Beschluss (vorläufig) Digitale Souveränität stärken: Unsere Unabhängigkeit, Freiheit und Demokratie schützen!

Gremium:	Bundesdelegiertenkonferenz
Beschlussdatum:	30.11.2025
Tagesordnungspunkt:	VR Im V-Ranking priorisierte V-Anträge

Antragstext

Europa und Deutschland befinden sich in einer Zeit tiefgreifender geopolitischer und technologischer Umbrüche. Digitale Technologien sind längst zu einem zentralen Machtfaktor in der globalen Ordnung geworden. Wer sie kontrolliert, bestimmt zunehmend auch über wirtschaftliche Stärke, politische Handlungsfähigkeit und gesellschaftliche Resilienz. Während autoritäre Staaten technologische Kontrolle gezielt ausbauen, geraten Demokratien unter Druck, ihre digitale Unabhängigkeit zu sichern. US-Präsident Donald Trump versucht europäische Digitalgesetze als Hebel in den Zoll- und Handelsverhandlungen zu nutzen, um mühsam erkämpfte europäische Standards gezielt zu schwächen und den Einfluss US-amerikanischer Konzerne zu sichern. Auch China drängt mit staatlich gestützten Tech-Konzernen auf europäische Märkte. Große Abhängigkeiten von einzelnen Anbietern bleiben ein großes Problem, wenn es darum geht, Eigenständigkeit zu wahren. Europas und Deutschlands Antwort auf diese Herausforderungen kann nur darin bestehen, diese Abhängigkeiten zu erkennen, sie zu reduzieren, offene, transparente und sichere Infrastrukturen zu fördern, eigene technologische Fähigkeiten auszubauen und eine größere digitale Souveränität als Leitlinie einer wertebasierten Außen-, Wirtschafts- und Digitalpolitik zu begreifen. Selbstbestimmt agiert nur, wer darüber entscheiden kann, wie digitale Infrastrukturen, Online-Plattformen und Daten ineinandergreifen und nach welchen Regeln sie funktionieren. Dafür braucht es Wahlfreiheit über digitale Dienste, die interoperabel ausgestaltet und modular kombinierbar sind.

Auch und gerade im Bereich der inneren Sicherheit zeigt sich ein besorgniserregender Trend: Noch immer sind – trotz jahrelanger Diskussionen und Warnungen - sehr relevante Teile unserer digitalen Infrastrukturen im Sicherheitsbereich, auf Servern und in Cloud-Lösungen, bei denen der Zugriff durch entsprechende rechtliche Regelungen nicht ausgeschlossen ist. Statt diese Abhängigkeiten und Risiken schnellstmöglich zu reduzieren und für angemessene Schutzstandards zu sorgen, versuchen Teile der aktuellen Bundesregierung weitere, extrem risikoreiche Abhängigkeiten und Gefahren zu schaffen. Gerade hat die Bundeswehr einen neuen Vertrag mit Google über die Nutzung der Cloud geschlossen. Die schwarz-rote Bundesregierung prüft derzeit den Einsatz der Analysesoftware des US-Unternehmens Palantir auch in Bundesbehörden, obwohl der Deutsche Bundestag dies ablehnt und die Innenministerkonferenz vor neuen Abhängigkeiten und Gefahren warnt.

Bereits in der vergangenen Wahlperiode haben wir Grünen uns dafür eingesetzt, grundrechtskonforme automatisierten Analysetools für die Polizei entwickeln zu lassen und dabei auf europäische Anbieter zurückzugreifen. Ihr Einsatz benötigt eine klare Rechtsgrundlage und effektive demokratische Kontrolle. Palantir wird diesem Anspruch nicht im Ansatz gerecht. Deshalb lehnen wir den Einsatz solcher

Analysesoftware der Firma Palantir grundsätzlich ab. Wir wollen KI-gestützte Analyseinstrumente nur dann nutzbar machen, wenn sie rechtsstaatlich klar begrenzt, datenschutzkonform gestaltet und jederzeit nachvollziehbar sind – mit transparenter Prüfung, Zweckbindung und voller Datenhoheit der Behörden.

Für digitale Souveränität müssen wir eigene europäische Lösungen aufbauen, leistungsfähige Konsortien fördern und als Staat verlässlich als Ankerkunde auftreten. Dass wir strategisch den Anschluss auch auf unserem eigenen Markt verpassen, zeigt die Entscheidung Europas größten Softwarekonzerns SAP mit dem KI-Anbieter OpenAI zu kooperieren, um künftig Verwaltungen, Schulen und Universitäten sowie andere öffentliche Einrichtungen in Deutschland mit Anwendungen der Künstlichen Intelligenz zu versorgen. Solche Kooperationen verschärfen nicht nur weiter Abhängigkeiten, sondern bedeuten auch die Verlagerung eines nicht unerheblichen Teils der Wertschöpfung sowie des Cashflows und verschaffen den US-Giganten möglicherweise einen unentgeltlichen Zugang zu weiteren wertvollen Datensätzen. Statt sich weiter von den großen Foundationmodellen abhängig zu machen, sollte auch der zielgenaue Einsatz kleinerer Modelle erwogen werden.

Die digitale Abhängigkeit von außereuropäischen Anbietern ist längst systemrelevant. Ob Cloud-Dienste, Betriebssysteme, KI-Anwendungen oder sicherheitskritische Hardware, zentrale technologische Infrastrukturen stammen überwiegend aus den USA oder China. Sowohl Wirtschaft, Verwaltung und Bürger*innen haben nur noch begrenzte Wahlfreiheit über Hardware, Software und Plattformen; oftmals geben marktdominante Akteure vor, wie wir digital agieren können, und wie unsere Daten verarbeitet werden.

Die Umsetzung der Europäischen Digitalgesetze wie DSA, KI-VO, DSGVO, Data Act und DMA muss nun zügig und einheitlich erfolgen. Dazu braucht es eine zügige und konsequente Umsetzung mit einer schlanken und klaren Aufsichtsstruktur. Durch die Bündelung zentraler Zuständigkeiten in einer gut ausgestatteten Digitalagentur als „One-Stop-Agency“ für Bürger*innen, Wirtschaft und Verwaltung kann die Durchsetzung des europäischen Regelungsrahmens effizient und transparent gewährleistet werden und so fairen Wettbewerb, den Schutz der Verbraucher*innen und Grundrechte sicherstellen. Deutschland und Europa müssen deshalb strategisch umsteuern und eigene technologische Kapazitäten aufbauen.

Ein wichtiger Schritt sind Investitionen in freie, offene und vertrauenswürdige Technologien, vor allem durch die öffentliche Hand als Kundin. Sie ist dem Gemeinwohl, der Verhältnismäßigkeit ihrer Ausgaben, dem verantwortlichen Umgang mit Ressourcen und einer langfristigen Servicesicherheit verpflichtet. Mit sogenannter Free and Open Source Software wird Wechselfähigkeit, Nähe zum Anbieter zwecks Weiterentwicklung und Wartung im Ernstfall leicht möglich sein.

Mit der Aufnahme der IT-Sicherheit in das 500 Mrd. Euro-Sondervermögen haben wir die Grundlage geschaffen, um Abhängigkeiten deutlich zu reduzieren und zukünftig verstärkt auf Eigenentwicklungen zurückgreifen zu können. Mit der Sovereign Tech Agency und dem Zentrum für Digitale Souveränität wurden in der vergangenen Wahlperiode wichtige Grundlagen geschaffen. Nun braucht es langfristige Förder-, Beschaffungs- und Investitionsstrategien, die Open Source, europäische Anbieter und faire Wettbewerbsbedingungen auf digitalen Märkten gezielt stärkt.

Gerade der digitalaffine deutsche Mittelstand kann von offenen, interoperablen und souveränen Technologien profitieren: Sie senken Abhängigkeiten von globalen

Konzernen, ermöglichen eigene Software- und Servicelösungen und schaffen neue Märkte für nachhaltige und sichere IT-Produkte "Made in Germany".

Unsere digitale Infrastruktur muss so gestaltet sein, dass sie vor Machtmissbrauch geschützt ist. Digitalisierung muss unserer Demokratie und Menschenrechten dienen und nicht eine Gefahr für sie sein. Beste Daten- und Grundrechtsschutz-Standards, Verschlüsselung und Dezentralität sind kein Selbstzweck, sondern Schutz vor Überwachung, Diskriminierung und Machtkonzentration. Dafür setzen wir uns im Sinne einer aktiven Digitalen Außenpolitik, zum Beispiel im Rahmen von UN-Prozessen, Standardisierungsgremien und multilateralen Foren, ein. Diese Standards sind zugleich Motor für vertrauensbasierte und transparent Innovation und somit ein Wettbewerbsvorteil auf dem Markt für Verbraucher*innen und Unternehmen, die Klarheit über ihre Rechte und ihre Daten wollen. Eine digitale Infrastruktur, die auf Offenheit sowie Kontrolle durch Parlamente und Öffentlichkeit setzt, ist die beste Versicherung gegen antidemokratische Versuchungen. Digitalisierung muss demokratisch kontrolliert, resistent gegenüber autoritärem Zugriff und faschismussicher sein!

Als Grüne machen wir seit langem auf den Mehrwert von besten IT-Sicherheitsstandards und Openness-Modellen, die Verbraucher*innen-Recht stärken und zentral für Vertrauen in digitale Anwendungen sind, aufmerksam. Schleswig-Holstein hat sich unter grüner Regierungsbeteiligung dafür entschieden, Souveränität mit Open Source zu realisieren und versteht die Schaffung von digitaler Souveränität durch Open Source Lösungen auch als Industriepolitik für die Digitalwirtschaft. Das Land fördert heimische IT-Unternehmen, stärkt damit den Standort für Fachkräfte und setzt darauf, dass entsprechende Lösungen, beispielsweise durch den Wegfall von teils horrenden Lizenzkosten längerfristig sogar günstiger als die Lösungen proprietärer Anbieter sind. Von solchen Best-Practice-Beispielen können sowohl Bund als auch andere Länder lernen. Deshalb sollte ein strukturierter Austausch über erfolgreiche Modelle digitaler Souveränität etabliert werden, auch gemeinsam mit europäischen Staaten, die auf diesem Weg bereits weiter sind.

Europa und Deutschland brauchen jetzt eine strategische Neuausrichtung ihrer Digitalpolitik. Statt jedes Jahr hunderte Millionen Euro in Lizenzgebühren an US-Konzerne zu zahlen, müssen öffentliche Mittel gezielt in deutsche und europäische Alternativen fließen. Langjährige Lizenzbindungen und geschlossene Systeme haben zu digitalen Pfadabhängigkeiten geführt, die neue Abhängigkeiten fortschreiben. Wer technologische Souveränität will, muss diese Lock-in-Effekte gezielt aufbrechen und den Umstieg auf offene Standards gezielt politisch forcieren. Nur durch Investitionen in offene, sichere und transparente Technologien kann Europa seine digitale Handlungsfähigkeit sichern. Auf europäischer Ebene ist eine wichtige Perspektive die EuroStack-Initiative, mit der europäische Akteur*innen gemeinsam an einer souveränen digitalen Infrastruktur arbeiten. Ziel ist es, offene und interoperable Technologien zu entwickeln, die zentrale staatliche und wirtschaftliche Anwendungen unabhängig von außereuropäischen Plattformen ermöglichen. Deutschland sollte die Initiative aktiv unterstützen und sich dafür einsetzen, dass sie zu einem strategischen Kernprojekt europäischer Digitalpolitik ausgebaut wird.

Digitale Souveränität ist mehr als Technologiepolitik. Sie ist eine Investition in die Menschen, die Europas digitale Zukunft gestalten. Wenn wir Innovation mit

Gemeinwohl, Transparenz und Nachhaltigkeit verbinden, schaffen wir nicht nur neue Arbeitsplätze, sondern auch Vertrauen in den digitalen Wandel. Wir wollen Talente fördern, die digitale Freiheit, Verantwortung und Demokratie zusammen denken. Dafür braucht es eine gezielte europäische Förderstrategie für Open-Source-Unternehmen, Start-ups und kleine sowie mittlere Betriebe, die faire Rahmenbedingungen und Planungssicherheit schafft. Durch Investitionen in Ausbildung, Fachkräfteentwicklung und Forschung können wir Talente in Europa halten und neue Fachkräfte gewinnen, die unsere Werte und unseren Gestaltungsanspruch teilen.

Wir Grüne wollen ein digitales Ökosystem, das demokratisch, nachhaltig und offen gestaltet ist, die Resilienz unserer Gesellschaft stärktund digitale Teilhabe unabhängig vom Einkommen und sozialem Status ermöglicht. Im Mittelpunkt stehen sechsHandlungsfelder, in denen politisches Handeln jetzt besonders gefragt ist.

1. Europäische digitale Infrastruktur ausbauen

Deutschland muss die bereits ressortübergreifend vereinbarten Absprachen zur Stärkung der digitalen Souveränität Deutschlands und Europas, etwa in der Nationalen Sicherheitsstrategie, endlich mit politischem Leben füllen und konsequent umsetzen. Europäische Initiativen wie die EuroStack-Initiative sollen aktiv vorangetrieben und eine souveräne, offene und interoperable Cloud- und Dateninfrastruktur in Europa gestärkt werden. Dazu braucht es klare Souveränitätsmaßstäbe in der Beschaffung, insbesondere bei Clouddiensten. Ein Baustein dabei sind gemeinwohlorientierte, offen zugängliche europäische Datenräume für Forschung und KI. Projekte, welche die europäischen Rechenkapazitäten stärken oder eigene LLMs sowie industrielle Foundation-Modelle entwickeln, gilt es besonders zu unterstützen. Ziel ist der Aufbau einer starken europäischen Cloud-, KI- und Halbleiterindustrie, die den europäischen Datenschutz- und Sicherheitsstandards entspricht und rechtswidrige Datenabflüsse, insbesondere ins Ausland effektiv zu unterbinden. So können wir auch für Länder außerhalb Europas eine attraktive Kooperationsmöglichkeit eröffnen. Ansätze aus Deutschland wie der „DeutschlandStack“ müssen europäisch kompatibel ausgestaltet werden.

2. Open Source zum Standard machen

Deutschland muss das Vergaberecht modernisieren! Bei öffentlichen IT-Beschaffungen müssen offene Standards, offene Schnittstellen und Open-Source-Lösungen Vorrang vor proprietärer Software haben. Bei neu entwickelter Software der öffentlichen Verwaltung soll "Public Money, Public Code" als Leitbild dienen. Souveränität muss in Vergabeverfahren der öffentlichen Hand stärker gewichtet werden. Folgekosten, die sich beim Einsatz von proprietären Lösungen durch den Lock-In-Effekt und mangelnde Wechseloptionen ergeben, müssen in die Wirtschaftlichkeitsbetrachtung aufgenommen werden. Bis 2029 muss ein Open-Source-Anteil von mindestens 70 % bei Vergaben erreicht werden. Hierbei gilt es, diesen Anteil genauer messbar zu machen: Wo proprietäre Lösungen vor allem Lizenzkosten verursachen, gelten für Open-Source-Kosten andere Strukturen. Ziel ist es Lösungen zu priorisieren, die zugleich Leistungsfähigkeit und Offenheit ermöglichen.

3. Digitale Souveränität in der Bildung und Wissenschaft stärken

Digitale Souveränität muss auch in Schulen und Hochschulen gewährleistet sein. Heute basieren zentrale Lern-, Kommunikations- und Forschungssysteme oft auf proprietären Plattformen außereuropäischer Konzerne – mit Risiken für Datenschutz, pädagogische und wissenschaftliche Unabhängigkeit sowie langfristige Sicherheit. Wir wollen deshalb, dass Bildungseinrichtungen schrittweise auf europäische, gemeinwohlorientierte und offene Technologien umsteigen, damit Forschung und Lehre nicht von geschlossenen KI- oder Cloud-Systemen abhängig ist. „Public Money, Public Code“ soll auch für öffentlich finanzierte Bildungs- und Forschungssoftware gelten. Digitale Kompetenz, Plattformkritik und ein grundlegendes Verständnis von KI gehören verbindlich in Curricula, damit kommende Generationen souverän und selbstbestimmt mit Technologie umgehen können.

4. Kritische digitale Infrastrukturen schützen und europäisch absichern

Wir müssen die digitalen Infrastrukturen unseres Landes insgesamt besser schützen. Anhaltende Fälle von Spionage, Sabotage und Cyberangriffen zeigen deutlich, wie gefährdet insbesondere die kritische Infrastruktur Deutschlands ist.Gerade hier gefährden auch Abhängigkeiten von außereuropäischen Anbietern die Sicherheit und Handlungsfähigkeit unseres Staates. Die EU verpflichtet mit der NIS-II- und der CER-Richtlinie zu einem umfassenden Schutz dieser zentralen Systeme. Wir fordern eine kohärente Umsetzung beider Vorgaben in einem Dachgesetz sowie den klaren Ausschluss unsicherer Komponenten in sensiblen Bereichen. Auch unser Finanzsystem muss vor neuen digitalen Abhängigkeiten geschützt werden; wir wollen seine Stabilität sichern, den Zugriff von Big Tech auf unsere Daten und Stablecoins begrenzen und zugleich europäische Innovationen stärken.

5. Europäische Innovationskraft stärken

Gezielte Investitionen in Forschung, Start-ups und mittelständische IT-Unternehmen und bessere Bedingungen für Gründungen fördern den Aufbau unabhängiger Schlüsseltechnologien. Um fairen Wettbewerb zu gewährleisten, braucht es zudem eine europäische Digitalkonzernsteuer, die große Plattformen angemessen am europäischen Gemeinwohl beteiligt. Open Source, faire Wettbewerbsbedingungen und europäische Zusammenarbeit sind die Grundlage für technologische Souveränität. Insbesondere der innovationsstarke Mittelstand profitiert, wenn offene Standards und europäische Technologien Planungssicherheit bieten. So entstehen neue Geschäftsmodelle, Wertschöpfungsketten und Exportchancen für Unternehmen, die auf Sicherheit, Nachhaltigkeit und digitale Eigenständigkeit setzen. Der Staat kann dabei als verlässlicher Ankerkunde auftreten, um europäischen Anbietern Planungssicherheit zu geben und selbst mit gutem Beispiel für souveräne und nachhaltige Beschaffung voranzugehen. Dafür braucht es praxistaugliche Beschaffungsinstrumente wie Direktvergaben bis 50.000€ sowie eine Innovationsklausel für Direktvergaben an Start-Ups. Zudem muss der europäische Rechtsrahmen klarer und leichter navigierbar werden. Eine gebündelte One-Stop-Agency für die nationale Umsetzung europäischer Digitalgesetze sowie eine bessere Harmonisierung schaffen verlässliche Bedingungen für die Digitalwirtschaft, wie es mit dem digitalen Omnibus in Europa angegangen wurde. Unternehmensgründungen sollten europaweit einfacher werden. Eine europäische Rechtsform wie eine "EU Inc." und das Ziel, Start-Up Gründungen innerhalb 24 Stunden zu ermöglichen, stärken europäische Innovationstreiber.

6. Nachhaltigkeit als Leitprinzip der Digitalisierung

Digitale Souveränität kann nur gelingen, wenn sie ökologisch und sozial verantwortungsvoll gestaltet ist. Digitale Anwendungen können sehr energie- und ressourcenintensiv sein, bieten zugleich aber auch enorme Chancen für Klimaschutz, Ressourceneffizeinz und nachhaltiges Wirtschaften. Insbesondere KI gestützte Analysen, Modelle und Anwendungen können Klimaschutzmaßnahmen gezielter und Ressourceneinsatz effizienter gestalten. Diese Potenziale müssen erschlossen werden. Nur eine nachhaltige Digitalisierung ist eine souveräne Digitalisierung. Wenn Europa auf Green IT und Kreislaufwirtschaft setzt, verbindet es technologische Unabhängigkeit mit Klimaschutz und Verantwortung für eine lebenswerte digitale Zukunft.

7. Demokratie und Gemeinwohl digital absichern

Daten- und Grundrechtsschutz, Verschlüsselung und Transparenz müssen Grundprinzipien staatlicher IT sein. Digitale Souveränität ist nur dann glaubwürdig, wenn sie nicht nur in Sonntagsreden beschworen, sondern auch mit konkretem politischem Leben gefüllt wird. Sie mussDemokratie, Grund- und Menschenrechte sowie dem Gemeinwohl nutzen. Sie bedeutet nicht Abschottung, sondernin einer zunehmend komplexen Welt, die Fähigkeit, technologische Entscheidungen zukünftig unabhängig und wertebasiert zu treffen. Dazu gehört auch, dass wir die Europäischen Gesetze in diesem Bereich effektiver machen und durch transparente Aufsicht - etwa eine öffentliche Compliance-Datenbank für Gatekeeper - stärken, statt sie als Spielball geopolitischer Interessen des Weißen Hauses oder als Zugeständnis an undifferenzierte Deregulierungswünsche nach dem Motto "anything goes" zu schwächen oder gar abzuschaffen. Um die Marktmacht großer Tech-Konzerne wirksam zu begrenzen, müssen Aufsichtsbehörden zudem ausreichend ausgestattet sein, damit sie fairen Wettbewerb durchsetzen können. Der Digitale Gesetzesrahmen der EU muss konsequent, schlank und mit klaren Zuständigkeiten umgesetzt werden. Die zuständigen Behörden und Agenturen müssen die Umsetzung der europäischen Vorgaben aktiv begleiten und gegenüber den Unternehmen transparent erklären. So entsteht ein klarer Rechtsrahmen, der Menschenrechte im Digitalen Raum garantiert und zugleich Investitionssicherheit sowie Freiräume für Innovation bietet.

8. Vielfalt statt Plattformdominanz - Kultur- und Medienvielfalt sichern

Kreativ- und Medienschaffende sind zunehmend von wenigen globalen Plattformen abhängig, deren intransparente, marktprägende Algorithmen Sichtbarkeit und Einkommen bestimmen. Diese Machtkonzentration gefährdet Vielfalt, faire Vergütung und eine unabhängige Medien- und Kulturlandschaft. Wir setzen uns für algorithmische Transparenz, faire Vergütungsmodelle und nutzerzentrierte Ausschüttungen ein, die besonders kleinere und unabhängige Akteur*innen stärken. Marktbeherrschende Strukturen im digitalen Werbemarkt müssen aufgebrochen werden, damit Einnahmen wieder bei den Inhaltproduzent*innen ankommen. Plattformdominanz entzieht Medienhäusern wesentliche Erlöse und bedroht die demokratische Öffentlichkeit; KI-Empfehlungssysteme verstärken dies. Die EU muss auf Basis des DMA und des Wettbewerbsrechts faire Bedingungen schaffen und Medieninhalte wieder sichtbar machen. Zur Sicherung kultureller und medialer Vielfalt fördern wir offene und unabhängige Alternativen. Europaweit entstehen Plattformen, die ohne Datenprofile, intransparente Algorithmen oder Konzernkontrolle auskommen. Sie sind ein wichtiger Baustein für offene digitale

Öffentlichkeiten. Wir wollen ihre Entwicklung politisch stärken und sie selbst nutzen, um Räume für vielfältige Inhalte, demokratischen Austausch und kulturelle Teilhabe zu schaffen.

Europas digitale Zukunft gehört uns allen und entsteht im Schulterschluss mit anderen Demokratien, die für offene Standards, souveräne Technologien und eine freie digitale Ordnung eintreten. Europa muss jetzt eine Führungsrolle übernehmen - gemeinsam können wir die freie Welt sichern und Demokratie und Freiheit gegenüber autoritären Tech-Modellen verteidigen. Wir haben die Chance, ein digitales Europa zu schaffen, das Freiheit, Innovation und Gerechtigkeit miteinander verbindet. Diese Chance dürfen wir nicht den Techkonzernen überlassen. Europas digitale Zukunft gehört uns allen!