Deutscher Bundestag **Drucksache 21/8145**

21. Wahlperiode 23.09.2026

Antrag

der Abgeordneten Lukas Benner, Dr. Konstantin von Notz, Jeanne Dillschneider, Marcel Emmerich, Dr. Irene Mihalic, Marlene Schönberger und der Fraktion BÜNDNIS 90/DIE GRÜNEN

Digitale Grundrechte sichern – Datenschutz einfach, wirksam und föderal stärken

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

Die Digitalisierung ist in den letzten Jahren und Jahrzehnten in sämtliche Lebensbereiche von Bürgerinnen und Bürgern vorgedrungen. Personenbezogene Daten und Informationen sind längst zu einer lukrativen Handelsware geworden. So wird etwa auch mit Blick auf die jüngsten Vorkommnisse bezüglich der behördlichen Dateninfrastruktur in Berlin wieder deutlich, von welcher zentralen Bedeutung hohe Datenschutz- und IT-Sicherheitsstandards sind.

Eine Vielzahl von Unternehmen wird ihrer großen gesellschaftlichen und rechtlichen Verantwortung als Gatekeeper im digitalen Zeitalter bis heute nicht gerecht. Tägliche Sicherheitsvorfälle, Datenleaks und das wachsende Geschäft halbseidener Data-Broker zeigen, wie groß die Risiken für die informationelle Selbstbestimmung sind.

Die Datenschutz-Grundverordnung (DSGVO) hat sich als weltweit anerkannter Standard für den Schutz personenbezogener Daten bewährt. Sie schafft Vertrauen in digitale Dienste, stärkt die Rechte der Bürgerinnen und Bürger und ist zugleich Grundlage für einen fairen digitalen Binnenmarkt. Gleichzeitig gibt sie, flankiert durch die nationalen Datenschutzgesetze, den Unternehmen Rechtssicherheit. Dem Vertrauen der Bürgerinnen und Bürger in den Schutz ihrer Persönlichkeitsrechte bei der Verwendung ihrer Daten und Informationen wird im Prozess der Digitalisierung wesentlich durch ein modernes Datenschutzrecht Rechnung getragen.

Zugleich zeigt die praktische Anwendung des europäischen und nationalen Datenschutzrechts Reformbedarf. Denn Datenschutz muss nicht nur wirksam, sondern auch verständlich und praktisch handhabbar sein. Gerade zu Beginn der Geltung der DSGVO wurden durch unnötige und unsachgemäße Verkomplizierung (wie beispielsweise das „Klingelgate“, vgl. https://www.haufe.de/immobilien/verwaltung/datenschutz-namen-an-der-klingel-duerfen-dranbleiben_258_475476.html) Ängste geschürt und damit teilweise auch Profit gemacht. Heute belasten Doppelzuständigkeiten zwischen Bundes- und Landesbehörden, etwa auch im Vollzug der sich teilweise überlagernden neuen Digitalrechtsakte, uneinheitliche Rechtsanwendungen sowie ein unverhältnismäßiger Aufwand gerade für Vereine, Ehrenamtliche sowie kleine und mittlere Unternehmen (KMU)

die Praktikabilität und Akzeptanz des Datenschutzes, ohne dass daraus mehr Schutz für Betroffene entsteht. Auf diesen Reformbedarf und die Notwendigkeit einer einheitlichen Anwendung bestehenden Datenschutzrechts im Föderalen wurde wiederholt von der antragstellenden Fraktion und zuletzt auch im Bundesrat (BR-Drs. 356/26) hingewiesen. Eine solche Reform ist auch im Sinne der Aufsichtsbehörden selbst, da sie die Akzeptanz für einen einheitlichen Grundrechtsschutz stärkt. Vor diesem Hintergrund wurden auch aus dem Kreis der gemeinsamen Datenschutzkonferenz (DSK) wiederholt Reformvorschläge unterbreitet (vgl. https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2026/06/Stuttgarter-Impulse.pdf).

Was wir derzeit erleben, ist der Versuch, mühsam erkämpfte Grundrechte massiv zurückzufahren. Datenschutzrechtliche Schutzstandards sind wichtige Errungenschaften und immanente Teile der europäischen Werte und dürfen nicht unter dem Vorwand von Bürokratieabbau oder Wettbewerbsfähigkeit ausgehöhlt werden: Datenschutz darf nicht der Sündenbock sein für ausgebliebene Reformen und häufig extrem defizitäre Digitalisierungsprozesse sowie eine weitgehend verfehlte IT-Sicherheitspolitik. Nicht das Grundrecht auf informationelle Selbstbestimmung ist dafür verantwortlich, wenn digitale Verwaltungsverfahren schlecht konzipiert sind, IT-Systeme nicht interoperabel sind, Schutzmechanismen entweder nicht existent oder nicht durchgesetzt werden, Zuständigkeiten ungeklärt bleiben oder Behörden keine rechtssicheren und verständlichen Hilfestellungen anbieten.

Bund und Länder haben es über Jahre versäumt, die Sicherheit unserer digitalen Infrastrukturen sowie die informationelle Selbstbestimmung der Nutzerinnen und Nutzer zu stärken und notwendige Reformen voranzutreiben. Eine bewusste Nicht-Regulierung in Zeiten konstanten gesellschaftlichen und digitalen Wandels hat über Jahre dazu beigetragen, dass sich sehr ernste – längst auch sicherheitspolitische und demokratiefeindliche – Problemlagen deutlich verstärkt haben. Dies gilt gerade mit Blick auf die weiterhin dringend notwendige rechtsstaatliche Regulierung der sozialen Netzwerke. Diskussionen etwa um generelle Social-Media-Verbote oder weiter grassierende Desinformation zeugen hiervon.

Ein zentraler Reformbedarf besteht bei der Datenschutzaufsicht. Deutschland verfügt mit den unabhängigen Aufsichtsbehörden des Bundes und der Länder über eine historisch gewachsene, föderale Struktur. Daraus entstehen in der Praxis Abstimmungsbedarfe und teilweise divergierende Auslegungen. Unternehmen, die in mehreren Bundesländern tätig sind, können mit unterschiedlichen Ansprechpartnern und Bewertungsmaßstäben konfrontiert sein. Behörden müssen unter Umständen mit den Betroffenen erst komplizierte Zuständigkeitsfragen klären, bevor eine Beschwerde bearbeitet wird. Die zuständigen Aufsichtsbehörden sind weiterhin häufig personell nicht gut genug ausgestattet, um stark gestiegenen Anforderungen und Bedarfen in der Realität gerecht werden zu können. Herausfordernd ist für die zuständigen Behörden insbesondere, dass der europäische Gesetzgeber bei einer Vielzahl der neuen Digitalrechtsakten ihr konkretes Zusammenspiel mit der DSGVO nicht geregelt hat.

Die Bundesregierung hat wiederholt in der öffentlichen Debatte Vorschläge platziert, die auf eine Zentralisierung der Datenschutzaufsicht beim Bund sowie auf eine materielle Absenkung von Schutzstandards und Kontrollbefugnissen hinauslaufen. Konkrete Vorschläge fehlen jedoch bislang in Gänze. Dies führt zu einer weiter zunehmenden Verunsicherung von Öffentlichkeit und Unternehmen.

Eine pauschale Zentralisierung der Datenschutzaufsicht beim Bund wäre indes nicht der richtige Weg – denn Qualität folgt nicht aus schlichter Zentralität. Auch bei einer weitgehenden Verlagerung der Aufsicht auf die Bundesebene blieben Abstimmungen zwischen Bund und Ländern notwendig. Hinzu kommt, dass

föderale Aufsichtsstrukturen Bürgernähe, unterschiedliche fachliche Expertisen und gegenseitige institutionelle Kontrolle gewährleisten können. Gerade mit Blick auf die wichtige Beratungsfunktion, die den Aufsichtsbehörden der Länder gegenüber regionalen Unternehmen und Bürgerinnen und Bürgern zukommt, droht hier ein echter Rückschritt. Es steht auch zu befürchten, dass sich so die Kontrolldichte insgesamt, also insbesondere im Hinblick auf systematische Vor-Ort-Prüfungen, verringern wird.

Notwendig ist daher vielmehr eine Modernisierung der föderalen Aufsichtsstruktur durch verbindliche Kooperation, klare Zuständigkeiten und wirksame Verfahrenserleichterungen – bei vollständigem Erhalt des materiellen Schutzniveaus der DSGVO. Dazu gehören eine gesetzlich gestärkte Datenschutzkonferenz (DSK) mit verbindlicheren Koordinierungsmechanismen, klare Zuständigkeiten bei länderübergreifenden Sachverhalten, ein niedrigschwelliger Zugang für Bürgerinnen und Bürger sowie bessere Beratungsangebote insbesondere für – häufig ehrenamtlich geprägte – Vereine, aber auch Start-ups und KMU.

Auch auf europäischer Ebene müssen Vereinfachungen konsequent am risikobasierten Ansatz der DSGVO ausgerichtet werden, ohne Betroffenenrechte, Aufsichtsbefugnisse oder materielle Schutzstandards zu schwächen. Datenverarbeitungen mit geringem Risiko können zweifellos einfacher und unbürokratischer ausgestaltet werden; wo teils hochsensible Daten und Informationen verarbeitet, Menschen profiliert, präzise Standortdaten ohne Transparenz verkauft oder automatisierte Entscheidungen getroffen werden, braucht es dagegen auch weiterhin hohe Schutzstandards und wirksame Kontrolle. Zugleich müssen bestehende Reformlücken endlich geschlossen werden: u.a. braucht Deutschland einen wirksamen Beschäftigtendatenschutz mit klaren Regeln zu Anwendungsbereich, Profilbildung sowie Überwachung am Arbeitsplatz (vgl. hierzu bereits BT-Drs. 17/4853).

Datenschutz und Digitalisierung sind ganz gewiss keine Gegensätze – im Gegenteil! Ein moderner, innovativer Datenschutz schafft für die weitere Digitalisierung zentrales Vertrauen, sichert digitale Freiheit und gibt Innovation einen verlässlichen Rahmen.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. das bestehende materielle Schutzniveau der Datenschutz-Grundverordnung (DSGVO) und insbesondere die Rechte auf informationelle Selbstbestimmung und Schutz personenbezogener Daten nicht nur zu erhalten und zu verteidigen, sondern entschlossen weiterzuentwickeln;

2. von einer pauschalen Zentralisierung der Datenschutzaufsicht für den nicht-öffentlichen Bereich beim Bund abzusehen und dementsprechend die in der Föderalen Modernisierungsagenda vorgesehene Prüfung einer Aufhebung der Pflicht zur Bestellung von Landesdatenschutzbeauftragten nicht weiterzuverfolgen;

3. vorliegende Reformvorschläge aufzugreifen und gemeinsam mit den Ländern und den zuständigen Aufsichtsbehörden die DSK als zentrales Koordinierungs- und Kohärenzgremium der unabhängigen Datenschutzaufsichtsbehörden von Bund und Ländern gesetzlich zu institutionalisieren und dabei insbesondere

    a) ihr eine klare gesetzliche Grundlage und transparente Verfahrensregeln zu geben,

b) eine dauerhaft arbeitende Geschäftsstelle mit angemessener personeller und finanzieller Ausstattung einzurichten,

c) die Möglichkeit bindender Mehrheitsentscheidungen der DSK in Fragen der einheitlichen Rechtsanwendung zu schaffen, um eine kohärente Auslegung des Datenschutzrechts sicherzustellen und divergierende Entscheidungspraxis zwischen den Aufsichtsbehörden zu vermeiden sowie

d) eine zentrale, öffentlich zugängliche Datenbank mit Beschlüssen und gemeinsamen Auslegungsmaßstäben der deutschen Datenschutzaufsichtsbehörden aufzubauen;

4. gemeinsam mit den Ländern und den Aufsichtsbehörden die Zuständigkeiten der Datenschutzaufsicht für länderübergreifende Sachverhalte klarer zu ordnen und hierzu

   a) ein funktionierendes One-Stop-Shop-Prinzip einzuführen, nach dem bei gleichartigen länderübergreifenden Datenverarbeitungen grundsätzlich eine federführende Aufsichtsbehörde bestimmt wird, sodass Unternehmen und Einrichtungen mit länderübergreifender Tätigkeit einen klar zuständigen Ansprechpartner erhalten,

   b) für Sachverhalte von besonderer bundesweiter oder europäischer Bedeutung anhand eines transparenten Kriterienkatalogs gezielte Zuständigkeitskonzentrationen zu ermöglichen und

   c) für wiederkehrende und bundesweit vergleichbare Prüfgegenstände ein „Einer für Alle“-Prinzip (EfA-Prinzip) zu schaffen, durch das Prüfergebnisse einer Aufsichtsbehörde nach einheitlichen Standards auch von anderen Aufsichtsbehörden genutzt werden können;

5. einen niedrigschwelligen digitalen Zugang zur Datenschutzaufsicht einzurichten, über den Bürgerinnen und Bürger sowie Unternehmen Beratungsanfragen sowie Meldungen von Datenschutzverletzungen einreichen können und der in Kohärenz und im Zusammenspiel mit der Umsetzung der Verfahrensverordnung zur DSGVO

   a) Anliegen gegebenenfalls verlässlich an die zuständige Behörde weiterleitet,

   b) einheitliche Eingabeprozesse schafft,

   c) den Bearbeitungsstand für die Beteiligten nachvollziehbar macht und

   d) während des Verfahrens einen klaren Ansprechpartner gewährleistet;

6. gemeinsam mit den Ländern die Datenschutzaufsichtsbehörden personell und technisch so auszustatten, dass sie ihre – in den vergangenen Jahren stark gestiegenen – Kontroll-, Durchsetzungs- und Beratungsaufgaben tatsächlich effektiv und risikoorientiert erfüllen können, dabei ihre Kontrollressourcen insbesondere auf Datenverarbeitungen mit hohen Risiken für die Rechte und Freiheiten der Betroffenen zu konzentrieren, vor allem mit Blick auf komplexe datengetriebene Geschäftsmodelle, Künstliche Intelligenz und Datenhandel;

7. Beratung, Prävention und Auditierungen als Bestandteil der Datenschutzaufsicht weiter zu stärken und gemeinsam mit den Ländern

   a) niedrigschwellige Beratungs- und Schulungsangebote insbesondere für Vereine, ehrenamtlich Engagierte, Start-ups sowie kleine und mittlere Unternehmen nach dem Vorbild bestehender erfolgreicher Angebote (etwa der „Starthilfe Datenschutz“ in Berlin) auszubauen,

   b) bundesweit abgestimmte Muster, Praxisleitfäden und branchenspezifische Orientierungshilfen bereitzustellen sowie

   c) digitale Selbstchecks flächendeckend anzubieten, die bei wiederkehrenden Datenschutzfragen eine schnelle erste Orientierung ermöglichen;

   d) bei typischen Datenverarbeitungen ohne Risiken nicht notwendige Dokumentations-, Nachweis- und Verfahrensaufwände abzubauen und hierfür insbesondere für Vereine, ehrenamtlich Engagierte, Start-ups sowie kleinere und mittlere Unternehmen einfache und standardisierte Verfahren zu entwickeln;

   e) zu prüfen, wie Vereine und ehrenamtliche Strukturen bei der Umsetzung datenschutzrechtlicher Anforderungen weiter unabhängig beraten und entlastet werden können, ohne das materielle Datenschutzniveau abzusenken;

8. sich auf europäischer Ebene im weiteren Verfahren zum Digital-Omnibus und auch darüber hinaus dafür einzusetzen,

   a) den sachlichen und räumlichen Anwendungsbereich der DSGVO zu erhalten, insbesondere damit auch von einer Verengung des Begriffs personenbezogener Daten abzusehen,

   b) keine pauschalen Privilegierungen der Verarbeitung personenbezogener Daten für die Entwicklung und den Einsatz Künstlicher Intelligenz und stattdessen Regelungen zu Betroffenenrechten oder funktionsäquivalente Schutzmechanismen in KI-Systemen zu schaffen,

   c) den risikobasierten Ansatz der DSGVO klarer zu verankern, sodass Unternehmen bei Datenverarbeitungen mit geringem Risiko von vereinfachten Dokumentationsanforderungen profitieren können,

   d) besonders risikoreiche Sachverhalte mit Datenschutzbezug, wie z. B. den Betrieb von Datenhandelsplattformen und den Handel mit präzisen Standortdaten, strenger zu regulieren sowie

   e) nutzungsgerechte Regelungen zu entwickeln für Einwilligungsentscheidungen, die wiederkehrende Cookie-Banner reduzieren und so einmal getroffene Entscheidungen zuverlässig durchgehend berücksichtigen und die Verantwortlichkeit von Herstellern klarstellen;

9. gemeinsam mit den Ländern die Reform der Datenschutzaufsicht spätestens zwei Jahre nach Inkrafttreten zu evaluieren und insbesondere die Entwicklung der Bearbeitungszeiten, die Einheitlichkeit der Rechtsanwendung, die Zahl länderübergreifender Verfahren, die Nutzung von

Beratungsangeboten und die praktische Wirksamkeit der neuen Koordinierungsmechanismen zu veröffentlichen;

10. einen Gesetzentwurf für ein eigenständiges Beschäftigtendatenschutzgesetz (vgl. etwa Bundestags-Drucksache 17/4853) vorzulegen, in dem unter Nutzung des Ausgestaltungsspielraums der Umgang mit Beschäftigtendaten umfassend geregelt wird und dabei insbesondere

    a) die Anforderungen an die Datenverarbeitungsgrundsätze im Beschäftigtenkontext zu konkretisieren, indem technische und organisatorische Maßnahmen zur Vermeidung von Beschäftigten-Profilings getroffen werden,

    b) klargestellt wird, dass es ein umfassendes Mitbestimmungsrecht für betriebliche Interessenvertretungen beim Datenschutz gibt,

    c) klargestellt wird, dass auch bestimmte nichtautomatisierte Informationsverarbeitungen wie etwa Regelungen zum Fragerecht der Arbeitgeber ebenfalls vom Anwendungsbereich des Datenschutzrechts umfasst sind,

    d) beim Beschäftigungsbegriff auch Werkvertragsbeschäftigte miteinbezogen werden und

    e) der Videoüberwachung von Beschäftigten in öffentlich zugänglichen Räumen klare Grenzen gesetzt werden, wobei dafür gesorgt wird, dass Beschäftigte bei der Videoüberwachung möglichst nicht erfasst werden;

11. sich parallel auf europäischer Ebene für harmonisierte Regelungen des Beschäftigtendatenschutzes einzusetzen.

Berlin, den 22. September 2026

Katharina Dröge, Britta Haßelmann und Fraktion