

VR-03 Digitale Souveränität stärken: Unsere Unabhängigkeit, Freiheit und Demokratie schützen!

Antragsteller*in: Rebecca Lenhard (KV Nürnberg-Stadt)

Tagesordnungspunkt: VR Im V-Ranking priorisierte V-Anträge

Antragstext

- 1 Europa und Deutschland befinden sich in einer Zeit tiefgreifender geopolitischer
2 und technologischer Umbrüche. Digitale Technologien sind längst zu einem
3 zentralen Machtfaktor in der globalen Ordnung geworden. Wer sie kontrolliert,
4 bestimmt zunehmend auch über wirtschaftliche Stärke, politische
5 Handlungsfähigkeit und gesellschaftliche Resilienz. Während autoritäre Staaten
6 technologische Kontrolle gezielt ausbauen, geraten Demokratien unter Druck, ihre
7 digitale Unabhängigkeit zu sichern. US-Präsident Donald Trump versucht
8 europäische Digitalgesetze als Hebel in den Zoll- und Handelsverhandlungen zu
9 nutzen, um mühsam erkämpfte europäische Standards gezielt zu schwächen und den
10 Einfluss US-amerikanischer Konzerne zu sichern. Auch China drängt mit staatlich
11 gestützten Tech-Konzernen auf europäische Märkte. Große Abhängigkeiten von
12 einzelnen Anbietern bleiben ein großes Problem, wenn es darum geht,
13 Eigenständigkeit zu wahren. Europas und Deutschlands Antwort auf diese
14 Herausforderungen kann nur darin bestehen, diese Abhängigkeiten zu erkennen, sie
15 zu reduzieren, offene, transparente und sichere Infrastrukturen zu fördern,
16 eigene technologische Fähigkeiten auszubauen und eine größere digitale
17 Souveränität als Leitlinie einer wertebasierten Außen-, Wirtschafts- und
18 Digitalpolitik zu begreifen. Selbstbestimmt agiert nur, wer darüber entscheiden
19 kann, wie digitale Infrastrukturen, Online-Plattformen und Daten
20 ineinandergreifen und nach welchen Regeln sie funktionieren. Dafür braucht es
21 Wahlfreiheit über digitale Dienste, die interoperabel ausgestaltet und modular
22 kombinierbar sind.
- 23 Auch und gerade im Bereich der inneren Sicherheit zeigt sich ein
24 besorgniserregender Trend: Noch immer sind – trotz jahrelanger Diskussionen und
25 Warnungen – sehr relevante Teile unserer digitalen Infrastrukturen im
26 Sicherheitsbereich, auf Servern und in Cloud-Lösungen, bei denen der Zugriff
27 durch entsprechende rechtliche Regelungen nicht ausgeschlossen ist. Statt diese
28 Abhängigkeiten und Risiken schnellstmöglich zu reduzieren und für angemessene
29 Schutzstandards zu sorgen, versuchen Teile der aktuellen Bundesregierung
30 weitere, extrem risikoreiche Abhängigkeiten und Gefahren zu schaffen. Gerade hat
31 die Bundeswehr einen neuen Vertrag mit Google über die Nutzung der Cloud
32 geschlossen. Die schwarz-rote Bundesregierung prüft derzeit den Einsatz der
33 Analysesoftware des US-Unternehmens Palantir auch in Bundesbehörden, obwohl eine
34 Beschlusslage des Deutschen Bundestages dies ablehnt und auch die
35 Innenministerkonferenz vor neuen Abhängigkeiten und Gefahren warnt. Bereits in
36 der vergangenen Wahlperiode haben wir Grüne uns dafür eingesetzt, den Einsatz
37 solcher, mit grundlegenden rechtsstaatlichen Prinzipien unvereinbarer Systeme zu
38 verhindern. Seitdem hat sich die Lage weiter zugespitzt. Es bleibt dabei: Der
39 Einsatz von Palantirs Technologie birgt erhebliche verfassungs- und
40 europarechtliche Risiken und basiert auf Geschäftsmodellen, die im Widerspruch
41 zu Datenschutz, Transparenz und Grundrechten stehen. Ein Rückgriff auf solche
42 Systeme würde digitale Souveränität weiter schwächen, Bürger*innenrechte

43 gefährden und das Vertrauen in den Rechtsstaat untergraben. Dass wir strategisch
44 den Anschluss auch auf unserem eigenen Markt verpassen, zeigt die Entscheidung
45 Europas größten Softwarekonzerns SAP mit dem KI-Anbieter OpenAI zusammen zu
46 gehen, und damit künftig Verwaltungen, Schulen und Universitäten sowie andere
47 öffentliche Einrichtungen in Deutschland mit Anwendungen der Künstlichen
48 Intelligenz zu versorgen. Auch mit solchen Kooperationen droht die deutsche
49 Verwaltung in weitere Abhängigkeiten zu geraten, statt souveräne europäische
50 Alternativen aufzubauen.

51 Die digitale Abhängigkeit von außereuropäischen Anbietern ist längst
52 systemrelevant. Ob Cloud-Dienste, Betriebssysteme, KI-Anwendungen oder
53 sicherheitskritische Hardware, zentrale technologische Infrastrukturen stammen
54 überwiegend aus den USA oder China. Sowohl Wirtschaft, Verwaltung und
55 Bürger*innen haben nur noch begrenzte Wahlfreiheit über Hardware, Software und
56 Plattformen; oftmals geben marktdominante Akteure vor, wie wir digital agieren
57 können, und wie unsere Daten verarbeitet werden. Die Digitalgesetze der EU – von
58 DSA, über KI-VO, DSGVO, Data Act und DMA – müssen starke Aufsichtsbehörden in
59 einem ersten Schritt konsequent durchsetzen, um fairen Wettbewerb, Schutz der
60 Verbraucher*innen und Grundrechtsschutz zu gewährleisten. Deutschland und Europa
61 müssen deshalb strategisch umsteuern und eigene technologische Kapazitäten
62 aufbauen. Ein wichtiger Schritt sind Investitionen in freie, offene und
63 vertrauenswürdige Technologien, vor allem durch die öffentliche Hand. Sie ist
64 dem Gemeinwohl, der Verhältnismäßigkeit ihrer Ausgaben, dem verantwortlichen
65 Umgang mit Ressourcen und einer langfristigen Servicesicherheit verpflichtet.
66 Mit sogenannter Free and Open Source Software wird Wechselfähigkeit, Nähe zum
67 Anbieter zwecks Weiterentwicklung und Wartung im Ernstfall leicht möglich sein.
68 Mit der Aufnahme der IT-Sicherheit in das 500 Mrd. Euro-Sondervermögen haben wir
69 die Grundlage geschaffen, um Abhängigkeiten deutlich zu reduzieren und zukünftig
70 verstärkt auf Eigenentwicklungen zurückgreifen zu können. Mit der Sovereign Tech
71 Agency und dem Zentrum für Digitale Souveränität wurden in der vergangenen
72 Wahlperiode wichtige Grundlagen geschaffen. Nun braucht es eine langfristige
73 Förderstrategie, die Open Source, europäische Anbieter und faire
74 Wettbewerbsbedingungen auf digitalen Märkten gezielt stärkt.

75 Unsere digitale Infrastruktur muss so gestaltet sein, dass sie vor
76 Machtmissbrauch geschützt ist. Digitalisierung muss unserer Demokratie und
77 Menschenrechten dienen und nicht eine Gefahr für sie sein. Beste Daten- und
78 Grundrechtsschutz-Standards, Verschlüsselung und Dezentralität sind kein
79 Selbstzweck, sondern Schutz vor Überwachung, Diskriminierung und
80 Machtkonzentration. Sie sind zugleich Motor für vertrauensbasierte und
81 transparent Innovation und somit ein Wettbewerbsvorteil auf dem Markt für
82 Verbraucher*innen und Unternehmen, die Klarheit über ihre Rechte und ihre Daten
83 wollen. Eine digitale Infrastruktur, die auf Offenheit und Kontrolle durch
84 Parlamente und Öffentlichkeit setzt, ist die beste Versicherung gegen autoritäre
85 Versuchungen. Digitalisierung muss faschismussicher sein!

86 Als Grüne machen wir seit langem auf den Mehrwert von besten IT-
87 Sicherheitsstandards und Openness-Modellen, die Verbraucher*innen-Recht stärken
88 und zentral für Vertrauen in digitale Anwendungen sind, aufmerksam. Schleswig-
89 Holstein hat sich unter grüner Regierungsbeteiligung dafür entschieden,
90 Souveränität mit Open Source zu realisieren und versteht die Schaffung von
91 digitaler Souveränität durch Open Source Lösungen auch als Industriepolitik für
92 die Digitalwirtschaft. Das Land fördert heimische IT-Unternehmen, stärkt damit

93 den Standort für Fachkräfte und setzt darauf, dass entsprechende Lösungen,
94 beispielsweise durch den Wegfall von teils horrenden Lizenzkosten längerfristig
95 sogar günstiger als die Lösungen proprietärer Anbieter sind. Von solchen Best-
96 Practice-Beispielen können sowohl Bund als auch andere Länder lernen. Deshalb
97 sollte ein strukturierter Austausch über erfolgreiche Modelle digitaler
98 Souveränität etabliert werden, auch gemeinsam mit europäischen Staaten, die auf
99 diesem Weg bereits weiter sind.

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

116 Digitale Souveränität ist mehr als Technologiepolitik. Sie ist eine Investition
117 in die Menschen, die Europas digitale Zukunft gestalten. Wenn wir Innovation mit
118 Gemeinwohl, Transparenz und Nachhaltigkeit verbinden, schaffen wir nicht nur
119 neue Arbeitsplätze, sondern auch Vertrauen in den digitalen Wandel. Wir wollen
120 Talente fördern, die digitale Freiheit, Verantwortung und Demokratie zusammen
121 denken. Dafür braucht es eine gezielte europäische Förderstrategie für Open-
122 Source-Unternehmen, Start-ups und kleine sowie mittlere Betriebe, die faire
123 Rahmenbedingungen und Planungssicherheit schafft. Durch Investitionen in
124 Ausbildung, Fachkräfteentwicklung und Forschung können wir Talente in Europa
125 halten und neue Fachkräfte gewinnen, die unsere Werte und unseren
126 Gestaltungsanspruch teilen.

127 Wir Grüne wollen ein digitales Ökosystem, das demokratisch, nachhaltig und offen
128 gestaltet ist und die Resilienz unserer Gesellschaft stärkt. Im Mittelpunkt
129 stehen sechs Handlungsfelder, in denen politisches Handeln jetzt besonders
130 gefragt ist.

131 1. Europäische digitale Infrastruktur ausbauen

132 Deutschland muss die bereits ressortübergreifend vereinbarten Absprachen zur
133 Stärkung der digitalen Souveränität Deutschlands und Europas, etwa in der
134 Nationalen Sicherheitsstrategie, endlich mit politischem Leben füllen und
135 konsequent umsetzen. Europäische Initiativen wie die EuroStack-Initiative sollen
136 aktiv vorangetrieben und eine souveräne, offene und interoperable Cloud- und
137 Dateninfrastruktur in Europa gestärkt werden. Ziel ist der Aufbau einer starken
138 europäischen Cloud-, KI- und Halbleiterindustrie, die den europäischen
139 Datenschutz- und Sicherheitsstandards entspricht und rechtswidrige Datenabflüsse
140 ins Ausland effektiv unterbinden. So können wir auch für Länder außerhalb

141 Europas eine attraktive Kooperationsmöglichkeit eröffnen. Ansätze aus
142 Deutschland wie der „DeutschlandStack“ müssen europäisch kompatibel ausgestaltet
143 werden.

144 2. Open Source zum Standard machen

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

156 3. Kritische digitale Infrastrukturen schützen und europäisch absichern

157 Wir müssen die digitalen Infrastrukturen unseres Landes insgesamt besser
158 schützen. Anhaltende Fälle von Spionage, Sabotage und Cyberangriffen zeigen
159 deutlich, wie gefährdet insbesondere die kritische Infrastruktur Deutschlands
160 ist. Gerade hier gefährden auch Abhängigkeiten von außereuropäischen Anbietern
161 die Sicherheit und Handlungsfähigkeit unseres Staates. Die EU verpflichtet mit
162 der NIS-II- und der CER-Richtlinie zu einem umfassenden Schutz dieser zentralen
163 Systeme. Wir fordern eine kohärente Umsetzung beider Vorgaben in einem
164 Dachgesetz sowie den klaren Ausschluss unsicherer Komponenten in sensiblen
165 Bereichen.

166 4. Europäische Innovationskraft stärken

167 Gezielte Investitionen in Forschung, Start-ups und mittelständische IT-
168 Unternehmen sollen den Aufbau unabhängiger Schlüsseltechnologien fördern. Open
169 Source, faire Wettbewerbsbedingungen und europäische Zusammenarbeit sind die
170 Grundlage für technologische Souveränität. Der Staat kann dabei als
171 verlässlicher Ankerkunde auftreten, um europäischen Anbietern Planungssicherheit
172 zu geben und selbst mit gutem Beispiel für souveräne und nachhaltige Beschaffung
173 voranzugehen.

174 5. Nachhaltigkeit als Leitprinzip der Digitalisierung

175 Digitale Souveränität kann nur gelingen, wenn sie ökologisch und sozial
176 verantwortungsvoll gestaltet ist. Die Digitalisierung verbraucht enorme Mengen
177 an Energie und Ressourcen und eröffnet zugleich neue Chancen für Klimaschutz,
178 Ressourceneffizienz und nachhaltiges Wirtschaften. Nur eine nachhaltige
179 Digitalisierung ist eine souveräne Digitalisierung. Wenn Europa auf Green IT und
180 Kreislaufwirtschaft setzt, verbindet es technologische Unabhängigkeit mit
181 Klimaschutz und Verantwortung für eine lebenswerte digitale Zukunft.

182 6. Demokratie und Gemeinwohl digital absichern

183 Daten- und Grundrechtsschutz, Verschlüsselung und Transparenz müssen
184 Grundprinzipien staatlicher IT sein. Digitale Souveränität ist nur dann
185 glaubwürdig, wenn sie nicht nur in Sonntagsreden beschworen, sondern auch mit

186 konkretem politischem Leben gefüllt wird. Sie muss Demokratie, Grund- und
187 Menschenrechte sowie dem Gemeinwohl nutzen. Sie bedeutet nicht Abschottung,
188 sondern in einer zunehmend komplexen Welt, die Fähigkeit, technologische
189 Entscheidungen zukünftig unabhängig und wertebasiert zu treffen. Dazu gehört
190 auch, dass wir die Europäischen Gesetze in diesem Bereich effektiver machen,
191 statt sie auf Druck des Weißen Hauses oder als Zugeständnis an Deregulierung
192 nach dem Motto "anything goes" schwächen oder gar abschaffen. DSA, DMA, das KI-
193 Gesetz und Datengesetz müssen effektiv umgesetzt werden, die Behörden und
194 Agenturen, müssen deren Umsetzung gegenüber Unternehmen betreuen und erklären.
195 Demokratie bedeutet im 21. Jahrhundert Innovation mit Steuerung, kein Fliegen
196 auf Sicht.

197 Wir haben die Chance, ein digitales Europa zu schaffen, das Freiheit, Innovation
198 und Gerechtigkeit miteinander verbindet. Diese Chance dürfen wir nicht den
199 Techkonzernen überlassen. Europas digitale Zukunft gehört uns allen!

Begründung

Dieser Antrag baut auf den zentralen Prinzipien grüner Digitalpolitik der vergangenen Jahre auf: Offenheit, Transparenz, Datenschutz, Dezentralität und die enge Zusammenarbeit mit der digitalen Zivilgesellschaft. Diese Prinzipien leiten unser Handeln in Parlamenten, Regierungen und Verwaltungen und bilden die Grundlage für eine Politik, die technologische Unabhängigkeit mit Demokratie und Gemeinwohl verbindet.

Dieser Antrag wurde unter Mitwirkung der BAG Digitales und Medien, Alexandra Geese, Sergey Lagodinsky und Konstantin von Notz erstellt.

weitere Antragsteller*innen

Sergey Lagodinsky (KV Berlin-Pankow); Alexandra Geese (KV Bonn); Konstantin von Notz (KV Herzogtum Lauenburg); Friederike von Franqué (KV Frankfurt); Robert Lemke (KV Lübeck); Michael Seyfried (KV München); Andreas Döhling (KV Bremen Links der Weser (LdW)); Nadine Reers-Kleinhenz (KV Nürnberg-Land); Thomas Karcher (KV München); Stephan Clemens (KV Berlin-Steglitz/Zehlendorf); Elena Lorente-Rodriguez (KV Mannheim); Elias Bamidis (KV München); Margarete Prowe (KV Hamburg-Altona); Angela Büttner (KV München); Jana Ketzenberg-Schmid (KV Barnim); Markus Richter (KV Schwalm-Eder); Nikita Belov (KV Hamburg-Nord); Grit Menzzer (KV Berlin-Tempelhof/Schöneberg); Nadine Ulrich (KV Stuttgart); sowie 132 weitere Antragsteller*innen, die online auf Antragsgrün eingesehen werden können.