Digitale und technologische Souveränität

DIHK-Positionspapier 2026

DIHK Deutsche Industrie- und Handelskammer

#GemeinsamDigital

Impressum

Deutsche
Industrie- und Handelskammer

Redaktion und Ansprechpartner

Arian Siefert
siefert.arian@dihk.de
Dr. Katrin Sobania
sobania.katrin@dihk.de

Weitere Mitarbeit und Ansprechpartner

Klemens Kober
kober.klemens@dihk.de
Philipp Flore
flore.phillip@dihk.de
Lorenz Kramer
kramer.lorenz@dihk.de
Susanne Gewinnus
gewinnus.susanne@dihk.de
Lukas Littmann
littmann.lukas@dihk.de
Jana Heiberger
heiberger.jana@dihk.de
Julia Flasdick
flasdick.julia@dihk.de

Herausgeber und Copyright

Bereich Digitale Wirtschaft, Infrastruktur, Regionalpolitik

DIHK Berlin
Postanschrift: 11052 Berlin | Hausanschrift: Breite Straße 29 | Berlin-Mitte
Telefon: 030 20308-0 | Telefax: 030 20308-1000

DIHK Brüssel
Vertretung der Deutschen Industrie- und Handelskammer bei der Europäischen Union
19 A-D, Avenue des Arts | B-1000 Bruxelles
Telefon: +32-2-286-1611 | Telefax: +32-2-286-1605

Internet
www.dihk.de

Grafik
Sven Ehling, DIHK

Bildnachweis
Getty Images)

Stand
Juni 2026

Digitale und technologische Souveränität – Potenziale nutzen, Wohlstand sichern, Geopolitik gestalten

Executive Summary

Der internationale Wettbewerb um digitale Schlüsseltechnologien hat sich zu einem zentralen geopolitischen Machtfaktor entwickelt. Für Deutschland und Europa geht es dabei nicht nur um Innovation und Wachstum, sondern um wirtschaftliche Resilienz, strategische Handlungsfähigkeit und geopolitische Gestaltungsspielräume. Digitale und technologische Souveränität ist dafür eine wesentliche Voraussetzung.

Derzeit sind Deutschland und Europa jedoch in zentralen Bereichen des digitalen Ökosystems stark abhängig von außereuropäischen Anbietern – etwa bei Cloud Infrastrukturen, Plattformen, KI-Frameworks und Teilen der öffentlichen IT. Diese Abhängigkeiten erhöhen die Verwundbarkeit von Wirtschaft und Staat gegenüber geopolitischen Spannungen, regulatorischen Konflikten und technologischen Lock-in-Effekten.

Gleichzeitig verfügt Deutschland über erhebliche industrielle, technologische und wissenschaftliche Potenziale. Starke Unternehmen mit tiefem Domänenwissen, hohe Forschungsleistung, steigende Patentanmeldungen in digitalen Schlüsseltechnologien und wachsende KI-Nutzung bilden eine solide Basis, um digitale Wertschöpfung und technologische Führungsrollen auszubauen. Das Problem liegt weniger in fehlenden Kompetenzen als in unzureichenden Skalierungsbedingungen und strukturellen Hemmnissen.

Ein resilientes und souveränes digitales Ökosystem erfordert daher klar definierte Bausteine: einen schlanken, technologieoffenen Rechtsrahmen, offene Standards und interoperable Technologien, klare Vertrags- und Datenkontrolle, leistungsfähige digitale Infrastrukturen und Schlüsseltechnologien, gesicherte Zugänge zu kritischen Rohstoffen sowie starke digitale Kompetenzen.

Damit vorhandene Potenziale gehoben werden können, muss die Politik gezielt handeln. Erforderlich sind der Abbau von Bürokratie und Rechtsunsicherheit, schnellere Genehmigungen, wettbewerbsfähige Energiepreise, priorisierte Investitionen in KI-Infrastrukturen und Rechenzentren sowie ein verbesserter Zugang zu Forschungsergebnissen, Rechenleistung und Testumgebungen. Die öffentliche Hand sollte zudem offene und interoperable Technologien konsequent einsetzen und als strategischer Ankerkunde Innovationen gezielt anschieben.

Auf europäischer Ebene gilt es, digitale Souveränität als strategisches Gemeinschaftsprojekt zu begreifen. Die EU muss gleichzeitig als intelligenter Regelsetzer wirken, internationale Standards aktiv mitgestalten, Abhängigkeiten durch Diversifizierung und offene Standards reduzieren und die digitale Vernetzung über Handels- und Digitalabkommen ausbauen. Zugleich sollte die Regulierungslast so gering wie möglich sein, um Rechtsunsicherheiten zu vermeiden und Compliance-Kosten zu verringern.

Digitale und technologische Souveränität sind erreichbar. Deutschland und Europa verfügen über die notwendigen Unternehmen, Kompetenzen und industriellen Stärken – entscheidend ist nun, die politischen und wirtschaftlichen Rahmenbedingungen konsequent auf Skalierung, Wettbewerbsfähigkeit und Resilienz auszurichten.

Einleitung

Der internationale Wettbewerb im Bereich digitaler Technologien ist von einer zunehmenden technologischen, wirtschaftlichen und geopolitischen Zuspitzung geprägt. Führende Volkswirtschaften investieren massiv in Schlüsseltechnologien wie Künstliche Intelligenz (KI), Cloud- und Plattforminfrastrukturen, Halbleiter, Cybersicherheit und Quantentechnologien, um technologische Abhängigkeiten zu reduzieren und globale Standards zu setzen. Für Deutschland und Europa geht es hier nicht allein um einen Innovations- und Standortwettbewerb, sondern auch darum, Wertschöpfung, Datenhoheit und strategische Autonomie zu erhalten. Digitale und technologische Souveränität ist entscheidend, damit deutsche Unternehmen ihre technologischen Fähigkeiten in skalierbare, international wettbewerbsfähige Lösungen überführen Wertschöpfung am Standort sichern und wirtschaftliche Abhängigkeiten in geopolitisch unsicheren Zeiten reduzieren können.

Digitale und technologische Souveränität

Unter digitaler und technologischer Souveränität wird in dem vorliegenden Papier die Fähigkeit von Unternehmen und Institutionen wie staatlichen Stellen oder Forschungsinstitutionen verstanden, digitale Technologien, Daten und Infrastrukturen selbstbestimmt zu gestalten und einseitige kritische Abhängigkeiten abzubauen, um jederzeit handlungsfähig zu bleiben. Dadurch sollen externe Risiken wie politische Einflussnahmen, Lock-in-Effekte und regulatorische Konflikte reduziert werden, um die digitale und technologische Wettbewerbsfähigkeit und Resilienz zu stärken. Dies umfasst auch Aspekte wie Kostenkontrolle, Vertragsfreiheit, Datenportabilität sowie faire wettbewerbliche und steuerliche Rahmenbedingungen.

Deutschland und Europa verfügen über die Kompetenz, Innovationskraft und industrielle Stärke, um im internationalen Wettbewerb um digitale Technologien zu bestehen und zu wachsen. Insbesondere deutsche Unternehmen vereinen tiefes Domänenwissen, industrielle Exzellenz und hohe Ingenieurskunst mit wachsender digitaler Innovationsfähigkeit. Deutschland nimmt in der Grundlagenforschung vielfach Spitzenpositionen ein. Die Zahl der Patentanmeldungen in digitalen Schlüsseltechnologien ist zuletzt deutlich gestiegen – insbesondere bei KI-nahen Anwendungen – und auch die Nutzung von KI in deutschen Unternehmen nimmt kontinuierlich zu. In Zukunftstechnologien wie der Quantentechnologie hat Europa den Rückstand zu den USA messbar verringert.

Deutsche Unternehmen können durch die intelligente Verknüpfung von Software, Daten, KI und industriellen Anwendungen Wettbewerbsvorteile schaffen, neue Geschäftsmodelle etablieren und Wertschöpfung am Standort sichern. Digitale und technologische Souveränität ist dabei kein Selbstzweck, sondern eine strategische Chance, Innovationszyklen zu beschleunigen, Resilienz zu erhöhen und technologische Führungsrollen im digital relevanten Technologie-Stack auszubauen.

Es besteht jedoch erheblicher Handlungsbedarf, weil zentrale Ebenen des digitalen Stacks – von Cloud-Infrastruktur und Betriebssystemen bis hin zu KI-Frameworks, Cybersicherheitslösungen und öffentlicher IT – weitgehend von außereuropäischen Anbietern kontrolliert werden.[1] Daraus entstehen kritische Abhängigkeiten und Risiken für die strategische Handlungsfähigkeit von Unternehmen und Staat. Die wachsenden geopolitischen Spannungen, insbesondere zwischen den USA und China, erhöhen diese Risiken zusätzlich, da deutsche Unternehmen zunehmend in globale Systemkonflikte und Abhängigkeiten geraten.

Die IHK-Organisation sieht zentralen Handlungsbedarf vor allem darin, offene und interoperable Technologien zu fördern, vertrauenswürdige digitale Infrastrukturen und Schlüsseltechnologien zu stärken sowie digitale und technologische Kompetenzen gezielt aufzubauen.

Zentrale Forderungen für digitale und technologische Souveränität

Rechtsunsicherheit und Bürokratie abbauen

Es braucht einen klaren, schlanken und technologieoffenen digitalen Rechtsrahmen. Gesetze und Regelwerke müssen

dafür besser aufeinander abgestimmt und praxistauglich ausgestaltet werden, um Unternehmen Planungssicherheit zu geben und Wettbewerbsverzerrungen sowie unnötige Bürokratie zu vermeiden.

Offene Standards, Interoperabilität und digitale Identitäten konsequent umsetzen

Die öffentliche Hand sollte konsequent auf offene Standards, interoperable Lösungen und souveräne Technologien setzen und den Deutschland-Stack verbindlich über alle Verwaltungsebenen hinweg nutzen. Gleichzeitig sollten digitale Identitäten auf Basis der European Business Wallets und der EUDI-Wallets als zentrales Fundament souveräner digitaler Ökosysteme etabliert und aktiv durch den Staat gefördert werden. Zudem braucht es eine nachhaltige Stärkung des europäischen Open-Source-Ökosystems. Daten als Grundlage für KI müssen auch in KMU stärker nutzbar gemacht werden. Dafür sollten interoperable Datenräume wie Manufacturing-X langfristig abgesichert, skaliert und für den Mittelstand aufgeschlossen werden.

Cyberresilienz ausbauen

Alle Unternehmen, und insbesondere im Bereich der kritischen Infrastrukturen, müssen Bedrohungen frühzeitig erkennen und resilient gegenüber Angriffen sein. Dafür braucht es eine engere Zusammenarbeit zwischen Wirtschaft und Staat, etwa beim Austausch von sicherheitsrelevanten Informationen, wobei Meldepflichten möglichst bürokratiearm gestaltet und in konkrete, nutzbare Lagebilder für Unternehmen überführt werden müssen. Gleichzeitig sind leistungsfähige europäische Reaktions- und Koordinationsmechanismen notwendig, um Bedrohungen wirksam und schnell begegnen zu können. Für KRITIS bedarf es darüber hinaus einer klaren, langfristigen Strategie mit dem Ziel, Abhängigkeiten von außereuropäischen Anbietern schrittweise zu reduzieren.

Schlüsseltechnologien systematisch ausbauen und skalieren

Industrielle Stärken sollten gezielter in marktfähige und international skalierbare Lösungen überführt werden. Dies betrifft vor allem industrielle Anwendungen in Verbindung mit Software, Daten und KI sowie die schnellere Überführung erfolgreicher Digital- und Technologie-Projekte in die Breite. Dafür braucht es klar priorisierte staatliche Investitionen in strategische Zukunftsfelder sowie regulatorische Planungssicherheit. Hinzu kommen klar priorisierte staatliche Investitionen in strategische Zukunftsfelder und eine deutliche Beschleunigung des Transfers von Forschung in die industrielle Anwendung, zum Beispiel durch eine von Beginn an konsequent integrierte Kommerzialisierung von Forschungsergebnissen, schnelleren und unbürokratischen Zugang der Unternehmen zu Testumgebungen und verstärkte Bereitstellung von Schlüsselressourcen wie Rechenleistung.

Infrastrukturausbau beschleunigen und Energiepreise senken

Digitale Infrastrukturen wie Glasfaser- und Mobilfunknetze sowie Rechenzentren sind entscheidend für den schnellen Auf- und Ausbau digitaler Innovationen und Geschäftsmodelle. Damit diese schnell entstehen und wachsen können, braucht es wettbewerbsfähige Energiepreise für den Betrieb von Rechenzentren und schnellere Planungs- und Genehmigungsverfahren sowie verfügbare Flächen.

Kritische Rohstoffe strategisch sichern

Digitale Souveränität erfordert einen europäisch koordinierten Ansatz zur Sicherung kritischer Rohstoffe. Dazu gehören strategische Partnerschaften, die stärkere Erschließung heimischer Potenziale und der Ausbau der Weiterverarbeitung, etwa im Rahmen des EU Chips Acts und des Critical Raw Materials Act.

Souveränes Europa: Rule maker statt rule taker

Die EU sollte internationale digitale Standards, Normen und Datenschutz proaktiv mitgestalten und digitale Kooperationen über Handels- und Digitalabkommen ausbauen. Normung muss strategisch gestärkt und die Beteiligung europäischer Unternehmen, insbesondere von KMU, erleichtert werden. Den digitalen Euro, sofern dieser eingeführt werden sollte, und europäische privatwirtschaftliche Initiativen sollte man zum Aufbau einer unabhängigen europäischen Zahlungsinfrastruktur nutzen.

Digitale Kompetenzen systematisch aufbauen

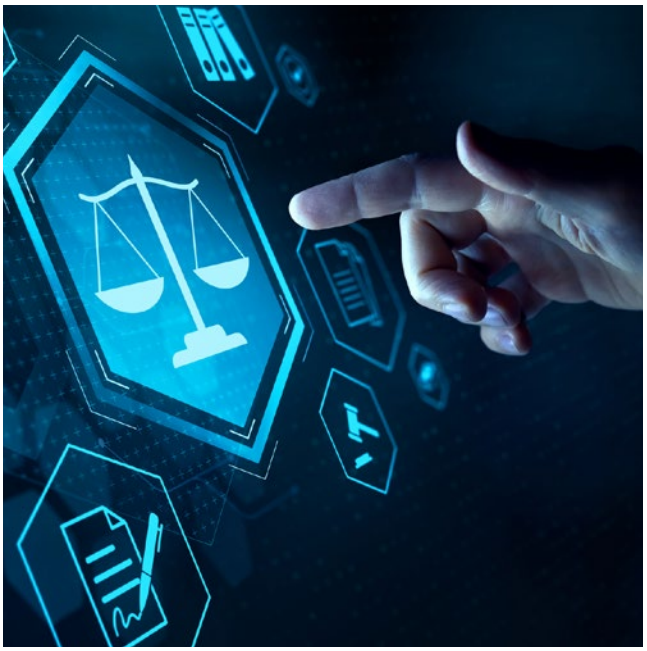
Wettbewerbsfähigkeit erfordert starke digitale Kompetenzen. Nötig sind eine leistungsfähige digitale Bildungsinfrastruktur, die gezielte Qualifizierung von Lehrkräften sowie der Ausbau europäischer Lernplattformen und von Bildungsdatenräumen.

Rechtsunsicherheit und Bürokratie abbauen

Technologischer Fortschritt und klare regulatorische Leitplanken sind keine Gegensätze, sondern bedingen sich gegenseitig: Nur ihr ausgewogenes Zusammenspiel ermöglicht eine verantwortungsvolle, nachhaltige und souveräne Entwicklung. Allerdings darf Regulierung Innovation nicht ausbremsen. Wenn ein Standort digitale Neuerungen von Anfang an mit zu vielen Prüf , Dokumentations- und Berichtspflichten belegt, verlangsamt das die Umsetzung erheblich – und gefährdet damit langfristig auch seine technologische Eigenständigkeit.

Unternehmen sind zudem mit einer wachsenden Zahl horizontaler und sektoraler Regelungen konfrontiert, die häufig nicht aufeinander abgestimmt sind. Überschneidungen, Regelungskonflikte, unklare Zuständigkeiten oder doppelte Berichtspflichten verursachen hohe bürokratische Belastungen und Rechtsunsicherheiten. Dies zeigt sich etwa beim Zusammenspiel der KI-Verordnung mit sektoralen Rechtsakten wie der Medizinprodukteverordnung oder der Funkanlagenrichtlinie sowie mit horizontalen Regelwerken wie der DSGVO. Hinzu kommen Regelungen, die technische Unterschiede nur unzureichend berücksichtigen, etwa wenn der KI-Rechtsrahmen nicht zwischen Allzweck-KI, verbrauchernahen Anwendungen und industriellen Assistenzsystemen differenziert. Dadurch werden der Einsatz von KI und Innovationsprozesse erschwert und Wettbewerbsnachteile geschaffen.

Weitere Unsicherheit entsteht, wenn gesetzlich vorgesehene Leitfäden oder technische Standards zu spät bereitgestellt werden, obwohl die entsprechenden Pflichten bereits gelten. Zusätzlich wird die Situation durch weitere Vorschriften aus angrenzenden Bereichen wie Lieferketten oder Corporate Social Responsibility komplexer.



In der Gesamtwirkung leidet die Wettbewerbsfähigkeit des Wirtschaftsstandorts Europa. Deutschland ist dabei besonders betroffen, da der hohe Anteil an kleinen und mittleren Unternehmen sowie mittelgroßen Weltmarktführern dazu führt, dass neue europäische Regulierungsvorhaben den deutschen Mittelstand überproportional belasten. Dies zeigt sich besonders in stark regulierten Anwendungsfeldern, in denen komplexe Nachweis-, Zulassungs- und Dokumentationsanforderungen häufig in keinem ausgewogenen Verhältnis zu den realisierbaren Markt- und Skalierungschancen stehen. Gerade für kleine und mittlere Unternehmen können daraus erhebliche wirtschaftliche Risiken entstehen, die Innovationen verzögern oder verhindern.

DIHK-Empfehlungen:

Digitalen Rechtsrahmen konsistent, schlank und technologieoffen gestalten

Unternehmen sind eher in der Lage, eigene digitale Lösungen selbstbestimmt zu entwickeln und einzusetzen, wenn die Regeln verständlich, planbar und rechtssicher sind.

Die europäische und nationale Digitalregulierung sollten gut aufeinander abgestimmt sein, damit unnötige Bürokratie, doppelte Pflichten und widersprüchliche Vorgaben vermieden werden. Wichtige allgemeine Regelwerke wie die KI-Verordnung, der Data Act, die DSGVO, NIS2, der Cyber Resilience Act, der Industrial Accelerator Act, die geplante Vergaberechtsreform, aber auch eher branchenspezifische Regulierungen wie die Maschinenverordnung, die Medizinprodukteverordnung, der European Health Data Space oder im Finanzanlagenbereich müssen besser miteinander verzahnt sowie praxisnah und möglichst unbürokratisch umgesetzt werden.

Regulierung wird nur dann wirksam und akzeptiert, wenn sie nicht als Wettbewerbsnachteil verstanden wird. Es sollte ein "Level-Playing-Field" gewährleistet sein und Regeln konsequent auch gegenüber Unternehmen aus Drittstaaten durchgesetzt werden. Dafür müssen Aufsichts- und Kontrollbehörden angemessen ausgestattet sein und effektiv zusammenarbeiten. Im Bereich der Zertifizierungen und Konformitätsbewertungen sind beschleunigte Verfahren und reduzierte Kosten nötig. Gleichzeitig ist eine enge internationale Zusammenarbeit erforderlich, um widersprüchliche Verpflichtungen für international agierende Unternehmen zu vermeiden. Insoweit bedarf es neuer Regulierungsansätze auch in der EU.

Insgesamt sollte die Regulierung technologieoffen bleiben, unnötige Dokumentations- und Berichtspflichten vermeiden und dazu beitragen, Innovation, internationale Zusammenarbeit und Wettbewerbsfähigkeit zu stärken.

Komplexitäts- und Wettbewerbsfähigkeitschecks könnten gerade für KMU Entbürokratisierung aktiv vorantreiben.

Umsetzung durch Leitfäden, Standards und Übergangsfristen absichern

Gesetzliche Anforderungen sollten so schlank und praxistauglich wie möglich sein, damit Regelungen verständlich und anwendbar sind. Unternehmen sollten Anforderungen eigenständig verstehen und umsetzen können. Falls Leitlinien, Durchführungsrechtsakte oder technische Standards erforderlich sind, sollten diese frühzeitig veröffentlicht werden. Dabei sind ausreichend lange Übergangsfristen wichtig, damit Unternehmen genügend Zeit haben, sich auf die neuen Vorgaben einzustellen und die notwendigen Maßnahmen umzusetzen. Sie gewinnen so mehr Kontrolle über ihre digitalen Prozesse und können Innovation gezielt vorantreiben.

Unternehmen sollten rechtzeitig vor Beginn neuer Pflichten passende Unterstützungsangebote erhalten. Dazu gehören zum Beispiel Self-Checks zur rechtssicheren Klärung der eigenen Betroffenheit sowie verlässliche Leitfäden und Musterverträge, etwa für KI- und Datenkooperationen, die in enger Abstimmung mit der Wirtschaft entwickelt und von zuständigen staatlichen Stellen und Aufsichtsbehörden bereitgestellt werden sollten.

Offene Standards, Interoperabilität und digitale Identitäten konsequent umsetzen

Fehlende Interoperabilität, proprietäre Schnittstellen und mangelnde offene Standards bremsen die digitale Transformation und verstärken Abhängigkeiten von einzelnen Herstellern. Insbesondere vor dem Hintergrund aktueller geopolitischer Entwicklungen wirkt sich dies gefährdend auf die digitale Souveränität und damit die Resilienz der Unternehmen aus.

Der DIHK-Digitalisierungsumfrage 2026 zufolge sehen sich deutsche Unternehmen vor allem im Bereich industrieller Software größtenteils digital souverän aufgestellt. In anderen Bereichen wie Office-Software, Hardware und Cloud bis hin zu KI und Plattformen sehen sie sich mehrheitlich weitgehend oder vollkommen abhängig von Anwendungen und Technologien aus dem Nicht-EU-Ausland. Die Datenbasis für digitale KI-gestützte Anwendungen bleibt zu häufig in Unternehmen und Politik unerschlossen.

Digitale Identitäten, die in verschiedenen Bereichen nutzbar sind, sind ein wichtiger Baustein für digitale Souveränität und Widerstandsfähigkeit. Bisher gibt es jedoch meist nur isolierte Lösungen für einzelne Branchen, zum Beispiel innerhalb von Datenräumen. Auch Lösungen der öffentlichen Verwaltung, wie das Unternehmenskonto für Behördengänge, sind bislang nicht darauf ausgelegt, in ein gemeinsames europäisches Vertrauenssystem eingebunden zu werden.

Auch die Handlungsfähigkeit des Staates hängt davon ab, dass die öffentliche Verwaltung selbst souveräne, sichere und vertrauenswürdige digitale Lösungen nutzt und Prozesse vereinfacht, bevor sie digitalisiert werden. In einigen Bereichen, etwa bei Fachanwendungen, werden bereits souveräne digitale Lösungen eingesetzt, nicht aber im Bereich der Desktop-Lösungen. Zudem verhindern zu oft fehlende einheitliche technische Standards und interoperable Schnittstellen, dass digitale Lösungen aus Mittelstand und Start-ups in der Verwaltung verbreitet genutzt werden.

Bund und Länder haben sich u. a. mit dem Deutschland-Stack, in der Digitalministerkonferenz und im IT-Planungsrat auf den Weg gemacht, das Innovationspotenzial von privatwirtschaftlichen Anbietern digital souveräner Lösungen stärker für die Digitalisierung der Verwaltung zu nutzen.

Die Implementierung neuer digitaler Technologien in der Verwaltung erfolgt dennoch oft zu langsam und wenig koordiniert. Dies liegt unter anderem an komplexen Governance-Strukturen und fehlender Digitaltauglichkeit rechtlicher Rahmenbedingungen. Es braucht stärker gebündelte Kompetenzen und eine klare zentrale Steuerung, um Lösungen schneller und im größeren Maßstab einsetzen zu können. Dafür sind zuerst die rechtlichen, aber auch die finanziellen Voraussetzungen zu schaffen und effektive Steuerungsstrukturen zu etablieren.

Der Koalitionsvertrag der Bundesregierung von 2025 enthält ein deutliches Bekenntnis zur digitalen Souveränität als zentrales politisches Ziel. Open Source wird dabei ausdrücklich als strategisches Fundament für den Aufbau eines souveränen digitalen Ökosystems verstanden. Konkrete, überprüfbare Zielgrößen oder verbindliche Vorgaben zur Umsetzung bleiben jedoch bislang weitgehend offen.

DIHK-Empfehlungen:

Offene Standards und interoperable Lösungen in der Verwaltung priorisieren

Die öffentliche Hand sollte konsequenter auf offene Standards, interoperable Architekturen und souveräne Technologien setzen. Das hilft, Abhängigkeiten zu vermeiden, fairen Wettbewerb zu fördern und die eigene Handlungsfähigkeit zu sichern. Ziel sollte ein leistungsfähiges, durchgängig digitales Gesamtökosystem für Deutschland sein.

Gerade bei der Verwaltungsdigitalisierung, der IT Sicherheit, bei Dateninfrastrukturen, KI Anwendungen oder digitalen Identitäten kann der Staat besonders von innovativen Lösungen der Privatwirtschaft profitieren. Mit dem Deutschland-Stack wurde hierfür ein wichtiger Grundstein gelegt. Entscheidend ist nun, dass diese Strukturen verbindlich in der gesamten Verwaltung genutzt werden – vom Bund über die Länder bis hin zu den Kommunen. Nur so lassen sich Effizienz- und Innovationspotenziale ausschöpfen und die Verwaltung insgesamt zukunftsfähiger, resilienter und souveräner aufstellen. Dafür braucht es passende rechtliche und organisatorische Rahmenbedingungen, etwa eine Anpassung der Kompetenzordnung des Grundgesetzes und konkrete Unterstützungsangebote für Kommunen.

Der Deutschland-Stack darf sich aber nicht nur auf Verwaltungsmodernisierung beschränken. Er sollte zur gemeinsamen digitalen Infrastruktur für Staat und Wirtschaft werden.

Digitale Identitäten als Fundament für souveräne digitale Ökosysteme etablieren

Sichere digitale Identitäten sind ein wesentlicher Erfolgsfaktor für souveräne, digitale Ökosysteme. Sie sind ein Schlüssel, um Kosten in den Unternehmen zu senken und sicheren Datenaustausch mit Kunden, Geschäftspartnern und mit der öffentlichen Hand zu ermöglichen.

Erforderlich ist ein funktionsfähiges Ökosystem von digital souveränen Unternehmensidentitäten auf Basis der European Business Wallets, in Verbindung mit der freiwilligen Nutzung von digitalen Identitäten für natürliche Personen wie den EUDI-Wallets, soweit diese geschäftlich tätig sind. Der Aufbau dieses Ökosystems sollte aktiv von der öffentlichen Hand unterstützt werden. So sollte die öffentliche Hand auch als großer Nutzer der in den Wallets enthaltenen Vertrauensdienste und als ausgebende Stelle von Nachweisen eine wesentliche Katalysatorfunktion einnehmen. Ziel muss sein, dass digitale Identitäten, Nachweise, Verwaltungsdaten, Unternehmensdatenräume und industrielle Datenökosysteme nicht nebeneinanderstehen, sondern interoperabel zusammenwirken können.

Europäisches Open-Source-Ökosystem nachhaltig unterstützen

Open-Source-Software bildet das Fundament nahezu aller modernen Softwareentwicklung. Gleichzeitig ist die zugrunde liegende offene digitale Infrastruktur häufig unterfinanziert und unzureichend unterstützt – ein strukturelles Problem mit weitreichenden Folgen. Dabei bieten Europas bestehende Open-Source-Stärken eine wichtige Grundlage für den Ausbau digitaler Souveränität.

Offene digitale Infrastrukturen und europäische Open-Source-Communities sollten gezielt und nachhaltig gestärkt werden. Sie ermöglichen es, Schwachstellen frühzeitig zu erkennen und eigene, souveräne digitale Lösungen zu entwickeln. Wo der Staat selbst Open-Source-Software einsetzt, muss er zudem Verantwortung für deren kontinuierliche Wartung und Weiterentwicklung übernehmen. Nur so bleiben diese Lösungen langfristig sicher, leistungsfähig und verlässlich.

Datenräume souverän ausrichten

Interoperable Datenräume wie Manufacturing-X ermöglichen effiziente Datenflüsse zwischen Unternehmen und können so europäische Technologie-Stacks stärken. Sie tragen zur Data-Readiness vieler Unternehmen bei und sollten finanziell, rechtlich und organisatorisch abgesichert und skaliert werden, über projektbasierte Förderlogiken hinaus. Dies schließt insbesondere die Etablierung von Umsetzungs- und Erprobungsumgebungen ein, die als stabile Plattformen für den Aufbau und die Pflege von Communities aus Industrie, Technologieanbietern und Anwendern dienen. Es sollte darauf hingewirkt werden, insbesondere kleine und mittlere Unternehmen in diese Ökosysteme rund um digitale und technologische Zukunftsthemen stärker einzubeziehen.

Cyberresilienz ausbauen

Die europäische Gesetzgebung adressiert zentrale Aspekte wie Lieferkettenrisiken, Betreiberverantwortung, Cybersicherheit, Datensouveränität und Abhängigkeiten von Drittstaaten unter anderem durch NIS2, den Cyber Resilience Act, den Data Act und die DSGVO.

Unternehmen sehen sich damit einer Vielzahl an Melde-, Dokumentations- und Nachweispflichten gegenübergestellt. Diese sind oft komplex, schwer verständlich oder überschneiden sich. Meldepflichten liefern bislang zu selten einen direkten Mehrwert für Unternehmen. Es fehlt an aufbereiteten, aktuellen Lagebildern und konkreten Handlungsempfehlungen. Der Austausch zwischen Behörden und Wirtschaft ist noch zu fragmentiert.

DIHK-Empfehlungen:

Sicherheitsvorgaben bürokratiearm und praxistauglich ausgestalten

Der Gesetzgeber sollte Vorgaben stärker harmonisieren, vereinfachen und konsequent auf Praxistauglichkeit ausrichten. Ziel muss sein: weniger Bürokratie, mehr tatsächlicher Sicherheitsgewinn.

Cyberresilienz durch Kooperation stärken

Digitale Souveränität im Bereich Cyberkriminalität und Wirtschaftsspionage erfordert ein abgestimmtes Vorgehen auf mehreren Ebenen. Dazu gehört eine engere Zusammenarbeit zwischen Wirtschaft und Staat, etwa beim Austausch von Informationen. Die zusätzlichen Belastungen – etwa durch Meldepflichten der Unternehmen – sind möglichst bürokratiearm auszugestalten. Aus den Meldungen müssen praxistaugliche Informationen über aktuelle Bedrohungen und Risiken erarbeitet und den Unternehmen zielgerichtet zur Verfügung gestellt werden. Dabei sollten Cyber- und analoge Risiken gesamtheitlich betrachtet werden.

Unterstützungsangebote für den Mittelstand ausbauen

Viele kleine und mittlere Unternehmen sind mit Cyberanforderungen überfordert. Staatlicher Handlungsbedarf besteht bei niederschwelliger Beratung, standardisierten Sicherheitslösungen sowie konkreten Umsetzungsangeboten nach dem Motto „Cyberresilienz-as-a-Service".

Cyberresilienz wird häufig technisch verstanden, das greift aber zu kurz. Unternehmen brauchen Unterstützung auch bei Business Continuity Management, Notfallplanung und Wiederanlaufprozessen. Der Staat sollte entsprechende Standards und Leitfäden bereitstellen.

Viele Unternehmen sind stark von Drittanbietern abhängig. Der Staat sollte – neben den bestehenden rechtlichen Vorgaben – bei der Bewertung von IT-Lieferkettenrisiken unterstützen sowie beim Aufbau vertrauenswürdiger europäischer Alternativen.

Innovation und Sicherheitslösungen fördern

Es fehlt an Skalierung innovativer Sicherheitslösungen „Made in Europe". Der Staat sollte gezielt Forschung, Entwicklung und Markteinführung von Cybersecurity-Technologien fördern und deren Einsatz in der Breite unterstützen. Die Entwicklung von Cyberresilienz erfordert nicht nur technische Sicherheitslösungen, sondern auch qualifizierte Mitarbeitende, die Risiken frühzeitig erkennen und angemessen reagieren können.

Europäische Reaktionsfähigkeit verbessern

Cyberangriffe sind grenzüberschreitend, die Reaktionsstrukturen häufig noch national fragmentiert. Es braucht schlagkräftige europäische Koordinations- und Eingreifmechanismen sowie klar definierte Verantwortlichkeiten im Krisenfall.

Kritische Infrastrukturen strategisch priorisieren

Für kritische Infrastrukturen (KRITIS) braucht Deutschland darüber hinaus eine klare, langfristige strategische Ausrichtung. Ziel muss sein, Abhängigkeiten von außereuropäischen Anbietern bei zentraler Software, Plattformen und Steuerungssystemen schrittweise zu reduzieren und gleichzeitig die internationale Wettbewerbsfähigkeit der betroffenen Unternehmen zu erhalten. In besonders sensiblen Bereichen sollte perspektivisch auf europäische oder deutsche Lösungen gesetzt werden. Digitale Souveränität ist dabei ähnlich strategisch zu behandeln wie Energieversorgung oder Verteidigungsfähigkeit.

Schlüsseltechnologien systematisch ausbauen und skalieren

Deutschland zählt bei den Patentanmeldungen bei der Europäischen Patentorganisation weltweit zu den führenden Nationen, hinter den USA. Diese Stärke in der Forschung und im Erfinden neuer Technologien übersetzt sich jedoch zusehends seltener in wirtschaftliches Wachstum auf dem Markt der innovationsgetriebenen Zukunftstechnologien. Genau an dieser Schnittstelle zwischen technologischer Exzellenz und marktwirksamer Umsetzung kommt Gründungen und Ausgründungen als zentrale Elemente leistungsfähiger Innovationsökosysteme eine entscheidende Rolle zu.

Doch spätestens bei der Skalierung stoßen hochinnovative Deep-Tech-Unternehmen [2] in Deutschland und Europa an ihre Grenzen. Während Europa in der Forschung aufgrund der vielfältigen Landschaft von Hochschulen und Forschungsinstituten und auch zunehmend in den frühen Gründungsphasen wettbewerbsfähig ist, fehlen häufig skalierungsfähige Kapitalmärkte, verlässliche öffentliche Ankerkunden und schnelle, umsetzungsstarke Strukturen. Unternehmen und Start-ups benötigen zudem schnellen und einfachen Zugang zu Ressourcen wie Rechenkapazitäten. Hinzu kommen fragmentierte Regulierung und Förderlandschaften innerhalb Europas sowie komplexe IP- und Genehmigungsregime, die Wachstum verzögern. In der Folge gelingt es Deutschland und Europa zu selten, das wirtschaftliche Potenzial eigener Schlüsseltechnologien vollständig zu heben – und die technologische Wertschöpfung verlagert sich dorthin, wo Kapital- und Umsetzungsgeschwindigkeit zusammenkommen.

Strategische Investitionen und Unterstützungsmaßnahmen von staatlicher Seite in Zukunftstechnologien müssen eine langfristige Hebelwirkung entfalten können. Die 2025 angelaufene Hightech Agenda der Bundesregierung setzt bereits auf die Unterstützung von sechs Schlüsseltechnologien und fünf strategischen Forschungsfeldern, um Deutschland zum führenden Standort für neue Technologien zu gestalten.

DIHK-Empfehlungen:

Schlüsseltechnologien gezielt stärken

Entscheidend für den Erfolg von Schlüsseltechnologien hierzulande sind eine frühzeitige Einbindung der Wirtschaft in Zusammenarbeit mit der Wissenschaft, klar definierte Meilensteine und wirkungsvolle Hebel beim Innovationstransfer, wie zum Beispiel im Rahmen der Roadmaps, die für die Schlüsseltechnologien entwickelt wurden. Technologiebereiche, in denen Stärken bestehen – beispielsweise dort, wo bestehende industrielle Kompetenzen systematisch mit digitalen Schlüsseltechnologien verbunden werden –, können damit auf- und ausgebaut werden. Weiterhin sollte der Blick auf Bereiche gelenkt werden, in denen Europa stark aufgestellt ist – etwa in Embedded Systems, Sensorik, industrieller Technologie und Software sowie bei Automatisierung und vernetzter Produktion oder in der Medizintechnik. KI wird zudem zentrale industrielle Branchen wie Fertigung, Maschinenbau, Automobilindustrie und industrielle Prozesssteuerung grundlegend transformieren.

Europa verfügt in diesen Bereichen über eine starke industrielle Basis, hohe Systemkompetenz und global wettbewerbsfähige Unternehmen. Eine zukunftsorientierte Strategie zur technologischen und digitalen Souveränität sollte konsequent auf diesen Stärken aufbauen, aber auch gegenüber neuen Entwicklungen technologieoffen sein, statt andere Erfolgsmodelle zu reproduzieren. Das stärkt

auch die Attraktivität des Investitionsstandortes Europa für Investitionen aus dem Ausland.

Einheitlicher europäischer Wagniskapitalmarkt für Start-ups und Scale-ups

Für ein schnelles Wachstum sind Kapitalmärkte essenziell. Nur über Wagniskapital können radikale Innovationen und schnelle Skalierungen finanziert werden. Um ein weiteres Abwandern erfolgreicher Start-ups und Scale-ups Richtung USA zu verhindern und in Europa größere Finanzierungsrunden anbieten zu können, braucht es einen einheitlichen europäischen Wagniskapitalmarkt. Vor allem in den Bereichen Mobilisierung von Kapital, Exit-Möglichkeiten und regulatorische Rahmenbedingungen gibt es in der politischen Diskussion erste Reformansätze zum Abbau der innereuropäischen Fragmentierung, die konstruktiv diskutiert und zügig beschlossen und umgesetzt werden sollten.

Europäische Technologieinfrastruktur stärken und Zugang zu Schlüsselressourcen sichern

Leistungsfähige digitale Infrastrukturen sind unverzichtbar. Dabei braucht es beides: große KI Rechenzentren wie die EU geförderten KI Gigafactories für besonders rechenintensive Anwendungen – und gleichzeitig gut ausgebaute regionale Rechenzentren, die eine flächendeckende und zuverlässige Versorgung sicherstellen.

Der Weg von der Forschung in die Praxis sollte verbessert werden, indem die Wirtschaft stärker in die Entwicklung und Umsetzung eingebunden wird. Unternehmen und Start-ups müssen daher einen einfachen und fairen Zugang zu wichtigen Ressourcen wie großer Rechenleistung haben. Dazu gehört ebenso ein niedrigschwelliger und unbürokratischer Zugang zu Forschungsinfrastrukturen. Hürden sollten daher so abgebaut werden, dass das Wissen aus der Wissenschaft schnell und unkompliziert in die Wirtschaft übertragbar ist.

Staat als Ankerkunde für Innovation und Souveränität

Als einer der größten Nachfrager kann die öffentliche Hand dazu beitragen, digitale und technologische Innovationen zur Marktreife zu bringen, Skalierung zu ermöglichen und technologische Kompetenz im Land und in Europa zu halten. Eine innovationsorientierte Beschaffung kann Nachfragesignale für Unternehmen und Start-ups und KMU setzen.

Der Staat kann zu einem gewissen Grad Pilotmärkte und Referenzen ermöglichen und den Übergang von der Entwicklung in den breiten Einsatz beschleunigen. Dabei ist immer der Wettbewerb zu wahren, zB indem mögliche Quersubventionierungen berücksichtigt werden. Investitionen in zukünftige Querschnittstechnologien sollten langfristig angelegt und an klaren Prioritäten, Meilensteinen und messbaren Hebelwirkungen ausgerichtet sein. Dabei sollte die Förderlogik im Bereich Innovation agiler sein und disruptive Innovationen und Innovationssprints fördern. Gleichzeitig dürfen strategische Ziele nach dem „Think small first"-Prinzip der EU nicht dazu führen, Vergabeverfahren komplexer zu machen und KMU über den bürokratischen Aufwand praktisch von Vergabeverfahren auszuschließen.

Forschungswissen zugänglich machen und Intellectual Property (IP)-Regeln innovationsfreundlich gestalten

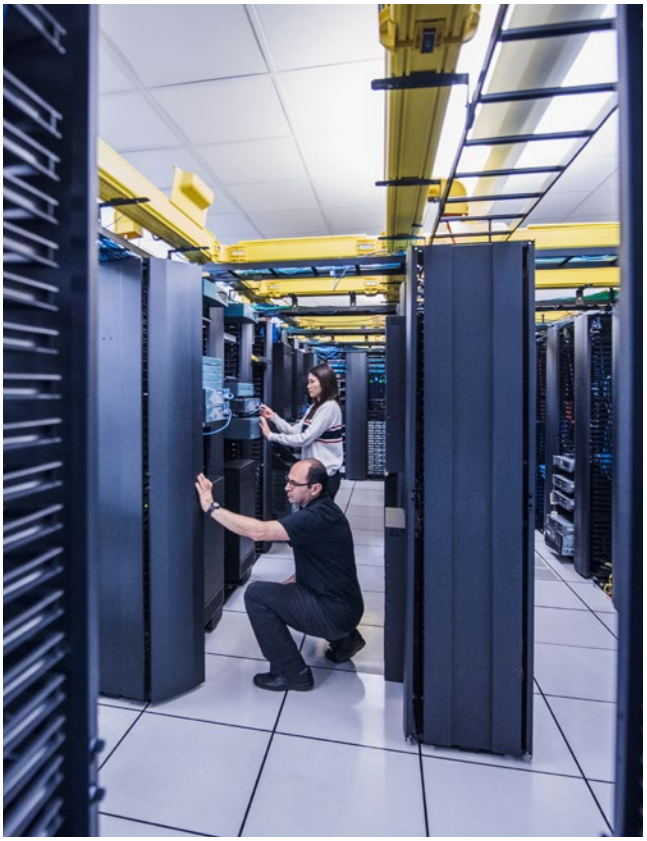
Ein modernes, transferorientiertes IPR-Regime[3] muss EU-weit einen niedrigschwelligen Zugang zu öffentlich finanzierter Forschung sichern, damit insbesondere Start-ups und KMU frühzeitig auf verwertbares Wissen, Daten und geistiges Eigentum zugreifen können. IP-Restriktionen in EU-Programmen sind dabei möglichst zu vermeiden: Geografische und zeitliche Begrenzungen sollten abgebaut und Übertragungsverbote – etwa im Europäischen Wettbewerbsfähigkeitsfonds oder im 10. EU-Rahmenprogramm für Forschung und Innovation – auf klar abschließend definierte sicherheitsstrategische Ausnahmefälle beschränkt werden.

Stattdessen sollten qualitative Kriterien und resilienzorientierte Bewertungen für europäische IPs gestärkt werden. Zudem sollte die Nutzung geistiger Eigentumsrechte als Finanzierungssicherheit ermöglicht werden, um insbesondere kapitalschwachen, forschungsintensiven Unternehmen den Zugang zu Innovationsfinanzierung und EU-Förderprogrammen zu erleichtern, auch wenn die Bewertung immaterieller Vermögenswerte herausfordernd bleibt.

Infrastrukturausbau beschleunigen und Energiepreise senken

Eine leistungsfähige digitale Infrastruktur ist eine zentrale Voraussetzung für Wettbewerbsfähigkeit, technologische Souveränität und Resilienz. Sie bildet die Grundlage für Cloud- und Edge-Computing, KI, Daten-Ökosysteme, vernetzte industrielle Prozesse sowie auch digitale Lieferketteninfrastrukturen oder Logistikplattformen. Mit fortschreitender Digitalisierung steigt der Bedarf an leistungsfähigen Netzen, Rechenzentren und Rechenkapazitäten deutlich. Auch der erfolgreiche Übergang von der Forschung zur Quantentechnologie in die Praxis wird nur mit leistungsfähiger digitaler Infrastruktur gelingen.

Frankfurt am Main hat durch seine zentrale Lage und die gute Infrastruktur rund um den Internetknoten DE-CIX einen klaren Vorteil für Rechenzentren: Daten können dort besonders schnell übertragen werden, weil die Verbindungen kurze Wege und geringe Verzögerungen haben. Deutsche Unternehmen profitieren so von schnelleren und



stabileren Datenverbindungen, etwa bei Cloud Diensten, digitalen Geschäftsprozessen oder datenintensiven Anwendungen wie KI. Gleichzeitig bieten auch andere Regionen gute Bedingungen für Rechenzentren und stellen wichtige Standorte dar, beispielsweise durch Verfügbarkeit erneuerbarer Energie.

Demgegenüber stehen strukturelle Standortnachteile in Deutschland, die den Ausbau von Rechenzentren und anderen digitalen Infrastrukturen bremsen. Hohe Strompreise können den wirtschaftlichen Einsatz von KI und datengetriebenen Anwendungen einschränken. Hinzu kommen fehlende geeignete Flächen für Rechenzentren oder Mobilfunkmasten, fehlende Stromnetzanschlüsse sowie lange und komplexe Planungs- und Genehmigungsverfahren. Kommunen sind häufig nicht ausreichend ausgestattet, um entsprechende Projekte zügig umzusetzen. Unter anderem begrenzte Kapazitäten in Energie-Netzgebieten erschweren es erheblich, überhaupt geeignete Flächen für neue Rechenzentren zu finden. Diese Faktoren verzögern Investitionen und verhindern schnelle Skalierung.

DIHK-Empfehlungen:

Wettbewerbsfähige Preise für Rechenzentren sichern

Souveräne Rechen- und KI-Kapazitäten erfordern international wettbewerbsfähige Stromkosten. Die Bundesregierung sollte Umlagen in den Bundeshaushalt übernehmen, die Stromsteuer auf das EU-Mindestmaß senken und grüne Direktstromlieferverträge (PPAs) erleichtern. Praktikable Rahmenbedingungen sollten die sinnvolle Nutzung von Abwärme ermöglichen, anstatt unwirtschaftliche Netzanbindungen zu erzwingen.

Planungs- und Genehmigungsverfahren für digitale Infrastrukturen grundlegend beschleunigen

Der Ausbau von Rechenzentren und Energienetzen sowie von Glasfaser- und Mobilfunknetzen wird häufig durch lange Genehmigungsprozesse gebremst. Verfahren sollten bundesweit standardisiert, digitalisiert und beschleunigt werden. Es sollten ausreichend geeignete Flächen etwa für Rechenzentrumsstandorte oder Mobilfunkmasten zur Verfügung stehen. Dafür braucht es eine grundlegende Reform des Planungs- und Genehmigungssystems statt punktueller Priorisierungsgesetze. Öffentliche Liegenschaften bei topografischen Gegebenheiten sind systematisch für Mobilfunkstandorte zu nutzen und eine nationale Koordinierung von Rechenzentren-Standorten ist erforderlich.

Kritische Rohstoffe strategisch sichern

Eine sichere und resiliente Rohstoffversorgung ist eine Grundvoraussetzung für digitale Souveränität. Alle technischen Innovationen und kritischen Technologien wie KI, Quantum oder Cloud, benötigen eine physische Infrastruktur, z. B. Halbleiter für Rechenzentren. Diese Infrastruktur beruht auf der Verfügbarkeit von kritischen Rohstoffen, wie Gallium, Germanium, Seltenen Erden oder auch Silizium. Deutschland und Europa sind besonders in diesen Bereichen stark von wenigen Drittstaaten abhängig. Dies gilt auch für Komponenten wie moderne und leistungsstarke Chips. Diese wirtschaftlichen Abhängigkeiten werden mit den zunehmenden geopolitischen Spannungen von Drittstaaten als Druckmittel missbraucht. Konflikte, wie zuletzt im Nahen Osten mit seinen Auswirkungen auf die Heliumversorgung, zeigen, wie anfällig zentrale Lieferketten der Halbleiterfertigung sind. Eine resilientere europäische Elektronik- und Komponentenbasis ist ein wesentlicher Bestandteil digitaler Souveränität.

DIHK-Empfehlungen:

Strategischen Ansatz bei Rohstoffpartnerschaften verfolgen

Kritische Abhängigkeiten lassen sich international nur mit Partnern lösen. Deutschland sollte weniger national und mehr europäisch oder multilateral agieren und sich stärker an EU-Initiativen oder internationalen Rohstoffallianzen beteiligen. Bei Abkommen mit rohstoffreichen

Ländern sollte die Wirtschaft von Beginn an eingebunden sein, damit sichergestellt ist, dass wirtschaftliche Bedarfe, auch mit Blick auf die kritischen Zukunftstechnologien, Berücksichtigung finden. Wichtig ist, dass solche Partnerschaften mit konkreten Projekten mit der Industrie unterlegt werden.

Rahmenbedingungen für Rohstoffförderung, Weiterverarbeitung und Wiedergewinnung in der EU verbessern

Deutschland und Europa sind nicht arm an mineralischen Rohstoffen, diese werden jedoch kaum erkundet, gefördert und ausgeschöpft. Es braucht bessere Rahmenbedingungen, schnellere Genehmigungsverfahren, zugänglichere Finanzierungsangebote und eine verbesserte öffentliche Wahrnehmung von Projekten.

Auch die Weiterverarbeitung von kritischen Rohstoffen bis hin zu finalen Produkten wie modernste Halbleiter muss gestärkt werden. Neben Förderung und Weiterverarbeitung sollte Europa die Rückgewinnung kritischer Rohstoffe konsequent fördern. Dazu sind verbesserte Prozesse vorgesehen, etwa beim Critical Raw Materials Act, RESourcEU oder beim EU-Chips Act. Diese gilt es zeitnah zu implementieren.

Strategische Reserven

Die von der EU-Kommission im Zuge der Lagerhaltungsstrategie angestrebte Bevorratung durch das in 2026 gegründete Critical Raw Materials Centre ist kritisch zu bewerten. Obwohl die strategische Bevorratung einen Mehrwert für die Unternehmen und die Resilienz bieten kann, würde eine staatliche Lagerhaltung in erster Linie zu zusätzlichen Preisspitzen führen, ohne die Versorgungslage der Wirtschaft signifikant zu verbessern. Zudem ist bereits die Bedarfsermittlung für kritische Rohstoffe schwierig, da Stücklisten wenig über den von den Unternehmen benötigten Verarbeitungszustand aussagen.

Stattdessen sollte geprüft werden, inwiefern die EU in bestimmten Bereichen Einkaufsgesellschaften zur Bündelung der Nachfrage, gemeinsam mit Partnern wie den G7-Staaten, organisieren kann. Um die Auswirkungen von Versorgungslücken zu minimieren, haben viele Unternehmen bereits ihre Lagerhaltung ausgebaut. Die Bundesregierung sollte prüfen, was Firmen an einer eigenständigen Bevorratung hindert bzw. diese einschränkt. Beispielsweise erschwert die vom Bundesministerium der Finanzen beschlossene und im April 2026 eingeführte Änderung der Besteuerung der Zollfreilager die Bevorratung.

Souveränes Europa: Rule maker statt rule taker

Digitalpolitik ist zunehmend Machtpolitik. In einer globalen Ordnung, die von geopolitischen Rivalitäten und technologischen Abhängigkeiten geprägt ist, entscheidet die Fähigkeit zur Setzung von Regeln, Normen und Standards über wirtschaftliche Handlungsspielräume und politische Gestaltungsmacht. Für die Europäische Union ist digitale Souveränität daher keine rein technologische Frage, sondern eine zentrale Voraussetzung, um als eigenständiger und handlungsfähiger Akteur im internationalen digitalen Ordnungsgefüge zu agieren.

Die fortschreitende Fragmentierung des digitalen Raums erhöht die strategische Bedeutung von Normen und Standards weiter. Internationale Standards prägen technologische Entwicklungspfade, definieren Marktanforderungen und beeinflussen langfristig Wertschöpfungsketten und Wettbewerbsfähigkeit. Während europäische Normen weltweit häufig als Qualitäts- und Vertrauensmaßstab gelten, verschärft sich der internationale Wettbewerb um ihre Setzung insbesondere in Zukunftsfeldern wie KI, vernetzter Industrie oder digitaler Infrastruktur. Kooperationen über Handels- und Digitalabkommen sind dabei ein zentrales Instrument zur Verbreitung europäischer Regeln und zur Sicherung offener, regelbasierter digitaler Räume.

DIHK-Empfehlungen:

EU-Einsatz für weltweite digitale Vernetzung und Diversifizierung

Datengetriebene Innovationen sind auf funktionierende, grenzübergreifende Datenflüsse angewiesen. Digitale Diskriminierung und Marktabschottung für europäische Waren und Dienstleistungen sollten weltweit zurückgedrängt werden.

Durch die Wiedereinsetzung des WTO-Moratoriums für Zölle auf digitale Übertragungen sollte Unternehmen weltweit Planungssicherheit zurückgegeben werden. Plurilaterale und bilaterale Abkommen sind bei mangelndem internationalen Konsens gangbare Alternativen. Hierfür sollte die EU ihr Netz an Handelsabkommen mit Digitalkapiteln sowie an Digitalabkommen weltweit mit relevanten Handelspartnern ausbauen. Wichtig ist bei diesen Abkommen der Einsatz für globale interoperable und offene Standards, um strategischen digitalen Abhängigkeiten vorzubeugen. EU als Rule Maker statt Rule Taker für die Weltstandards von morgen

Für die EU ist es wichtig, gemeinsam mit ihren Partnern die Ausgestaltung internationaler Digitalstandards mitzubestimmen und ihre eigenen Lösungsansätze international zu bewerben. Große Bedeutung kommt dabei dem Datenschutz zu. Der Datenschutz muss internationaler ausgestaltet, um- und durchgesetzt werden. Hierfür sollte sich die Bundesregierung für eine Europäisierung der Aufsichtsstrukturen einsetzen, damit die EU mit einem harmonisierten, effizienten Datenschutzraum eine stärkere Position in internationalen Verhandlungen erlangt. Die Bundesregierung sollte außerdem für EU-Adäquanzentscheidungen für vertrauensvolle Partner werben.

Deutschland sollte zudem sein Engagement in internationalen Foren und Organisationen wie dem Internet Governance Forum (IGF) und der International Telecommunication Union (ITU) ausbauen.

Europäisches Normungssystem beschleunigen, ohne seine Stärken zu gefährden

Die Überarbeitung der EU-Normungsverordnung sollte genutzt werden, um das europäische Normungssystem schneller und reaktionsfähiger zu machen. Dabei müssen die bewährten Grundprinzipien – breite Beteiligung, hohe Qualität sowie transparente und konsensbasierte Verfahren – erhalten bleiben. Insbesondere die Annahme von Normungsaufträgen, die Veröffentlichung harmonisierter Normen und der Prüfprozess durch HAS-Consultants[4] sollten effizienter und planbarer gestaltet werden; digitale Instrumente sind konsequent zur Beschleunigung zu nutzen.

Internationale Normungsarbeit deutscher und europäischer Unternehmen gezielt stärken

Um den europäischen Einfluss in internationalen Normungsgremien zu sichern, sollte das Engagement von Unternehmen – insbesondere von KMU – finanziell und organisatorisch unterstützt werden. Nur so kann sichergestellt werden, dass europäische technologische Stärken und Marktinteressen in globalen Standards angemessen berücksichtigt werden und nicht durch andere Akteure verdrängt werden.

Industriespionage und Cyberkriminalität auch international bekämpfen

Die Bundesregierung sollte den Unternehmen Handlungsempfehlungen unterbreiten und sich weltweit sowie in internationalen UN-Gremien für den Kampf gegen Cybercrime und Industriespionage einsetzen. Um internationale Cyberkriminalität besser zu bekämpfen, braucht es ein System von Regeln im internationalen Cyberspace, an dem sich möglichst viele Staaten beteiligen. Es gilt, die Kooperation mit internationalen Sicherheitsbehörden zu verstärken und dem UN Cybercrime Treaty mehr Aufmerksamkeit zu widmen.

Marktprinzip wahren, Abhängigkeiten gezielt reduzieren

Die Wirtschaft steht staatlichen Vorgaben wie „Buy European" grundsätzlich kritisch gegenüber, da Entscheidungen

über Technologien und Anbieter möglichst im Wettbewerb getroffen werden sollten. Zusätzliche Auflagen, bürokratische Ursprungsnachweise oder Nachweise zur Eigentümerstruktur sowie potenzielle Gegenreaktionen von Handelspartnern belasten vor allem kleine und mittelständische Unternehmen. Gleichzeitig wächst angesichts geopolitischer Risiken die Bereitschaft vieler Unternehmen, gezielt auf europäische Anbieter und Technologien zu setzen, um Abhängigkeiten zu verringern – vor allem bei kritischen Infrastrukturen und Aspekten, die die digitale Resilienz betreffen wie sensible Daten, Cloud-Dienste und sicherheitsrelevante IT-Komponenten. Ein ähnliches Bild zeigt sich im digitalen Zahlungsverkehr, wo viele Länder des Euroraums für die technische Durchführung und Abwicklung von digitalen Zahlungen auf außereuropäische Unternehmen angewiesen sind. Den digitalen Euro, sofern dieser eingeführt werden sollte, und europäische privatwirtschaftliche Initiativen sollte man zum Aufbau einer unabhängigen europäischen Zahlungsinfrastruktur nutzen.

Wenn in sicherheitsrelevanten digitalen Infrastrukturen europäische Anbieter bevorzugt werden sollen – zum Beispiel beim Ausschluss von Drittstaaten-Anbietern oder bei Vorgaben zur Datenverarbeitung – sollten klare, eng begrenzte Kriterien dafür definiert werden. Die Eingriffe sollten gut begründet sein und sich auf wirklich sensible Bereiche beschränken. Um alternative eigene Technologien aufzubauen, sind gezielte Förderprogramme oder Initiativen wie IPCEI[5] oft wirksamer als starre Vorgaben. Die Vermeidung von Vendor-Lock-In sollte durch die Schaffung von alternativen Modellen oder Anbietern begünstigt werden. Werden ganze Sektoren als strategisch eingestuft, sollte sich Regulierung auf klar definierte, sensible Komponenten beschränken und eng mit Wirtschafts- und Sicherheitsexperten abgestimmt sein, um Wettbewerbsnachteile entlang der Wertschöpfungsketten zu vermeiden. Es sollten Möglichkeiten geprüft werden, wie KMU in Praxis noch stärker an EU-Programmen wie IPCEI partizipieren können.

Digitale Kompetenzen systematisch aufbauen

Die DIHK-Digitalisierungsumfrage hat einmal mehr gezeigt: Digitale Kompetenzen sind eine zentrale Voraussetzung für Wettbewerbsfähigkeit und digitale Souveränität. Die berufliche Aus- und Weiterbildung bildet eine tragende Säule der digitalen Souveränität, da sie digitale Kompetenzen praxisnah, arbeitsmarktorientiert und technologieoffen vermittelt und so Resilienz und Innovationsfähigkeit von Wirtschaft und Beschäftigten stärkt. Ergänzend kommt Schulen und Hochschulen eine Schlüsselrolle zu, die digitale Souveränität institutionell verankern und Digital- sowie KI-Kompetenzen flächendeckend in Curricula integrieren können.

Die digitale Bildungsinfrastruktur ist bislang stark von Anbietern aus Drittstaaten geprägt, während vertrauenswürdige europäische Lösungen für Bildungsdaten, Lernsysteme sowie Identitäts- und Bezahldienste fehlen. Moderne, interoperable und sichere Infrastrukturen sowie qualifiziertes Personal – perspektivisch unterstützt durch einen europäischen Bildungsdatenraum – sind daher entscheidend, um Fachkräftemobilität und digitale Souveränität nachhaltig zu stärken.

DIHK-Empfehlungen:

Digitale Kompetenzen und KI-Know-how systematisch in Bildung verankern

Digitale Souveränität erfordert, dass KI-Kompetenzen flächendeckend in den Curricula von Schulen, beruflichen Schulen und Hochschulen verankert werden. Dies sollte im Gleichklang mit den europäischen Partnern erfolgen, damit digitale Kompetenzen verbessert grenzüberschreitend genutzt werden und erfolgreiche Modelle leichter in anderen Mitgliedstaaten Anwendung finden können. Bund und Länder sollten die Aus- und Weiterbildung von Lehrkräften in den Bereichen Digitalisierung und KI gezielt stärken. Dazu gehören insbesondere die praxisnahe Qualifizierung im Einsatz konkreter KI Werkzeuge (z.B. zur Unterrichtsvorbereitung, zur rechtskonformen Leistungsbewertung und individuellen Förderung) sowie der systematische Zugang zu und die didaktische Nutzung geeigneter KI Werkzeuge im Unterrichtsalltag, damit technologische Entwicklungen didaktisch fundiert und auf Augenhöhe mit der betrieblichen Praxis vermittelt werden können. So bleibt unser Bildungssystem anschlussfähig an den digitalen Wandel der Wirtschaft.

KI-Kompetenz im Wirtschaftsleben festigen

Wachstum und die Wettbewerbsfähigkeit der europäischen Wirtschaft werden auch davon abhängen, wie schnell KI-Kompetenz in der Erwerbsbevölkerung verbreitet und professionalisiert werden kann. Berufliche Weiterbildung

und KMU-Beratung spielen hier eine wesentliche Rolle, um KI-Kompetenzen auf die jeweiligen betrieblichen Bedarfe zu fokussieren und so Produktivitätsgewinne zu erzielen und neue Geschäftsmodelle zu entwickeln.

Dafür muss die Umsetzung des gesetzlichen Auftrags an Betriebe, die mit der Nutzung von KI-Systemen befassten Mitarbeitenden ausreichend zu schulen und zu sensibilisieren (Art. 4 der KI-VO), einen Mindeststandard erfüllen, der alle Beschäftigten in die Lage versetzt, mit KI-Anwendungen erfolgreich umzugehen sowie eine fundierte menschliche Letztentscheidung treffen zu können. Ein solcher Mindeststandard muss stets offen für technologische Weiterentwicklungen sein.

Zeitgemäße digitale Bildungsinfrastruktur flächendeckend sicherstellen

Bund und Länder müssen allen beruflichen Schulen ausreichende Mittel für eine moderne, sichere und leistungsfähige digitale Infrastruktur bereitstellen. Dazu gehören leistungsfähige und stabile Breitband-Internetverbindungen, branchenübliche und interoperable Software, berufstypische technische Endgeräte sowie qualifiziertes Personal für Betrieb und Weiterentwicklung dieser Infrastruktur. Nur mit einer solchen Ausstattung kann digitale Souveränität im Bildungsbereich praktisch umgesetzt werden.

Europäische Lernplattformen und KI-Anwendungen stärken

Die Abhängigkeit von außereuropäischen Anbietern im Bildungsbereich sollte reduziert werden, indem alternative interoperable europäische Lernplattformen, vertrauenswürdige Lösungen für Bildungsdaten, digitale Lernsysteme und Identitätsdienste gezielt gestärkt werden. Gleichzeitig sollte die Bundesregierung darauf hinwirken, dass insbesondere kleine und mittelständische Ausbildungsbetriebe bei der Nutzung und Anpassung von in der EU entwickelten und trainierten KI-Anwendungen unterstützt werden. KI sollte dabei – auch mit Blick auf den EU-AI-Act – als strategisches Entwicklungsfeld für europäische Anbieter und Anwender genutzt werden, um international wettbewerbsfähig zu bleiben.

[1] Siehe u. a. **Digitalisierungsumfrage 2026: Trends und Erkenntnisse für Unternehmen**

[2] Unter Deep Tech werden grundlegende, wissenschafts- und forschungsbasierte Spitzentechnologien wie KI, Quantentechnologien, Biotechnologie oder Robotik, verstanden, die tiefgreifende industrielle Transformationen ermöglichen. Sie gelten als zentrale Treiber für zukünftige Wertschöpfung, Wettbewerbsfähigkeit und technologische Souveränität.

[3] Ein IPR-Regime bezeichnet den rechtlichen und institutionellen Rahmen, der den Schutz, die Nutzung und die Durchsetzung geistiger Eigentumsrechte wie Patente, Marken oder Urheberrechte regelt. In Innovations- und Wirtschaftskontexten beschreibt der Begriff häufig die Gesamtheit nationaler und internationaler Regelungen, die Einfluss auf Technologietransfer, Skalierung und Verwertung von Innovationen haben.

[4] HAS-Consultants (Harmonised Standards Consultants) sind unabhängige, von der Europäischen Kommission beauftragte Expertinnen und Experten, die prüfen, ob europäische Normen den Vorgaben der EU-Gesetzgebung und den jeweiligen Normungsaufträgen entsprechen. Ihre Bewertungen sind eine zentrale Voraussetzung dafür, dass harmonisierte Normen im Amtsblatt der EU veröffentlicht werden und rechtliche Wirkung entfalten.

[5] IPCEI (Important Projects of Common European Interest) sind paneuropäische Kooperationsprojekte in strategischen Schlüsseltechnologien, die einen klaren europäischen Mehrwert schaffen und Innovationsfähigkeit sowie Wettbewerbsstärke der EU nachhaltig stärken sollen.