WIRTSCHAFTS
FORUM
DER SPD E.V.

Digitalagenda 2030

Maßnahmen und Handlungsfelder im Bereich Digitalisierung für eine neue Bundesregierung in der neuen Legislaturperiode

Ein Positionspapier des
Wirtschaftsforums der SPD e.V.

Inhaltsverzeichnis

1. **Einleitung** 4
2. **Leistungsfähige digitale Infrastrukturen** 5
   - Frequenzpolitik gestalten 5
   - Mobilfunkausbau vorantreiben 5
   - Breitbandausbau neudenken 6
   - Gesamtstrategie für Rechenzentren entwickeln 6
3. **Digitale Schlüsseltechnologien** 7
   - Künstliche Intelligenz: Klarheit schaffen, Innovation fördern, Sicherheit gewährleisten 7
   - Schlüsseltechnologien und Technologietransfer fördern 8
4. **Datenwirtschaft** 10
   - Rechtliche Rahmenbedingungen harmonisieren 10
   - Datennutzung verbessern 10
   - Investitionen in Datenräume stärken 11
   - Digitale Betriebsanleitung ermöglichen 11
5. **Cybersicherheit** 12
   - Rechtsrahmen und praxisnahe Umsetzung harmonisieren 12
   - Praxisorientierte Umsetzung sicherstellen 13
   - Desinformation entgegensteuern 14
6. **Digitalisierung und Modernisierung der Verwaltung** 15
   - Verwaltungsprozesse effizient und zukunftssicher machen 15
   - Moderne IT-Infrastruktur und Standards etablieren 16
7. **Maßnahmenpaket konsequent und schnell umsetzen** 18

1. Einleitung

Die digitale Transformation in Deutschland muss endlich den Stellenwert erlangen, der ihr ökonomisch, innovations- und standortpolitisch zukommen muss. Die Standortqualität, die Wettbewerbsfähigkeit, die Innovationsfähigkeit, das Potenzialwachstum, die Steigerung der Produktivität der Unternehmen wird entscheidend davon abhängen, ob und wie schnell es gelingt den Digitalisierungsgrad und die Nutzung von digitalen Technologien in Industrie, Dienstleistungen und dem staatlichen Sektor zu realisieren. **Zukünftiges Wachstum und Beschäftigung sowie Wettbewerbsfähigkeit wird es für die Unternehmen und den Standort Deutschland ohne eine beschleunigte Digitalisierung nicht geben.**

Dazu muss es in der neuen Bundesregierung eine kohärente politische Digitalstrategie mit klaren Strukturen, Verantwortlichkeiten und einem eigenständigen Budget geben, die den Digitalisierungsgrad und -geschwindigkeit deutlich erhöhen. Der Teil der Bundesnetzagentur, der sich mit Digitalisierung und Telekommunikation auseinandersetzt, wird zu einer eigenständigen Digitalagentur entwickelt, die neben regulatorischen und technischen Fragen, zu einem Kompetenzzentrum weiterentwickelt, das die Arbeit der Bundesregierung unterstützt. Zudem bedarf es einer starken Umsetzungseinheit des Bundes.

Der Ausbau der digitalen Infrastruktur muss schneller und entschiedener vorangetrieben werden. 5G und Glasfasernetze müssen zum Standard überall in Deutschland werden.

Zudem ist eine digitale Industriepolitik erforderlich, die Schlüsseltechnologien und Wachstumsmärkte wie Halbleiter, Green-Energy-Technologien, Quanten- und Automatisierungstechnologien, Medizintechnik, Deep Tech, Robotik, 6G oder industriellen KI-Anwendungen vorantreibt sowie ein Ökosystem mit entsprechenden Instrumenten aufbaut, das endlich eine Wachstumsfinanzierung für deutsche Startups auf den Weg bringt, die eine Abwanderung oder den Aufkauf dieser Unternehmen möglichst verhindert. Diese industriepolitische Ausrichtung sollte auch im Rahmen von Vergabeverfahren Berücksichtigung finden.

Ein wesentlicher Punkt ist dabei eine zukunftsorientierte Datenpolitik, denn die Nutzung von Daten ist der Schlüssel für Innovationen, neue Geschäftsmodelle und virtuelle Wertschöpfungsketten.

Der Staat darf nicht weiter Schlusslicht bei der Digitalisierung in Deutschland bleiben. Nur durch Digitalisierung können die Leistungsfähigkeit und die Bürgerfreundlichkeit der öffentlichen Verwaltung, damit deren Akzeptanz verbessert und für Unternehmen Genehmigungsverfahren beschleunigt werden.

Die digitale Transformation macht gezielte Qualifikation und Weiterbildung erforderlich. Dies muss zur Pflichtaufgabe sowohl in den Unternehmen als auch im öffentlichen Dienst werden. Digitale Kompetenzen müssen bereits in der schulischen Ausbildung aufgebaut werden.

In Europa muss es darum gehen, die Vielzahl von digitalpolitischen Rechtsakten im Hinblick auf eine sich überlappende Gesetzgebung, die Innovationen und die Nutzung digitaler Technologien erschwert oder sogar verhindert, einzuschränken. Gut gemeint ist nicht gut gemacht – deswegen muss es auch in Europa zu einer umfassenden Re-Evaluation des Rechtsrahmens kommen. Regulatorische Inkohärenzen und Doppelregulierungen gilt es entsprechend abzubauen.

2. Leistungsfähige digitale Infrastrukturen

Eine leistungsfähige digitale Infrastruktur ist das Rückgrat einer modernen und wettbewerbsfähigen Volkswirtschaft. Sie bildet die Grundlage für Innovation, Teilhabe und wirtschaftliches Wachstum. Obgleich in der letzten Legislaturperiode enorme Fortschritte bei der 5G-Netzabdeckung erreicht wurden, bildet Deutschland bei der Versorgung mit Glasfaseranschlüssen (FTTB/FTTH) eines der Schlusslichter in der EU. Die folgenden Forderungen skizzieren zentrale Maßnahmen, um gezielte Investitionen in digitale Infrastruktur zu fördern und die Technologieführerschaft zu verbessern.

Frequenzpolitik gestalten

- Es ist essenziell, eine investitions- und technologiefreundliche Frequenzpolitik zu fördern, insbesondere im Hinblick auf die Entwicklung von 6G und Open-RAN. Dies schließt eine flexible und bedarfsgerechte Vergabe von Frequenzen ein, um Unternehmen die Planungssicherheit zu geben, die sie für die Entwicklung und Implementierung neuer Technologien benötigen.

- Nicht genutzte oder nicht ausgeschöpfte Frequenzen müssen effizienter genutzt werden, um Ressourcen optimal einzusetzen. Gleichzeitig sollte Deutschland aktiv die notwendige Koordination der Frequenzpolitik auf internationaler Ebene fördern.

- Die Verlängerung der Frequenznutzungsrechte, die Aussetzung von Auktionen sind notwendig, um Investitionskapital im Markt zu erhalten und Innovation zu fördern.

Mobilfunkausbau vorantreiben

- Die Entscheidung, den Mobilfunkausbau als »überragendes öffentliches Interesse« einzustufen, ist absolut richtig. Es gilt, bürokratische Hürden abzubauen und Verfahren zu vereinfachen, um den Ausbau zu beschleunigen.

- Für Mobilfunkstandorte sollte eine verpflichtende Anbindung an das Stromnetz geschaffen werden, um deren Betrieb sicherzustellen.

- Die Einführung einer bundesweiten Genehmigungsfiktion im Baurecht für Mobilfunkmasten ist notwendig, um Genehmigungsverfahren zu vereinfachen und zu beschleunigen.

- Das Mitnutzungspotenzial bestehender Mobilfunkstandorte muss ausgeschöpft werden: Um beurteilen zu können, ob ein Standort für zusätzliche Funkanlagen geeignet ist und entsprechende Baumaßnahmen realisiert werden können, ist es entscheidend, den investierenden Unternehmen umfassende Transparenz über die vorhandene behördliche Datenlage der Immissionswirkungen zu ermöglichen.

Breitbandausbau neudenken

- Die bisherige Strategie zum Breitbandausbau zeigt sich als nicht zielführend. Anstatt eines Doppelausbaus muss der Zugang verschiedener Anbieter von Telekommunikationsdiensten zu bestehenden Glasfasernetzen zu marktgerechten Preisen erfolgen, um die Infrastruktur effizienter zu nutzen, den Wettbewerb und damit attraktivere Preise für Endkunden zu fördern und somit die Akzeptanz und Nutzung von Glasfaser zu erhöhen. Auch die Kupfer-Glas-Migration sollte diskriminierungsfrei, wettbewerbskonform und verbraucherfreundlich erfolgen.

- Funkbasierte Technologien wie Mobilfunk und Satelliten sollten als Übergangslösungen genutzt werden, um digitale Teilhabe zu gewährleisten. Sie bieten eine schnelle und flexible Möglichkeit, insbesondere in unterversorgten Regionen eine Grundversorgung mit digitalen Diensten sicherzustellen, bis dauerhafte Infrastrukturen aufgebaut sind.

- Die staatlich finanzierte Förderung des Netzausbaus weiterhin nur dort eingesetzt werden, wo ein eigenwirtschaftlicher Ausbau aufgrund fehlender wirtschaftlicher Abbildbarkeit auch langfristig nicht erfolgen wird.

Gesamtstrategie für Rechenzentren entwickeln

- Deutschland sollte proaktiv die Ansiedlung von energieeffizienten Rechenzentren fördern, da sie essenzielle Infrastruktur für Cloud- und KI-Lösungen sowie die Digitalisierung insgesamt sind. Die neue Bundesregierung wird aufgefordert eine Gesamtstrategie für den Aufbau energieeffizienter Rechenzentren in Deutschland zu entwickeln und die Rahmenbedingungen für eine zielgerichtete Umsetzung vorzulegen.

3. Digitale Schlüsseltechnologien

Digitale Schlüsseltechnologien bieten Deutschland und Europa eine unverzichtbare Möglichkeit, technologiegetriebenes Wachstum zu fördern und die internationale Wettbewerbsfähigkeit langfristig zu sichern. Sie bilden dabei die Grundlage für Innovation, wirtschaftliche Wettbewerbsfähigkeit und technologische Souveränität. Sie treiben nicht nur die Entwicklung zentraler Zukunftsbereiche wie KI, Cloud-Infrastrukturen und High-Tech-Industrien voran, sondern stärken auch die Resilienz in einer zunehmend vernetzten Welt. Digitale Schlüsseltechnologien sind für den Aufbau eines Halbleiter-Ökosystems oder die Fortschritte im Bereich des autonomen und vernetzten Fahrens von grundlegender Relevanz.

Um im globalen Wettbewerb zu bestehen, müssen Deutschland und Europa strategische Investitionen vorantreiben, innovationsfreundliche Rahmenbedingungen schaffen und eine leistungsstarke Forschungs- und Transferlandschaft fördern. Dies erfordert gezielte Maßnahmen zur Entwicklung digitaler Kompetenzen, die Beseitigung bürokratischer Hürden und eine konsequente Förderung von Innovationen, um eine nachhaltige und souveräne digitale Zukunft zu sichern.

Künstliche Intelligenz: Klarheit schaffen, Innovation fördern, Sicherheit gewährleisten

- Deutschland sollte auf einen EU-Rechtsrahmen hinarbeiten, der Kohärenz, Sicherheit und die praktische Anwendung von KI fördert. Zusätzliche KI-spezifische Regulierungen sollten sorgfältig geprüft werden, um unnötige Hürden, sich überlappende Regulierung und Doppelstrukturen zu vermeiden. Um schlanke Strukturen und klare Verantwortlichkeiten sicherzustellen, ist auf bestehenden, sektorspezifischen Aufsichten aufzubauen. Die Kombination aus risikobasierten Vorschriften und flexiblen Selbstverpflichtungen bietet die Möglichkeit, sowohl Sicherheitsstandards zu wahren als auch Innovationskraft in einem sich schnell entwickelnden Technologiefeld wie der KI zu stärken.

- Die Industrie wird in Zukunft einen großen Teil der Wertschöpfung mithilfe von KI erwirtschaften. Daher müssen Leitlinien zur Auslegung der Vorschriften aus dem europäischen AI Act müssen zeitnah klargestellt werden, um Unternehmen rechtliche Sicherheit bei der Produktentwicklung zu bieten. Dies ist insbesondere im Zusammenspiel mit anderen regulatorischen Vorgaben wie der Maschinen- oder Medizinprodukte-Verordnung oder den Vorgaben für Finanzdienstleistungen entscheidend. Zudem dürfen die zusätzlichen Leitlinien (bzw. auch delegierte Rechtsakte) nicht über den eigentlichen Regelungsgehaltes des AI Actes hinausgehen und etablierte statische Verfahren und einfache Algorithmen, die keine Form des maschinellen Lernens oder der Selbstoptimierung enthalten, als KI einstufen. Die Klärung der Verantwortlichkeiten in KI-Systemen ist dringend erforderlich; die Rolle der Maschinenhersteller, KI-Entwickler und Unternehmen als Anwender sollte klar differenziert werden. Es sollte zudem auch auf eine strikte Harmonisierung in den 27 Mitgliedstaaten geachtet werden.

- Ein konsistentes und zuverlässiges Umfeld für die Entwicklung von KI ist unerlässlich. Deutschland sollte eine aktive Rolle in der globalen KI-Governance übernehmen und kann somit einen Beitrag zur Schaffung sicherer und vertrauenswürdiger KI und einheitlicher Standards leisten.

- Ein eigenes KI-Sicherheitsinstitut dient der Institutionalisierung von KI-Forschung und der Beratung von Politik, Behörden und Anwendern. Die neue Bundesregierung wird aufgefordert ein solches Institut schnell auf den Weg zu bringen, im Zusammenhang mit dem Aufbau einer Digitalagentur. Die Digitalagentur soll Kompetenzen aufbauen und bündeln und im Bereich KI-Sicherheit mit den Datenschutzbeauftragten zusammenarbeiten.

Schlüsseltechnologien und Technologietransfer fördern

- Die effektive Entwicklung sicherer und vertrauenswürdiger KI-Systeme erfordert eine enge Kooperation und die Verbesserung des Technologietransfers zwischen Unternehmen, Regierungen und Forschungseinrichtungen. Diese Partnerschaften können Standards und Best Practices schaffen, die Innovationen fördern und gleichzeitig Sicherheitsbedenken adressieren.

- Insgesamt müssen digitale Schlüsseltechnologien in Deutschland konsistent, zielgerichtet und effizient entwickelt und gefördert werden. Dazu gehören Quantentechnologien, Mikro- & Nanoelektronik, digitale Zwillinge und Simulationstechnologien, Konnektivität, 5G & 6G, Cybersicherheit. Dazu muss eine digitale Industriepolitik, die ein intelligentes Zusammenspiel von staatlicher Förderung und unternehmerischen Initiativen und Projekten befördert, entwickelt werden und mit entsprechenden Instrumenten für F&E-Ausgaben, Investitionen und dem Aufbau digitaler Ökosysteme in diesen Bereichen ausgestattet werden. Dazu gehört vor allem auch eine stärkere Abstimmung, Koordination und Konzentration der politischen Maßnahmen der unterschiedlichen Ministerien der Bundesregierung.

- Standardisierung ist dabei eine Schlüsselaufgabe, um im internationalen Wettbewerb bestehen zu können. In diesem Kontext sollten Aktivitäten von Unternehmen in internationalen Gremien zu diesem Thema eine steuerliche Anrechnung der Kosten ermöglicht werden, zum Beispiel über die Erweiterung der steuerlichen Forschungsförderung.

- Der Staat sollte sich als Ankerkunde für nachhaltige digitale und KI-Technologien positionieren, indem er gezielt Abnahmeverpflichtungen eingeht und klare Standards in Ausschreibungen festlegt. Dies könnte beispielsweise durch die Kriterien-Aufnahme von Ansätzen wie Green Software Engineering in Ausschreibungen erfolgen, die auf energieeffiziente und umweltfreundliche Softwareentwicklung abzielen. Auf diese Weise kann der öffentliche Sektor nicht nur nachhaltige Innovationen vorantreiben, sondern auch als Vorbild für andere Marktteilnehmer agieren.

- Zur Stärkung der strategischen Souveränität und um sicher handlungsfähig zu bleiben, muss der Staat gewisse Schlüsseltechnologien national vorhalten. Gerade unter den aktuellen geopolitischen Rahmenbedingungen muss es das Ziel der Bundesregierung sein, im Zusammenschluss mit der spezialisierten Industrie technologische Souveränität im Bereich staatlicher Sicherheit zu gewährleisten.

- Die Entwicklung und Anwendung von Schlüsseltechnologien entstehen im Ökosystem. Ein solches Innovations-Ökosystem aus Forschung, Staat, Unternehmen und Start-ups muss gefördert werden. Der Zugang zu Venture Capital sollte erleichtert werden, insbesondere in der Wachstumsphase.

- Digitale Technologien und Produkte bieten insbesondere im Gesundheitsbereich enorme Potenziale, um die Pflegeversorgung effizienter, sicherer und patientenzentrierter auszugestalten. Dafür wurden in der vergangenen Legislatur wichtige Impulse gesetzt. Um das Potenzial der Digitalisierung weiter auszuschöpfen, sollten sektorenübergreifende Digitalisierungsprojekte konsequent und gezielt weitergefördert werden. Der Zugang zur Telematikinfrastruktur ist dabei die Voraussetzung.

- Der Digitale Produktpass ist ein zentraler Baustein, um den Informationsfluss entlang des Produktlebenszyklus zu verbessern. Die standardisierte und vergleichbare Strukturierung umweltrelevanter Daten schafft eine gemeinsame Grundlage für alle Akteure entlang der Wertschöpfungs- und Lieferkette, um die Transformation hin zu einer Kreislaufwirtschaft gezielt voranzutreiben. Die Ausgestaltung sollte interoperabel sein und eine einfache Anknüpfung an (europäische) Datenräume ermöglichen.

- Standard-Essential Patents (SEPs) sind zentral für 5G, IoT und KI, doch unklare Lizenzierungsbedingungen und hohe Kosten, insbesondere in Deutschland, behindern den Marktzugang von Unternehmen. Einstweilige Verfügungen ohne endgültige Patentprüfung gefährden den Wirtschaftsstandort und verteuern Produkte. Deutschland sollte die Verhältnismäßigkeitsklausel konsequent anwenden und sich auf EU-Ebene für eine einheitliche SEP-Regelung einsetzen, um faire Lizenzbedingungen und Innovationsförderung sicherzustellen.

4. Datenwirtschaft

Eine leistungsfähige Datenwirtschaft ist der Schlüssel zu Innovation, wirtschaftlichem Wachstum und einer erfolgreichen digitalen Transformation. Daten bilden die Grundlage für neue technologische Entwicklungen, Geschäftsfelder und die Optimierung bestehender Dienstleistungen. Um das Potenzial der Datenwirtschaft voll auszuschöpfen, sind klare und einheitliche rechtliche Rahmenbedingungen und der Abbau von Überregulierung, ein strategischer Aufbau von Datenräumen und eine stärkere Vorbildfunktion des Staates entscheidend. Dies erfordert auch den zeitnahen Aufbau der Governance-Strukturen zum EU Data Act sowie ein Sanktionsrahmen, der nicht innovationshemmend wirkt. Die folgenden Forderungen zeigen Wege auf, wie Deutschland und Europa eine zukunftsfähige und faire Datenökonomie gestalten können, die sowohl Innovationen als auch Nachhaltigkeit fördert. Gleichwohl sind pauschale Verpflichtungen zur Datenweitergabe abzulehnen; die Datensouveränität sowie eine gerechte Teilhabe müssen gesichert bleiben. Denkbar sind Lizenzmodelle zum Datenaustausch.

Rechtliche Rahmenbedingungen harmonisieren

- Es müssen klare und harmonisierte Regelungen für Pseudonymisierung, Anonymisierung und den internationalen Datentransfer geschaffen werden. Diese Regelungen sollten Unternehmen und Institutionen eine verlässliche Grundlage bieten, um Daten rechtskonform zu verarbeiten und grenzüberschreitend zu nutzen, ohne dabei den Schutz persönlicher Daten zu gefährden.

- Einheitliche Datenschutzvorgaben auf nationaler und europäischer Ebene sind entscheidend, um rechtliche Unsicherheiten zu beseitigen und Effizienz zu fördern. Es sollte eine behördliche Entscheidung verbindlich für alle gelten, unterstützt durch klare Zuständigkeiten, eine enge Abstimmung der Behörden und eine erweiterte Kompetenz für Datennutzung, um Innovation und Wachstum voranzutreiben. Der Datenschutz sollte praxistauglich und innovationsfreundlich ausgelegt werden. Es sollte der Weg zu einem »ermöglichenden Datenschutz« gefunden werden, der den restriktiven Charakter der DSGVO in eine Balance bringt, die Innovation erlaubt, aber den Schutz der Privatsphäre gewährleistet. Ein ausgewogenes Verhältnis ist hierbei entscheidend, um die Potenziale datengetriebener Technologien zu fördern, ohne dabei die Rechte der Bürgerinnen einzuschränken.

Datennutzung verbessern

- Kommunale und öffentliche Unternehmen sollten die Nutzung von Daten aktiv vorantreiben, um Dienstleistungen gezielt zu verbessern und neue Geschäftsfelder zu entwickeln. Beispiele hierfür sind datenbasierte Verkehrslösungen, Transparenz des Bauwerkbestands oder optimierte Energieversorgung.

- Faire Wettbewerbsbedingungen zwischen öffentlichen und privaten Akteuren, aber auch zwischen privaten Akteuren, müssen sichergestellt werden. Insbesondere bei der Nutzung wettbewerblich relevanter Daten ist ein »Level-Playing-Field« erforderlich, damit keiner der Akteure durch privilegierten Datenzugang bevorzugt wird.

- Der Zugang zu Forschungsdaten sollte für die Industrie erleichtert werden, um wissenschaftliche Erkenntnisse und Innovationen schneller in marktfähige Produkte und Dienstleistungen zu überführen und so den gesellschaftlichen Mehrwert zu maximieren. Dies kann durch gezielte Kooperationen zwischen Forschungseinrichtungen und Unternehmen sowie durch offene Datenplattformen unterstützt werden.

Investitionen in Datenräume stärken

- Die Weiterentwicklung und Vernetzung von Datenräumen ist erfolgskritisch. Um Skalierungshürden zu überwinden, sind gesicherte Folgefinanzierungen und eine enge Abstimmung mit den sektoralen European Data Spaces sowie internationalen Interoperabilitätsstandards erforderlich. Mit einer Investitionszulage und Super-Abschreibungen soll auch die Möglichkeit geschaffen werden, Investitionen von Unternehmen für die Erschließung und die anschließende Nutzung von Daten zu fördern.

Digitale Betriebsanleitung ermöglichen

- Bei der Einführung neuer Regulierungen sollte konsequent darauf geachtet werden, dass sämtliche Informations- und Dokumentationspflichten vollständig digital umgesetzt werden können – einschließlich der Informationen für Endanwender. Um dieses Ziel zügig zu verwirklichen, bietet sich eine umfassende Anpassung aller produktharmonisierenden Vorschriften im Rahmen einer Omnibus-Regulierung an.

5. Cybersicherheit

Cybersicherheit ist die Grundlage einer wachsenden digitalen Zukunft. Sie ist als gemeinschaftliche Aufgabe zu verstehen und bedarf der Verantwortung aller Akteure in Wirtschaft, Verwaltung und Gesellschaft. Unternehmen sowie staatliche Einrichtungen müssen gleichermaßen zur Cybersicherheit betragen. Ausnahmen für staatliche Akteure untergraben den Schutz aller. Im Zusammenspiel mit Wirtschaftsvertreterinnen, Sicherheitsexperten und Risikoträgern sollten daher Mittel und Wege gesucht werden, die Cyberresilienz der deutschen Wirtschaft dauerhaft und in der Breite zu stärken und damit die Attraktivität des Standortes für Investoren zu stärken.

Rechtsrahmen und praxisnahe Umsetzung harmonisieren

- Der Cyber Resilience Act (CRA) stellt hohe Anforderungen an die Sicherheit vernetzter Produkte, was für Unternehmen mit erheblichen Verpflichtungen verbunden ist. Die Bundesregierung sollte darauf hinwirken, dass harmonisierte Normen etabliert werden, die den Unternehmen klare und einheitliche Leitlinien bieten. Gleichzeitig müssen ausreichend Stellen für Konformitätsbewertungen geschaffen werden, um Engpässe zu vermeiden, die zu Verzögerungen bei der Markteinführung oder gar Verkaufsstopps führen könnten.

- Die Umsetzung des NIS2-Gesetzes sollte pragmatisch und unternehmerfreundlich erfolgen. Dies könnte durch eine anfängliche Kulanzphase erreicht werden, die Unternehmen Zeit gibt, die neuen Anforderungen zu erfüllen. Gleichzeitig sollte die Zahl der Berichtspflichten auf ein notwendiges Maß beschränkt werden, um bürokratischen Aufwand zu minimieren. Zudem sollte die Anerkennung internationaler Nachweise gefördert werden, um Doppelarbeit zu vermeiden und Unternehmen die Anpassung zu erleichtern. Eine Ausnahme des Regelungsvorhabens für verschiedene Verwaltungsebenen ist nicht nur ineffizient, sondern schwächt die Cybersicherheitslage insgesamt und muss unbedingt vermieden werden. Der Schwerpunkt sollte ausschließlich auf objektiven und überprüfbaren Kriterien für IT- und Cybersicherheit liegen.

- Da harmonisierte Anforderungen entscheidend sind, müssen diese auch auf kommunaler Ebene umsetzbar sein. Diese Prüfung können durch eine Harmonisierung der Bund-Länder-Cybersicherheitsarchitektur begleitet werden. Deutschland sollte sich für eine schnelle Verabschiedung des European Cloud Certification Schemes (EUCS) einsetzen. Dabei sollte der Fokus klar auf technischer IT-Sicherheit liegen, ohne die Aufnahme von politischen Immunitätskriterien, die unnötige Hürden schaffen könnten. Ziel ist es, ein praxisorientiertes und international anschlussfähiges Zertifizierungssystem zu etablieren.

- Ein konsistenter, länderübergreifender Rechtsrahmen zur Bekämpfung von Cyberkriminalität ist essenziell. Nationale Alleingänge führen oft zu Inkonsistenzen und Lücken in der Strafverfolgung. Deutschland sollte sich stattdessen für eine europaweite Strategie einsetzen, die harmonisierte Gesetze und eine abgestimmte Zusammenarbeit zwischen den EU-Staaten umfasst.

- Der Ausbau des Bundesamts für Sicherheit in der Informationstechnik (BSI) als Zentralstelle ist ein wichtiger Schritt, um einer übergreifenden Gefährdungslage effektiv zu begegnen, Kompetenzen zu bündeln und Kooperation zu ermöglichen. Auch die Rolle des CISO Bund sollte im BSI angesiedelt werden. Ein konsistenter innenpolitischer Rechtsrahmen sollte geschaffen werden, der eine länderübergreifende Zusammenarbeit ermöglicht. Das BSI sollte zentrale Erkenntnisse nutzen, um Cyberangriffe frühzeitig zu erkennen und abzuwehren. Gleichzeitig sollte das Meldewesen für Unternehmen und Behörden bürokratiearm und vollständig digital ausgestaltet werden, um Prozesse effizienter zu gestalten und die Reaktionszeit bei Cybervorfällen zu verkürzen. Das BSI sollte auch im Bereich der KRITIS den Single Point of Contact für alle Nachweisverfahren und Meldepflichten übernehmen. Es bedarf ferner eines konsequenten Umsetzungsplans für den staatlichen Umgang mit IT-Sicherheitslücken, um die Risiken für Wirtschaft, Staat und Gesellschaft zu reduzieren.

Praxisorientierte Umsetzung sicherstellen

- Die Integration der Industrie in die Entwicklung von Anforderungen muss intensiviert werden. Dies erfordert regelmäßige Konsultationen mit Unternehmen, um sicherzustellen, dass die technischen Vorgaben praxisnah und umsetzbar sind. Gleichzeitig sollten politische Interessen klar von den technischen Standards getrennt werden, um sicherzustellen, dass die Anforderungen ausschließlich auf funktionalen und sicherheitstechnischen Erfordernissen basieren und nicht durch politische Ziele verwässert werden.

- Cybersicherheitsstandards sollten bei den Vergabekriterien im öffentlichen Beschaffungswesen stärker berücksichtigt werden. Das bedeutet, dass Anbieter öffentlicher Aufträge nur dann zum Zuge kommen, wenn sie definierte Mindeststandards in der IT-Sicherheit nachweislich erfüllen. Dies würde nicht nur die Sicherheit staatlicher IT-Systeme verbessern, sondern auch Unternehmen dazu motivieren, stärker in die Cybersicherheit ihrer Produkte und Dienstleistungen zu investieren.

- Um Unternehmen bei der Umsetzung von Sicherheitsmaßnahmen zu unterstützen, sollte die Einführung steuerlicher Anreize erfolgen. Dazu zählen etwa Investitionszulagen, die gezielt für Cybersicherheitsprojekte bereitgestellt werden, sowie die Möglichkeit, Investitionen in Sicherheitsmaßnahmen abzuschreiben. Diese Maßnahmen würden insbesondere kleinen und mittelständischen Unternehmen den Zugang zu hochentwickelten Sicherheitslösungen erleichtern.

Desinformation entgegensteuern

- Deutschland sollte die Rechtsdurchsetzung bestehender (europäischer) Regelungen unterstützen, u.a. mit ausreichend Budget und Personalkapazitäten, um die Integrität des digitalen Raums zu schützen. Ein verbindlicher Content-Faktencheck auf Plattformen sollte darüber hinaus ein zusätzlicher Beitrag zum Schutz gegen Desinformation sein. Dies würde Plattformanbieter anhalten, Inhalte systematisch auf ihre Richtigkeit zu prüfen.

- Diese Maßnahmen würden die Verbreitung von Fake News signifikant eindämmen und das Vertrauen der Nutzer in digitale Plattformen stärken. Darüber hinaus würden sie zur Verbesserung der Informationsqualität in Europa beitragen und die Grundlage für eine fundierte öffentliche Meinungsbildung schaffen. Sie wären zentrale Maßnahmen, um die demokratische Debatte im digitalen Raum zu schützen und langfristig zu sichern.

6. Digitalisierung und Modernisierung der Verwaltung

Eine moderne und digitalisierte Verwaltung ist der Schlüssel zu einer effizienten und bürgernahen staatlichen Handlungsfähigkeit. Sie bildet das Fundament für eine erfolgreiche digitale Transformation und trägt maßgeblich zur Stärkung von Demokratie und wirtschaftlicher Wettbewerbsfähigkeit bei. Die Novellierung des Onlinezugangsgesetz und sein Inkrafttreten war ein sehr wichtiger Kraftakt der Ampel-Regierung. Die Modernisierung der Verwaltung ist ein kontinuierlicher Prozess und soll zu einer wirkungsvollen, kommunalen Daseinsvorsorge beitragen. Die Verwaltung muss ihre Rolle als Dienstleister für seine Bürger und Unternehmen wahrnehmen (können).

Verwaltungsprozesse effizient und zukunftssicher machen

- Das Recht auf eine vollständig digitale Abwicklung von Verwaltungsleistungen sollte konsequent umgesetzt werden. Es sollte eine Priorisierung der Digitalisierung von Verwaltungsleistungen für Bürgerinnen stattfinden mit einer verpflichtenden Frist für deren Umsetzung. Hierbei muss sichergestellt werden, dass die Tools auch den Ansprüchen der Industrie gerecht werden, vor allem im Hinblick auf die Übermittlung von sensiblen Daten. Entlang einer Meilensteine-Planung soll dieses Recht nach und nach etabliert werden. Verbunden mit diesem Recht ist die Einklagbarkeit seiner Umsetzung nach Ablauf einer bestimmten Karenzzeit. Auch das Once-Only-Prinzip sollte konsequent umgesetzt werden. Dieses erfordert ein einheitliches und intelligentes Datenmanagement (Registermodernisierung), das redundante Berichtspflichten für Unternehmen und Verwaltung minimiert. Dabei sollte immer die Nutzung vorhandener Infrastruktur vor deren Neuentwicklung stehen.

- Die Schriftformerfordernis sollte umfassend per Generalklausel abgeschafft werden. Bei der Digitalisierung von Prozessen stellt sich immer wieder heraus, dass Medienbrüche eine der größten Herausforderungen darstellen. Sobald digitale Abläufe durch einzelne Schritte in Papierform unterbrochen werden, gehen wesentliche Effizienzgewinne verloren. Die doppelte Führung von elektronischen und papierbasierten Akten führt zudem nicht nur zu Mehraufwand, sondern auch zu vermeidbaren Kosten. Eine klare, einheitliche Regelung ist dringend erforderlich, um die Potenziale der Digitalisierung voll auszuschöpfen und die damit verbundenen rechtlichen Unsicherheiten zu beseitigen. Die Einführung einer sicheren, europaweit einsetzbaren digitalen Identität für Bürger und Unternehmen ist entscheidend, um Behördengänge vollständig online abwickeln zu können. Dies ermöglicht eine eindeutige Identifikation und Authentifizierung, die gleichzeitig höchste Datenschutzstandards einhält.

- Ein umfassendes Ökosystem digitaler Identitäten muss neben Personen auch Organisationen und Objekte wie Maschinen oder Autos im Internet der Dinge einbeziehen. Die für Industrie 4.0 nötigen Identitätskonzepte sollten innerhalb der eIDAS 2.0-Infrastruktur realisierbar sein, um Anwendungen wie digitale Zwillinge und vernetztes Fahren zu ermöglichen. Gleichzeitig können Unternehmen durch digitale Identitäten Bürokratieaufwände reduzieren.

- Genehmigungsverfahren für industrielle Anlagen (insbesondere nach BImSchG) müssen vollständig digitalisiert werden. Die neue Bundesregierung wird aufgefordert einen konkreten Umsetzungsplan vorzulegen. Dies beinhaltet sowohl die Bereitstellung einheitlicher Schnittstellen für die Einreichung der Genehmigungsanträge durch den Anlagenbetreiber als auch die behördeninterne Kommunikation bis hin zur Erteilung des Genehmigungsbescheides. Hierfür müssen ggf. die Verfahren selbst angepasst werden. Die hohen Anforderungen an die Vertraulichkeit sensibler Daten muss durchgehend gewährleistet sein.

Moderne IT-Infrastruktur und Standards etablieren

- Die IT-Infrastruktur der Verwaltung muss stärker harmonisiert und standardisiert werden, um den Datenaustausch zwischen Behörden auf kommunaler, Landes- und Bundesebene effizient zu gestalten. Möglichkeiten der Zentralisierung für Leistungen (Government as a platform), sollten ausgeschöpft werden, um bundesweit einheitliche Inanspruchnahme und Leistungsniveau sowohl von Bürgerinnen und Bürgern als auch von Unternehmen zu ermöglichen und den bestehenden Flickenteppich zu beseitigen. Eine interoperable IT-Architektur erleichtert die Zusammenarbeit und verhindert Dateninseln. Die Hardware der Verwaltung sollte technisch modernisiert werden, u.a. um eine einheitliche BIM-Reife in den Baudienststellen zu erreichen.

- Wettbewerb ist ein bewährter Treiber für schnellere, bessere und kosteneffizientere Lösungen – ein Prinzip, das gerade bei der technischen Umsetzung der Digitalisierung gelten muss. Es sollte ein vielfältiger und dynamischer Wettbewerb ohne Marktverzerrung durch einseitige Inhouse-Vergaben gefördert werden, um die besten innovativen und resilienten Lösungen für die Verwaltung zu fördern.

- Standards sind die Grundlage sowohl für den Wettbewerb als auch für die digitale Souveränität. Im Rahmen einer langfristig angelegten deutschen Verwaltungs-Cloud-Strategie ist ein Level-Playing-Field für alle Cloud-Provider im Rahmen von Vergabeverfahren sicherzustellen. Sie gewährleisten die Interoperabilität und Austauschbarkeit von Software und fördern dadurch Wettbewerb und Vielfalt. Die Politik muss diesen bislang vernachlässigten Aspekt stärker in den Fokus nehmen und die Standardisierung von Datenformaten und Schnittstellen in der öffentlichen Verwaltung aktiv vorantreiben.

- Reallabore sollen eingerichtet werden, in denen innovative Ansätze für die digitale Verwaltung getestet und optimiert werden können, bevor sie flächendeckend eingeführt werden. Dies ermöglicht eine praxisnahe und risikoarme Erprobung neuer Technologien.

7. Maßnahmenpaket konsequent und schnell umsetzen

Wird die Digitalisierung entschlossen vorangetrieben, ergeben sich enorme Chancen für den Wirtschaftsstandort Deutschland. Dafür ist das genannte Maßnahmenpaket von entscheidender Bedeutung.

Es muss in der Priorität einer neuen Bundesregierung einen zentralen Platz einnehmen und durch Maßnahmen einer konsequenten Kompetenzverteilung in der Regierung und durch entsprechende Strukturen umgesetzt werden. Ein wesentlicher Bestandteil muss dabei eine konsistente Digital Governance sein. Die hier nötige Umsetzungseinheit soll die Digitalprojekte des Bundes ganzheitlich steuern und zentral Basiskomponenten rund um digitale Identitäten, Register etc. zur Verfügung ſtellen.

Es ist insgesamt entscheidend, dass die Kompetenzen der Unternehmen genutzt werden, um einen praxisorientierten Rahmen und Umsetzung zu ermöglichen und um überlappende Gesetzgebung, Doppelförderungen und -strukturen zu vermeiden. Dazu müssen auch entsprechende Weichenstellung auf europäischer Ebene erfolgen. Die neue Bundesregierung sollte entsprechende Initiativen auf den Weg bringen.

Mit einer zukunftsweisenden Digitalpolitik kann Deutschland nicht nur seine Wettbewerbsfähigkeit sichern, sondern auch zum führenden digitalen Innovationsstandort Europas aufsteigen.

Impressum

Herausgeber	**Wirtschaftsforum der SPD e.V.** vertreten durch das geschäftsführende Präsidium Prof. Dr. Ines Zenke (Präsidentin) Prof. Dr. Susanne Knorre (Schatzmeisterin) Dr. Peter Güllmann (Vizepräsident) Matthias Machnig (Vizepräsident) Philipp Schlüter (Vizepräsident) Dr. Tanja Wielgoß (Vizepräsidentin) Michael Wiener (Vizepräsident)
V.i.S.d.P.	Dr. Frank Wilhelmy, Geschäftsführer
	Registereintrag im Vereinsregister beim Amtsgericht Charlottenburg unter der Registernummer VR 33920. Das Wirtschaftsforum der SPD e.V. ist registrierter Interessenvertreter zur Registernummer: R000328 des Lobbyregisters beim Deutschen Bundestag und unterliegt dem gesetzlichen Verhaltenskodex des LobbyRG.
Anschrift	Dorotheenstraße 35 10117 Berlin
Telefon	+49 (0)30 86388330
E-Mail	mail@spd-wirtschaftsforum.de
Internet	spd-wirtschaftsforum.de
Gestaltung und Satz	Anette Gilke, Hannover
	Februar 2025