetzung reduzieren staatliche Handlungsfähigkeit.
  Daraus resultiert eine verzögerte Digitalisierung der öffentlichen Verwaltung (hohe Bürokratie, fragmentierte Systeme, mangelnde Interoperabilität, geringe Qualität).
- **Security:** Unzureichende IT-Sicherheit und Krisenfestigkeit öffentlicher und öffentlich-naher Systeme (Patch-Management, Awareness, Incident-Response). Auch in weiten Teilen der Privatwirtschaft werden diesbezüglich immer wieder Schwächen festgestellt.
- **Schwache Förderstruktur für Software-Ökosysteme:** Geringe Unterstützung für nationale Plattformen, Open-Source-Entwicklung und skalierbare Software-Unternehmen im Vergleich zu Hardware- oder Infrastrukturförderung.
- **Investitions- und Förderlücken:** Teils unklare Verantwortlichkeiten zwischen Bund, Ländern und Kommunen hinsichtlich Investitions- und Förderprogrammen.
- **Mangelnde Innovationskraft**: Es gibt eine Schwäche in der Innovationsförderung. Oftmals fehlt es an ausreichenden Investitionen in Forschung und Entwicklung, um neue Technologien und Lösungen zu entwickeln, die die digitale Souveränität stärken könnten
- **Lieferketten- und Produktionsabhängigkeiten:** Abhängigkeit von ausländischen Herstellern für kritische Hard- und Softwarekomponenten sowie für entsprechende Rechenzentrumskapazitäten (Beispiel KI).
- **Regulatorische Trägheit und Fragmentierung:** Verzögerte Gesetzgebung, uneinheitliche Umsetzung auf Länderebene und komplexe Compliance-Anforderungen

hemmen schnelle Anpassungen. Abhängigkeiten zu EU-Recht welches in nationale Governance umgesetzt werden muss, trägt nicht zur Beschleunigung bei.

- **Datenschutz vs. Innovation:** Datenschutz- und Sicherheitsbedenken, die Innovationen bremsen (Abwägung zwischen Datenschutz und Nutzbarkeit). Dazu gehört auch eine begrenzte Datenhoheit in Praxisfeldern wie Gesundheitswesen, Bildung, Verwaltung (Datenzugang, -weitergabe, Standards
- **Trägheit**: Geringere Geschwindigkeit bei Innovation und Skalierung im Vergleich zu Wettbewerbern (z. B. in Infrastrukturentwicklung, öffentlicher Beschaffung).
- **Mitarbeiter**: Träge, desinteressierte, unmotivierte und damit letztendlich auch unfähige Mitarbeiter, sowohl im öffentlichen Bereich wie auch in privatwirtschaftlichen Unternehmen, denen es völlig egal ist, wie lange etwas dauert, wieviel es kostet, ob beauftragte externe Dienstleister abliefern, in welcher Qualität, zu welchen Kosten usw. Die primäre Zielsetzung dieses Personenkreises geht in die Richtung, ein ruhiges Dasein zu fristen, unter dem Radar zu fliegen und frühzeitig den Eintritt ins Rentenstadium vorzubereiten.
- **Politische und gesellschaftliche Naivität**: Es gibt eine gewisse Naivität im Umgang mit den Risiken, die mit der Abhängigkeit von großen Tech-Unternehmen verbunden sind. Oft wird blindes Vertrauen in diese Unternehmen gesetzt, ohne die langfristigen Konsequenzen zu bedenken. Risiken werden oftmals bewusst falsch eingeschätzt, um ökonomisch motivierte Entscheidungen zu rechtfertigen
- **Fehlende Umsetzungskompetenz:** Erwiesenermaßen ist Deutschland nach wie vor sehr gut aufgestellt, wenn es um wissenschaftliche Grundlagenforschung geht. Das bestätigt sich immer wieder in allen wichtigen wissenschaftlichen Disziplinen, sei es Medizin, seien es Ingenieurwissenschaften, aber auch in sehr aktuellen Bereichen wie KI. Was uns hierbei fehlt, ist die Fähigkeit, aus den Ergebnissen dieser Forschungen marktreife Spitzenprodukte zu entwickeln, und diese auf dem Weltmarkt entsprechend zu positionieren.

4. Maßnahmen zur Herstellung der Digitalen Souveränität

Es ist keineswegs ausreichend, die gemachten Fehler erkannt zu haben, sich in gewisser Weise dafür auch ein gutes Stück weit das eigen Versagen einzugestehen und Besserung zu geloben. Hier sind dringend gezielte Maßnahmen erforderlich. Keine Schnellschüsse, außer diese treffen präzise das anvisierte Ziel, kein Aktionismus, sondern gut durchdachte Maßnahmen, die im Rahmen eines ebenso gut durchdachten Plans umgesetzt werden. Klar definierte Ziele, Zeiträume, die anspruchsvoll, aber nicht illusorisch sind, und KPIs an Hand deren Erreichung der Erfolg der Maßnahmen gemessen wird.

Konkrete Gegenmaßnahmen (operativ-strukturell)

- **Infrastruktur beschleunigen:** Der Ausbau der Infrastruktur muss da beschleunigt werden, wo es am meisten bringt. Wir werden kurzfristig nicht die Menge an Fachkräften und finanziellen Mitteln haben, um Deutschland flächendeckend mir Glasfaser und 5G

zu überziehen. Das ist aber auch nicht erforderlich. Wir fangen da an, wo es am dringendsten benötigt wird. Der Rest dann, wenn Prio 1 bedient ist. Wie genau wird man sich überlegen können, während man die wichtigen Standorte (Flächen) und Routen erschließt.

- **Cloud-Strategien diversifizieren:** Erfahrungen aus zahlreichen Gesprächen zeigen, die wenigsten deutschen Unternehmen sind wirklich glücklich darüber, Ihre Anwendungen und Daten in Clouds mit unklarer Rechtslage liegen zu haben. Unterhält man sich mit den Leuten in den Unternehmen, die sich mit IT-Security beschäftigen, wird das Bild noch klarer. Mangels nationaler oder europäischer Alternativen, bzw. des Wissens darüber, und den ökonomischen Prinzipien geschuldet, führt der Weg dann aber doch meistens zu AWS, Google oder Microsoft. Sobald es hierzu brauchbare Alternativen gibt, die Lösungsansätze wie Multi-/Hybrid-Cloud, Portabilität, offene Standards, föderierte Architekturen ermöglichen, wird ein Umdenken wahrscheinlich. Exit-Strategien, Datenklassifizierung und Workload-Platzierung können diesbezüglich aber jetzt schon vorbereitet werden.

- **Fachkräfte und Bildung ausbauen:** Wir brauchen mehr Fachkräfte. Nicht nur aktuell, sondern auch in Zukunft. Man kann versuchen, als Sofortmaßnahme, den aktuellen Bedarf durch Anwerbung von IT-Spezialisten aus dem Ausland zu decken. Der Erfolg ist nicht gewiss. Es ist aber dringend erforderlich in die Ausbildung von IT-Nachwuchskräften zu investieren, um, wenn nicht schon kurzfristig, dann zumindest mittelfristig den Bedarf zu decken. Geeignete Mittel dazu sind frühes Erkennen und Fördern von IT-Talenten, Aufbau einer breiten allgemeinen IT-Wissensbasis und eines IT-Bewusstseins bereits in den Schulen, kontinuierliche, den sich ändernden Bedarfen angepasste Aus- und Weiterbildungspfade.

- **Öffentliche IT modernisieren:** Die öffentlichen IT-Betreiber von Bund, Länder, Kommunen, Verbände, öffentlich-rechtliche Organisationen, usw. sind in Ihren Umfängen beachtliche IT-Bedarfsträger. Diese Position soll dazu verwendet werden, um Standards zu definieren, sowohl technologisch als auch prozessual. In Zusammenarbeit mit Universitäten und anderen wissenschaftlichen Einrichtungen können hier Grundsteine gelegt werden für gezielte bedarfsorientierte Entwicklungen, die dann sowohl in öffentliche als auch in privatwirtschaftliche IT Infrastrukturen einfließen.

- **Förderprogramme reformieren:** Förderprogramme benötigen maximale Transparenz. Gefördert werden sollte in erster Linie das, was am dringendsten benötigt wird. Es ist darauf zu achten, dass durch entsprechende Vermarktungsoptionen ein kontinuierlicher Rücklauf in die Förderprogramme stattfindet, so dass hier ein technologisch-ökonomischer Kreislauf aufgebaut wird.

- **Wirtschaftspolitik digital schärfen:** Junge Technologieunternehmen, die schon erste Erfolge haben, weiteres Potenzial, einen Plan dieses auszuschöpfen und nun schnell wachsen wollen, müssen unterstützt werden. Besonders wenn es dabei um Förderung von besonders komplexen und forschungsintensiven Technologien (z. B. Künstliche Intelligenz, Quantencomputing, Robotik) geht, die lange Entwicklungszeiten haben und damit auch ein langes Durchhalten erfordern. Der Staat und öffentliche Einrichtungen sollen selbst auf diese Technologien setzen und damit aufzeigen, was möglich ist und wie es funktioniert, wenn es funktioniert.

- **Sicherheit und Resilienz erhöhen:** Es müssen einheitliche Sicherheitsregeln vorgegeben werden (BSI), die für Organisationen verbindlich sind und deren Einhaltung

auch kontrolliert wird. Des Weiteren müssen Angriffe in realistischen zu erwartenden Dimensionen simuliert werden, und dabei Abwehrmaßnahmen und Notfallpläne entwickelt, verprobt und verbessert werden

Priorisierung von Maßnahmen

Im Folgenden eine Aufstellung wie die erforderlichen Maßnahmen beispielhaft priorisiert werden können. Nicht in ausreichender Menge vorhandener Ressourcen lassen es nicht zu, alle erforderlichen Maßnahmen sofort zu planen und umzusetzen. Es muss zunächst eine Priorisierung vorgenommen werden, gefolgt von der Planung dessen, was am dringlichsten erscheint.

Priorisierung (erste 12 Monate)

- **Modernisierung öffentlicher IT**
    - Nutzerzentrierte Gestaltung digitaler Dienste
    - Überführung in sichere und skalierbare Plattformen
    - Stärkung von Interoperabilität und Sicherheit
    - Modernisierung von Beschaffung und Organisation
- **Cloud-Diversifizierung und Portabilität.**
    - Verteilung von Clouddiensten über mehrere Anbieter
    - Portabilität zur Reduzierung von Abhängigkeiten
    - Flexible Optimierung von Kosten und Leitungen
- **Gezielte Personalentwicklungs-Programme**
    - Regelmäßige Bedarfsanalysen
    - Maßgeschneiderte Lernpfade und Formate
    - Messung, Anreize und Skalierung
    - Flexible Anpassung an sich ändernde Bedarfe
- **Aufsetzen erforderlicher Infrastrukturprojekte**
    - Reihenfolge der Maßnahmen durch Dringlichkeit festlegen
    - Behördliche Hindernisse aus dem Weg räumen
    - KPIs und Meilensteine festlegen und prüfen
    - Agieren statt reagieren

Mittelfrist (12–36 Monate)

- **Gemeinsame öffentliche Plattformbausteine:**
    - einheitliches, interoperables Identitätsmanagement
    - Standardisierte Datenräume (Gesundheit, Mobilität, Energie) mit Governance, Katalogen und Zugriffskontrollen.
    - Zentrale Bereitstellung von Basisdienste wie Zahlung, Dokumentenzustellung, Terminbuchung und Signaturen zentral bereitzustellen

- **Europa-kompatible Cloud-Souveränität:**
    - vorkonfigurierte Cloud-Umgebungen, die Behörden helfen, EU-konform, sicher und mandantenfähig zu arbeiten – mit eingebauten Kontrollmechanismen und klarer Trennung zwischen verschiedenen Nutzern.
    - Erstellung einer offenen, standardisierten und herstellerunabhängigen Infrastruktur, die auf (z.B.) Kubernetes, Open Source und virtualisierten Netzfunktionen basiert und den Teilnehmern eine umfassende Kontrolle und Variabilität ermöglicht.
- **Halbleiter- und Edge-Strategie:**
    - Aufbau lokaler Rechenzentren (Edge-Standorte) für latenzkritische Anwendungen (Verkehr, Notfall, Industrie 4.0).
    - Festlegung von Beschaffungsrichtlinien, die dafür sorgen, dass Hardware sicher, langfristig nutzbar und von verschiedenen Quellen bezogen werden kann, damit Organisationen widerstandsfähig und unabhängig bleiben..
- **Beschaffung und Governance reformieren:**
    - Offene Gestaltung von öffentlichen IT-Projekten um diese durch Wiederverwendbarkeit der Strukturen, Schritte, Organisation nachhaltig zu machen.
    - Sichere Finanzierungsmöglichkeiten schaffen für Projekte und digitale Services über unterschiedliche Zeiträume
    - Einsatz von KPIs hinsichtlich Wirkung, Nutzung, Verfügbarkeit, Sicherheit kontrolliert durch öffentliches Monitoring.
- **Talentpipeline verstetigen:**
    - Neugestaltung von Bildungs- und Qualifikationsbausteinen mit dem Ziel Kompetenzen flexibler und bedarfsorientierter erweitern zu können.
    - Schaffung von gemeinsamen Testräumen zur Förderung der Zusammenarbeit zwischen öffentlichen Einrichtungen und privaten Unternehmen.
    - Programme zur Gewinnung und Bindung vom IT-Fachkräften durch klare Karrierewege, bessere Bezahlung und attraktive Zusatzleistungen

Langfrist (36–120 Monate)

- **Institutionelle Verankerung digitaler Souveränität:**
    - **Nationale bzw. regionale Digitalfonds:** Dauerhafte Finanzierung, um wichtige digitale Basisbausteine sowie die Pflege von Open-Source-Software zuverlässig zu sichern.
    - **Digitale Daseinsvorsorge:** Ein klarer Rechtsrahmen, der zentrale IT-Dienste wie eine grundlegende öffentliche Infrastruktur behandelt – also mit Vorgaben zu

Verfügbarkeit, Zusammenarbeit zwischen Systemen (Interoperabilität) und Sicherheit.

  - **Architekturboard:** Ein föderal besetztes Gremium, das gemeinsame Standards festlegt, Referenzarchitekturen entwickelt, die Einhaltung überwacht und Veröffentlichungszyklen koordiniert

- **Europäische Wertschöpfungsketten:**
  - **Chips/Photonik/Sensorik:** Aufbau und Ausbau von Produktionskapazitäten sowie von Design- und Entwicklungskompetenzen in europäischen Technologie-Clustern.
  - **Sichere Lieferketten:** Einführung von Zertifizierungen, mehr Transparenz und regelmäßigen Stresstests; zudem eine geostrategisch breit aufgestellte Diversifizierung von Bezugsquellen.
- **Regulatorik als Enabler:**
  - **Interoperabilitätsgebote:** Vorgaben, die öffentliche IT verpflichten, offene und kompatible Schnittstellen zu nutzen, damit Systeme leichter zusammenarbeiten können.
  - **Datennutzung:** Klare rechtliche Regeln für den Betrieb von vertrauenswürdigen Datenräumen sowie konkrete Rechte und Anreize, damit insbesondere KMUs Daten sicher nutzen und teilen können.
  - **Langzeit-Sicherheit:** Einführung und Förderung von Post-Quanten-Kryptografie, verbindliche Updatepflichten und Anforderungen an digitale Nachhaltigkeit – etwa in Bezug auf Energieverbrauch und den gesamten Lebenszyklus von IT-Systemen.

- **Resiliente Infrastruktur:**
  - **Mehrschichtige Netze:** Aufbau redundanter Backbone-Strukturen sowie die Kombination aus Satelliten-, 5G- und Glasfasertechnologien. Zusätzlich sollen Netze über autonome Notfallbetriebsmodi verfügen, um auch bei Störungen weiter zu funktionieren.
  - **Kritische Dienste:** Festgelegte und priorisierte Wiederanlaufpläne für zentrale Systeme, regelmäßige groß angelegte Krisenübungen und ein gemeinsames, aktuelles Lagebild für alle relevanten Akteure.

5. Zu erwartenden Schwierigkeiten

Wo werden wir im Rahmen der Umsetzung der aufgeführten Maßnahmen in der Praxis vermutlich mit größeren Schwierigkeiten rechnen müssen ?

Aufbau strategischer Unabhängigkeit in kritischen Schlüsseltechnologien (Langfristig):

- **Herausforderung** Eigene Halbleiterproduktion, eigene Hardware-Entwicklung, Entwicklung von Betriebssystemen oder KI-Plattformen, die mit globalen Playern konkurrieren können.
- **Warum schwierig?** Dies erfordert **enorme Investitionen** (Milliardenbeträge), einen **sehr langen Atem**, den Aufbau kompletter, hochkomplexer Wertschöpfungsketten und die Gewinnung von **Spitzenfachkräften** in einem globalen Wettbewerb. Die technologische Dominanz und die Skaleneffekte der bestehenden globalen Giganten sind immens, und es ist extrem schwer, hier aufzuholen oder eine echte Alternative zu etablieren. Es geht nicht nur um die Entwicklung, sondern auch um die Marktakzeptanz und Wettbewerbsfähigkeit.
- **Priorisierte Gegenmaßnahmen:** Zum einen sollte eine strategische Spezialisierung auf priorisiere Bereiche mit hohem strategischem Wert und realistischem Aufholpotenzial stattfinden. Daneben sollte eine regionale, modulare Wertschöpfungskette ausgebaut werden. Das alles muss verbunden sein mit einer Personalstrategie, die sicherstellt, dass zu jedem Entwicklungsstand ausreichend Ressourcen mit den erforderlichen Qualifikationen vorhanden sind.

Eigenständige Cloud-Kapazitäten und Hyperscaler-Alternativen

- **Herausforderung:** Aufbau von konkurrenzfähigen, souveränen Rechenzentrums- und Cloud-Anbietern
- **Warum schwierig?** Diese Vorhaben sind extrem kapital- und know-how-intensiv. Dabei trifft man auf globale Netzwerkeffekte und Marktbeherrschung durch existierende Hyperscaler. Die zentralen Herausforderungen dabei sind technische Skalierung, internationale Kundengewinnung und das langfristige Beherrschen der entstehenden Betriebs- und Weiterentwicklungskosten
- **Priorisierte Gegenmaßnahmen:** Public-private-Partnerships mit klaren Staatsgarantien, langfristige Förderprogramme und fokussierte Nischenstrategie statt generischem Konkurrenzanspruch. Schaffen von unabhängigen Infrastruktur-Ökosysteme durch Aufbau national unabhängiger Clouds / Rechenzentren. Unterstützung durch EU-weite Beschaffungsgemeinschaften zur Steuerung und Reduzierung der massiven Investitionen ist ebenso erforderlich, wie ein gesteuerter Know-how-Aufbau und politische Koordination über Organisationsgrenzen hinweg. Dabei ist darauf zu achten, nationale Abhängigkeiten aufzulösen, politische/rechtliche Hürden zu beseitigen und Standards, nicht zuletzt auch hinsichtlich der Finanzierung, zu schaffen.

Konsolidierung und Modernisierung öffentlicher IT

- **Herausforderung:** Veraltete und heterogene Fachverfahren sowie Infrastrukturen im laufenden Betrieb sicher, budget- und rechtskonform zu konsolidieren und gleichzeitig moderne, interoperable und nutzerzentrierte IT-Plattformen aufzubauen.

- **Warum schwierig?** Heterogene Legacy-Landschaften, föderale Zuständigkeiten und politische Zyklen blockieren schnelle Konsolidierung. Migrationsrisiken, Datenschutzfragen und interne Widerstände verlangsamen Projekte.

- **Priorisierte Gegenmaßnahmen:** Verbindliche Mandate für Standardbaukästen, zentrale Migrationsteams mit Durchgriffsrechten, Pilot-First-Ansatz und Budgetgarantien sind hierfür zu organisieren.

Skalierung eines heimischen Software- und Open-Source-Ökosystems

- **Herausforderung:** Das heimisches Software- und Open-Source-Ökosystem muss so skalierbar sein, dass es durch nachhaltige Finanzierung, qualifizierte Entwickler, professionelle Governance, interoperable Standards und staatliche Nachfragemacht langfristig konkurrenzfähig, sicher und wartbar wird.

- **Warum schwierig?** Technologie-Ökosysteme entstehen durch Marktdynamik, Talent, Investoren und Kundenreferenzen; staatliche Förderung kann Marktmechanismen nicht vollständig ersetzen.

- **Priorisierte Gegenmaßnahmen:** Regelmäßig wiederkehrende Förderprogramme, der gezielte Einsatz öffentlicher Aufträge als Anschub für neue Märkte, steuerliche Anreize sowie dauerhaft institutionalisierte Finanzierung für Wartung und Weiterentwicklung.

Fachkräfteaufbau und Bildungsreformen

- **Herausforderung:** Maßnahmen zur schnellen und systematischen Gewinnung und Sicherung ausreichend qualifizierte Fachkräfte, indem Ausbildung, Studium und berufliche Weiterbildung technologisch aktualisiert, Karrierepfade attraktiver gestaltet und Bildungsreformen eng mit den konkreten Arbeitsmarktbedarfen verzahnt werden.

- **Warum schwierig?** Ausbildungssysteme, Anerkennung von Qualifikationen und berufliche Weiterbildung brauchen Jahre, während der Markt kurzfristig Fachkräfte verlangt. Konkurrenz um Talente mit globalen Unternehmen erhöht Kosten.

- **Priorisierte Gegenmaßnahmen:** Beschleunigte Anerkennungsverfahren, umfangreiche Aus- und Weiterbildungs-Programme mit aktiver Beteiligung der Arbeitgeber sowie zielgerichtete Einwanderungs- und Rückkehrprogramme. Dazu kommen frühzeitige Identifikation von IT-Talenten und gezielte Überleitung dieser Personen in passende Ausbildungs- und Qualifizierungspfade.

Netzausbau (Strom, Glasfaser und 5G) in ländlichen Regionen

- **Herausforderung:** Aufbau von tragfähigen und zukunftssicheren Netzinfrastrukturen für Strom, Glasfaser und 5G. Hohe Investitions- und Betriebskosten, lange Genehmigungs- und Bauzeiten, fragmentierte Eigentums- und Förderstrukturen sowie lokale Akzeptanz und Versorgungssicherheit müssen früh- und gleichzeitig adressiert werden.

- **Warum schwierig?** Infrastrukturprojekte stoßen auf Genehmigungsstau, Koordinationsprobleme und niedrige Wirtschaftlichkeit in dünn besiedelten Gebieten. Regionale Kapazitäten und langfristige Investitionssicherheit fehlen.

- **Priorisierte Gegenmaßnahmen:** Genehmigungsverfahren müssen vereinfacht werden, dazu müssen modulare Finanzierungsmodelle (öffentlicher Anteil + Betreiberanreize), und lokale Kooperationsmodelle (Kommunen, Energieversorger) geschaffen werden.

Regulatorische und legislative Agilität

- **Herausforderung:** Flexible und zügige Anpassung des rechtlichen und regulatorischen Rahmens, so dass Innovationen nicht ausgebremst werden. Gleichzeitig muss darauf geachtet werden, dass Rechtssicherheit, Datenschutz und demokratische Kontrolle gewährleistet bleiben.

- **Warum schwierig?** Gesetzgebung ist träge, föderale Umsetzung inkonsistent und rechtliche Harmonisierung auf EU-Ebene zeitaufwendig. Komplexe, sich schnell ändernde Technologien sowie Entwicklungen außerhalb des technologischen Sektors überfordern traditionelle Regelwerke.

- **Priorisierte Gegenmaßnahmen:** Agile Gesetzgebungsmechanismen (Sunset-Clauses), standardisierte Umsetzungsleitfäden für Länder und eine ständige Tech-Expertengruppe im Parlament können dafür geeignete Maßnahmen sein.

Starke gemeinsame europäische Souveränität

- **Herausforderung**: Synchronisation politischer, rechtlicher und wirtschaftlicher Interessen auf EU-Ebene. Schaffung von verbindlichen, übergreifenden Standards ohne dabei die technologische Unabhängigkeit, Innovationsdynamik oder vertrauenswürdige internationale Partnerschaften zu gefährden

- **Warum schwierig?** Unterschiedliche nationale Interessen, Rechtsrahmen, Genehmigungsprozesse, Tempo der Umsetzung.

- **Priorisierte Gegenmaßnahmen:** EU-weite Harmonisierung bzw. Vereinheitlichung von spezifischem Recht, Datenschutz, Sicherheitsnormen und Beschaffungspraktiken sind dazu erforderliche Schritte.

Zusammenfassend:

Die größten Schwierigkeiten liegen dort, wo es darum geht, bestehende globale Marktstrukturen aufzubrechen, technologische Abhängigkeiten in Kernbereichen zu überwinden und komplexe, kapitalintensive Ökosysteme von Grund auf neu aufzubauen, die international wettbewerbsfähig sind. Dies erfordert nicht nur immense finanzielle und technologische Anstrengungen, sondern auch einen starken politischen Willen und eine beispiellose Kooperation auf europäischer Ebene über viele Jahre hinweg.

6. Erweiterung: Data Center Technologien

E1. *Digitale Souveränität im Bereich Data Center Hardware*

Eines der größten Probleme für die Erlangung digitaler Souveränität ist, dass derzeit nahezu keine der für Rechenzentren benötigten Hardware von deutschen oder europäischen Herstellern stammt.

Für die meisten kritischen Data-Center-Hardwarekomponenten existiert in Deutschland und Europa nur eine begrenzte Fertigungskapazität, wodurch eine deutliche Abhängigkeit von außereuropäischen Lieferanten besteht.

Die Abhängigkeit von nicht-europäischen Hardware-Herstellern für Data-Center-Komponenten (Server, Storage, Netzwerkgeräte, Chips usw.) birgt mehrere Risiken:

- **Versorgungsrisiken** bei geopolitischen Spannungen oder Exportbeschränkungen können Verfügbarkeit beeinträchtigen und Preise erhöhen.
- **Sicherheitsrisiken** durch schwer überprüfbare Lieferketten und potenziell eingeschleuste Hardware-Bedrohungen.
- **Wirtschaftliche Verwundbarkeit**: Know-how und Wertschöpfung wandern ins Ausland, was Europas Innovationskraft schmälert.
- **Resilienzverlust** bei Störungen in globalen Fertigungszentren.

Nahezu alle Server-, Speicher- oder Netzwerkkomponentenhersteller stammen aus den USA oder Asien. Dies schafft Abhängigkeiten.

- **Technologische Abhängigkeit:** Ohne eigene Produktion oder zumindest Beeinflussung der Hardware-Designs bleibt Europa technologisch abgehängt hinter anderen Regionen.

  Lieferkettenrisiken: Halbleiterknappheit, geopolitische Spannungen und Zertifizierungsanforderungen beeinflussen Verfügbarkeit und Kosten.

Konkrete Risikobereiche

- Halbleiter und spezialisierte Chips für Server und Netzwerkhardware
- High-End-Serverplattformen und Switches mit proprietären Komponenten

- Speicherkomponenten mit globaler Produktion
- Kritische Peripherie wie Netzteile und Optikmodule

Was helfen könnte (stichwortartig)

- Stärkere europäische Standardisierung, Sicherheits- und Anforderungsnormen
- Unterstützung lokaler OEMs durch langfristige Ausschreibungen und modulare, offene Architekturen
- Öffentliche Beschaffung gezielt nutzen, Lieferanten diversifizieren, Exit-Optionen vertraglich sichern
- Aufbau regionaler Montage- und Testkapazitäten; Förderung regionaler Fertigungspartnerschaften

Kurzfristige Maßnahmen (0–12 Monate)

- Lieferantenvielfalt erhöhen; strategische Lagerhaltung kritischer Komponenten
- Lieferkettenprüfungen und Audits bei Schlüsselzulieferern
- Verträge mit Exit-Optionen und alternativen Lieferanten
- Priorisierte Beschaffung für kritische Infrastruktur

Mittelfristige Maßnahmen (1–3 Jahre)

- Förderprogramme für regionale Fertigungspartnerschaften; Pilotfabriken
- Public-Private-Partnerships für vertrauenswürdige Hardware-Stacks
- Standardisierung und Modularisierung; lokale Montage- und Testkapazitäten aufbauen

Langfristige Strategie (3–10 Jahre)

- Aufbau einer europäischen Halbleiter- und Elektronikindustrie an strategischen Knotenpunkten
- Investitionen in F&E für Chipdesigns, vertrauenswürdige Hardware und Fertigungstechnologien
- Ökosystemförderung durch steuerliche Anreize und Nachfragesicherung
- EU-koordiniert größere Beschaffungsprogramme und Investitionsskalierung

Die Umsetzung der genannten Strategien erfordert Ausdauer, Geld und Standhaftigkeit. Die jeweiligen Prozesse erfordern eine gut durchdachte Planung, eine konsequente Umsetzung aber auch die Fähigkeit Fehler zu erkennen, den Mut diese einzugestehen und die Kraft diese zu korrigieren. Das alles ist durch eine engmaschige Überwachung möglich, die sich an Quality

Gates und Meilensteinen orientiert. Der Erfolg einzelner Entwicklungs- und Umsetzungsschritte wird anhand erreichter KPIs gemessen.

Beispiele für KPIs (Auszug)

- Anteil europäischer Bauteile in europäischen Rechenzentren
- Anzahl laufender Förderprogramme; Investitionsvolumen
- Anzahl neuer oder expandierter Fertigungsstandorte
- EU-weite Beschaffungsrahmenverträge; Zeit bis Freigabe neuer Hardware
- Anteil offener Standards (Open Compute/Open Racks/Open Firmware)

E2. Digitale Souveränität im Bereich Data Center Software und Services

Neben der Abhängigkeit von Hardwareherstellern aus USA und Asien gibt es in Europa und speziell in Deutschland die Abhängigkeit von US-Amerikanischen Softwareherstellern und Serviceanbietern, wie zum Beispiel Microsoft, AWS, Google, Oracle.

Diese Abhängigkeit ist hoch und strategisch relevant. Viele europäische Unternehmen und Behörden nutzen zentralisierte US-Dienste für Cloud, E-Mail, Betriebssysteme, Bürosoftware und KI-Plattformschichten. Die dadurch entstandene Abhängigkeit von ausländischen Softwareherstellern oder Anbietern entsprechender Dienstleistungen erzeugt technische, rechtliche und geopolitische Risiken, die bei Ausfällen, Sanktionen oder Änderungen in Gesetzen der Herstellerländer schnell Wirkung entfalten können. Darüber hinaus sind wirtschaftliche, sicherheitsrelevante sowie datenpolitische Risiken festzuhalten.

Wo die ist Abhängigkeit derzeit am stärksten

- **Cloud und Hosting:** Große Teile von Infrastruktur und KI-Hosting laufen auf Plattformen von US-Hyperscalern; Ausfall oder Policy-Änderung trifft viele Dienste gleichzeitig
- **Betriebssysteme und Endgeräte:** Server-, Desktop- und Mobile-Betriebssysteme werden dominiert von US-Anbietern; Lieferketten und Sicherheitsupdates sind zentralisiert
- **Produktivitätssoftware und Collaboration:** E-Mail, Kalender, Office-Suiten sind oft US-basiert; Datenlokation und Compliance damit schwer steuerbar
- **KI-Plattformen und Modelle:** Trainings- und Inferenzökosysteme basieren auf US-Angeboten und US-Hardware/Cloud-Stacks

Daraus resultieren Deutschland und Europa folgende Risiken

- **Souveränitätsverlust über Daten und Prozesse**: Kontrolle über sensible Daten und kritische Geschäftsprozesse liegt außerhalb der nationalen Rechts- und Kontrollsphäre.
- **Vendor Lock-in**: Hohe Migrationskosten und technische Abhängigkeiten erschweren Wechsel zu Alternativen.
- **Regulatorische und geopolitische Exposition**: US-Gesetze oder Exportkontrollen können Zugriff, Betrieb oder Verfügbarkeit beeinflussen.
- **Betriebsrisiken**: Zentralisierte Ausfälle großer US-Provider können ganze Branchen gleichzeitig treffen.
- **Datenhoheit und Datenschutz**: US-Cloudanbieter unterliegen US-Behördenrecht (Cloud Act). Das erschwert uneingeschränkte Kontrolle über Daten europäischer Nutzer.
- **Abhängigkeit und Souveränität:** Hohe Abhängigkeit von wenigen Anbietern kann Liefer- und Innovationsrisiken erhöhen und politische Handlungsspielräume einschränken.
- **Wettbewerbs- und Innovationsfragen:** Kosten- und Abhängigkeitsstrukturen können lokale Anbieter benachteiligen, aber auch Open-Source-Alternativen und europäische Ökosysteme stärken.
- **Sicherheits- und Resilienzrisiken:** Einseitige Abhängigkeit erhöht Angriffsziele; geografisch verteilte und mehrgleisige Architekturen (Multi-Cloud, Edge) verbessern die Resilienz.
- **Rechtsrahmen und Verträge**: Datenschutzverträge, Data-Processing-Addendums, Standardvertragsklauseln, und strenge Compliance-Anforderungen beeinflussen die Machbarkeit.

Beschreibung der operativ und strategisch Kritikalität

Viele Unternehmen sind operativ kurzfristig verwundbar – etwa durch Ausfälle oder Änderungen verwendeter und etablierter Services. Aus strategischer Sicht ist die Lage langfristig kritisch. Ohne gezielte Maßnahmen drohen wiederkehrende Abhängigkeiten von Schlüsseltechnologien und eine eingeschränkte Handlungsfreiheit in Krisensituationen.

- Hoch bis kritisch: Da Deutschland stark reglementiert ist (DSGVO, BDSG, Bundesdatenschutzgesetz) und diese Reglementierungen öffentliche Verwaltungen sowie kritische Infrastrukturen betreffen, ist die Abhängigkeit von US-Anbietern problematisch für Datensicherheit, Souveränität und Kosteneffizienz.
- Perspektivischer Ansatz: Durch EU-Initiativen wie GAIA-X, Open-Source-Strategien, europäische Cloud-Anbieter (z. B. Deutsche Cloud, Jean-Cloud-Initiativen) soll Souveränität gestärkt werden.

E3. Maßnahmen im Bereich Data Center Software und Services

1. Politische und regulatorische Maßnahmen

- **Förderprogramme und Beschaffungsregeln**: Durch gezielte Förderung und klare Beschaffungsregeln öffentliche Vergaben so ausrichten, dass europäische Anbieter mit nachweislicher digitaler Souveränität, Datenschutzkonformität und offenen Standards priorisiert werden.
- **Rechtliche Absicherung**: Zur rechtlichen Absicherung sind Vergabeverfahren und Vertragswerke so zu gestalten, dass verbindliche Vorgaben zur Datenlokation, umfassende Auditrechte sowie klar definierte Exit- und Übergangsklauseln enthalten sind. Diese Regelungen schützen die operative Souveränität, ermöglichen kontrollierte Audits und sichern einen reibungslosen Anbieterwechsel ohne Datenverlust oder Betriebsunterbrechung.

2. Technische Architektur und Betrieb

- **Klassifizierung von Workloads**: Die Klassifizierung von Workloads nach Sensitivität und Souveränitätsbedarf ist essenziell, um Risiken zu minimieren. Kritische Systeme sind ausschließlich in vertrauenswürdigen Jurisdiktionen zu betreiben, um Handlungsfreiheit und Sicherheit langfristig zu gewährleisten.“
- **Multi-Cloud und Multi-Vendor**: Um Single-Point-of-Failure-Risiken wirksam zu minimieren, sollten Dienste bewusst auf mehrere Anbieter und Jurisdiktionen verteilt werden. So entsteht eine höhere Ausfallsicherheit und zugleich mehr Handlungsfreiheit in kritischen Szenarien.
- **Portabilität und offene Schnittstellen**: Die Sicherung von Portabilität und offenen Schnittstellen ist zentral für digitale Souveränität. Durch den Einsatz offener Standards, containerisierter Deployments wie Kubernetes und garantierter Datenexportfähigkeit lassen sich Vendor-Lock-in-Risiken wirksam reduzieren und langfristige Handlungsfreiheit bewahren
- **Verschlüsselung und eigenes Key-Management**: Ende-zu-Ende-Verschlüsselung mit eigenem, national kontrolliertem Key Management implementieren, sodass weder Drittanbieter noch ausländische Behörden Zugriff erlangen können und die Souveränität über sensible Daten gewahrt bleibt.

3. Markt- und Innovationsförderung

- **Aufbau souveräner Cloud-Infrastruktur**: Zur Stärkung digitaler Souveränität sind gezielte Investitionen in europäische Hyperscaler-Alternativen sowie in lokale Rechenzentren erforderlich. Diese Maßnahmen schaffen unabhängige Kapazitäten, reduzieren Abhängigkeiten von außereuropäischen Anbietern und ermöglichen kontrollierte, rechtskonforme Datenhaltung und Betriebsführung.
- **Stärkung von Open-Source-Ökosystemen**: Die gezielte Förderung auditierbarer Open-Source-Projekte schafft eine verlässliche Basis für souveräne Software-Stacks. Durch finanzielle Unterstützung, klare Qualitäts- und Sicherheitskriterien sowie aktive

Förderung von Community-Governance lassen sich langfristig transparente, wartbare und unabhängige Software-Ökosysteme aufbauen

4. Beschaffungspraxis und Vertragsgestaltung (praxisnah)

- **SLA- und Exit-Klauseln**: Klare Anforderungen zu Datenrückgabe, Schnittstellen, Interoperabilität und Notfallplänen verankern.
- **Audit- und Transparenzpflichten**: Lieferanten verpflichten, Sicherheits- und Rechtsprüfungen zu ermöglichen.
- **Risikobasierte Beschaffung**: Bei strategisch sensiblen Diensten ausschließlich Anbieter mit geprüfter Rechts- und Sicherheitslage zulassen.

5. Operative Maßnahmen und Skills

- **Resilienz-Tests und Migrationsübungen**: Regelmäßige Failover- und Portierungsübungen durchführen, um Exit-Szenarien realistisch zu prüfen.
- **Know-how-Aufbau**: Ausbildung, Rekrutierung und Förderung von Fachkräften für Cloud-Architektur, Open-Source-Entwicklung und Security.
- **Hybrid-Modelle nutzen**: Kombination aus On-Premise, lokalen Clouds und internationalen Anbietern für optimale Balance aus Kontrolle und Effizienz.

Im Folgenden die Beschreibung einiger Maßnahmen im Detail:

Förderung von Open-Source-Software und offenen Standards

Vorteile: Open-Source-Lösungen bieten Transparenz, ermöglichen die Kontrolle über den Quellcode, reduzieren Vendor Lock-in und fördern die Kollaboration. Sie sind oft kostengünstiger und können an spezifische Bedürfnisse angepasst werden.

Maßnahmen: Bevorzugung bei öffentlichen Ausschreibungen: Die öffentliche Verwaltung sollte Open-Source-Software bevorzugen, wo immer dies möglich ist. Projekte wie "Sovereign Workplace" oder "Open CoDE" sind gute Beispiele.

Finanzielle Unterstützung: Förderung der Entwicklung und Wartung von Open-Source-Projekten in Europa.

Standardisierung: Etablierung und Nutzung offener Standards, um Interoperabilität zu gewährleisten und die Abhängigkeit von proprietären Formaten zu verringern.

Aufbau und Stärkung europäischer digitaler Infrastrukturen und Cloud-Anbieter

Ziel:
Eine unabhängige und sichere europäische Cloud-Infrastruktur schaffen, die den europäischen Datenschutzstandards entspricht.

Maßnahmen:

GAIA-X: Weiterentwicklung und Implementierung von GAIA-X als europäische Dateninfrastruktur, die Vertrauen, Souveränität und Interoperabilität gewährleistet.

Investitionen: Gezielte Investitionen in den Aufbau und die Skalierung europäischer Cloud-Anbieter und Rechenzentren.

Edge Computing: Förderung von Edge-Computing-Lösungen, um Daten näher am Entstehungsort zu verarbeiten und die Abhängigkeit von zentralisierten Hyperscalern zu reduzieren.

Stärkung digitaler Kompetenzen und Bildung

Ziel:
Die Fähigkeit entwickeln, digitale Technologien nicht nur zu nutzen, sondern auch zu verstehen, zu entwickeln und anzupassen.

Maßnahmen:
Bildung und Ausbildung: Investitionen in MINT-Fächer, Informatikunterricht in Schulen und Universitäten sowie Weiterbildungsprogramme für Fachkräfte.

Forschung und Entwicklung: Förderung von Forschung und Innovation im Bereich Schlüsseltechnologien (z.B. KI, Quantencomputing, Cybersicherheit) innerhalb Europas.

Talentförderung: Anreize schaffen, um digitale Talente in Europa zu halten und anzuziehen.

Regulatorische Maßnahmen und Datenschutz

Ziel:
Ein starker Rechtsrahmen, der Datenschutz, Datensicherheit und fairen Wettbewerb gewährleistet.

Maßnahmen:
DSGVO: Konsequente Durchsetzung der Datenschutz-Grundverordnung (DSGVO), um den Schutz personenbezogener Daten zu gewährleisten.

Digital Markets Act (DMA) und Digital Services Act (DSA): Nutzung dieser Gesetze, um die Marktmacht großer Tech-Konzerne zu regulieren und fairen Wettbewerb zu fördern.

Datenhoheit: Sicherstellen, dass Daten europäischer Bürger und Unternehmen in Europa gespeichert und verarbeitet werden und nicht dem Zugriff ausländischer Behörden unterliegen (z.B. durch den CLOUD Act der USA).

Strategische Beschaffung und Diversifizierung

Ziel:
Die Abhängigkeit von einzelnen Anbietern reduzieren und eine breitere Basis an vertrauenswürdigen Lieferanten schaffen.

Maßnahmen:
Diversifizierung: Nicht alle Eier in einen Korb legen, sondern verschiedene Anbieter und Technologien nutzen.

Langfristige Planung: Strategische Beschaffungsentscheidungen treffen, die die digitale Souveränität berücksichtigen und nicht nur kurzfristige Kostenoptimierung.

Vendor Lock-in vermeiden: Verträge so gestalten, dass ein Wechsel des Anbieters technisch und wirtschaftlich möglich bleibt.

Förderung eines europäischen Ökosystems für Softwareentwicklung

Ziel:
Ein lebendiges und innovatives Ökosystem für Softwareentwicklung in Europa schaffen.

Maßnahmen:
Start-up-Förderung: Unterstützung von europäischen Start-ups im Tech-Bereich durch Finanzierung, Mentoring und Zugang zu Märkten.

Kooperationen: Förderung der Zusammenarbeit zwischen Unternehmen, Forschungseinrichtungen und der öffentlichen Hand.

Europäische Champions: Gezielte Unterstützung beim Aufbau von europäischen Technologie-Champions, die global wettbewerbsfähig sind.

7. Fazit

Die Auflösung der beschriebenen Abhängigkeiten und damit verbunden das Erlangen der dringend benötigen Digitalen Souveränität ist ein langfristiger Prozess, der einen koordinierten Ansatz auf nationaler und europäischer Ebene erfordert.

Es geht darum, die Kontrolle über die eigene digitale Zukunft zurückzugewinnen und die Resilienz gegenüber externen Einflüssen zu stärken. Wir haben über Jahrzehnte alles, was an Digitaler Infrastruktur und Digitalen Services zur Verfügung stand in unsere Unternehmen und Verwaltungen integriert. Dabei ist es nicht so, dass man die Bedenken gegen diesen Kurs und die damit verbundenen Risiken nicht schon frühzeitig erkannt hätte, oder dass es keine warnenden Stimmen gab. Die Entscheider, egal, ob in der Politik, den öffentlichen Verwaltungen, oder in der Privatwirtschaft haben die Risiken bewusst außer Acht gelassen und anderen, vermutlich meist ökonomischen, Zielen untergeordnet.

Und all denen gesagt, die es bis dato noch nicht realisiert haben, wacht endlich auf. Überdenkt Eure Prioritäten und beginnt damit Verantwortung für die Zukunft zu übernehmen.