Plattform Privatheit und selbstbestimmtes
Leben in der digitalen Welt

Plattform Privatheit

Michael Friedewald, Alexander Roßnagel und Christian Geminn

INNOVATION, WETTBEWERB UND WERTEORIENTIERUNG

Datenschutz- und Digitalregulierung zwischen Innovationshemmnis und Standortvorteil

Hintergrundbericht

Herausgegeben von Michael Friedewald, Alexander Roßnagel, Christian Geminn und Murat Karaboga

Impressum

Forschungsberichte der Plattform Privatheit Nr. 9

Autorinnen und Autoren

Michael Friedewald[1], Alexander Roßnagel[2,3], Christian Geminn[2]
(1) Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe
(2) Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG)
(3) Hessischer Beauftragter für Datenschutz und Informationsfreiheit, Wiesbaden

Reihe

ISSN (Print)	2199-8906
ISSN (Online)	2199-8914
DOI	10.24406/publica-9910

Veröffentlichung

September 2026, 1. Auflage
Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe

Zitierempfehlung

Friedewald, M. et al. (2026): Innovation, Wettbewerb und Werteorientierung: Datenschutz- und Digitalregulierung zwischen Innovationshemmnis und Standortvorteil. Forschungsberichte der Plattform Privatheit Nr. 9. Karlsruhe: Fraunhofer ISI.

Hinweise

Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung – Nicht kommerziell – Keine Bearbeitungen 4.0 International Lizenz.
Die Informationen wurden nach bestem Wissen und Gewissen unter Beachtung der Grundsätze guter wissenschaftlicher Praxis zusammengestellt. Die Autorinnen und Autoren gehen davon aus, dass die Angaben in diesem Bericht korrekt, vollständig und aktuell sind, übernehmen jedoch für etwaige Fehler, ausdrücklich oder implizit, keine Gewähr. Die Darstellungen in diesem Dokument spiegeln nicht notwendigerweise die Meinung des Fördergebers wider.

Inhalt

1 Weniger Datenschutz, mehr Innovation? Warum die Gleichung nicht aufgeht 5

2 Was die Debatte behauptet – und was die Evidenz zeigt 7

2.1 Blockiert der Datenschutz die Forschung? Wo das Problem wirklich liegt 7

2.2 Mehr Daten, bessere KI? Warum Quantität nicht Qualität ersetzt 10

2.3 Wer verliert durch die DSGVO – und wer gewinnt? 12

2.4 Compliance-Kosten: Teuer für alle – aber für wen zu teuer? 15

2.5 Wer nicht reguliert, verteilt Risiken – aber maximiert nicht den Nutzen 18

3 Was Europa von Innovationen verlangen darf – und muss 20

3.1 Nicht jede Innovation verdient Förderung – Werte sind der Maßstab 20

3.2 Die DSGVO privilegiert Forschung, doch Forschungsfreiheit endet, wo Grundrechte anderer beginnen 21

3.3 Wer Risiken schafft, muss Vorausschau üben – der Markt allein entscheidet nicht 22

3.4 Vertrauen wirkt – aber nicht überall und nicht für alle gleich 23

3.5 Digitale Souveränität: Datenschutz als Fundament europäischer Selbstbestimmung 25

4 Wie lassen sich Innovation und Werteorientierung praktisch verbinden? ..27

4.1 Forschung braucht Rechtssicherheit – nicht Rechtsfreiheit 27

4.2 Datenschutz als Designprinzip: Werteorientierte Technikgestaltung als Innovationstreiber 28

4.3 Governance neu denken: Datenschutz als strategische Organisationsaufgabe 30

4.4 Datenschutz und Wettbewerbsfähigkeit: Asymmetrien abbauen, Innovationsstärken skalieren 31

4.5 Datenschutz und IT-Sicherheit: Synergie statt Zielkonflikt 32

5 Fazit 34

6 Literaturverzeichnis 35

1 Weniger Datenschutz, mehr Innovation? Warum die Gleichung nicht aufgeht

Europa steht an einem Scheideweg: In strategischen Zukunftstechnologien droht der Anschluss verloren zu gehen. Die USA und China dominieren bei KI, Cloud-Infrastrukturen und Quantencomputing mit massiven Investitionen, während europäische Unternehmen zurückfallen – mit Folgen für Wettbewerbsfähigkeit, Wohlstand und geopolitische Handlungsfähigkeit. In dieser Situation fordern Teile der Wirtschaft eine grundlegende Kurskorrektur: weniger Regulierung, weniger Bürokratie, mehr unternehmerische Freiheit. Insbesondere die Datenschutz-Grundverordnung (DSGVO) und andere europäische Datengesetze werden als „Innovationsbremse" gebrandmarkt. Die Forderung lautet: Befreiung von „lästigen Vorgaben", um im globalen Wettbewerb bestehen zu können. Wie lässt sich in dieser Situation eine Politik gestalten, die Datenschutz und wirtschaftliche Innovationsfähigkeit nicht gegeneinander ausspielt, sondern wertorientiert miteinander verbindet?

Dieses White Paper prüft, ob wissenschaftliche Evidenz die oft emotional geführten Debatten tatsächlich stützt und zeigt einen wertorientierten Weg auf, wie sich Datenschutz und digitale Innovationsfähigkeit in Deutschland und Europa verbinden lassen. Im Zentrum steht dabei nicht Innovation im Allgemeinen, sondern speziell digitale, datenbasierte Innovation: KI- und Big-Data-Anwendungen, datengetriebene Geschäftsmodelle und Infrastrukturen, die auf umfänglicher Datennutzung beruhen. Statt pauschaler Antworten analysiert es differenziert: Welche Wirkungen hat Datenregulierung nachweislich auf verschiedene Innovationstypen? Welche Unternehmen sind tatsächlich betroffen? Wo liegen die realen Probleme – und wo werden Einzelfälle verallgemeinert?

Zugleich ist klar: Der Status quo ist verbesserungswürdig. Komplexität, Rechtsunsicherheit und Compliance-Aufwände belasten insbesondere KMU und Start-ups überproportional. Eine Reform muss praxistaugliche Lösungen finden, die Innovation erleichtern, ohne Grundrechte zu gefährden. Die zentrale Herausforderung lautet: Wie gelingt dieser Balanceakt?

Das White Paper nähert sich dieser komplexen Fragestellung aus drei komplementären Perspektiven, die gemeinsam den Raum für einen europäischen Weg aufspannen:

Die *Wirtschaftsperspektive* in Abschnitt 2 stellt Einschätzungen und Forderungen aus der Wirtschaft vor, die als notwendig angesehen werden, um die Wettbewerbsfähigkeit europäischer Unternehmen entscheidend zu verbessern. Diesen werden aus einer Evidenzperspektive Erkenntnisse gegenübergestellt, was wir tatsächlich über die Bedingungen digitaler Innovationen in Europa wissen. Stellt der Datenschutz einen Ballast dar – oder können Datenschutz, Transparenz und Vertrauenswürdigkeit nicht gezielt als Differenzierungsmerkmal genutzt und vermarktet werden. Welche Rahmenbedingungen benötigen Innovationen tatsächlich – und welche gängigen Annahmen halten einer empirischen Überprüfung stand?

Die *Werteperspektive* in Abschnitt 3 kehrt die Fragerichtung um: Was darf und muss Europa von Innovationen verlangen? Welche Innovationen fördern gesellschaftlichen Zusammenhalt, Demokratie und Gemeinnutz – statt ausschließlich kurzfristigem Profit zu dienen? Sie fragt, welche Innovationspfade mit europäischen Grundwerten vereinbar sind, und entwickelt in fünf Schritten einen normativen Rahmen: von Akzeptabilität als Maßstab über die Reichweite der Forschungsfreiheit, das Vorsorgeprinzip und die Vertrauensdividende bis zum Datenschutz als Fundament digitaler Souveränität.

Die *Integrationsperspektive* in Abschnitt 4 untersucht schließlich, wie beide Ansätze praktisch zusammengeführt werden können – durch politische Instrumente (z. B. reformierte Regulierung), wirtschaftliche Anreize (z. B. Förderung werteorientierter Innovation) und technologische Gestaltung (z. B. Werteberücksichtigung by Design). Entsteht ein nachhaltiger europäischer Weg, wenn beide Dimensionen nicht gegeneinander ausgespielt, sondern strategisch verzahnt werden?

Ziel dieses White Papers ist es, einen Weg aufzuzeigen, der weder naive Regulierungsskepsis noch unreflektierten Wettbewerbspessimismus zulässt, sondern werteorientierte Innovation als eine Strategie versteht, die wirtschaftliche Chancen – neue Märkte, Vertrauen, Wettbewerbsfähigkeit – aktiv nutzt und zugleich offen benennt, dass Datenschutz stets auch Kosten und Nebenwirkungen hat, die abgewogen, ausgehandelt und politisch entschieden werden müssen – fundiert auf wissenschaftlicher Evidenz statt auf Behauptungen.

2 Was die Debatte behauptet – und was die Evidenz zeigt

Innovationen – verstanden als die Einführung eines neuen oder wesentlich verbesserten Produkts, Prozesses oder einer organisatorischen Methode in der Unternehmenspraxis, am Markt oder in der Gesellschaft[1] – sind eine zentrale Triebkraft wirtschaftlicher und gesellschaftlicher Entwicklung. Sie gehen über die bloße Erfindung hinaus und schließen deren praktische Anwendung, Markteinführung oder gesellschaftliche Adoption ein. Im Unterschied zur Forschung – der systematischen Suche nach neuen Erkenntnissen mit dem primären Ziel der Wissensgenerierung[2] – zielt Innovation auf die Nutzung und Verwertung dieses Wissens zur Lösung konkreter Probleme. Zwischen diesen Bereichen besteht ein enges Wechselverhältnis: Forschung kann ein wesentlicher Input für radikale Innovationen sein, doch führt nicht jede Forschung zu Innovation; umgekehrt entstehen viele Innovationen auch ohne neue Forschung, etwa durch Rekombination bestehenden Wissens oder durch organisatorische Veränderungen. Innovationen sind kontextabhängig und entstehen in komplexen Interaktionsprozessen zwischen Akteuren wie Unternehmen, Forschungseinrichtungen, Nutzern und Politik; sie folgen dabei keinem linearen, sondern einem iterativen und systemischen Prozess, der sowohl beabsichtigte als auch unbeabsichtigte Folgen haben kann und dessen Erfolg maßgeblich von institutionellen Rahmenbedingungen, gesellschaftlicher Akzeptanz sowie der Absorptions- und Anpassungsfähigkeit des jeweiligen Systems abhängt.

Digitale, datenbasierte Innovationen wie KI/Machine Learning, Cloud-Infrastrukturen oder IoT-Plattformen werden aktuell als strategisch wichtig betrachtet, da sie fundamentale Wettbewerbsvorteile verschaffen, Geschäftsmodelle transformieren oder kritische Erfolgsfaktoren einer Volkswirtschaft nachhaltig verbessern. Ihre Bedeutung ergibt sich aus dem Potenzial für Skalierbarkeit, Netzwerkeffekte sowie ihrer Fähigkeit, neue Wertschöpfungslogiken zu ermöglichen. Unbestritten ist dabei, dass die Gestaltung digitaler Innovationen im Einklang mit Werten wie Demokratie, Menschenwürde, Datenschutz, sozialer Gerechtigkeit und ökologischer Nachhaltigkeit sein sollte. Dies schließt die Absicht ein, die technologische Leistungsfähigkeit nach ethischen Prinzipien und gesellschaftlichen Zielen voranzutreiben.

Doch was bedeutet dies konkret für die Gestaltung der Rahmenbedingungen? Die folgenden fünf Abschnitte untersuchen das Verhältnis von Datenregulierung und Innovationsprozess – vom Forschungsprozess über die Innovationsentwicklung bis hin zu Markteinführung und Wettbewerb.

2.1 Blockiert der Datenschutz die Forschung? Wo das Problem wirklich liegt

Aus Wirtschaftsperspektive sind Forschung und auf dieser Forschung basierende Innovationen Voraussetzungen für die Fortentwicklung unserer Wirtschaft und Gesellschaft. Derzeit findet ein tiefgreifender technologischer Wandel statt. Schlüsseltechnologien wie künstliche Intelligenz und andere datengetriebene Technologien entscheiden nicht nur über den individuellen Erfolg einzelner Unternehmen, sondern sind sogar zentrale Faktoren für das weitere Wohlergehen von ganzen Staaten. Deutschland und Europa müssen diese Entwicklung aktiv und an der Spitze des Wettbewerbs mitgestalten, um auf die eigene künftige Entwicklung Einfluss zu behalten.[3] Dabei muss differenziert werden: Strukturelle Erkenntnisse stehen dem individuellen Nutzen von Forschung gegenüber. Beide Ebenen müssen Beachtung finden, damit Forschung sich in spürbare Verbesserung des täglichen Lebens übersetzt. Gefördert werden sollte deshalb nicht allein die akademische Forschung, sondern auch die Forschung im industriellen Kontext.

---

1 OECD und Eurostat, *Oslo-Handbuch 2018*, Kap. 2, m.w.N. Rammert, „Die Innovationen der Gesellschaft".

2 OECD, *Frascati-Handbuch 2015*.

3 Weber u. a., *Wege zur Stärkung der Forschung und Anwendung von künstlicher Intelligenz in Europa*.

Hierfür werden insbesondere datenschutzrechtliche Vorgaben vielfach als Hindernis für eine international konkurrenzfähige Forschung empfunden. Häufig wird die Frage gestellt, ob forschungsbezogene Datenerhebungen oder Zugriffe auf bestehende Datensammlungen rechtlich zulässig sind, und oft fehlt vor Ort die rechtliche Expertise, um diese Fragen zuverlässig, eindeutig und schnell zu beantworten. In solchen Konstellationen wird das Datenschutzrecht tatsächlich zu einem Forschungshindernis. Im schlimmsten Fall werden Forschungsvorhaben bereits im Vorhinein verworfen, weil rechtliche Vorgaben und Risiken falsch eingeordnet werden. Weiter verschlimmert wird die Situation, wenn vor Ort unterschiedliche Behauptungen über die Interpretation von datenschutzrechtlichen Vorgaben vorliegen.

Der Impuls, Forschung ohne (datenschutz-)rechtliche Grenzen zu fordern („Innovation first, Bedenken second"[4]), ist vor diesem Hintergrund weit verbreitet. Jede wertebezogene Anforderung wird zunächst als ein Hindernis für Forschung empfunden: Solche Anforderungen führten zu Wettbewerbsnachteilen und politischen Schwachstellen, die sich Deutschland und Europa nicht leisten können.

Dabei sollte jedoch beachtet werden, dass Forschung schließlich in die Praxis überführt werden muss, damit (unter anderem) technische Innovationen oder innovative Geschäftsmodelle entstehen. Diese müssen dann den geltenden rechtlichen Anforderungen und den dahinterliegenden Wertvorstellungen entsprechen. Es ist somit in vielen Kontexten erforderlich, rechtliche Anforderungen bereits im Rahmen der Forschung mitzudenken.

Anders sind Fälle zu beurteilen, bei denen Daten lediglich zur Erkenntnisgewinnung im Forschungsprozess dienen. Hier bietet das geltende Recht bereits beträchtliche Spielräume, die außerhalb des Forschungssektors nicht zur Verfügung stehen. Aber auch hier gilt, dass die Forderung nach einer schrankenlosen Forschung, die gänzlich auf datenschutzbezogene Anforderungen verzichtet, zu kurz gegriffen ist, da auch im Bereich der Forschung Risiken bestehen, die vermieden oder minimiert werden müssen.

Lediglich dort wo tatsächlich rechtliche Hürden gesellschaftlich wünschenswerte Forschung behindern, müssen die rechtlichen Spielräume aktualisiert und erweitert werden. Hier stellen sich jedoch mitunter wichtige Grundsatzfragen – etwa ob eine schrankenlose Auswertung sämtlicher im Internet frei verfügbarer Informationen notwendig ist, um international konkurrenzfähige Forschung und schließlich auf ihrer Basis konkurrenzfähige Dienstleistungen zu ermöglichen, oder ob existierende Schranken zurecht bestehen, um zu verhindern, dass der einzelne Mensch und seine Lebensäußerungen zur Datenquelle reduziert werden.

Am lautesten und drastischsten dürfte die Kritik am Datenschutz im Bereich der medizinischen Forschung sein. In kaum einem anderen Bereich wird in der öffentlichen Debatte so häufig behauptet, datenschutzrechtliche Vorgaben behinderten die Forschung: Die Datenschutz-Grundverordnung blockiere klinische Studien, verhindere die Nutzung von Patientendaten und treibe die europäische Pharmaforschung in asiatische Länder mit laxeren Datenschutzstandards. Ist die DSGVO also tatsächlich ein strukturelles Hindernis für medizinischen Fortschritt – oder liegt das Problem an anderer Stelle?

Systematische quantitative Evidenz ist in diesem Bereich rar. Verfügbar sind lediglich Fallberichte und qualitativen Studien, die reale Probleme im Forschungsalltag dokumentieren. Eine der wenigen quantitativen Fallstudien beziffert den Compliance-Aufwand für ein öffentlich gefördertes palliativmedizinisches Forschungsprojekt auf rund 1.713 Arbeitsstunden und Kosten von knapp 55.000 Euro

[4] Slogan der FDP im Bundestagswahlkampf 2017, der seither die Überzeugung auf den Punkt bringt. dass zu viele regulatorische Einschränkungen Innovationen in Deutschland behindern, siehe z.B. die Website der Friedrich-Naumann-Stiftung https://www.freiheit.org/de/zukunft-durch-innovation, aber auch https://eco.de und https://ki-verband.de/

– etwa 4 % der Gesamtfördersumme, welche ausschließlich für datenschutzrechtliche Aufgaben aufgewendet werden mussten (u.a. Änderung des Studiendesigns, Reduktion des Datenumfangs).[5]

Ein skandinavisches Forschungskonsortium zur personalisierten Medizin berichtete, mehr Zeit mit der DSGVO-Compliance verbracht zu haben als mit der eigentlichen Forschung – ausgelöst nicht durch das EU-Recht selbst, sondern durch fehlende einheitliche Vertragsvorlagen und divergierende institutionelle Auslegungen.[6] Eine breit angelegte empirische Studie aus 25 EU-Ländern bestätigte diesen Befund: Als größte Herausforderung gilt nicht die DSGVO als solche, sondern die mangelnde Harmonisierung ihrer Auslegung durch nationale Behörden, Ethikkommissionen und andere Kontrollinstitutionen – bis hin zu widersprüchlichen Entscheidungen verschiedener Häuser in derselben Stadt.[7] Gleichzeitig identifizierte eine weitere Studie die DSGVO ausdrücklich als Enabler: Sie stärke das Patientenvertrauen und schaffe Transparenz – hemmend wirke sie fast ausschließlich dort, wo heterogene Implementierung und Überinterpretation dominieren.[8] Die Deutsche Gesellschaft für Innere Medizin (DGIM) und der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) haben im November 2025 einen Leitfaden zur datenschutzgerechten Forschung mit Gesundheitsdaten veröffentlicht, der anhand realer Beispiele aus der Inneren Medizin zeigt, wie Forschungsprojekte rechtssicher und zugleich praktikabel umgesetzt werden können.[9]

Ein in der Debatte oft unterschätzter Befund betrifft nicht allein die rechtlichen Hürden, sondern die grundsätzliche *Bereitschaft zum Datenaustausch*: Die Neigung von Wissenschaftlerinnen und Wissenschaftlern, eigene Daten zu teilen oder auf geteilte Daten anderer zurückzugreifen, ist ausgesprochen gering – und dies selbst dort, wo politischer Wille und technische Infrastruktur vorhanden sind. Konzepte wie die „Datenspende" finden bislang kaum praktische Nutzung.[10] Ob diese Abneigung primär auf datenschutzrechtliche Anforderungen zurückzuführen ist oder tieferliegenden kulturellen und strukturellen Faktoren geschuldet ist, lässt sich empirisch nicht abschließend klären – und verdient in der Reformdebatte deutlich mehr Aufmerksamkeit.

Besonders aufschlussreich ist ein finnischer Befund, der zwischen den Effekten der DSGVO und denen eines *nationalen Folgegesetzes* differenziert: Der Geltungsbeginn der DSGVO 2018 hatte demnach keinen messbaren negativen Effekt auf die registerbasierte Forschung. Erst der finnische Secondary Use Act von 2020, der erheblich mehr Bürokratie und Kosten mit sich brachte, führte zu einem Einbruch der genehmigten Datenpermits von geschätzt 47 % im Jahr 2023. Für den European Health Data Space, der 2025 verabschiedet wurde und bis März 2027 schrittweise in den Mitgliedsstaaten umgesetzt werden muss (und dem finnischen Modell strukturell ähnelt), sind dies ernüchternde Vorzeichen.[11]

Ein weiteres dokumentiertes Problemfeld ist der *Datentransfer in Drittländer*: Nach dem Schrems-II-Urteil des Europäischen Gerichtshofs[12] – das den Angemessenheitsbeschluss der EU-Kommission für das EU-US Privacy Shield für ungültig erklärte und strengere Anforderungen an die Datenübertragung stellte – wurden mindestens 40 klinische Studien suspendiert oder verzögert[13]; europäische Pharmaunternehmen wichen zunehmend auf Gesundheitsdaten aus Ländern wie Japan oder Taiwan aus. Die praktische Konsequenz erschien paradox: Die Aufkündigung freien Datenverkehrs trieb die Forschung in Länder mit tendenziell höheren Schutzstandards. Seit 2023 gibt es jedoch

5 Kurkowski u. a., „Mehr Barrieren als Brücken".
6 Glintborg u. a., „Legal Obstacles Jeopardise Research in Personalised Medicine".
7 Lalova-Spinks u. a., „Challenges Related to Data Protection in Clinical Research before and during the COVID-19 Pandemic".
8 Vukovic u. a., „Enablers and Barriers to the Secondary Use of Health Data in Europe".
9 HBDI und DGIM, *Datenschutz in der medizinischen Forschung*.
10 Vukovic u. a., „Enablers and Barriers to the Secondary Use of Health Data in Europe"; Bobrov u. a., „Six Solutions for Clinical Study Data Sharing in Germany".
11 Brück u. a., „European Health Regulations Reduce Registry-Based Research"; Becker und Dove, „The EU GDPR and secondary use of health and genetic data for research support purposes".
12 EuGH vom 16.7.2020 – C-311/18 – ECLI:EU:C:2020:559.
13 Bentzen u. a., „Remove Obstacles to Sharing Health Data with Researchers Outside of the European Union".

mit dem EU-US Data Privacy Framework (DPF) und dem Angemessenheitsbeschluss der EU-Kommission direkte Nachfolgeregelungen für das EU-US Privacy Shield, wodurch der Datenaustausch mit den USA wieder erleichtert wurde.[14] Auch der Datenaustausch mit Japan, Brasilien, Kanada, Südkorea, Schweiz, dem Vereinigten Königreich und weiteren Staaten[15] ist auf der Grundlage von Anerkennungsbeschlüssen grundsätzlich möglich. Dies gilt nach Art. 46 Abs. 2 Buchst. c DSGVO auch für Empfänger, die ihren Sitz in Ländern ohne angemessenes Datenschutzniveau haben, wenn mit diesen Standardvertragsklauseln abgeschlossen worden sind.[16] Allerdings wird auch das EU-US Data Privacy Framework nach einer Entscheidung des US Supreme Courts[17] jüngst wieder stark in Zweifel gezogen.

Das Gesamtbild ist damit klarer als die öffentliche Debatte suggeriert: Die DSGVO schließt medizinische Forschung nicht aus und bietet durch ihre Forschungsprivilegien erhebliche Spielräume (vgl. dazu Abschnitt 3.2). Die eigentlichen, praktischen Herausforderungen liegen auf drei Feldern: erstens der Harmonisierung von Verfahren und Vorlagen für grenzüberschreitende Forschungskooperationen innerhalb Europas, zweitens praxistauglichen Regelungen für den Datentransfer zu öffentlichen Forschungseinrichtungen außerhalb des EWR und drittens einer kritischen Prüfung, inwieweit der European Health Data Space tatsächlich zur Entbürokratisierung beiträgt – oder die finnischen Erfahrungen europaweit repliziert.

2.2 Mehr Daten, bessere KI? Warum Quantität nicht Qualität ersetzt

In der digitalen Gesellschaft entstehen Innovationen vor allem durch die Nutzung von Daten. Die zunehmende Digitalisierung von gesellschaftlichen und wirtschaftlichen Prozessen führt zu einer Vielzahl von Daten, die entsprechend ausgetauscht werden. Produktion, Logistik, Dienstleistungen, Kommunikation, Mobilität, Energieversorgung, Handel und Werbung, Unterhaltung, medizinische Versorgung und Verwaltung werden durch Informationstechnik unterstützt oder beruhen auf Informationstechnik. Dadurch entstehen in allen Prozessen Daten, die es ermöglichen, diese Prozesse zu steuern und nachzuvollziehen. Die Nutzung dieser Daten wird damit zur Grundlage von Forschung und Innovation, die an diese Prozesse anknüpfen, deren Probleme lösen und sie in ihrer Wertschöpfung weiterentwickeln können.

Big-Data-Auswertungen versprechen, bei der Verfügbarkeit großer Datenmengen Strukturen zu erkennen und Prozesse zu steuern und so in allen Gesellschafts- und Wirtschaftsbereichen die Effizienz und Effektivität zu steigern.

Systeme Künstlicher Intelligenz versprechen, Wissen praxisorientiert und problemorientiert zur Verfügung zu stellen und als Agenten für die nutzenden Instanzen selbständig Aufgaben zu lösen. Hierfür lernen sie auf der Grundlage von Daten in jeder Form: Schriften, Bilder, Sprache, Programm-Code. Notwendig sind riesige Mengen an Daten aus dem jeweiligen Einsatzfeld der geplanten KI. Für KI mit allgemeinem Verwendungszweck sind Daten aus allen Lebensbereichen erforderlich.

Sowohl für Big Data als auch für KI sind Skalenerträge entscheidend: Je mehr Daten sie miteinander verknüpfen können, desto mehr Erträge sind möglich. Es gilt daher der Grundsatz: je mehr geeignete Daten zur Verfügung stehen, desto besser ist die Arbeitsgrundlage für Forschung und Innovation und umso besser sind ihre Ergebnisse.

---

14 Europäische Kommission, „Durchführungsbeschluß (EU) 2023/1795".

15 Europäische Kommission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

16 vgl. z.B. Schantz, in: Simitis u. a., *Datenschutzrecht DSGVO mit BDSG*, Art. 46, Rn. 32 ff.

17 Trump v. Slaughter, 609 U.S. (U.S. Supreme Court 2026).

Umfragen unter Forschungseinrichtungen und Wirtschaftsunternehmen kommen regelmäßig zu dem Ergebnis, dass der fehlende Zugang zu ausreichenden Datenmengen für das Training von KI-Modellen ein erhebliches Hemmnis für die akademische Forschung und die industrielle Entwicklung darstellt.[18] Den Zugang zu Daten sehen viele als entscheidenden Wettbewerbsfaktor und fordern, dass der Zugang zu Daten in Europa genauso einfach sein sollte wie in den USA oder China.

Für viele Prozesse in der Wirtschaft fehlt jedoch die Bereitschaft der Dateninhaber, ihre Daten der Allgemeinheit inklusive der Wettbewerber zur Verfügung zu stellen. Viele Prozess- und Struktur-, Planungs- und Ergebnisdaten werden als Geschäfts- und Betriebsgeheimnisse sorgsam gehütet und gerade nicht geteilt.

Soweit Big Data genutzt werden soll, um auch das Verhalten von einzelnen Menschen und großen Gruppen zu analysieren und zu steuern, sind sie auch auf die Erhebung personenbezogener Daten angewiesen. Das gleiche gilt für KI-Systeme, die personalisierte Ergebnisse und individuelle Unterstützung bieten sollen. Vielfach genügt es, die personenbezogenen Daten zu aggregieren oder zu anonymisieren, um mit ihnen arbeiten zu können. Wo dies aber nicht möglich ist, kann das Datenschutzrecht der Erfassung großer Datenmengen entgegenstehen.

Auch für diese Fälle wird vertreten, dass „Datenreichtum besser sei als Datenarmut".[19] Viele sehen das Gebot der Datenminimierung in Art. 5 Abs. 1 Buchst. c DSGVO dazu als strukturellen Widerspruch, der daher einer positiven Entwicklung von Wirtschaft und Gesellschaft durch datengestützte Forschung und Innovation entgegenstehe. Daher wird bisweilen gefordert, dass – insbesondere für medizinische Forschung das Minimierungsgebot ausgesetzt werden müsste.[20]

Die pauschale These, ein maximaler Datenzugang sei die entscheidende Voraussetzung für KI-Innovation, ist an großen Sprachmodellen orientiert und muss bei genauerer Analyse empirischer Studien für die Situation in Europa stark differenziert werden.

So zeigte beispielsweise eine amerikanische Befragung von 325 KI-Startups, dass nicht die bloße Datenmenge, sondern die Exklusivität und Passgenauigkeit der Trainingsdaten über den Markterfolg von KI-Unternehmen entscheidet. Startups, die proprietäre – also selbst erhobene und nicht allgemein zugängliche – Trainingsdaten einsetzen, erhalten signifikant mehr Wagniskapital als solche, die ausschließlich auf öffentlich verfügbare Datensätze zurückgreifen. Dieser Zusammenhang ist besonders ausgeprägt, wenn Daten einen starken Wettbewerbsvorteil im jeweiligen Markt darstellen.[21] Dieser Befund stellt die verbreitete politische Forderung in Frage, ein weniger streng geregelter Datenzugang würde KI-Startups automatisch begünstigen: Wenn alle Unternehmen gleichermaßen auf dieselben Datenpools zugreifen können, entsteht kein differenzierender Innovationsvorteil.

Parallel dazu zeigt die KI-Forschung, dass die unkritische Anhäufung großer Datenmengen keineswegs zuverlässig zu besseren KI-Modellen führt. Die Grenzerträge beim bloßen Hinzufügen großer Datenmengen nehmen systematisch ab. Das viel zitierte Prinzip „garbage in, garbage out" beschreibt diesen Effekt treffend: Fehlerhafte, verzerrte oder nicht-repräsentative Daten in großem Maßstab erzeugen fehlerhafte Ergebnisse – und können im schlimmsten Fall zu systematischer Diskriminierung und Grundrechtsverletzungen führen. Was für verlässliche KI-Systeme benötigt wird,

---

18 Dehmel, „Wo steht die deutsche Wirtschaft beim Datenschutz?"; Erdsiek, „Optimismus in der Informationswirtschaft"; Rammer, *Dokumentation zur Innovationserhebung 2024*.

19 Ursprünglich vom Digitalverband Bitkom 2015 in seinem Positionspapier „Digitale Souveränität" formuliert. Darin fordert er, die Datenschutzprinzipien Datensparsamkeit und Zweckbindung durch „Prinzipien der Datenvielfalt und des Datenreichtums" zu ergänzen oder zu ersetzen, um eine wettbewerbsfähige Datenwirtschaft zu ermöglichen.

20 *Wenn der Notarzt nicht weiß, wie der Facharzt behandelt hat – Wie Datenschutz in Deutschland Patienten gefährdet*.

21 Bessen u. a., „The role of data for AI startup growth".

sind nicht notwendigerweise mehr, sondern Daten, die für die Zielsetzungen der jeweiligen KI-Systeme besser geeignet sind.[22]

Ein weiterer Befund relativiert die Datenmaximierungsthese: Die aktuelle KI-Forschung und -entwicklung tendiert zunehmend zu dateneffizienteren Verfahren. Techniken wie föderiertes Lernen, synthetische Datengenerierung, Transfer Learning und gezielte Datenselektion ermöglichen leistungsfähige KI-Anwendungen auch bei begrenzten oder datenschutzkonformen Datensätzen. Dieser Trend wird dabei nicht primär durch datenschutzrechtliche Anforderungen angetrieben, sondern ebenso durch wirtschaftliche Faktoren – insbesondere den erheblichen Rechenleistungsbedarf und den Energieverbrauch datenintensiver Trainingsprozesse.[23] Die technologische Entwicklung legt nahe, dass Datensparsamkeit und Innovation keine grundsätzlichen Gegensätze darstellen.[24]

Die empirische Forschungslage stützt also weder das Bild einer grundsätzlichen Unvereinbarkeit von Datenschutz und KI-Innovation noch die Forderung nach einem möglichst uneingeschränkten Zugang zu personenbezogenen Daten. Entscheidend für KI-Innovation sind Datenqualität, Passgenauigkeit und Exklusivität – nicht die bloße Datenmenge.

Repräsentative Unternehmensdaten aus der Innovationserhebung 2024 zeigen zudem, dass die Voraussetzungen für eine produktive Datennutzung in der Breite noch schwach ausgeprägt sind: Nur 33 % der Unternehmen verfügen über eine datenschutzkonforme technische Infrastruktur für Datenanalysen, 26 % über Beschäftigte mit spezifischem Know-how im Datenmanagement und in der Datenanalyse; Methoden der Künstlichen Intelligenz werden lediglich von 13 % genutzt, Big-Data-Analysen sogar nur von 6 %. Selbst unter diesen Bedingungen weisen innovationsaktive Unternehmen deutlich häufiger entsprechende Kompetenzen auf.[25] Der Engpass liegt damit häufig weniger in fehlenden Daten oder zu strengen Datenschutzregeln als vielmehr in fehlender Infrastruktur, mangelnden Kompetenzen und ungenutzten innerbetrieblichen Datenbeständen.

2.3 Wer verliert durch die DSGVO – und wer gewinnt?

Forschung und Innovation sollten grundsätzlich auf die Ressourcen und Entwicklungsbedingungen zurückgreifen können, die sie für ihren Erfolg benötigen. Im Zuge der Digitalisierung ist dies vor allem: Zugang zu allen erforderlichen Daten (vgl. auch Abschnitt 2.2). In der Debatte wird kritisiert, dass der Datenschutz die notwendige Datennutzung verhindere. Bereits 2017 forderte der digitalpolitische Arbeitskreis von CDU/CSU: „Datensparsamkeit kann heute nicht mehr die generelle Verhaltensleitlinie sein."[26] Die vom Bitkom seit Einführung der DSGVO erhobenen Zahlen scheinen diese Kritik zu bestätigen: 2024 haben demnach knapp zwei Drittel der 600 befragten Unternehmen mindestens ein Innovationsprojekt wegen konkreter DSGVO-Vorgaben abgebrochen oder gar nicht erst gestartet.[27] Besonders häufig betroffen ist mittlerweile der Bereich Künstliche Intelligenz. Gleichzeitig geben 58 % der von Bitkom befragten Unternehmen an, dass Datenschutz Rechtssicherheit bei der Entwicklung von KI-Anwendungen schafft.[28]

Diese Kritik lässt sich mit weiteren, methodisch differenzierteren Daten unterlegen: Die ZEW-Innovationserhebung 2024[29] identifiziert das Datenschutzrecht als das am häufigsten genannte Hemmnis der wirtschaftlichen Datennutzung unter zwölf abgefragten Faktoren – 65 % der Unternehmen

[22] Quezada-Tavarez u. a., „Voicing Challenges"; Weber u. a., *Wege zur Stärkung der Forschung und Anwendung von künstlicher Intelligenz in Europa*.
[23] Beckert, „Is the Future of AI Really Federated?"
[24] Quezada-Tavarez u. a., „Voicing Challenges"; Frey u. a., *Data-Biased Innovation*; Weber u. a., *Wege zur Stärkung der Forschung und Anwendung von künstlicher Intelligenz in Europa*.
[25] Rammer, *Dokumentation zur Innovationserhebung 2024*, 25.
[26] https://archiv.cdu.de/system/tdf/media/dokumente/smart-data_1.pdf
[27] Dehmel, „Wo steht die deutsche Wirtschaft beim Datenschutz?"
[28] Bitkom e.V., *Datenschutz in der deutschen Wirtschaft*, 25.
[29] Rammer, *Dokumentation zur Innovationserhebung 2024*.

berichten eine Behinderung in unterschiedlichem Ausmaß, davon 20 % eine starke. Bemerkenswert ist, dass innovationsaktive Unternehmen durchgängig häufiger von dieser Behinderung berichten als nicht-innovationsaktive Unternehmen (z. B. 84 % vs. 51 % bei der Verfolgung jeglicher Datenstrategie) – ein Beleg dafür, dass die Regulierungsbelastung überproportional jene Unternehmen trifft, die versuchen, datenbasiert zu innovieren.

Wissenschaftliche Untersuchungen auf Basis des Mannheimer Innovationspanels kommen zu einem differenzierteren Ergebnis.[30] Die Studien analysieren den Anteil des Umsatzes deutscher Unternehmen mit völlig neuen Produkten und Diensten („Produktinnovationen")[31] vor und nach Inkrafttreten der DSGVO. Die Befunde zeigen: Zwar sind nahezu alle Unternehmen von der DSGVO betroffen, doch nur 36,4 % der Unternehmen berichten von unmittelbaren Auswirkungen auf ihre Innovationsaktivitäten – vorrangig im IKT-Sektor sowie bei wissensintensiven Dienstleistungen.

Bei diesen Branchen blieb der Umsatzanteil aus Produktinnovationen in den ersten drei Jahren nach Einführung der DSGVO konstant. Es kam jedoch zu einer Verschiebung von radikalen zu inkrementellen Innovationen – also von grundlegend neuen Produkten hin zu schrittweisen Verbesserungen bestehender Angebote. Der Umsatzanteil aus inkrementellen Innovationen stieg um 1,8 %, während der Anteil radikaler Innovationen um 0,9 % sank.[32] Eine naheliegende Erklärung hierfür liegt in der Priorisierung durch die Unternehmen: Sie setzten ihre begrenzten Forschungs- und Entwicklungskapazitäten zunächst dafür ein, ihr bestehendes Produkt- und Dienstleistungsportfolio an die DSGVO-Anforderungen anzupassen. Ziel war es, Compliance-Verstöße zu verhindern und die befürchteten Bußgelder zu vermeiden. Die für diese Anpassung notwendigen Ressourcen fehlten den Unternehmen bei der Entwicklung radikaler Innovationen, die die Basis für Wettbewerbsfähigkeit und Wachstum bilden.[33] Heute kommen im Bereich der Künstlichen Intelligenz Unsicherheiten darüber hinzu, welche neuen datenbasierten Innovationen künftig zulässig sind und welche nicht. Die Verschiebung von radikalen zu inkrementellen Innovationen zeigte sich vor allem bei kleinen und jungen Unternehmen, die Datenschutz-Compliance-Prozesse erst aufbauen mussten. Größere und etablierte Unternehmen konnten die durch die DSGVO notwendigen Anpassungen hingegen meistern, ohne Abstriche bei radikalen Innovationen machen zu müssen.[34] Die Befunde legen nahe, dass es sich nur um einen *vorübergehenden Anpassungseffekt* handeln könnte. Unternehmen handeln rational, wenn sie zunächst verstärkt in inkrementelle Innovationen investieren, um zunächst Compliance-Sicherheit zu erlangen. *Mittelfristig* ist aber zu erwarten, dass Unternehmen wieder stärker in radikale Innovationen investieren – sobald die regulatorischen Anforderungen internalisiert sind.[35]

Ergänzend zeigt sich, dass größere und ältere Unternehmen (über 30 Jahre) hingegen keinen negativen Effekt auf radikale Innovation aufwiesen. Interessant ist zudem ein komplementärer Befund: Von der DSGVO betroffene Produktinnovatoren verfügen über signifikant höhere Big-Data- und KI-Kompetenzen als rein inkrementelle Innovatoren (17,9 % vs. 8,2 % bei Big-Data-Analyse) – ein Hinweis darauf, dass Compliance-Prozesse in Teilen auch als Katalysator für die Modernisierung von Dateninfrastrukturen wirken können, im Sinne der Porter-Hypothese, wonach eine strenge

[30] Blind u. a., „The Impact of the EU General Data Protection Regulation"; kritisch: Martin und von Grafenstein, „Innovation and the GDPR".

[31] Die Studie geht davon aus, dass anhand des Umsatzanteils mit Produktneuheiten (Innovation Output) eine präzisere Messung der Auswirkungen der DSGVO möglich ist als über die Forschungsaufwendungen (Innovation Input). Blind u. a., „The Impact of the EU General Data Protection Regulation", 316.

[32] Blind u. a., „The Impact of the EU General Data Protection Regulation", 333.

[33] Blind u. a., „The Impact of the EU General Data Protection Regulation", 322, 328; Erdsiek, „Viele Unternehmen stellen DSGVO schlechtes Zeugnis aus", 3.

[34] Blind u. a., „The Impact of the EU General Data Protection Regulation", 325.

[35] Blind u. a., „The Impact of the EU General Data Protection Regulation", 332.

Regulierung die Innovativität und Wettbewerbsfähigkeit von Unternehmen steigern kann, anstatt sie zu beeinträchtigen.[36]

Diese auf den deutschen Mittelstand bezogenen Befunde bedürfen der Ergänzung durch international angelegte Studien zu Markteintritt, Risikokapital und Konzentrationsdynamiken. So führte die DSGVO laut einer Analyse von 4,1 Mio. Apps im Google Play Store (2016–2019) zum Exit von rund einem Drittel aller Apps; der Markteintritt neuer Apps sank um 47,2 % – ein Befund, der im Apple App Store bestätigt wurde.[37] Da dieser Rückgang erfolgreiche Apps fast ebenso stark traf wie erfolglose, belegt er die grundsätzliche Unvorhersehbarkeit von Innovationserfolg. Im langfristigen Gleichgewicht schätzt diese Studie einen Rückgang der Gesamtnutzung um 30,6 %. Eine begleitende Befragung von 650 Entwicklern ergab, dass 85 % der Befragten den Verwaltungsaufwand als Hauptherausforderung nannten, ein Siebtel Apps vom Markt nahm und ein Elftel fertige Apps nicht veröffentlichte. Parallel dazu dokumentiert eine Studie für die Jahre 2014–2019 persistente Effekte bei der Risikokapitalfinanzierung: Die von US-Investoren in der EU investierten Beträge sanken demnach um 13,15 %.[38] Da die Studie nur Zahlen bis 2019 betrachtet ist aber unklar, ob es sich tatsächlich um einen dauerhaften, durch Einführung der DSGVO verursachten Effekt handelt. Dass negative Innovationseffekte global wirksam sind, belegt eine Parallelstudie zu US-App-Startups, bei denen die DSGVO ebenfalls Finanzierungsrunden reduzierte und Schließungswahrscheinlichkeiten erhöhte.[39] Diesen Effekten liegen strukturelle Mechanismen zugrunde, die systematisch zu Marktkonzentration zu Gunsten großer, internationaler Unternehmen mit Datenmacht tendieren.[40]

Während diese Studien vor allem negative Effekte diagnostizieren, zeigen andere Untersuchungen, dass die DSGVO auch produktive Anpassungsreaktionen und – bei bestimmten Unternehmenstypen – positive Performanceeffekte auslösen kann. Eine Studie legt etwa nahe, dass die DSGVO dazu geführt hat, dass insbesondere Start-ups mit innovativen Datenschutz-Lösungen (z.B. Compliance-fördernde Softwareanwendungen, Privacy Enhancing Technologies) neue Marktsegmente erschließen konnten. Gleichzeitig wurde aber auch festgestellt, dass die entsprechenden Märkte häufig in noch stärkerem Maße von nicht-europäischen Unternehmen durch eigene Angebote oder die Übernahme europäischer Start-ups erschlossen wurden.[41] Dass es zu innovationsfördernden Wirkungen kommt, stellt sich aber insgesamt als sehr voraussetzungsreich dar und erfolgt am ehesten in bereits stark regulierten Bereichen mit einer existierenden Compliance-Infrastruktur, wie beispielsweise im Finanzsektor.[42]

Die Forschungsbefunde zeigen somit ein gemischtes Bild. Die empirische Evidenz belegt eine strukturelle Marktkontraktion im App-Bereich, Rückgänge bei transatlantischen Risikokapitalinvestitionen, globale Spillover-Effekte auch außerhalb der EU und systematische Konzentrationsdynamiken zugunsten großer Datenkontrolleure – Effekte, die nach Branche, Unternehmensgröße, Innovationstyp und Datenintensität erheblich variieren. Diese Befunde zeigen klare Gewinner und Verlierer: Etablierte, datenreiche Plattformunternehmen profitieren strukturell von Marktanteilsgewinnen; kleine, junge Unternehmen und neue EU-Ventures tragen die größten Lasten. Positive

[36] Der Ökonom Michael Porter formulierte diese Hypothese 1991 mit Blick auf die Umweltschutzregulierung. Demnach zwingen anspruchsvolle Umweltregulierungen Unternehmen zu Innovationen, die Produktionsprozesse optimieren, die Ressourceneffizienz erhöhen und letztlich zu Kostensenkungen sowie technologischen Vorsprüngen führen. Verschiedene Studien (z. B. Niebel, „The impact of the general data protection regulation on innovation"; Lefouili u. a., „Privacy Regulation and Quality-Enhancing Innovation".) sind in den letzten Jahren der Frage nachgegangen, ob sich dieser Effekt auch im Bereich des Datenschutzes nachweisen lässt.

[37] Janßen u. a., „GDPR and the Lost Generation of Innovative Apps".

[38] Jia u. a., *How Does Privacy Regulation Affect Transatlantic Venture Investment?*

[39] Kircher und Foerderer, „Does EU-Consumer Privacy Harm Financing of US-App- Startups? Within-US Evidence of Cross-EU-Effects".

[40] Gal und Aviv, „The Competitive Effects of the GDPR".

[41] Martin u. a., „How Data Protection Regulation Affects Startup Innovation"; Frey und Presidente, „Privacy Regulation and Firm Performance".

[42] Cao und Kretschmer, „Regulation as opportunity".

Gegenbeispiele zeigen zugleich, dass Compliance-Expertise und durchdachte Governance-Architekturen diese Effekte abmildern können – jedoch nur dort, wo ausreichende Ressourcen für deren Aufbau vorhanden sind. Diese Verteilungsdynamik ist politisch unmittelbar relevant: Wenn der Anteil radikaler Innovationen dauerhaft niedrig bleibt und strukturelle Konzentrationseffekte nicht adressiert werden, ist die langfristige Wettbewerbsfähigkeit gefährdet – hier ist die Politik gefordert, Rechtssicherheit und Praxistauglichkeit so zu gestalten, dass vor allem weiterhin radikale Innovationstypen möglich bleiben.

2.4 Compliance-Kosten: Teuer für alle – aber für wen zu teuer?

Die DSGVO belegt Organisationen, die personenbezogene Daten verarbeiten mit zahlreichen Pflichten. Vertreter von Wirtschaftsverbänden kritisieren seit Einführung der Verordnung deren Umfang und den damit verbundenen Aufwand – mitunter in drastischen Worten: „Datenschutz zerstört die Wirtschaft und kostet Millionen Jobs" hieß es von Seiten des Bundesverbands der Deutschen Industrie; der Bitkom beklagte, die europäischen Digitalregulierungen wirkten „wie ein Korsett – oder als ob die europäischen Unternehmen mit Bleiwesten spielen müssten".[43] Hierfür werden vor allem drei Ursachen ausgemacht: zunehmende Dokumentations- und Rechenschaftspflichten, Rechtsunsicherheiten durch unterschiedliche Auslegungen von Aufsichtsbehörden und Gerichten sowie die Höhe potenzieller Bußgelder.

In der Bitkom-Umfrage 2025 berichten nahezu alle Unternehmen (97 %) von hohem oder sehr hohem bürokratischem Aufwand für den Datenschutz, und 69 % stellten eine weitere Zunahme fest. Zudem gaben 86 % an, dass die Umsetzung des Datenschutzes im Unternehmen nie vollständig abgeschlossen sei.[44] Dass es sich hierbei nicht um einen vorübergehenden Anpassungseffekt handelt, sondern um eine über Jahre stabile Belastungswahrnehmung, zeigt ein Vergleich der ZEW-Konjunkturumfragen aus den Jahren 2017 (Erwartungen vor Inkrafttreten), 2020 und 2024. Der Anteil der Unternehmen, die eine Verkomplizierung ihrer Geschäftsprozesse durch die DSGVO berichten, lag 2020 bei 61 % und 2024 bei 58 % – beide Werte deutlich über der 2017 geäußerten Erwartung von 49 %. Auch der als hoch empfundene Arbeitsaufwand für die Umsetzung blieb mit 68 % (2020) bzw. 63 % (2024) konstant hoch.[45] Die Unternehmen hatten die tatsächliche Belastung also tendenziell unterschätzt.

Weitere empirische Untersuchungen und Fallstudien bestätigen, dass Unternehmen seit 2018 tatsächlich erhöhte Aufwendungen für die Erfüllung gesetzlicher Vorgaben hatten.[46] Die größten zeitlichen und finanziellen Belastungen ergeben sich demnach aus Dokumentationspflichten, Schulungen, der Behandlung von Datenschutzvorfällen und Betroffenenanfragen.[47]

Eine detaillierte Analyse der Aufwandstreiber unterscheidet dabei zwischen gut planbaren und kaum planbaren Kostenkategorien.[48] Zu den gut planbaren Kosten zählen die Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten sowie die Benennung eines Datenschutzbeauftragten – beides mit hohem Initialaufwand, aber überschaubarem Folgeaufwand. Deutlich schwerer kalkulierbar sind hingegen die Bearbeitung von Betroffenenbegehren und die Reaktion auf Datenschutzvorfälle, da beide weder in ihrer Häufigkeit noch in ihrem Umfang zuverlässig prognostizierbar sind. Aus Sicht der Unternehmen besteht der größte Reformbedarf deshalb primär bei der Entbürokratisierung und Harmonisierung der Prozesse, nicht in einer Absenkung materieller Schutzstandards.

---

43 Ralf Wintergerst (Bitkom Präsident), 13.1.2025, https://www.springerprofessional.de/wirtschaftsfoerderung/risikomanagement/aufwaendiger-datenschutz-bremst-unternehmen/50138870.

44 Bitkom e.V., *Datenschutz in der deutschen Wirtschaft*, 8.

45 Erdsiek, „Viele Unternehmen stellen DSGVO schlechtes Zeugnis aus"; Erdsiek, „Optimismus in der Informationswirtschaft".

46 Erdsiek, „Viele Unternehmen stellen DSGVO schlechtes Zeugnis aus", 3.

47 Beenken und Vogel, „Effizienz im Datenschutz"; Engels und Scheufen, *Wettbewerbseffekte der Europäischen Datenschutzgrundverordnung*, 12; Rammer, *Dokumentation zur Innovationserhebung 2024*, 41.

48 Beenken und Vogel, „Effizienz im Datenschutz".

Diese Selbsteinschätzung wird durch eine repräsentative Unternehmensbefragung des Instituts der deutschen Wirtschaft bestätigt und präzisiert.[49] 34 % der befragten Unternehmen sieht demnach die DSGVO eher als nachteilig für ihre Wettbewerbsposition an, während nur 5 % überwiegend Vorteile wahrnehmen. Dabei stellt wiederum der Umsetzungsaufwand das zentrale Problem dar – wobei größere Unternehmen (gemessen an Umsatz oder Mitarbeiterzahl) diesen Aufwand signifikant häufiger als hoch bewerten als kleinere. Dies lässt sich dadurch erklären, dass größere Unternehmen typischerweise mehr Unternehmensbereiche und Datenverarbeitungsprozesse koordinieren müssen, während kleinere Unternehmen einen besseren Überblick über ihre meist einfacheren Datenverarbeitungsstrukturen behalten – die relative finanzielle Belastung liegt, wie die folgenden Befunde zeigen, dennoch bei kleinen Unternehmen höher.

Vertiefte Analysen deuten aber darauf hin, dass sich empirisch keine überproportional hohen Compliance-Kosten speziell für deutsche oder europäische Unternehmen nachweisen lassen.[50] Die DSGVO gilt für alle in der EU tätigen Unternehmen, unabhängig davon, wo diese ihren Hauptsitz haben.

Nichtsdestotrotz stellen DSGVO-bedingte Pflichten für kleinere Unternehmen nachweislich eine größere Belastung dar– durch aufwändige Dokumentations-, Governance- und Technikpflichten. Auch für große, international tätige Unternehmen sind wirtschaftliche Effekte nachweisbar: Eine Studie zu global agierenden Technologieunternehmen zeigt, dass Firmen mit hoher Umsatzexposition gegenüber dem EU-Markt nach Einführung der DSGVO einen Rückgang ihrer Gewinne um durchschnittlich 2 % verzeichneten – bei gleichzeitig unverändertem Umsatzniveau.[51]

Eine strukturelle ökonomische Analyse auf Basis von Cloud-Computing-Nutzungsdaten liefert eine präzise Quantifizierung wie sich Datenschutzanforderungen auf die Kosten auswirken:[52] Erstens erhöhte die DSGVO die variablen Kosten der Datennutzung im Durchschnitt um 22,4 %, wobei diese Kostensteigerung mit sinkender Unternehmensgröße deutlich zunimmt. Zweitens übersetzt sich dieser Kostenanstieg nur in eine moderate Erhöhung der Gesamtkosten für Dateninfrastruktur (Daten und Rechenleistung zusammen) von durchschnittlich 3,9 % . Drittens schlägt sich dies wiederum nur in einem geringen Anstieg der gesamten Produktionskosten nieder – zwischen 0,08 % (verarbeitendes Gewerbe) und 0,62 % (Software-Unternehmen) –, da die Kosten für die Dateninfrastruktur nur einen kleinen Anteil an den Gesamtkosten ausmachen. Diese mehrstufige Kostenkette relativiert die pauschale Erzählung einer existenzbedrohenden Kostenlast, bestätigt aber gleichzeitig, dass die Belastung besonders datenintensive und kleine Unternehmen – vor allem im Software-Sektor – überproportional trifft.

Ob sich die regulatorisch angestrebte „Vertrauensdividende" gesamtwirtschaftlich rechnet, ist empirisch bislang nicht beantwortet. Kritisch ist jedoch: Der Vertrauenseffekt funktioniert asymmetrisch. Größere Unternehmen können Datenschutz-Investitionen durch Skaleneffekte amortisieren und als Differenzierungsmerkmal nutzen. KMU tragen hingegen überproportionale Compliance-Lasten bei oft geringerem Return on Investment. Zudem profitieren europäische Unternehmen vom Forschungsvorsprung bei Datenschutztechnologien bislang weniger als erhofft – während die DSGVO global als Standard wahrgenommen wird (vgl. Abschnitt 3.4).[53]

Die Feststellung, dass die Umsetzung des Datenschutzes im Unternehmen nie vollständig abgeschlossen sei, ist hingegen ein Kennzeichen einer sich transformierenden Wirtschaft, in der Daten und datenbasierte Angebote eine immer zentralere Rolle einnehmen. Hier sind Datenschutz und

[49] Engels und Scheufen, *Wettbewerbseffekte der Europäischen Datenschutzgrundverordnung*.
[50] Blind u. a., „The Impact of the EU General Data Protection Regulation", 315.
[51] Frey und Presidente, „Privacy Regulation and Firm Performance", 10–11; Demirer u. a., *Data, Privacy Laws and Firm Production*.
[52] Demirer u. a., *Data, Privacy Laws and Firm Production*.
[53] Martin u. a., „How Data Protection Regulation Affects Startup Innovation".

Datenschutzmanagement wichtige Komponenten eines kontinuierlichen Verbesserungsprozesses bzw. des Risikomanagements.[54]

Ein zweiter Kritikpunkt an der derzeitigen Datenschutzordnung ist die fortbestehende *Rechtsunsicherheit*, die aus Widersprüchen zwischen verschiedenen europäischen Digitalrechtsakten und aus einer uneinheitlichen Aufsichtspraxis resultiere. Branchenverbände wie der Bitkom verweisen darauf, dass „die hohe Komplexität sowie die Vielzahl von Aufsichtsbehörden und deren unterschiedliche Auslegung des Datenschutzes … Unternehmen verunsichert" – mit der Folge, dass sie häufig auf datengetriebene digitale Innovationen verzichten. Diese Einschätzung spiegelt reale Probleme wider, greift aber zugleich zu kurz.[55]

Eines der erklärten Ziele der DSGVO war es, die zuvor stark zersplitterten Datenschutzregelungen durch einheitliche Begriffe und Verfahren zu harmonisieren. Dieses Ziel wurde formal dadurch erreicht, dass jetzt in der EU und im EWR in allen Mitgliedstaaten der gleiche Text den Datenschutz regelt. Es wurde aber zugleich wieder dadurch gefährdet, dass die insgesamt 49 Öffnungsklauseln der DSGVO es den Mitgliedstaaten erlauben, für bestimmte Bereiche die vielen bestehenden nationalen Regelungen beizubehalten oder neue zu erlassen. Damit wurde zwar Raum für spezifische Lösungen und damit mehr Rechtssicherheit in dem jeweiligen Mitgliedstaat geschaffen, zugleich sind in diesen Bereichen aber neue Differenzen und Unsicherheiten entstanden – etwa bei Beschäftigtendaten, Forschung, Medien oder Verwaltung.[56]

Auch bei den Aufsichtsbehörden war vorgesehen, durch das sogenannte Kohärenzverfahren eine stärker vereinheitlichte Praxis sicherzustellen. Bei grenzüberschreitenden Fällen ist die Behörde am europäischen Hauptsitz eines Unternehmens federführend; andere betroffene Behörden werden unter Koordination des Europäischen Datenschutzausschusses eingebunden. Ein vergleichbares Modell existiert in Deutschland mit der Datenschutzkonferenz (DSK), die die Positionen der Bundesbeauftragten und der Landesaufsichtsbehörden abstimmt. In der Praxis erweisen sich diese Verfahren jedoch häufig als langwierig. Zudem bestehen weiterhin erhebliche, historisch gewachsene Unterschiede im Verständnis von Zielen, Schwerpunkten und Vorgehensweisen der einzelnen Aufsichtsbehörden in Europa – auch wenn sich diese Unterschiede in der konkreten Interpretation der DSGVO in der Praxis meist in Grenzen halten.[57]

Noch stärker sind die Unterschiede zwischen den Gerichtsentscheidungen in den verschiedenen Instanzen und Mitgliedsstaaten. Diese können zwar nach und nach durch die Rechtsprechung des Europäischen Gerichtshofs (EuGH) schrittweise geklärt werden. Viele zentrale Fragen – etwa zu Datentransfers in Drittländer, Einwilligung, Auskunftsrechte oder berechtigten Interessen – konnten erst im Laufe der letzten Jahre durch EuGH-Urteile präzisiert werden, nachdem nationale Gerichte diese zur Vorabentscheidung vorgelegt hatten. Viele EuGH-Entscheidungen werfen aber auch neue Fragen auf, über deren Beantwortung erst einmal wieder neuer Streit entsteht. In vielen praxisrelevanten Fragen nimmt die rechtliche Unsicherheit zwar kontinuierlich ab, sie wird in dynamischen und innovationsnahen Bereichen jedoch immer bestehen, weil die dort entstehenden Fragen neu sind.

Ein häufig genannter Grund für die von Unternehmen wahrgenommene Rechtsunsicherheit ist die mit der DSGVO verbundene deutliche Anhebung der möglichen *Geldbußen* bei

---

54 Insb. DIN EN ISO/IEC 27701, *Informationssicherheit, Cybersicherheit und Datenschutz – Datenschutz-Managementsysteme – Anforderungen und Hinweise*; auch Barafort u. a., „Integrating risk management in IT settings"; nach Bitkom e.V., *Datenschutz in der deutschen Wirtschaft*, 10 geben 67% der befragten Unternehmen an, dass die DSGVO die Datensicherheit im eigenen Unternehmen verbessert hat. .

55 Bitkom, 23. Mai 2025, https://www.bitkom.org/Presse/Presseinformation/Datenschutz-Innovations-Bremse.

56 Roßnagel, *Das neue Datenschutzrecht*.

57 Nach der Studie des Bitkom e.V., *Datenschutz in der deutschen Wirtschaft*, 8 beklagen zwar 82 % der Unternehmen ihre Rechtsunsicherheit im Datenschutzrecht, aber nur 37 % geben uneinheitliche Auslegung durch die Aufsichtsbehörden als eine der größten Herausforderungen bei der Umsetzung von Datenschutzvorgaben an.

Datenschutzverstößen – kombiniert mit der Unsicherheit darüber, wie konsequent die Aufsichtsbehörden diese Spielräume ausschöpfen. Zu Beginn stand daher die Befürchtung im Raum, Geldbußen könnten „im allerschlimmsten Fall … eine Firma ruinieren".[58] Diese Sorge hat einen theoretischen Kern: Mit Inkrafttreten der DSGVO wurden die Obergrenzen massiv angehoben – auf 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes.

Die tatsächliche Sanktionspraxis zeichnet jedoch ein wesentlich nuancierteres Bild. Nach einer anfänglichen Toleranzphase ist das Geldbußenniveau zwar deutlich gestiegen, gleichzeitig zeigt der Blick auf die Daten des „GDPR Enforcement Trackers":[59] Von 3.062 zwischen Mai 2018 und März 2026 erfassten Geldbußen reichen die Beträge von 28 Euro bis 1,2 Milliarden Euro, der Median liegt bei 6.000 Euro. Die überwiegende Mehrheit der Geldbußen bewegt sich damit innerhalb eines Rahmens, der in etwa den Obergrenzen vor Geltung der DSGVO entspricht.[60] Eine systematische Gefährdung der wirtschaftlichen Existenz von Unternehmen lässt sich daraus nicht ableiten.

Geldbußen betreffen sowohl Privatpersonen als auch Organisationen sämtlicher Größenordnungen. Die allerhöchsten Sanktionen von mehr als 200 Millionen Euro richten sich bislang ausschließlich gegen große internationale Digitalkonzerne wie Meta, Amazon, TikTok, LinkedIn, Uber und Google. Zugleich zeigt sich ein klares Muster in der Bewertung der Verstöße: Härter sanktioniert werden systematische, strukturelle und organisatorische Mängel – etwa fehlende Rechtsgrundlagen für die Verarbeitung, rechtswidrige Datentransfers in Drittländer oder unzureichende Transparenz gegenüber Betroffenen. Demgegenüber fallen Geldbußen bei Sicherheitsmängeln tendenziell niedriger aus; gerade diese Verstöße machen jedoch den Großteil der Fälle im Bereich kleiner und mittlerer Unternehmen aus.

Insgesamt macht das Sanktionsregime der DSGVO deutlich, dass die Risiken der Verarbeitung personenbezogener Daten in einer hypervernetzten Welt erheblich zugenommen haben. Unternehmen erleben dies nicht nur in Form von aufsichtsbehördlichen Verfahren, sondern ganz unmittelbar durch die stark steigende Zahl von Cyberangriffen und anderen IT-Sicherheitsvorfällen, die regelmäßig auch Datenschutzverletzungen nach sich ziehen. Die verschärften Sanktionen sind damit weniger Ausdruck einer generellen Innovationsfeindlichkeit, sondern eine Reaktion auf reale Gefährdungslagen in digitalisierten Märkten.

Hieraus ergeben sich aus Unternehmenssicht klare Präferenzen für eine gezielte Entbürokratisierung, insbesondere vereinfachte Regelungen zu Verarbeitungsverzeichnissen, geringere Auskunfts-, Lösch- und Dokumentationspflichten sowie vereinfachte Anonymisierungsvorschriften. Die Absenkung der Geldbußen bei Verstößen hat hingegen keine hohe Priorität.[61]

2.5 Wer nicht reguliert, verteilt Risiken – aber maximiert nicht den Nutzen

Der amerikanische Technikhistoriker Melvin Kranzberg prägte mit dem Satz „Technik ist weder gut noch böse; noch ist sie neutral" ein vielzitiertes Statement über das Wesen der Technik. Damit meinte er, dass technische Entwicklungen derart mit der gesellschaftlichen Ökologie interagieren, dass ihre Konsequenzen häufig weit über die unmittelbaren Zwecke der technischen Geräte und Praktiken hinausgehen – und dass ein und dieselbe Technologie je nach Kontext und Umständen höchst unterschiedliche Ergebnisse hervorbringen kann. Viele technologiebezogene Probleme entstehen gerade durch unvorhergesehene Folgen scheinbar harmloser Technologien, wenn diese in

[58] Handelsverband Baden-Württemberg, zitiert in Gräfe, „Datenschutz-Grundverordnung"; vgl. auch Engels und Scheufen, *Wettbewerbseffekte der Europäischen Datenschutzgrundverordnung*, 10.

[59] https://www.enforcementtracker.com/ (Stand 25.03.2026)

[60] Wolff und Atallah, „Early GDPR Penalties".

[61] Rammer, *Dokumentation zur Innovationserhebung 2024*.

großem Maßstab eingesetzt werden.[62] Technische Entwicklungen entstehen stets im menschlichen Kontext und verfolgen konkrete Zwecke; sie sind daher kaum je wertfrei. Ob Technik letztlich als Gewinn oder als Bedrohung wahrgenommen wird, hängt daher maßgeblich davon ab, wie die Gesellschaft mit ihr umgeht, wie sie reguliert und ethisch verantwortungsvoll eingesetzt wird. Die Frage, ob Nutzen oder Schaden überwiegt, liegt damit immer in menschlicher Hand.

Damit stellt sich die Frage, ob und wann eine Gesellschaft steuernd in die Innovationstätigkeit eingreifen sollte, um unerwünschte Innovationsfolgen zu verhindern und nur gesellschaftlich nützliche Innovationen zuzulassen. Dies wirft zugleich die Frage auf, wann man überhaupt in der Lage ist, Innovationsfolgen sicher vorherzusagen und zu bewerten. Genau hier greift das sogenannte Collingridge-Dilemma: Der Versuch, eine Technologie zu regulieren, ist schwierig und nicht selten unmöglich, da in ihren frühen Phasen, in denen eine Regulierung noch möglich wäre, noch nicht genug über ihre schädlichen gesellschaftlichen Folgen bekannt ist, um eine Regulierung ihrer Entwicklung zu rechtfertigen; doch wenn diese Folgen erst einmal offensichtlich werden, ist eine Regulierung kostspielig und langwierig.[63] Auf der anderen Seite weisen Forscher darauf hin, dass eine offene, wenig regulierte Innovationsumgebung Serendipität, also überraschende und nicht geplante Entdeckungen, fördert, aus denen wirtschaftlich und gesellschaftlich disruptive Innovationen hervorgehen.[64]

Gleichzeitig ist offensichtlich, dass ein Verzicht auf Regulierung nicht den Nutzen maximiert, sondern diesen lediglich zu Lasten weniger gut geschützter Gruppen verschiebt und systemische Risiken vergrößert. Bei datenbasierten Innovationen führt fehlende Regulierung zu Schäden wie Diskriminierung und Datenmissbrauch, die Vertrauen und Adoption senken.[65] Datenmärkte ohne Regeln tendieren zu Monopolkonzentrationen.[66]

Die Herausforderung besteht also darin, das Innovationssystem so offen wie notwendig zu gestalten, um möglicherweise vorteilhafte Innovationen nicht aus irrealer Furcht vor Risiken frühzeitig abzuwürgen,[67] aber rechtzeitig so in den Innovationsprozess einzugreifen, dass die entstehenden Systeme werteorientiert gestaltet und damit für alle Seiten nützlich und akzeptabel sind. Die Forschung empfiehlt deshalb adaptive, risikobasierte Regulierungsansätze wie regulatorische Reallabore oder prinzipienbasierte Regulierung.[68] Das Prinzip des „Privacy by Design" (vgl. ausführlich Abschnitt 4.2) macht deutlich, wie Regulierung Innovation nicht blockiert, sondern ihr einen stabilen Rahmen gibt.

---

62 Kranzberg, „Technology and History", 545f.

63 Collingridge, *The social control of technology*, 19.

64 Thierer, *Permissionless Innovation*.

65 OECD, *An Introduction to Online Platforms and Their Role in the Digital Transformation*.

66 Ezrachi und Stucke, *Virtual Competition*.

67 Nach der Studie des Bitkom e.V., *Datenschutz in der deutschen Wirtschaft*, 10 halten sich deutsche Unternehmen aus Angst vor DSGVO-Verstößen übermäßig streng an Datenschutzregeln.

68 Baldwin u. a., *Understanding regulation*; zu AI Act Reallaboren für die Gesundheitsforschung siehe z.B. Schwartmann und Sahm, „Schutzräume für die Forschung".

3 Was Europa von Innovationen verlangen darf – und muss

Europäische Werte beschreiben die normativen Grundlagen für das gesellschaftliche Zusammenleben in Freiheit und Demokratie. Auch in einer digitalen Welt soll die Gesellschaft geprägt sein von Menschenwürde, individueller und kollektiver Selbstbestimmung, Rechtsstaatlichkeit und Schutz vor Risiken. Digitale Innovationen dürfen diese Werte nicht gefährden, sondern sollen von ihnen geleitet werden. Sie sollen Teil einer funktionierenden, freien und offenen Gesellschaft sein. Doch wie lässt sich dieser Anspruch konkretisieren? Nach welchen Maßstäben sollten Innovationsprozesse gestaltet werden – und wer legt diese Maßstäbe fest? Die folgenden fünf Abschnitte beleuchten dieses Spannungsfeld aus dem Blickwinkel europäischer Werte.

3.1 Nicht jede Innovation verdient Förderung – Werte sind der Maßstab

Nicht jede Neuerung ist für den technischen Fortschritt und das gesellschaftliche Zusammenleben förderlich. Eine Innovation kann auch im negativen Sinne disruptiv wirken und Schäden anrichten, die mitunter tiefgreifend sind und gesamtgesellschaftliche und langfristige Negativfolgen entfalten. Entscheidend ist somit nicht die Innovation an sich, sondern entscheidend sind die Wirkungen von Innovationen. Es geht nicht um Neuerung um der Neuerung willen, sondern um Innovationen, die *positive* Effekte entfalten – vereinfacht ausgedrückt um Innovationen, die die Welt zu einem besseren Ort machen. Aus europäischem Blickwinkel ist dies dann der Fall, wenn Innovationen europäische Werte fördern oder zumindest sicherstellen, dass diese Werte nicht gefährdet werden. Diese Feststellung scheint trivial; ihre Überführung in die Praxis stellt sich jedoch mitunter als hochkomplex heraus, wenn es darum geht, die fraglichen Werte zu definieren und auf eine konkrete Technik oder Innovation anzuwenden. Die Frage, wie (zu definierende – das heißt demokratisch auszuhandelnde – und vor allem auf die konkrete Innovation hin zu konkretisierende) Werte zum Leitbild technischer und gesellschaftlicher Innovation werden können, ist somit von zentraler Bedeutung.

Innovationen müssen gesellschaftlich wünschenswert sein. Dies ist dann der Fall, wenn sie nicht nur akzeptiert werden, sondern auch *akzeptabel* sind.[69] Akzeptabilität setzt voraus, dass Innovationen mit der bestehenden Werteordnung vereinbar sind. So entstehen Innovationen, mit der die Menschen besser leben als ohne sie; es entstehen Innovationen, die das gesellschaftliche Fundament stärken, anstatt es zu schwächen. Trotz allen Freiraums wird deshalb ein normativer Rahmen benötigt, innerhalb dessen sich Technik entwickelt; ein rein reaktives Vorgehen reicht nicht aus. Mit anderen Worten: Innovationen werden nur dann das Wertefundament stärken, wenn dieses im Innovationsprozess mitberücksichtigt wird. Dies sollte in Form von bereichsspezifischen Gestaltungsprinzipien erfolgen, die als Messlatte im Innovationsprozess dienen können. Sich widersprechende Werte sollten dabei zu einem angemessenen Ausgleich gebracht werden. So kann beispielsweise der Grundsatz von Transparenz in der Form von Open Source mit dem Geheimhaltungsinteresse gewinnorientierter Unternehmen kollidieren.

Ein solcher Ausgleich setzt allerdings voraus, dass überhaupt mehrere Werte in die Abwägung einfließen. Wird Innovation hingegen *ausschließlich* am Gewinninteresse einzelner Unternehmen ausgerichtet, ist dies mit dem Ziel einer werteorientierten Gestaltung unvereinbar. Das Gewinninteresse hat zwar selbst einen Gemeinwohlbezug, indem das betroffene Unternehmen die Volkswirtschaft insgesamt stärkt; wird es jedoch zum einzigen Bewertungsfaktor gemacht, so besteht die Gefahr, dass das Gemeinwohl Schaden nimmt, weil das fragliche Produkt oder die Dienstleistung sich negativ auf das gesellschaftliche Zusammenleben auswirkt. Besonders deutlich wird dieses

[69] Siehe hierzu und zum Folgenden die Grand Challenge „Selbstbestimmung in der digitalen Gesellschaft" der Gesellschaft für Informatik, abrufbar unter https://gi.de/grand-challenges/selbstbestimmung-in-der-digitalen-gesellschaft

Spannungsverhältnis bei den großen US-amerikanischen KI-Anbietern, deren Modelle auf dem Training von Daten basieren, die buchstäblich das ganze frei verfügbare Wissen im Internet umfassen. Während sie von frei verfügbaren Massendaten profitieren, positionieren sie sich selbst als Gatekeeper und monopolisieren den ökonomischen Nutzen, oft unter Missachtung von Urheber- und Datenschutzrecht.[70]

3.2 Die DSGVO privilegiert Forschung, doch Forschungsfreiheit endet, wo Grundrechte anderer beginnen

Forschungsfreiheit ist Teil des Kanons europäischer Werte. Nach Art. 13 der Europäischen Grundrechtecharta (GRCh) ist Forschung frei. Forschung liegt auch im Allgemeininteresse. Insofern sind die Bedingungen gelingender Forschung möglichst zu gewährleisten und zu schützen. Dieses Freiheitsrecht erlaubt aber nicht, durch den Forschungsprozess in Grundrechte anderer Personen einzugreifen und demokratische oder rechtsstaatliche Prozesse zu gefährden. Forschung muss daher z. B. Betriebs- und Geschäftsgeheimnisse von Unternehmen beachten, darf nicht geheime staatliche Prozesse gefährden, nicht die Würde und informationelle Selbstbestimmung betroffener Menschen verletzen und nicht die Voraussetzungen eines freien Marktes in Frage stellen.

Europäische Grundrechte können nicht einfach ignoriert werden, weil sie vermeintlich Forschung im Wege stehen. Dies gilt auch dann, wenn Forschung und Innovation darauf angewiesen sind, möglichst viele Daten zu verarbeiten. Soweit diese Daten personenbezogen sind, fordert etwa Art. 8 Abs. 2 Satz 1 GRCh, dass sie nur „mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden" dürfen.[71] Eine Streichung des sogenannten „Verbots mit Erlaubnisvorbehalt"[72] im Datenschutzrecht, nach dem die Verarbeitung personenbezogener Daten nur nach Einwilligung oder auf gesetzlicher Grundlage rechtlich möglich ist, wäre daher unionsrechtswidrig und könnte auch nicht durch eine Änderung der DSGVO erreicht werden.

Daher sind die Vor- und Nachteile, die Chancen und Risiken einer Innovation für das Wohlergehen der Gesellschaft gegeneinander abzuwägen. Wissenschaftliche Forschung bedingt einen möglichst großen Freiraum für gedankliche oder reale Experimente. Nur durch Versuch und Irrtum kann Forschung Fortschritte erzielen. Der Forschungsprozess als solcher führt selten bereits zu unumkehrbaren Wirkungen. Insofern dürften Chancen die Risiken für Individuen und Gesellschaft meist überwiegen. Für den Umgang mit personenbezogenen Daten berücksichtigt dies die DSGVO dadurch, dass sie Forschungszwecke stärker als alle anderen Verarbeitungszwecke privilegiert und von vielen Datenschutzvorgaben befreit. Art. 5 Abs. 1 Buchst. b DSGVO erleichtert eine Zweckänderung, Art. 9 Abs. 2 Buchst. j DSGVO ermöglicht die Verarbeitung besonders schützenswerter Daten, Art. 14 Abs. 5 Buchst. b DSGVO schränkt Informationspflichten ein, Art. 17 Abs. 3 Buchst. d DSGVO schließt Löschverpflichtungen aus, Art. 21 Abs. 6 DSGVO schränkt das Widerspruchsrecht ein und Art. 89 DSGVO enthält Ausnahmen vom Minimierungsgebot.[73]

Nach Erwägungsgrund 159 Satz 2 DSGVO soll die Verarbeitung personenbezogener Daten zu wissenschaftlichen Forschungszwecken im Sinne der DSGVO weit ausgelegt werden und die technologische Entwicklung und Demonstration, die Grundlagenforschung, die angewandte Forschung und die privat finanzierte Forschung einschließen. Zugleich soll diese Forschung nach

---

70 Siehe z.B. Ruschemeier, „Künstliche Intelligenz als soziotechnische Entwicklung"; Lango, „What You're Not Being Told About the AI Economy".

71 Ähnlich Art. 16 Abs. 2 Satz 1 AEUV.

72 Dieser Begriff ist falsch, weil Art. 8 Abs. 2 GRCh die Datenverarbeitung nicht von einer Erlaubnis abhängig macht, sondern nur die Grundregel des Art. 52 Abs. 1 Satz 1 GRCh präzisiert, dass jeder Grundrechtseingriff einer gesetzlichen Grundlage bedarf, s. näher Roßnagel, „Kein ‚Verbotsprinzip' und kein ‚Verbot mit Erlaubnisvorbehalt' im Datenschutzrecht".

73 vgl. näher Roßnagel, „Datenschutz in der Forschung" m. w. N.; der Vorschlag der Europäischen Kommission für eine Änderung der DS-GVO im Rahmen der Digitale-Omnibus-Verordnung, sieht weitere Privilegierungen vor.

Erwägungsgrund 159 Satz 3 DSGVO den festgelegten Zielen aus Art. 179 Abs. 1 AEUV Rechnung tragen, was den sozialen Fortschritt, ein ausgewogenes Wirtschaftswachstum, die Verbesserung der Lebensqualität und Themen der öffentlichen Daseinsvorsorge umfasst. Damit schließt das Verfolgen begleitender wirtschaftlicher Motive nicht die wissenschaftliche Forschung im Sinne der DSGVO aus, solange die Tätigkeit auf Erzielung eines gesellschaftlichen Nutzens gerichtet ist.[74]

3.3 Wer Risiken schafft, muss Vorausschau üben – der Markt allein entscheidet nicht

Werden Forschungsergebnisse in Innovationen überführt, ist dieser Prozess als Ausübung unternehmerischer Freiheit anerkannt (Art. 16 GRCh). Im Gegensatz zu einem Forschungsergebnis tritt eine digitale Innovation als Software, Hardware, Dienst oder Prozess konkretisiert mit bestimmten Verarbeitungszwecken in die Gesellschaft ein. Ihr geht ein Auswahlprozess unter vielen Forschungsergebnissen voraus. Innovationen sind aber nicht allein deshalb wertvoll, weil sie Neues hervorbringen. Über ihren gesellschaftlichen Wert kann nicht allein die Möglichkeit der Gewinnerzielung oder die Akzeptanz am Markt entscheiden. Vielmehr müssen Innovationen auch den gesellschaftlichen Fortschritt vorantreiben, das tägliche Leben verbessern und in eine demokratische und freie Gesellschaft passen. Zentraler Bestandteil einer solchen Gesellschaft ist der Schutz von individueller und kollektiver Selbstbestimmung. Ein wichtiges Gestaltungsprinzip digitaler Innovationen muss daher der Schutz europäischer Werte wie Grundrechte und Demokratie sein.

Diesem Anspruch wird oft entgegengehalten, Innovationswirkungen seien vorab nicht bewertbar und erst der Markt könne darüber entscheiden, welche Innovation individuell und gesellschaftlich erwünscht sei. Diese Behauptung ist analytisch jedoch verkürzt. Unstrittig ist: Innovation verläuft nicht linear, Nebenwirkungen sind oft unerwartet und exakte Prognosen über Gewinner und Verlierer gibt es nicht. Daraus folgt jedoch nicht, dass Vorausschau nutzlos wäre oder Regulierung auf eine systematische Bewertung verzichten müsste. Für eine werteorientierte Digitalpolitik in Deutschland und Europa ist gerade eine vorausschauende Technikbewertung zentral, um Datenschutz, Wettbewerb und Innovation zusammen zu denken.[75]

Doch wie lässt sich eine solche Vorausschau praktisch leisten, wenn exakte Prognosen unmöglich sind? Entscheidend ist, dass Bewertung keine Gewissheit voraussetzt. Häufig lassen sich unter bestimmten gesellschaftlichen Rahmenbedingungen plausible Nutzungsszenarien identifizieren, aus denen sich absehbare oder zumindest begründet befürchtete Wirkungen ergeben. Wer Risiken für Individuen oder die Gesellschaft schafft, muss sich um Vorausschau bemühen – mindestens in Form einer Plausibilitätsprüfung.[76] Dieser Grundsatz ist nicht nur ethisch geboten, sondern auch rechtlich verankert: Sowohl die DSGVO als auch die KI-Verordnung haben konkrete Instrumente geschaffen, die eine solche vorausschauende Bewertung operationalisieren und in den Innovationsprozess integrieren.

Methoden der wissenschaftlichen *Vorausschau* liefern zwar keine exakten Prognosen, strukturieren aber Unsicherheit, indem sie aufzeigen, welche Kombinationen von Technologien, Geschäftsmodellen und Regulierungsoptionen wahrscheinlich zu welchen Wirkungen führen. Beispielsweise können Pfadabhängigkeiten (Dominanz von Plattformen, Lock-in-Effekte) und Trade-offs zwischen Datennutzung, Grundrechten und Wettbewerbsdynamiken frühzeitig sichtbar gemacht werden. Auf dieser Grundlage sind bewusste Entscheidungen über gewünschte Innovationspfade möglich, etwa für datenintensive KI unter strengen Grundrechtsgarantien statt flächendeckender Überwachung.

---

74 DSK, *DS-GVO privilegiert wissenschaftliche Forschung*; EDPB, *Guidelines 1/2026*.

75 Steinberg und Roser, „Wirtschaftspolitische Herausforderungen der Digitalisierung"; Schieferdecker und March, „Digitale Innovationen und Technologiesouveränität".

76 BMFTR, „Eckpunktepapier Cybersicherheit", 2.

Vorausschau ist damit ein Instrument der Verantwortungsübernahme und wendet sich bewusst gegen das Laissez-faire-Diktum „Der Markt wird es richten".

Methoden der *Technikfolgenabschätzung* konkretisieren diesen Ansatz. Sie motivieren Akteure, explizit über potenzielle soziale, ethische und wirtschaftliche Konsequenzen technischer Entwicklungen nachzudenken. Dabei geht es weniger um punktgenaue Prognosen als vielmehr um strukturierte Sensibilität, also das systematische Erkennen möglicher Risiken, Zielkonflikte und Gestaltungsoptionen.[77] Die in Art. 35 DSGVO für besonders risikoreiche Verarbeitungen vorgeschriebene Datenschutz-Folgenabschätzung (DSFA) operationalisiert beispielsweise das normative Prinzip der präventiven Verantwortung. Sie versetzt Organisationen in die Lage, Auswirkungen auf Grundrechte ex ante zu bewerten und in technische und organisatorische Maßnahmen zu übersetzen.[78] Solche Mechanismen der „vorausschauenden Regulierung" sind ein Governance-Tool, um verantwortungsvolle Innovationen zu ermöglichen.

Das *Vorsorgeprinzip* ergänzt diese Perspektive als Leitprinzip für eine risikobasierte Steuerung. Es begründet das Handeln unter Unsicherheit, wenn potenziell schwerwiegende Schäden möglich sind, und eröffnet regulatorische Spielräume, je besser Risiken durch technische und organisatorische Maßnahmen beherrschbar sind. Dadurch können sich auch positive Effekte für Europa als Standort ergeben: Unternehmen wissen, welche Praktiken in Europa nicht erwünscht sind, und können ihre Pläne entsprechend anpassen.[79]

Die Märkte allein über Innovationen entscheiden zu lassen, ist eine normative Position und kein Naturgesetz. Märkte entscheiden innerhalb des rechtlichen und institutionellen Rahmens, den demokratische Gesellschaften setzen. Die Behauptung, Ex-ante-Bewertungen seien unmöglich, impliziert, dass die Entscheidung über die Verteilung von Risiken und Lasten faktisch den Akteuren mit der größten Kapital- und Datenmacht zufällt. Für Deutschland und Europa stellt sich daher vorrangig die Frage, welche Risiken wir aus Gründen der Wettbewerbsfähigkeit akzeptieren wollen, welche werteorientierten Grenzen wir Innovationen setzen wollen und wie die Abstimmungsprozesse zwischen Markt und Regulierung organisiert werden sollen.[80]

3.4 Vertrauen wirkt – aber nicht überall und nicht für alle gleich

Werteorientierte Gestaltung – also die systematische Berücksichtigung von Datenschutz, Transparenz, Fairness und Sicherheit – kann zu einem eigenständigen Wettbewerbsfaktor werden. Sie adressiert eine zentrale Knappheitsressource digitaler Märkte: Vertrauen. Die Europäische Kommission begründete die DSGVO ausdrücklich u. a. damit, dass strengerer Datenschutz das Vertrauen stärken und wirtschaftliches Wachstum fördern solle.[81] Dieses „Vertrauensargument" prägt bis heute die politische Debatte. Die Stiftung Datenschutz geht noch weiter und bezeichnet Datenschutz in einer datengetriebenen Wirtschaft als „strategischen Erfolgsfaktor". Professionell implementierte Datenschutzmaßnahmen stärkten demnach das Vertrauen von Kundinnen und Kunden, Partnerunternehmen und Investoren, was sich positiv auf Kaufentscheidungen und somit gewinnbringend für Unternehmen auswirke.[82] Doch lässt sich dieser Zusammenhang zwischen Regulierungsstrenge, Vertrauen und Innovationsdiffusion empirisch belegen?

---

77 Grunwald, „Die hermeneutische Erweiterung der Technikfolgenabschätzung"; zu den Grenzen der Gestaltbarkeit vgl. Grunwald, „Die Unterscheidung von Gestaltbarkeit und Nicht-Gestaltbarkeit der Technik".

78 Friedewald u. a., „Datenschutz-Folgenabschätzung in der Praxis"; Hötzendorfer, „IT-Projektmanagement by Datenschutz-Folgenabschätzung".

79 Calliess, „Vorsorgeprinzip".

80 Passoth, „Digitale Souveränität in und für Europa".

81 European Commission, *A Digital Agenda for Europe*; European Commission, *Impact assessment accompanying the General Data Protection Regulation*, 7; kritisch: Karaboga, *Die Entstehung der EU-Datenschutz-Grundverordnung*, 347, 619.

82 Stiftung Datenschutz, *Wirtschaftsvorteil Datenschutz*, 7.

Datenschutz stärkt Vertrauen nur unter bestimmten Bedingungen. Erstens müssen Regeln für alle verständlich und in der Nutzungspraxis erfahrbar sein. Zweitens brauchen Betroffene echte Wahl- und Widerspruchsmöglichkeiten, die nicht durch „Dark Patterns" ausgehöhlt werden, die Nutzer zur unbewussten Einwilligung in Datenverarbeitungen verleiten sollen. Drittens muss der Rechtsrahmen glaubwürdig durchgesetzt werden – mit wirksamer Aufsicht und spürbaren Sanktionen unabhängig von der Marktmacht der Beteiligten. Viertens ist eine risikobasierte, konsistente Regulierung nötig: Hohe Anforderungen, wo Grundrechte stark berührt sind; pragmatische Vorgaben, wo Risiken gering sind.

Die DSGVO hat die Grundlage für mehr Vertrauen zumindest auf dem Papier geschaffen, die praktische Durchsetzbarkeit bleibt jedoch begrenzt: Die Aufsichtsbehörden agieren – vor allem im europäischen Kohärenzverfahren – oft langsam, die Praxis der Sanktionierung ist je nach Land sehr unterschiedlich, während Unternehmen zum Teil Strategien entwickelt haben, Regelungen der DSGVO kreativ auszuweichen.[83] Ein weiterer Befund dämpft die Erwartung substanzieller Vertrauensgewinne: Ein Eurobarometer-Survey aus dem Jahr 2019 – mehr als ein Jahr nach DSGVO-Geltungsbeginn – ergab, dass 81 % der befragten Europäer angaben, keine oder nur teilweise Kontrolle über ihre eigenen Online-Daten zu haben.[84] Der erwartete Vertrauensgewinn bei den Nutzern ist damit bis dato empirisch nur begrenzt belegt.

Die Haltung der *Bürgerinnen und Bürger* zum Datenschutz ist ambivalent. Viele betonen die Wichtigkeit von Datenschutz, nutzen aber dennoch datenintensive Dienste – das Privacy Paradox. Studien zeigen allerdings, dass die Nutzung von Diensten auch als systematische Reaktion auf Voreinstellungsarchitekturen zu verstehen ist. So teilen in Opt-out-Regimes die meisten Nutzer nahezu alle Daten – unabhängig von der Stärke ihrer erklärten Datenschutzpräferenzen.[85] Dieses Paradoxon widerlegt die politische Formel vom „strengen Datenschutz als Voraussetzung jeder Akzeptanz": In bestimmten Kontexten (etwa Social Media oder Entertainment) setzen sich komfortable, gut designte Dienste trotz schwachem Datenschutz durch. Zugleich zeigt die Forschung, dass in Bereichen mit hohem Risikoempfinden (Gesundheit, Finanzen, staatliche Überwachung) ein glaubwürdiger Datenschutz eine wichtige Voraussetzung für gesellschaftliche Akzeptanz ist.[86] Die politische Behauptung trifft also sektorspezifisch zu, nicht pauschal. Empirisch präzisiert wird dieser Befund durch eine Studie, bei der die Downloads von Apps im Apple App Store über 26 Monate analysiert wurden: Nach Mai 2018 stieg der Anteil ausländischer Apps unter den beliebtesten Apps signifikant an – besonders in datensensitiven Kategorien und in Ländern mit höherer Datenschutzsensitivität. Gleichzeitig sank der Anteil EU-nativer Apps, während Apps aus den USA und China zulegten: Der Vertrauensgewinn aus der DSGVO kommt damit primär nicht-europäischen Anbietern zugute.[87]

Auch für *Unternehmen* kann Werteorientierung Wettbewerbsvorteile generieren. Empirisch bewerten gerade innovative und digitalisierte Unternehmen die DSGVO überdurchschnittlich häufig als Vorteil – sie nutzen ein hohes Datenschutzniveau gezielt, um sich gegenüber Kundinnen und Kunden sowie Partnerunternehmen und internationalen Auftraggebern als verlässliche, rechtskonforme Anbieter zu positionieren. Eine Studie des Instituts für Deutsche Wirtschaft dokumentiert, dass innovative und digitalisierte Unternehmen die DSGVO dreimal häufiger als Wettbewerbsvorteil einschätzen als nicht-innovierende Unternehmen. Diese Unternehmen nennen als Hauptgrund „größeres Vertrauen von Kunden und Kooperationspartnern".[88]

Im B2B-Umfeld hat „Vertrauen" allerdings einen anderen Charakter, hier handelt es sich eher um ein vertragliches Vertrauen als um das für den B2C-Bereich typische Verhältnis zwischen

83 Dachwitz und Fanta, „5 Jahre Datenschutzgrundverordnung".
84 European Commission, *The General Data Protection Regulation*.
85 Lin, „Valuing Intrinsic and Instrumental Preferences for Privacy"; ähnlich: Gal und Aviv, „The Competitive Effects of the GDPR".
86 Kettl u. a., „Privacy matters"; Deutschland sicher im Netz e. V., *DsiN Sicherheitsindex 2025*.
87 Li u. a., „Impact of the GDPR on the Global Mobile App Market".
88 Engels und Scheufen, *Wettbewerbseffekte der Europäischen Datenschutzgrundverordnung*, 12.

Verbraucher und Kauf- bzw. Nutzungsentscheidung. Hier wird Datenschutzkonformität zunehmend als Indikator für professionelles Risikomanagement und langfristige Resilienz gewertet.[89] Dies kann den Zugang zu globalen Wertschöpfungsketten sichern[90] und Finanzierungen erleichtern – auch wenn es nach Inkrafttreten der DSGVO zunächst zu einem Rückgang von VC-Investments gekommen ist.[91] Auch muss man nach Wirtschaftssektor differenzieren: In Branchen mit hoher Datensensibilität (Gesundheit, Soziales, Finanzen) war wirksamer und nachweisbarer Datenschutz schon immer ein wettbewerbskritischer Faktor, während vor allem in Branchen mit mittlerer Sensibilität (Immobilien, Bildung, Karriere) die Einführung der DSGVO einen erheblichen Schub zur Verbesserung der Compliance und damit der Vertrauenswürdigkeit gegenüber anderen Marktteilnehmern bewirkte.[92]

Aus der Werteperspektive ergibt sich daraus eine unbequeme Einsicht: Das Vertrauensargument trägt als *pauschale* Legitimation der DSGVO nicht. Es überzeugt dort, wo Vertrauen tatsächlich handlungsleitend ist – in risikosensiblen Bereichen wie Finanzen, Gesundheit oder staatlicher Datenverarbeitung. Es verliert an Überzeugungskraft, wo Komfort und Funktionalität Datenschutzbedenken faktisch überlagern – und es wird normativ fragwürdig, wenn seine Erträge systematisch ungleich verteilt sind (vgl. Abschnitt 2.4). Eine werteorientierte Innovationspolitik muss diese Differenzierung ernst nehmen, statt das Vertrauensversprechen als Universalrechtfertigung zu verwenden. Und sie muss die Frage beantworten, durch welche flankierenden Maßnahmen sichergestellt werden kann, dass die durch die DSGVO erzeugten Vertrauensgewinne auch europäischen Unternehmen zugutekommen.

3.5 Digitale Souveränität: Datenschutz als Fundament europäischer Selbstbestimmung

Für die Sicherheit, Wettbewerbsfähigkeit und Innovationskraft, für die Entwicklung der Demokratie, die politische Selbstbestimmung und die Verantwortung für die sozialen Folgen der Digitalisierung wie auch für den Rechtsstaat und den Grundrechtsschutz in Europa sind digitale Souveränität und Resilienz entscheidend. Welche Werte Europa wichtig sind und wie sie auf dem Weg der Digitalisierung umgesetzt werden sollen, können und dürfen nur die verfassungsmäßigen Organe in demokratischen Prozessen unter Einbeziehung der jeweiligen Bürgerschaft bestimmen. Weder fremde Regierungen noch digitale Weltkonzerne dürfen in diesen Fragen einen bestimmenden Einfluss haben.

Die Datenstrategie der EU verfolgt in expliziter Abgrenzung zu USA und China das Ziel, „unseren eigenen, europäischen Weg [zu] finden, indem wir den Austausch und die breite Nutzung von Daten kanalisieren und gleichzeitig hohe Datenschutz-, Sicherheits- und Ethik-Standards wahren".[93]

Für digitale Souveränität und Resilienz ist der Datenschutz eine entscheidende Zielsetzung und zugleich ein wichtiges Instrument. Das Grundrecht auf Datenschutz verpflichtet die EU und alle Mitgliedstaaten, Unionsbürgerinnen und -bürger gegenüber jedem unberechtigten Eingriff in dieses Grundrecht zu schützen. Zu dieser Gewährleistung muss sie auch dann stehen, wenn deren Daten in Drittländern oder in der Union durch Verantwortliche aus Drittländern verarbeitet werden. Daher müssen Datenschutzrecht und Grundrechtsschutz auch dann gelten und durchgesetzt werden, wenn die Hersteller von IT-Systemen und Diensteanbieter aus Drittländern von geringeren Anforderungen ausgehen, weil in ihrem Heimatland geringere Schutzanforderungen gelten. Will die

89 Swani u. a., „The Benefits of Meeting Buyer Privacy Expectations across Information, Time, and Space Dimensions".
90 Stiftung Datenschutz, *Wirtschaftsvorteil Datenschutz*, 17.
91 Jia u. a., „The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment".
92 Li u. a., „A roadmap to achieving a healthier information ecosystem through GDPR implementation and privacy compliance technologies.
93 Europäische Kommission, *Eine europäische Datenstrategie*, 4.

Union ihr Schutzversprechen einhalten und für alle Anbieter gleiche Wettbewerbsbedingungen gewährleisten, muss sie darauf bestehen, dass jeder, der auf dem europäischen Markt auftritt, die hier geltenden Schutzanforderung erfüllt. Ein niedrigeres Schutzniveau in anderen Ländern darf nicht auf die Union übertragen werden. Digitale Souveränität besteht dann, wenn die in der EU gebotene Schutz in all diesen Fällen durchgesetzt werden kann.[94]

Hierzu hilft das Datenschutzrecht, weil es alle Verantwortlichen verpflichtet, zur digitalen Souveränität beizutragen. Sie müssen sicherstellen, dass sie durch die Auswahl der von ihnen verwendeten Technik, ihrer Auftragnehmer und der in Anspruch genommenen Dienste ihre datenschutzrechtlichen Handlungserfordernisse sichern. Sie dürfen sich nicht selbst in Sachzwänge oder Abhängigkeiten bringen, die es ihnen unmöglich machen, ihrer Verantwortung gerecht zu werden. Umgekehrt können sie nicht geltend machen, dass bestimmte datenschutzrechtliche Pflichten für sie deshalb nicht gelten, weil sie wegen der von ihnen verwendeten Techniken und der in Anspruch genommenen Dienste nicht in der Lage ist, sie zu erfüllen. Aus diesem Grund darf auch die Auswahl von Techniken oder Dienstleistungen nicht dazu führen, dass es (faktisch) zu einem niedrigeren Schutzniveau kommt.[95] Dadurch steigt die Nachfrage nach datenschutzgerechten Alternativen.

Die notwendigen Voraussetzungen für die erforderliche Vielfalt technischer und organisatorischer Alternativen in möglichst vielen Bereichen der Verarbeitung personenbezogener Daten zu fördern, ist vorrangig eine politische Aufgabe. Sie zu erfüllen erfordert Maßnahmen in vielen Politikbereichen – von der Beschaffungs- über die Forschungs- und Innovationspolitik bis hin zur Industriepolitik (vgl. dazu im Einzelnen Abschnitt 4.2).

Letztlich ist die Durchsetzung des Grundrechts- und Datenschutzes gegenüber Herstellern und Anbietern aus Drittländern eine Maßnahme zur Selbstbehauptung europäischer Demokratie: Die Regeln des Zusammenlebens in der digitalen Welt sind demokratisch zu bestimmen. Sie dürfen nicht privater Marktmacht globaler Konzerne und den von ihnen gesetzten privaten Rechtsordnungen überlassen werden. Im Konfliktfall sind die demokratisch gesetzten Regeln durchzusetzen.

[94] Roßnagel, „Roßnagel“, 64ff.

[95] Vgl. z.B. für Cloud-Dienste den Forderungskatalog des BSI, *Criteria Enabling Cloud Computing Autonomy (C3A)*.

4 Wie lassen sich Innovation und Werteorientierung praktisch verbinden?

Für die Gestaltung eines europäischen Wegs ergeben sich daraus zwei Handlungslinien. Die erste betrifft die normative Rahmensetzung: Forschungsfreiheit muss praktisch abgesichert werden, ohne sie schrankenlos zu stellen; Vorausschau und Risikobewertung gehört als fester Bestandteil in den Innovationsprozess, statt dem Markt allein überlassen zu werden; digitale Souveränität muss aktiv – auch gegenüber außereuropäischen Anbietern – durchgesetzt werden.

Die zweite betrifft die wirtschaftliche Flankierung: institutionelle und technische Lösungen dort verbessern, wo dies möglich ist, ohne den Kern des Datenschutzes zu berühren; Vertrauen als Wettbewerbsfaktor gezielt stärken, wo es tatsächlich trägt, und zugleich sicherstellen, dass die entstehenden Erträge nicht strukturell an europäischen Unternehmen vorbeigehen; und reale Zielkonflikte zwischen Schutzniveau und wirtschaftlicher Leistungsfähigkeit politisch offen benennen und ausbalancieren, statt sie zu leugnen.

4.1 Forschung braucht Rechtssicherheit – nicht Rechtsfreiheit

Wissenschaftliche Forschung ist bereits der Zweck, für den die DSGVO die meisten Erleichterungen und Ausnahmen von datenschutzrechtlichen Anforderungen vorsieht. Dennoch ist nach weiteren Möglichkeiten zwischen gesellschaftsnützlicher Forschung und dem Schutz der informationellen Selbstbestimmung der betroffenen Personen zu suchen und es ist ein weiterer Ausgleich zu finden. Außerdem sollten tatsächliche datenschutzrechtliche Hindernisse für förderliche Innovationen soweit wie möglich verringert werden.

Was als privilegierte wissenschaftliche Forschung angesehen werden kann, hat der Europäische Datenschutzausschuss in Leitlinien zum Datenschutz in der wissenschaftlichen Forschung am 15.4.2026 festgelegt.[96] Dem war bereits ein Beschluss der deutschen Datenschutzkonferenz vom 11.9.2024 vorausgegangen.[97] Durch diese Dokumente besteht nun größere Rechtssicherheit, welche Forschung – inklusive für industrielle Forschung – von Erleichterungen und Ausnahmen profitiert.

Hinsichtlich der wissenschaftlichen Forschung hat die Europäische Kommission in ihrem Entwurf zu einer Änderung der DSGVO in einer Digitalen-Omnibus-Verordnung vom 19.11.2025[98] weitere Erleichterungen vorgesehen, insbesondere hinsichtlich der einfacheren Veränderung des Verarbeitungszwecks für Forschungszwecke, einer Einschränkung der Informationspflicht gegenüber betroffenen Personen und der Einschränkung von Löschpflichten. Diese Ausnahmen und Erleichterungen dürften ebenfalls datengetriebene Forschung rechtlich vereinfachen und mit mehr Rechtsicherheit ausstatten.

Mehr Rechtssicherheit sieht auch der Bundesgesetzgeber vor. Er will den Zugang zu Registerdaten für die empirische Forschung durch ein Gesetz zur verbesserten Nutzung von Daten für die Forschung (Forschungsdatengesetz) ermöglichen.[99] Für den Bereich der medizinischen Forschung hat er bereits den Datenzugang bereichsspezifisch durch das Gesetz zur Nutzung von Gesundheitsdaten zu gemeinwohlorientierten Forschungszwecken und zur datenbasierten Weiterentwicklung des Gesundheitswesens (Gesundheitsdatennutzungsgesetz) geregelt.[100] Für Mobilitätsdaten sieht er ebenfalls Regelungen zum Datenzugang in einem Mobilitätsdatengesetz vor. Die Europäische

[96] EDPB, *Guidelines 1/2026*.
[97] DSK, *DS-GVO privilegiert wissenschaftliche Forschung*.
[98] European Commission, *Proposal for a Digital Omnibus Regulation*.
[99] BMFTR, *Entwurf eines Gesetzes zur verbesserten Nutzung von Daten für die Forschung*.
[100] Gesundheitsdatennutzungsgesetz vom 22. März 2024 (BGBl. 2024 I Nr. 102).

Kommission will insgesamt 13 Datenräume kreieren, in denen die Forschung jeweils einen bevorzugten Zugang zu Daten erhält. Als ersten Datenraum hat der europäische Gesetzgeber den Gesundheitsdatenraum mit einer entsprechenden Verordnung geregelt.[101] Datenzugänge für Forschungszwecke wurden also bereits rechtssicher eröffnet und werden nach und nach auf weitere Bereiche ausgeweitet.

Die europäische Data-Governance-Verordnung regelt Datentreuhänder und Datenaltruismus, um rechtssicher und in geschützter Umgebung freiwillig Daten für Zwecke der Forschung und Innovation zur Verfügung stellen zu können. Nach dieser Verordnung können auch neue Beteiligungs- und Einwilligungsmodelle (z. B. Datengenossenschaften, persönliche Datenkonten, PIMS) entwickelt werden, die Selbstbestimmung und Datenzugang für Innovation zugleich stärken. Diese gesetzlich eröffneten Möglichkeiten wurden bisher aber kaum genutzt. Daher hat die Europäische Kommission in ihrem Entwurf einer Digitalen-Omnibus-Verordnung vom 19.11.2025 vorgesehen, die Data-Governance-Verordnung mit der Daten-Verordnung zusammenzuführen und neu zu gestalten.[102]

Für Forschung und Innovationen jeweils einen rechtssicheren Rahmen zu finden, ist eigentlich ein Widerspruch in sich selbst. Die Forschungsidee ist dann neu und der Innovationsansatz dann innovativ, wenn noch niemand auf diese Idee gekommen ist. Dann kann es aber auch noch keine ausgereifte Vorstellung für den konkreten rechtlichen Rahmen geben. Für diese Situation sieht die KI-VO in Art. 57 bis 59 „Reallabore" und in Art. 60 bis 63 „Tests unter Realbedingungen außerhalb von Reallaboren" vor.[103] Durch sie sollen Umgebungen geschaffen werden, in denen erprobt werden kann, welche Risiken mit KI-Forschungsergebnissen und KI-Innovationen verbunden sein können und wie mit diesen umgegangen werden kann, auch wenn noch keine abschließende verbindliche Regelung für diese Innovationen bestehen. Diese Formen des Erprobens von Innovationen und des Suchens nach hilfreicher rechtlicher Rahmensetzung sollte für KI-Forschungen- und Innovationen erprobt und im positiven Fall auch für andere Innovationen ermöglicht werden.[104]

4.2 Datenschutz als Designprinzip: Werteorientierte Technikgestaltung als Innovationstreiber

Werteorientierte Innovationen setzen sowohl ein innovationsförderndes Umfeld als auch eine Orientierung an europäischen Werten bereits im Entstehungsprozess voraus. Das zentrale Mittel für die Integration von beiden ist Technikgestaltung. In den meisten Fällen bietet innovative Technik so viele Gestaltungsmöglichkeiten, dass ein Ausgleich zwischen unterschiedlichen Zielsetzung im Sinn einer praktischen Konkordanz gefunden werden kann. Werteorientierte Technikgestaltung kann dadurch Innovationen befördern.

Werteorientierte Technikgestaltung als Gestaltungsprinzip statt Compliance-Pflicht. Die DSGVO verpflichtet in Art. 25 Unternehmen, Datenschutz nach dem Konzept des Data Protection by Design von Beginn an in ihre Systeme zu integrieren – nicht als nachträglichen Korrekturposten. Ebenso fordert die KI-VO für Hochrisiko-KI-Systeme in Art. 9 und 10 ein Risikomanagement und eine Daten-Governance, die sich an den konkreten Risiken für die Schutzgüter der KI-VO orientiert. Richtig verstanden verschiebt sich durch diese Vorgaben der bürokratische Aufwand von der

[101] „Verordnung (EU) 2025/327".

[102] European Commission, *Proposal for a Digital Omnibus Regulation*., COM(2025) 837 final.

[103] In Deutschland sieht das KI-Marktüberwachungs-und-Innovationsförderungs-Gesetz vom 22. Juli 2026 (BGBl. 2026 I Nr. 223) in § 13 eine Verpflichtung der Bundesnetzagentur vor, mindestens ein KI-Reallabor zu errichten und zu betreiben und der Forschung einen privilegierten Zugang zu diesem zu gewähren. § 14 regelt ein Genehmigungsverfahren für Tests von Hochrisiko-KI-Systemen unter Realbedingungen außerhalb von KI-Reallaboren.

[104] Außer Spanien hat bislang noch kein EU-Mitgliedstaat Überlegungen für die Umsetzung dieser Möglichkeiten angestellt. Von der OECD wurden aber Anforderungen an rechtlich sauber ausgestaltete Experimentierklauseln definiert: eine eindeutige Zweckbestimmung, eine gesetzlich verankerte zeitliche Befristung, transparente Auswahl- und Zugangskriterien, ein strukturiertes Risiko- und Datenmanagement sowie eine verpflichtende Evaluation der gewonnenen Erkenntnisse. Vgl. Pilichowski u. a., *Regulatory Sandbox Toolkit*.

nachträglichen Korrektur in die frühe Entwicklungsphase – wo er insgesamt geringer ausfällt als bei nachgelagerter Anpassung. Datenschutzanforderungen fließen in Produktarchitekturen und Datenflüsse ein, bevor die Entwicklung beginnt. Es verhindert strukturelle Schwachstellen, senkt langfristige Nachbesserungskosten und stärkt das Vertrauen aller Stakeholder. Wertebasierte Technikgestaltung muss so zum systematischen Innovations- und Differenzierungsansatz für Unternehmen werden.

Datenschutz- und Grundrechtstechnik: Europäisches Innovationsfeld mit globalem Potenzial. Privacy-Enhancing Technologies (PETs) wie Anonymisierung, Pseudonymisierung, Postquanten-Kryptografie oder föderales Lernen ermöglichen es, datengetriebene Wertschöpfung und Grundrechtsschutz technisch zu verbinden. Deutschland verfügt in Kryptografie, formalen Methoden und IT-Sicherheit über internationale Forschungsstärken, die konsequenter in marktfähige Produkte überführt werden müssen.[105] PETs sind mehr als Compliance-Werkzeuge – sie können zu einem Schlüsselbereich europäischer Innovationspolitik werden.

Europäische KI-Strategie: Grundrechtskonform statt datenmaximierend. Die verbreitete Forderung, Europa müsse den Vorsprung der USA und Chinas bei großen KI-Modellen aufholen, ist weder realistisch noch wünschenswert. Die Entwicklung solcher Modelle beruht auf der massenhaften Auswertung frei verfügbarer Daten – häufig ohne Wissen oder Einwilligung der Betroffenen – und steht damit in offenem Widerspruch zum europäischen Grundrechtsschutz. Europa sollte stattdessen einen Innovationspfad verfolgen, der angepasste KI-Technik und Grundrechtskonformität zum Ausgangspunkt nimmt.[106]

Ungenutzte Datenpotenziale erschließen – zum Wohle aller: In zentralen Sektoren – Mobilität, Gesundheitswesen, öffentliche Verwaltung – verfügt Europa über umfangreiche, unter klaren Rechtsgrundlagen erhobene Datenbestände, die für datengetriebene Innovation bislang ungenügend erschlossen werden. Das liegt nicht primär am Datenschutz, sondern an fragmentierten Infrastrukturen, fehlender Interoperabilität und mangelndem Vertrauen zwischen datengebenden und datennutzenden Stellen.[107] Eine europäische Datenstrategie sollte diese Daten unter Gewährleistung eines hohen Datenschutz- und Sicherheitsniveaus nutzbar machen – nicht durch Absenkung von Schutzstandards, sondern durch sichere Dateninfrastrukturen, standardisierte Schnittstellen und vertrauenswürdige Governance-Modelle. Datenschutz und IT-Sicherheit wirken als Voraussetzung dafür, dass Dateninhaber ihre Daten überhaupt zur Verfügung stellen.

Dateneffiziente Verfahren ermöglichen leistungsfähige KI-Anwendungen ohne zentrale Zusammenführung großer personenbezogener Datenbestände – und sind damit strukturell besser mit den Anforderungen der DSGVO vereinbar. Eine europäische KI-Strategie, die Datenschutz als Designvorgabe begreift, ist eine bewusste Entscheidung für einen grundrechtskonformen Innovationspfad.[108]

Vom Forschungsergebnis zum Marktprodukt. Forschungsförderung allein genügt nicht. Es muss auch sichergestellt werden, dass sichere, grundrechtskonforme und demokratiefördernde Forschung auch in erfolgreiche Produkte und Dienste überführt werden. Dafür ist ein Zusammenwirken mehrerer Politikbereiche entlang der gesamten Innovationskette erforderlich:

- Die Erforschung, Entwicklung und Umsetzung datenschutzkonformer Alternativen müssen gezielt gefördert werden – nicht nur in der Grundlagenforschung, sondern bis zur Marktreife.
- Vertrauen in Innovationen ist unterschiedlich wichtig. In bestimmten Sektoren ist die Vertrauenswürdigkeit ein unverzichtbares Versprechen. Werteorientierte Technikgestaltung ist der Ansatz, es dort operativ einzulösen, wo es empirisch trägt.

---

105 BMFTR, „Eckpunktepapier Cybersicherheit", 5.

106 Ähnlich auch Weber u. a., *Wege zur Stärkung der Forschung und Anwendung von künstlicher Intelligenz in Europa*.

107 Rammer, *Dokumentation zur Innovationserhebung 2024*.

108 Weber u. a., *Wege zur Stärkung der Forschung und Anwendung von künstlicher Intelligenz in Europa*.

- Die Wettbewerbsfähigkeit europäischer Anbieter werteorientierter Technologien muss aktiv unterstützt werden (vgl. Abschnitt 4.4).
- Entbürokratisierung beim Markteintritt: Bestehende Hürden müssen abgebaut werden, damit innovative Produkte und Dienstleistung rasch auf den Markt kommen können.
- Staatliche Vorbildfunktion und Beschaffungspolitik: Öffentliche Einrichtungen sollten bei Beschaffungen systematisch Produkte mit nachgewiesenem Datenschutz- und Sicherheitsdesign sowie Eigenschaften, die digitale Souveränität fördern, bevorzugen. Das schafft Nachfrage und setzt Marktstandards.

Ziel ist ein europäisches Ökosystem für werteorientierte Technik. „Made in Europe" kann – wenn wertebasierte Technikgestaltung konsequent als Innovationsstrategie verfolgt wird – zu einem international anerkannten Qualitätsmerkmal werden.[109] Das setzt voraus, dass Unternehmen, Forschung, Staat und Regulierung in dieselbe Richtung wirken: nicht Datenschutz *gegen* Innovation, sondern Datenschutz *durch* Innovation.

4.3 Governance neu denken: Datenschutz als strategische Organisationsaufgabe

Datenschutz wird in vielen datenverarbeitenden Organisationen noch immer als operative Compliance-Pflicht behandelt – als abzuarbeitende Checkliste, nicht als kontinuierliche Gestaltungsaufgabe. Diese Haltung ist strukturell riskant: Wer Datenschutz nachgelagert verwaltet statt vorausschauend integriert, produziert kostspielige Nachbesserungen, erhöht rechtliche Haftungsrisiken und verpasst Innovationschancen. Der notwendige Wandel beginnt in den Organisationen selbst – und erfordert ein Verständnis von Datenschutz als strategischer Architekturaufgabe, die es fortlaufend zu verbessern gilt.

Frühzeitige Folgenabschätzung statt nachträglicher Korrekturen. Der Übergang von Forschung zu Innovation verlangt eine bewusste Gestaltung: Datenschutzfolgen müssen frühzeitig und aus verschiedenen Perspektiven bewertet werden – unter Einbeziehung realer Nutzungsszenarien, nicht nur technischer Parameter. Die bereits erwähnte Datenschutz-Folgenabschätzung und die neue Grundrechtsfolgenabschätzung der KI-VO sind keine bürokratische Pflichtübung, sondern institutionalisierte Vorausschau – vorausgesetzt, Organisationen verankern sie als festen Bestandteil ihrer Entwicklungsprozesse statt als nachgelagerte Prüfung.

Regulierung als Gestaltungsrahmen, nicht als Bremse. Werteorientierte Innovation entsteht nicht trotz, sondern durch bessere Regulierung – sofern diese prinzipienbasiert, risikogestuft und lernfähig ist. Für das risikobegrenzte Erproben von Innovationen sind über die KI-VO hinaus weitere Experimentierräume in Form von Reallaboren und Experimentierklauseln erforderlich.[110] Regulatorische Reallabore ermöglichen es, innovative Lösungen unter Aufsichtsbegleitung zu erproben, ohne eine vollständige Compliance-Infrastruktur vorauszusetzen.[111] Verhaltensregeln und Zertifizierungen können branchenspezifische Rechtssicherheit kooperativ herstellen und individuellen Auslegungsaufwand reduzieren – wobei Zertifizierungen für schnelllebige digitale Produkte nur bedingt geeignet sind und nicht als universelles Governance-Instrument überbewertet werden sollten. Regelmäßige Wirksamkeitsprüfungen stellen sicher, dass Regelwerke mit der Technologieentwicklung Schritt halten.

Demokratische Innovationssteuerung institutionalisieren. Die Frage, welche Innovationsrisiken eine Gesellschaft zu tragen bereit ist und welche Innovationspfade sie bevorzugt, ist keine rein

[109] BMFTR, „Eckpunktepapier Cybersicherheit", 3.

[110] Innovationsrat für Deutschland, http://www.innovationsrat.de.

[111] Eine Studie der OECD warnt allerdings davor, Sandboxes zum Standardwerkzeug zu erheben; sie sollten nur dann eingesetzt werden, wenn sie gegenüber klassischen Instrumenten wie Regulierungsfolgenabschätzungen, Leitlinien oder Standardisierung einen klaren zusätzlichen Erkenntnisgewinn versprechen. Vgl. Pilichowski u. a., *Regulatory Sandbox Toolkit*.

technische, sondern eine genuin demokratische Entscheidung. Sie darf nicht allein den Akteuren mit der größten Kapital- und Datenmacht überlassen werden. Erforderlich sind daher institutionalisierte Formate gesellschaftlicher Deliberation, die Tradeoffs zwischen wünschenswerten und unerwünschten Innovationsfolgen transparent machen und in politische Entscheidungsprozesse einspeisen.

Datenschutz-und Risiko-Governance als kontinuierlicher Verbesserungsprozess. Vergleichbar mit Qualitätsmanagement oder IT-Sicherheit ist Datenschutz- und Risiko-Governance kein einmaliges Projekt. Organisationen, die ihn als strategische Architekturaufgabe begreifen, schaffen Verlässlichkeit für Innovatoren, Vertrauen bei Nutzenden und Resilienz gegenüber einer sich wandelnden Rechtslage – und leisten damit einen eigenständigen Beitrag zum europäischen Innovationsweg.[112]

4.4 Datenschutz und Wettbewerbsfähigkeit: Asymmetrien abbauen, Innovationsstärken skalieren

Die datenbasierte Wirtschaft verteilt Risiken und Chancen neu – und wer dies ignoriert, verkennt die eigentliche Herausforderung. Nicht Regulierung an sich, sondern ihre konkrete Ausgestaltung entscheidet darüber, ob Europa im globalen Innovationswettbewerb bestehen kann.[113] Ein grundlegendes Umdenken ist nötig: Manche Compliance-Kosten sind keine Belastung, sondern notwendige Investitionen in Vertrauen, Resilienz und langfristige Wettbewerbsfähigkeit.

Der Brüssel-Effekt – und die Frage nach den Gewinnern. Der Brüssel-Effekt entfaltet seine Wirkung nicht neutral, sondern verteilungswirksam: Strukturell profitieren vor allem große, datenreiche und häufig nicht-europäische Anbieter, während kleine und junge europäische Unternehmen die Kosten der Vorreiterrolle tragen, ohne im gleichen Maß an ihrem Vertrauensertrag zu partizipieren. Diese Asymmetrie ist kein vorübergehendes Anpassungsproblem, sondern eine strukturelle Eigenschaft des bisherigen Regulierungsdesigns – und damit eine genuin politische Gestaltungsaufgabe. Drei Ansatzpunkte erscheinen zentral: erstens eine Skalierungspolitik, die europäischen Compliance- und PET-Anbietern den Sprung vom nationalen zum europäischen Markt erleichtert; zweitens eine kritischere wettbewerbsrechtliche Prüfung von Übernahmen vielversprechender europäischer Start-ups durch kapitalstarke, außereuropäische Akteure[114]; drittens ein systematisches Monitoring, das die Verteilungswirkung europäischer Digitalregulierung – wer trägt die Kosten, wem kommt der Vertrauensertrag zugute – zu einem festen Bestandteil der Evaluation nach Art. 97 DSGVO macht, statt sie dem Zufall künftiger Forschung zu überlassen. Im Detail:

Strukturelle Asymmetrien gezielt adressieren. Die in Abschnitt 2.4 beschriebenen Marktasymmetrien – Skalenvorteile großer Plattformunternehmen bei der Compliance, überproportionale Belastung von KMU und Start-ups – erfordern eine politische Antwort, die nicht in einer Absenkung des Schutzniveaus für alle bestehen darf. Vielmehr muss sie eine konsequent risikoorientierte Differenzierung der Pflichten bedeuten: Dokumentations- und Nachweisanforderungen sollten sich am tatsächlichen Risiko für Betroffene orientieren, nicht primär an der Organisationsgröße.

Um KMU wirkungsvoll und risikogerecht zu entlasten, sollte die DSGVO – ähnlich wie der Cyber Resilience Act und die KI-VO – neben den für die Verarbeitung Verantwortlichen auch die Hersteller und Anbieter von IT-Systemen in die Pflicht nehmen.[115] Damit würden diejenigen verpflichtet, die

---

[112] Stiftung Datenschutz, *Wirtschaftsvorteil Datenschutz*, 9.

[113] Innovationsrat für Deutschland, https://www.innovationsrat.de.

[114] Cao und Kretschmer, „Regulation as opportunity".

[115] Vgl. z.B. DSK, *Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO*, 15f.; DSK, *Stellungnahme zum Digital Fitness Check / Vorschläge zu Modifikationen der DSGVO*, 5; *Beschluss des Bundeskanzlers und der Regierungschefinnen und Regierungschefs der Länder zur Staatsmodernisierung vom 4.12.2025*, Zeile 166; Bundesregierung, *German proposal for simplification of the GDPR vom 23.10.2025*, 5f.; Schild, „Schild"; Hansen u. a., „Gedanken zur Reform der DSGVO aus Sicht der Aufsichtspraxis".

die datenschutzrechtlichen Vorgaben am besten und am kostengünstigsten erfüllen können.[116] Entlastet würden Millionen von verantwortlichen Nutzern, die die Standardlösungen unkompliziert und rechtssicher nutzen könnten. Hersteller und Anbieter sollten den Nutzern die notwendigen Konformitätsnachweise bereitstellen, wie z.B. Musterverarbeitungsverzeichnisse, Vorlagen für Datenschutzfolgenabschätzungen oder Musterschreiben zur Beantwortung von Betroffenenanfragen.[117]

Datenschutztechnologien als strategisches Marktfeld. Die DSGVO hat neue Märkte für Privacy-Enhancing Technologies und Compliance-Software angestoßen – ein Befund, der die Porter-Hypothese stützt, aber nur unter bestimmten Voraussetzungen greift. Die in Abschnitt 4.2 beschriebenen deutschen Stärken in Kryptografie und IT-Sicherheit werden bislang unzureichend in marktfähige, skalierte Angebote überführt. Problematisch ist, dass davon bislang überproportional nicht-europäische Anbieter profitieren – teils durch eigene Markterschließung, teils durch gezielte Übernahmen europäischer Start-ups. Das strukturelle Problem dahinter: Europäische Innovatoren entwickeln zwar technologisch leistungsfähige Lösungen, ihnen fehlt aber häufig die Kapitalausstattung und die Marktreichweite, um sich dauerhaft zu behaupten. Europa muss daher nicht nur Forschungsförderung, sondern auch Transferförderung und Skalierungsunterstützung stärken – kombiniert mit einer kritischeren Prüfung von Übernahmen in strategisch relevanten Datenschutztechnologien.

Lernfähige Regulierung als Daueraufgabe. Die These, dass datenschutzorientierte Regulierung wettbewerbsfähige Innovationen hervorbringen kann, ist theoretisch plausibel und durch erste Befunde gestützt – empirisch belastbar bewiesen ist sie nicht. In welche Richtung sich diese Innovationen entwickeln und ob europäische Unternehmen sie am Markt behaupten können, werden erst künftige Entwicklungen und ihre Beforschung zeigen. Entscheidend ist deshalb eine Regulierung, die risikoorientiert, praxistauglich und lernfähig ist[118] – flankiert durch ein systematisches Monitoring der Innovationswirkungen und eine aktive Industriepolitik, die verhindert, dass Europa die Regeln setzt, aber andere die Früchte ernten. Die regelmäßige Evaluierung der DSGVO durch die EU-Kommission gemäß Art. 97 DSGVO sollte sich deshalb nicht nur auf den Grad der Umsetzung fokussieren, sondern auch die *Wirkungen der DSGVO*, u.a. auf die Innovationstätigkeit, im Blick behalten und immer wieder Verbesserungen und Anpassungen der DSGVO thematisieren.[119]

4.5 Datenschutz und IT-Sicherheit: Synergie statt Zielkonflikt

Datenschutz und IT-Sicherheit können sich gegenseitig stärken, haben aber auch in bestimmten Situationen widersprüchliche Zielsetzungen, die es durch Gestaltung der Sicherheitsmaßnahmen aufzulösen gilt. IT-Sicherheit will IT-Systeme gegen Fehler oder Angriffe schützen. Hierzu benötigt IT-Sicherheit bisweilen personenbezogene Daten der Nutzer, um Unregelmäßigkeiten erkennen und bewerten und mögliche Täter identifizieren zu können. Dagegen schützt Datenschutz die informationelle Selbstbestimmung der betroffenen Personen gegen die Verarbeitung ihrer Daten. Daher kann IT-Sicherheit an weiteren Datenverarbeitungen und mehr erfassbaren Daten interessiert sein, während Datenschutz das Interesse vertreten kann, solche Datenverarbeitungen auf das notwendige Maß zu reduzieren.

Datenschutz erfordert aber auch, wie Art. 32 DSGVO zeigt, Maßnahmen der IT-Sicherheit, die Verarbeitungssysteme gegen den Zugriff Unbeteiligter schützen, die Vertraulichkeit personenbezogener Daten gewährleisten, Manipulationen solcher Daten verhindern und die Verfügbarkeit der Daten und ihrer Verarbeitung sicherstellen. Für IT-Sicherheit ist Datenschutz eines der zu schützenden

[116] Roßnagel und Geminn, *Datenschutz-Grundverordnung verbessern*, 91f., 132 ff.; Roßnagel, „7 Jahre DSGVO", 123.
[117] Vgl. z. B. Ziebarth, „Kontrollaufgaben und Gesetzesbindung der Datenschutzaufsicht", 53.
[118] Zu Möglichkeiten der Entbürokratisierung im Datenschutz s. z.B. Roßnagel, „Weniger Bürokratie im Datenschutz"; Roßnagel und Wallmann, *Bürokratieabbau im Datenschutz*.
[119] Vgl. Roßnagel und Geminn, *Datenschutz-Grundverordnung verbessern*.

Rechtsgüter. Insofern sind IT-Sicherheit und Datenschutz gemeinsam an einer sicheren Datenverarbeitung interessiert. Zusammen fördern sie außerdem grundlegende gesellschaftliche Güter wie Vertraulichkeit, Integrität, Fairness und Respekt. Sie tragen mit dazu bei, dass die Gesellschaft insgesamt eine stabile Entwicklung Richtung Freiheit, Demokratie und Rechtstaatlichkeit nimmt.

Ziel muss sein, IT-Sicherheitstechnik zu entwickeln, die Sicherheit, Innovation und Grundrechtsschutz von Beginn an in digitale Systeme integriert. Hierfür wäre auch Sicherheitstechnik von Anfang an werteorientiert zu entwickeln und müsste in der Gestaltung der Systeme einen Ausgleich zwischen Sicherheitszielen und der Beschränkung auf die wirklich unabdingbaren Verarbeitungen personenbezogener Daten finden. Solche digitalen Systeme, die Funktionalität, Sicherheit und europäische Werte, technologische Souveränität und internationale Verantwortung integriert („Made in Germany") können Vorbildfunktion für die ganze Welt haben.

Cybersicherheit ist nicht nur eine technische Herausforderung, sondern auch eine gesellschaftliche Verantwortung. Digitale Sicherheit ist daher mehr als nur Schutz vor Angriffen: Sie steht für die Wahrung von Grundrechten, Transparenz und demokratischer Kontrolle. Werteorientierte Technikgestaltung stellt sicher, dass europäische Werte wie Datenschutz, Rechtsstaatlichkeit und Menschenwürde von Anfang an in die Entwicklung digitaler Systeme integriert werden.[120]

[120] BMFTR, „Eckpunktepapier Cybersicherheit", 6.

5 Fazit

Im globalen Technologiewettbewerb greift die gängige Gleichung „weniger Datenschutz = mehr Innovation" zu kurz. Die DSGVO ist weder pauschale Innovationsbremse noch automatischer Standortvorteil. Ihre Wirkungen sind real, aber ungleich verteilt: Kleine und junge Unternehmen tragen die größten Anpassungslasten, während sich Marktanteile und neu entstehende Vertrauens- und Compliance-Märkte strukturell zugunsten großer, datenreicher – häufig nicht-europäischer – Akteure verschieben. Zugleich sind neue Märkte für Privacy-Tech, Compliance-Lösungen und werteorientierte Geschäftsmodelle entstanden, die dieses Muster zumindest teilweise durchbrechen könnten.

Empirisch bestätigt sich, dass nicht Datenmaximierung, sondern Datenqualität, Passgenauigkeit und Exklusivität über den Erfolg datengetriebener Innovationen entscheiden. Die Forschung wird durch Datenschutzrecht weniger strukturell blockiert, als oft behauptet; reale Probleme liegen in Rechtsunsicherheit, Fragmentierung und Bürokratie – insbesondere bei grenzüberschreitenden Projekten. Vertrauen wirkt zwar als Wettbewerbsfaktor, jedoch nicht pauschal, sondern sektorspezifisch – verlässlich vor allem in risikosensiblen Bereichen wie Gesundheit, Finanzen und staatlicher Datenverarbeitung. Doch selbst dort, wo Vertrauen trägt, kommt sein ökonomischer Ertrag bislang nicht gleichmäßig an: Er fließt überproportional großen, international agierenden Anbietern zu, während europäische Unternehmen ihn seltener in eigene Marktanteile übersetzen können. Das Vertrauensargument allein trägt damit als Rechtfertigung nicht – es muss um die Frage ergänzt werden, wer von diesem Vertrauen tatsächlich profitiert.

Diese Befunde verweisen auf eine tieferliegende Frage: Was sollen Innovationen leisten? Innovation ist kein Selbstzweck. Sie muss mit europäischen Grundwerten – Menschenwürde, Selbstbestimmung, Demokratie, Nachhaltigkeit – vereinbar sein und demokratische Selbstbestimmung sowie digitale Souveränität sichern. Dass die ökonomischen und vertrauensbasierten Erträge europäischer Regulierung bislang ungleich verteilt sind, ist deshalb nicht allein ein wirtschaftspolitisches, sondern ein genuin normatives Problem: Digitale Souveränität setzt voraus, dass europäische Akteure an den Früchten der von ihnen mitgetragenen Standards auch tatsächlich teilhaben. Regulierung ist dabei kein Gegensatz zur Innovationsförderung, sondern deren Rahmen: Durch Data Protection by Design, risikobasierte Vorgaben, Technikfolgenabschätzung und Vorsorgeprinzip werden gewünschte Innovationspfade gestützt und riskante begrenzt. Datenschutz und IT-Sicherheit sind keine konkurrierenden Ziele, sondern zwei Seiten einer werteorientierten digitalen Infrastruktur

Ein zukunftsfähiger europäischer Weg erfordert daher: (1) Forschungsspielräume konsequent zu nutzen und zielgenau zu erweitern, wo gesellschaftlich wünschenswerte Vorhaben blockiert werden; (2) Datenschutz als Design- und Innovationsprinzip zu verankern und PETs sowie dateneffiziente KI strategisch zu fördern; (3) Datenschutz-Governance als Führungsaufgabe zu verankern und die Lastenverteilung zwischen kleinen und großen Akteuren aktiv zu korrigieren, statt sie dem Markt zu überlassen; (4) Datenschutz, IT-Sicherheit und Industriepolitik so zu verzahnen, dass Europa nicht nur die Regeln setzt, sondern diese auch konsequent gegenüber allen Marktteilnehmerinnen durchsetzt – unabhängig von deren Unternehmenssitz – und strukturell sicherstellt, dass die ökonomischen und gesellschaftlichen Erträge seiner Standards den eigenen Unternehmen und Bürgerinnen und Bürgern zugutekommen.. So wird ein eigenständiger europäischer Innovationspfad möglich, der Grundrechtskonformität nicht als Kostenfaktor, sondern als Qualitätsmerkmal begreift.

6 Literaturverzeichnis

Baldwin, Robert, Martin Cave, und Martin Lodge. *Understanding regulation: theory, strategy, and practice*. 2. Aufl. Oxford University Press, 2012.

Barafort, Béatrix, Antoni-Lluís Mesquida, und Antonia Mas. „Integrating risk management in IT settings from ISO standards and management systems perspectives". *Computer Standards & Interfaces* 54 (November 2017): 176–85. https://doi.org/10.1016/j.csi.2016.11.010.

Becker, Regina, und Edward S. Dove. „The EU GDPR and secondary use of health and genetic data for research support purposes". *International Data Privacy Law*, 28. Januar 2026, ipag001. https://doi.org/10.1093/idpl/ipag001.

Beckert, Bernd. „Is the Future of AI Really Federated? Federated Learning as an Emerging Market". *2025 3rd International Conference on Federated Learning Technologies and Applications (FLTA)*, 14. Oktober 2025, 1–6. https://doi.org/10.1109/FLTA67013.2025.11336434.

Beenken, Petra, und Simone Vogel. „Effizienz im Datenschutz: Wege zur Entbürokratisierung. Systemische Aufwandstreiber und ihre Bedeutung für die geplante Entbürokratisierung des Datenschutzes in Deutschland am Beispiel eines Unternehmens". *Datenschutz und Datensicherheit - DuD* 50, Nr. 1 (2026): 7–10. https://doi.org/10.1007/s11623-026-2195-7.

Bentzen, Heidi Beate, Rosa Castro, Robin Fears, George Griffin, Volker Ter Meulen, und Giske Ursin. „Remove Obstacles to Sharing Health Data with Researchers Outside of the European Union". *Nature Medicine* 27, Nr. 8 (2021): 1329–33. https://doi.org/10.1038/s41591-021-01460-0.

Beschluss des Bundeskanzlers und der Regierungschefinnen und Regierungschefs der Länder zur Staatsmodernisierung vom 4.12.2025. 2025. https://bmds.bund.de/fileadmin/BMDS/Dokumente/2025-12-04-mpk-staatsmodernisierung-data_CDR.pdf.

Bessen, James, Stephen Michael Impink, Lydia Reichensperger, und Robert Seamans. „The role of data for AI startup growth". *Research Policy* 51, Nr. 5 (2022): 104513. https://doi.org/10.1016/j.respol.2022.104513.

Bitkom e.V., Hrsg. *Datenschutz in der deutschen Wirtschaft*. Mit Susanne Dehmel, Isabelle Stroot, Lange, Bettina, und Alissa Geffert. Bitkom, 2026. https://doi.org/10.64022/2026-datenschutz.

Blind, Knut, Crispin Niebel, und Christian Rammer. „The Impact of the EU General Data Protection Regulation on Product Innovation". *Industry and Innovation* (London ; New York) 31, Nr. 3 (2024): 311–51. https://doi.org/10.1080/13662716.2023.2271858.

BMFTR. „Eckpunktepapier Cybersicherheit — Kommunikationstechnologien und Cybersicherheit". Bundesministerium für Forschung, Technologie und Raumfahrt, Februar 2026. https://www.forschung-it-sicherheit-kommunikationssysteme.de/forschung/it-sicherheit/eckpunktepapier-cybersicherheit.

BMFTR. *Entwurf eines Gesetzes zur verbesserten Nutzung von Daten für die Forschung*. Referentenentwurf. Bundesministerium für Forschung, Technologie und Raumfahrt, 2025.

https://www.bmftr.bund.de/DE/Ministerium/Gesetze/Gesetze-Einzeln/Forschungsdatengesetz.html.

Bobrov, Evgeny, Christina Habermehl, Daniel Strech, Tracey Weissgerber, und René Bernard. „Six Solutions for Clinical Study Data Sharing in Germany". *BMC Medical Research Methodology* 25, Nr. 1 (2025): 140. https://doi.org/10.1186/s12874-025-02560-y.

Brück, Oscar, Enni Sanmark, Ville Ponkilainen, u. a. „European Health Regulations Reduce Registry-Based Research". *Health Research Policy and Systems* 22, Nr. 1 (2024): 135. https://doi.org/10.1186/s12961-024-01228-1.

BSI. *Criteria Enabling Cloud Computing Autonomy (C3A)*. Federal Office for Information Security, 2026. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/C3A_Cloud_Computing_Autonomy.pdf.

Bundesregierung. *German proposal for simplification of the GDPR vom 23.10.2025*. 2025.

Calliess, Christian. „Vorsorgeprinzip". In *Handbuch Technikethik*, herausgegeben von Armin Grunwald und Rafaela Hillerbrand. J.B. Metzler, 2021. https://doi.org/10.1007/978-3-476-04901-8_83.

Cao, Ruiqing (Sam), und Tobias Kretschmer. „Regulation as opportunity: proactive GDPR compliance in the US financial services industry". *Industrial and Corporate Change* 35, Nr. 1 (2026): 150–70. https://doi.org/10.1093/icc/dtaf031.

Collingridge, David. *The social control of technology*. Pinter, 1980.

Dachwitz, Ingo, und Alexander Fanta. „5 Jahre Datenschutzgrundverordnung: Die fünf größten Schwächen der DSGVO". Netzpolitik.org, 24. Mai 2023. https://netzpolitik.org/2023/5-jahre-datenschutzgrundverordnung-die-fuenf-groessten-schwaechen-der-dsgvo/.

Dehmel, Susanne. „Wo steht die deutsche Wirtschaft beim Datenschutz?" Bitkom, 1. Oktober 2024. https://www.bitkom.org/sites/main/files/2024-09/241001-Bitkom-Charts-Datenschutz-final.pdf.

Demirer, Mert, Diego J. Jiménez Hernández, Dean Li, und Sida Peng. *Data, Privacy Laws and Firm Production*. NBER Working Paper Nr. 32146. National Bureau of Economic Research, 2026. https://doi.org/10.3386/w32146.

Deutschland sicher im Netz e. V., Hrsg. *DsiN Sicherheitsindex 2025: Vertrauen in der Digitalen Welt*. Deutschland sicher im Netz e. V., 2025. https://www.sicher-im-netz.de/dsin-sicherheitsindex-2025/.

DIN EN ISO/IEC 27701. *Informationssicherheit, Cybersicherheit und Datenschutz – Datenschutz-Managementsysteme – Anforderungen und Hinweise*. DIN Media, Februar 2026.

DSK. *DS-GVO privilegiert wissenschaftliche Forschung. Positionspapier zum Begriff „wissenschaftliche Forschungszwecke"*. Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. September 2024. 2024. https://www.datenschutzkonferenz-online.de/media/dskb/2024-09-11_DSK_Positionspapier%20_Wissenschaftliche_Forschungszwecke.pdf.

DSK. *Erfahrungsbericht der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder zur Anwendung der DS-GVO*. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, 2019. https://www.datenschutzkonferenz-online.de/media/dskb/20191213_erfahrungsbericht_zur_anwendung_der_ds-gvo.pdf.

DSK. *Stellungnahme zum Digital Fitness Check / Vorschläge zu Modifikationen der DSGVO*. Entschließung der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 10. März 2026. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder, 2026. https://www.datenschutzkonferenz-online.de/media/en/2026-03-10_DSK_Entschliessung-Digital_Fitness_Check.pdf.

EDPB. *Guidelines 1/2026 on processing of personal data for scientific research purposes*. European Data Protection Board, 2026. https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2026/guidelines-12026-processing-personal-data_en.

Engels, Barbara, und Marc Scheufen. *Wettbewerbseffekte der Europäischen Datenschutzgrundverordnung*. IW-Report Nr. 1/20. Institut der deutschen Wirtschaft, 2020.

Erdsiek, Daniel. „Optimismus in der Informationswirtschaft". *ZEW Branchenreport Informationswirtschaft*, Mai 2024, 1–2. https://www.zew.de/fileadmin/FTP/brepikt/202401BrepIKT.pdf.

Erdsiek, Daniel. „Viele Unternehmen stellen DSGVO schlechtes Zeugnis aus". *ZEW Branchenreport Informationswirtschaft*, Mai 2020, 3–4. https://www.zew.de/fileadmin/FTP/brepikt/202001BrepIKT.pdf.

Europäische Kommission. „Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA". *Amtsblatt der Europäischen Union* L 231 (September 2023): 118–229. http://data.europa.eu/eli/dec_impl/2023/1795/oj.

Europäische Kommission. *Eine europäische Datenstrategie*. COM(2020) 66 final. Europäische Kommission, 2020. https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=COM%3A2020%3A66%3AFIN.

European Commission. *A Digital Agenda for Europe*. COM(2010) 245. Brussels, 2010.

European Commission. *Impact assessment accompanying the General Data Protection Regulation*. SEC(2012) 72 final. European Commission, 2012. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:en:PDF.

European Commission. *Proposal for a Digital Omnibus Regulation*. COM(2025) 837 final. Brussels, 2025. https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal.

European Commission. *The General Data Protection Regulation*. Special Eurobarometer Nr. 487a. Mit Kantar. Brussels, 2019. https://doi.org/10.2838/579882.

Ezrachi, Ariel, und Maurice E. Stucke. *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*. Harvard University Press, 2016.

Frey, Carl Benedikt, und Giorgio Presidente. „Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally". *Economic Inquiry* 62, Nr. 3 (2024): 1074–89. https://doi.org/10.1111/ecin.13213.

Frey, Carl Benedikt, Giorgio Presidente, und Pia Andres. *Data-Biased Innovation: Directed Technological Change and the Future of Artificial Intelligence*. The Oxford Martin Working Paper Series on Technological and Economic Change. Oxford Martin School, Oxford University, 2024.

Friedewald, Michael, Ina Schiering, und Nicholas Martin. „Datenschutz-Folgenabschätzung in der Praxis: Herausforderungen bei der Implementierung eines innovativen Instruments der DSGVO". *Datenschutz und Datensicherheit - DuD* 43, Nr. 8 (2019): 473–77. https://doi.org/10.1007/s11623-019-1146-y.

Gal, Michal S., und Oshrit Aviv. „The Competitive Effects of the GDPR". *Journal of Competition Law & Economics* 16, Nr. 3 (2020): 349–91. https://doi.org/10.1093/joclec/nhaa012.

Glintborg, Bente, Mats Hansson, Hilde Berner Hammer, u. a. „Legal Obstacles Jeopardise Research in Personalised Medicine – Experiences from a Nordic Collaboration within Rheumatology". *Scandinavian Journal of Public Health* 52, Nr. 8 (2024): 1019–25. https://doi.org/10.1177/14034948231212711.

Gräfe, Daniel. „Datenschutz-Grundverordnung: Neuer EU-Datenschutz stärkt Bürgerrechte und verärgert Firmen". *Stuttgarter Nachrichten*, 21. Februar 2018. https://www.stuttgarter-nachrichten.de/inhalt.datenschutz-grundverordnung-neuer-eu-datenschutz-staerkt-buergerrechte-und-veraergert-firmen.564a5c9c-da01-493e-9c5d-c120b6a37963.html.

Grunwald, Armin. „Die hermeneutische Erweiterung der Technikfolgenabschätzung". *TATuP - Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis* 24, Nr. 2 (2015): 65–69. https://doi.org/10.14512/tatup.24.2.65.

Grunwald, Armin. „Die Unterscheidung von Gestaltbarkeit und Nicht-Gestaltbarkeit der Technik". In *Technikgestaltung zwischen Wunsch und Wirklichkeit*, herausgegeben von Armin Grunwald. Springer Berlin Heidelberg, 2003. https://doi.org/10.1007/978-3-642-55473-5_2.

Hansen, Marit, Meike Kamp, und Tobias Keber. „Gedanken zur Reform der DSGVO aus Sicht der Aufsichtspraxis: Potentiale und Synergien heben, bürokratischen Aufwand reduzieren". *Datenschutz und Datensicherheit - DuD* 50, Nr. 1 (2026): 22–27. https://doi.org/10.1007/s11623-026-2198-4.

HBDI, und DGIM. *Datenschutz in der medizinischen Forschung: Leitfaden für Forschende in der Medizin*. Deutsche Gesellschaft für Innere Medizin (DGIM) und Hessischer Beauftgragter für Datenschutz und Informationsfreiheit (HBDI), 2025. https://www.dgim.de/fileadmin/bildarchiv/PDF/Publikationen/20251205_DGIM_HBDI_Leifaden_Datenschutz_1.01.pdf.

Hötzendorfer, Walter. „IT-Projektmanagement by Datenschutz-Folgenabschätzung". *Jusletter-IT*, Online-Vorab-Publikation, 29. Juni 2023. https://doi.org/10.38023/4964a828-aafe-4d38-8a61-16d1767505d8.

Janßen, Rebecca, Reinhold Kesler, Michael E. Kummer, und Joel Waldfogel. „GDPR and the Lost Generation of Innovative Apps". Working Paper Nr. 30028. Working Paper Series. National Bureau of Economic Research, Mai 2022. https://doi.org/10.3386/w30028.

Jia, Jian, Ginger Zhe Jin, Mario Leccese, und Liad Wagman. *How Does Privacy Regulation Affect Transatlantic Venture Investment? Evidence from GDPR*. NBER Working Papers Nr. 33909. National Bureau of Economic Research, Inc, 2025. https://ideas.repec.org//p/nbr/nberwo/33909.html.

Jia, Jian, Ginger Zhe Jin, und Liad Wagman. „The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment". *Marketing Science* 40, Nr. 4 (2021): 661–84. https://doi.org/10.1287/mksc.2020.1271.

Karaboga, Murat. *Die Entstehung der EU-Datenschutz-Grundverordnung: Das Politikfeld Datenschutz im Spannungsverhältnis zwischen Grundrechtsschutz und Binnenmarktregulierung*. Privatheit und Selbstbestimmung in der digitalen Welt, herausgegeben von Michael Friedewald und Alexander Roßnagel, Nr. 3. Nomos, 2024. https://doi.org/10.5771/9783748915898.

Kettl, Julian, Klaus Schäfer, und Niklas Buchauer. „Privacy matters: Welchen Wert hat der Schutz persönlicher Daten bei Online-Girokonten?" *HMD Praxis der Wirtschaftsinformatik* 58, Nr. 6 (2021): 1552–65. https://doi.org/10.1365/s40702-021-00738-8.

Kircher, Tobias, und Jens Foerderer. „Does EU-Consumer Privacy Harm Financing of US-App-Startups? Within-US Evidence of Cross-EU-Effects". *Proceedings of the 42nd International Conference on Information Systems (ICIS), 2020, Austin, United States, December 12-15*, 2020.

Kranzberg, Melvin. „Technology and History: ‚Kranzberg's Laws'". *Technology and Culture* 27, Nr. 3 (1986): 544–60. https://doi.org/10.2307/3105385.

Kurkowski, Sandra, Kerstin Ziegler, Christian Jäger, u. a. „Mehr Barrieren als Brücken – Forschung in Zeiten der DSGVO". *Zeitschrift für Palliativmedizin* 23, Nr. 02 (2022): 86–89. https://doi.org/10.1055/a-1744-5270.

Lalova-Spinks, Teodora, Evelien De Sutter, Peggy Valcke, u. a. „Challenges Related to Data Protection in Clinical Research before and during the COVID-19 Pandemic: An Exploratory Study". *Frontiers in Medicine* 9 (Oktober 2022). https://doi.org/10.3389/fmed.2022.995689.

Lango, Luke. „What You're Not Being Told About the AI Economy". Yahoo Finance, 22. März 2026. https://finance.yahoo.com/news/hidden-wealth-transfer-inside-ai-135500192.html.

Lefouili, Yassine, Leonardo Madio, und Ying Lei Toh. „Privacy Regulation and Quality-Enhancing Innovation". *The Journal of Industrial Economics* 72, Nr. 2 (2024): 662–84. https://doi.org/10.1111/joie.12374.

Li, Wilson, Bingqing Xiong, und Chaofan Yang. „A Roadmap to Achieving a Healthier Information Ecosystem through GDPR Implementation and Privacy Compliance Technologies". *Journal of the Association for Information Science and Technology* 75, Nr. 10 (2024): 1182–201. https://doi.org/10.1002/asi.24878.

Li, Ziru, Gunwoong Lee, T. S. Raghu, und Zhan (Michael) Shi. „Impact of the GDPR on the Global Mobile App Market: Digital Trade Implications of Data Protection and Privacy Regulations". SSRN Scholarly Paper Nr. 4320436. Social Science Research Network, 4. März 2024. https://papers.ssrn.com/abstract=4320436.

Lin, Tesary. „Valuing Intrinsic and Instrumental Preferences for Privacy". *Marketing Science* 41, Nr. 4 (2022): 663–81. https://doi.org/10.1287/mksc.2022.1368.

Martin, Nicholas, und Max von Grafenstein. „Innovation and the GDPR: Much ado about quite a lot". *Computer Law & Security Review* 60 (April 2026): 106270. https://doi.org/10.1016/j.clsr.2026.106270.

Martin, Nicholas, Christian Matt, Crispin Niebel, und Knut Blind. „How Data Protection Regulation Affects Startup Innovation". *Information Systems Frontiers* 21, Nr. 6 (2019): 1307–24. https://doi.org/10.1007/s10796-019-09974-2.

Niebel, Crispin. „The impact of the general data protection regulation on innovation and the global political economy". *Computer Law & Security Review* 40 (2021): 105523. https://doi.org/10.1016/j.clsr.2020.105523.

OECD, Hrsg. *An Introduction to Online Platforms and Their Role in the Digital Transformation*. OECD Publishing, 2019. https://doi.org/10.1787/53e5f593-en.

OECD, Hrsg. *Frascati-Handbuch 2015: Leitlinien für die Erhebung und Meldung von Daten über Forschung und experimentelle Entwicklung*. 7. Auflage. Paris, 2018. https://doi.org/10.1787/9789264291638-de.

OECD und Eurostat, Hrsg. *Oslo-Handbuch 2018: Leitlinien für die Erhebung, Darstellung und Nutzung von Innovationsdaten*. 4. Aufl. Paris, 2024. https://doi.org/10.1787/9d73fbba-de.

Passoth, Jan-Hendrik. „Digitale Souveränität in und für Europa: Infrastrukturen, Plattformen und ein gemeinwohlorientiertes Ökosystem". *MedienWirtschaft* 16, Nr. 3 (2019): 21–23. https://doi.org/10.15358/1613-0669-2019-3-21.

Pilichowski, Elsa, Anna Pietikäinen, Miguel Amaral, u. a. *Regulatory Sandbox Toolkit: A Comprehensive Guide for Regulators to Establish and Manage Regulatory Sandboxes Effectively*. Herausgegeben von OECD. OECD Publishing, 2025. https://doi.org/10.1787/de36fa62-en.

Quezada-Tavarez, Katherine, Lidia Dutkiewicz, und Noémie Krack. „Voicing Challenges: GDPR and AI Research". *Open Research Europe* 2 (November 2022). https://doi.org/10.12688/openreseurope.15145.1.

Rammer, Christian. *Dokumentation zur Innovationserhebung 2024*. ZEW-Dokumentation Nr. 25–01. ZEW – Leibniz-Zentrum für Europäische Wirtschaftsforschung, 2025. https://www.zew.de/fileadmin/FTP/docus/dokumentation2501.pdf.

Rammert, Werner. „Die Innovationen der Gesellschaft". In *Soziale Innovation: Auf dem Weg zu einem postindustriellen Innovationsparadigma*, herausgegeben von Jürgen Howaldt und Heike Jacobsen. VS Verlag für Sozialwissenschaften, 2010. https://doi.org/10.1007/978-3-531-92469-4_2.

Roßnagel, Alexander. „7 Jahre DSGVO – Ein Blick zurück und ein Blick voraus aus Sicht der Datenschutzaufsicht". *PinG Privacy in Germany*, Nr. 3 (April 2025): 8. https://doi.org/10.37307/j.2196-9817.2025.03.08.

Roßnagel, Alexander, Hrsg. *Das neue Datenschutzrecht: Europäische Datenschutz-Grundverordnung und deutsche Datenschutzgesetze*. Nomos, 2018.

Roßnagel, Alexander. „Datenschutz in der Forschung: Die neuen Datenschutzregelungen in der Forschungspraxis von Hochschulen". *Zeitschrift für Datenschutz* 9, Nr. 4 (2019): 157–63.

Roßnagel, Alexander. „Digitale Souveränität im Datenschutzrecht". *Multimedia und Recht* 26, Nr. 1 (2023): 64–68.

Roßnagel, Alexander. „Kein ‚Verbotsprinzip' und kein ‚Verbot mit Erlaubnisvorbehalt' im Datenschutzrecht: Zur Dogmatik der Datenverarbeitung als Grundrechtseingriff". *Neue Juristische Wochenschrift (NJW)* 2019, Nr. 1–2 (2019): 1–5.

Roßnagel, Alexander. „Weniger Bürokratie im Datenschutz". *Zeitschrift für Datenschutz* 16, Nr. 7 (2026): 375–81.

Roßnagel, Alexander, und Christian Geminn. *Datenschutz-Grundverordnung verbessern: Änderungsvorschläge aus Verbrauchersicht*. Nomos, 2020. https://doi.org/10.5771/9783748920991.

Roßnagel, Alexander, und Astrid Wallmann, Hrsg. *Bürokratieabbau im Datenschutz*. Nomos, 2025.

Ruschemeier, Hannah. „Künstliche Intelligenz als soziotechnische Entwicklung". Forschung & Lehre, 9. September 2025. https://www.forschung-und-lehre.de/recht/kuenstliche-intelligenz-als-soziotechnische-entwicklung-7278.

Schieferdecker, Ina, und Christoph March. „Digitale Innovationen und Technologiesouveränität". *Wirtschaftsdienst* 100, Nr. 13 (2020): 30–35. https://doi.org/10.1007/s10273-020-2612-8.

Schild, Hans-Hermann. „Erste geplante Änderung der DS-GVO zur Entlastung der KMU". *ZD-Aktuell* 15, Nr. 12 (2025): 01300. https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2Fzdaktuell%2F2025%2Fcont%2Fzdaktuell.2025.01300.htm&anchor=Y-300-Z-ZDAKTUELL-B-2025-N-01300.

Schwartmann, Rolf, und Felix Sahm. „Schutzräume für die Forschung". *Frankfurter Allgemeine Zeitung*, 6. Mai 2026.

Simitis, Spiros, Gerrit Hornung, und Indra Spiecker Döhmann, Hrsg. *Datenschutzrecht DSGVO mit BDSG*. 2. Aufl. Nomos, 2025.

Steinberg, Philipp, und Gero Roser. „Wirtschaftspolitische Herausforderungen der Digitalisierung". *Wirtschaftsdienst* 100, Nr. 13 (2020): 54–56. https://doi.org/10.1007/s10273-020-2616-4.

Stiftung Datenschutz. *Wirtschaftsvorteil Datenschutz: Warum DSGVO-Standards Unternehmen resilient und erfolgreich für die Zukunft aufstellen*. White Paper. Stiftung Datenschutz, 2026. https://stiftungdatenschutz.org/fileadmin/Redaktion/Dokumente/WhitePaper_Wirtschaftsvorteil_Datenschutz/WhitePaper_Standortvorteil_Datenschutz.pdf.

Swani, Kunal, George R. Milne, und Brian P. Brown. „The Benefits of Meeting Buyer Privacy Expectations across Information, Time, and Space Dimensions". *Industrial Marketing Management* 112 (Juli 2023): 14–26. https://doi.org/10.1016/j.indmarman.2023.04.013.

Thierer, Adam D. *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom*. Mercatus Center, George Mason Univ., 2014.

„Verordnung (EU) 2025/327 des Europäischen Parlaments und des Rates vom 11. Februar 2025 über den europäischen Gesundheitsdatenraum sowie zur Änderung der Richtlinie 2011/24/EU und der Verordnung (EU) 2024/2847". *Amtsblatt der Europäischen Union*, L, 5. März 2025, 2025/327. https://eur-lex.europa.eu/eli/reg/2025/327/oj.

Vukovic, Jakov, Damir Ivankovic, Claudia Habl, und Jelena Dimnjakovic. „Enablers and Barriers to the Secondary Use of Health Data in Europe: General Data Protection Regulation Perspective". *Archives of Public Health* 80, Nr. 1 (2022): 115. https://doi.org/10.1186/s13690-022-00866-7.

Weber, Matthias, Bernhard Dachs, Krisztina Rozgonyi, u. a. *Wege zur Stärkung der Forschung und Anwendung von künstlicher Intelligenz in Europa*. Studie zum deutschen Innovationssystem Nr. 6–2026. Herausgegeben von Expertenkommission Forschung und Innovation (EFI). AIT Austrian Institute of Technology, Fraunhofer ISI, Karlsruher Institut für Technologie, 2026.

Wenn der Notarzt nicht weiß, wie der Facharzt behandelt hat – Wie Datenschutz in Deutschland Patienten gefährdet. Pressemitteilung. Deutsche Gesellschaft für Innere Medizin, 2022.

Wolff, Josephine, und Nicole Atallah. „Early GDPR Penalties: Analysis of Implementation and Fines Through May 2020". *Journal of Information Policy* 11 (Dezember 2021): 63–103. https://doi.org/10.5325/jinfopoli.11.2021.0063.

Ziebarth, Wolfgang. „Kontrollaufgaben und Gesetzesbindung der Datenschutzaufsicht - Möglichkeiten und Grenzen der Entbürokratisierung". In *Bürokratieabbau im Datenschutz*, herausgegeben von Alexander Roßnagel und Astrid Wallmann. Nomos, 2025.

Plattform Privatheit

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

PROJEKTPARTNER

Fraunhofer

Natur
Technik
Kultur
Gesellschaft
UNIKASSEL
VERSITÄT