10 Jahre DS-GVO

Eine Zwischenbilanz des Datenschutzes
in Unternehmen

bitkom

10 Jahre DS-GVO

Eine Zwischenbilanz des Datenschutzes in Unternehmen

Bitkom-Dataverse

Diese und weitere Bitkom-Studien finden Sie in unserem Datenportal.

Zum Bitkom-Dataverse

Zu den Studienberichten

DOI
10.64022/2026-DSGVO

Executive Summary

Am 25. Mai 2026 wird die Datenschutz-Grundverordnung (DS-GVO) zehn Jahre alt. Seit ihrem Inkrafttreten in 2016 begleitet der Bitkom den Datenschutz in Deutschland mit regelmäßigen Unternehmensbefragungen – von der Vorbereitungsphase vor Anwendbarkeit der DS-GVO (2016-2018) bis zu aktuellen Herausforderungen rund um Digitalisierung, internationale Datentransfers und Künstliche Intelligenz. So ergibt sich in diesem Jahr ein Zehn-Jahres-Blick auf zentrale Entwicklungen aus Sicht der Wirtschaft. Die Ergebnisse zeigen: Datenschutz ist in den Unternehmen längst Teil des organisatorischen Alltags geworden. Zugleich bleiben Prüf- und Umsetzungsaufwand und rechtliche Unsicherheit für viele Unternehmen hoch.

Dieser Bericht analysiert die Entwicklung einzelner Aspekte der Jahre 2016 bis 2025 und zieht eine Zwischenbilanz zur DS-GVO. Grundlage sind repräsentative Erhebungen, die Bitkom Research mittels computergestützter telefonischer Interviews (CATI) durchgeführt hat. Befragt wurden Unternehmen aller Branchen in Deutschland ab 20 Beschäftigten.

Die zentralen Ergebnisse:

- **Datenschutz ist in den Unternehmen angekommen – aber nicht abgeschlossen**
  2024 geben 71 Prozent der Unternehmen an, die DS-GVO vollständig oder größtenteils umgesetzt zu haben – der höchste Wert der Zeitreihe. Gleichzeitig sehen 28 Prozent die Vorgaben weiterhin nur teilweise oder noch nicht umgesetzt. Die Umsetzung der DS-GVO bleibt damit auch Jahre nach ihrer Anwendbarkeit für viele Unternehmen eine dauerhafte Aufgabe.

- **Datenschutz ist für Unternehmen mit immer höherem und weiter steigendem Aufwand verbunden**
  2025 bewerten 97 Prozent der Unternehmen den Aufwand für Datenschutz als hoch – 44 Prozent als sehr hoch und 53 Prozent als eher hoch. Zugleich sagen 84 Prozent der Unternehmen, dass sich ihr Aufwand für Datenschutz seit Einführung der DS-GVO erhöht hat. Ein Entlastungseffekt durch mehr Erfahrung und Routine stellt sich damit nicht ein.

- **Die DS-GVO macht die Geschäftsprozesse aus Sicht vieler Unternehmen komplizierter**
  81 Prozent der Unternehmen sagen 2025, dass die DS-GVO ihre Geschäftsprozesse komplizierter macht. 2016 lag dieser Anteil noch bei 25 Prozent. Die Wahrnehmung zusätzlicher Komplexität hat sich damit über die Jahre stark verfestigt.

- **Rechtsunsicherheit bleibt eine der größten Herausforderungen**
  82 Prozent der Unternehmen nennen 2025 Unsicherheit bezüglich der genauen Datenschutzvorgaben als Herausforderung. Zugleich sagen 86 Prozent, dass die Umsetzung nie vollständig abgeschlossen ist, weil Unternehmen kontinuierlich auf technische und rechtliche Entwicklungen reagieren müssen. Datenschutz wird so als besonders herausfordernde, andauernde Compliance-Aufgabe wahrgenommen.

- **Datenschutz wird zunehmend als Innovationshemmnis erlebt**
  Besonders datengetriebene Vorhaben sind betroffen. 2025 berichten 59 Prozent der Unternehmen, dass der Aufbau von Datenpools aufgrund von Datenschutzvorgaben gescheitert ist oder gar nicht erst in Angriff genommen wurde. Auch bei Datenanalysetools, KI-Anwendungen und der Digitalisierung von Geschäftsprozessen bleiben die Werte hoch. Datenschutzvorgaben werden damit vor allem dort als Hürde wahrgenommen, wo Innovationen auf die Nutzung großer Datenmengen angewiesen sind.
- **Beim Verhältnis von Datenschutz und KI zeigt sich ein Spannungsverhältnis**
  59 Prozent der Unternehmen sehen europäischen Datenschutz 2025 im internationalen Vergleich als Vorteil für die KI-Entwicklung in Deutschland und Europa. Gleichzeitig sagen 69 Prozent, dass Datenschutz erschwert, KI-Modelle mit genügend Daten zu trainieren, und 63 Prozent meinen, Datenschutz vertreibe KI-entwickelnde Unternehmen aus der EU. Datenschutz wird also als mögliches Qualitätsversprechen gesehen, in der praktischen KI-Entwicklung aber häufig als Standortnachteil erlebt.
- **Internationale Datentransfers bleiben unverzichtbar – aber politisch ungelöst**
  Die USA bleiben das wichtigste Drittland für personenbezogene Datentransfers außerhalb der EU. 2025 übermitteln 61 Prozent der Unternehmen personenbezogene Daten dorthin. Zugleich wünschen sich 71 Prozent der Unternehmen von der Politik tragfähige Lösungen für internationale Datentransfers. Das zeigt: Globale Datenflüsse sind wirtschaftliche Realität, ihre rechtliche Absicherung bleibt aber eine zentrale Herausforderung.
- **Die Reform der DS-GVO ist aus Sicht der Wirtschaft notwendig**
  72 Prozent der Unternehmen sagen 2025, dass »wir es mit dem Datenschutz in Deutschland übertreiben«. Diese Kritik richtet sich nicht gegen Datenschutz als Grundrecht, sondern gegen eine Umsetzungspraxis, die aus Sicht vieler Unternehmen zu komplex, zu unsicher und zu aufwendig ist. Eine Reform sollte daher mehr Rechtssicherheit, mehr Risikoorientierung und bessere Rahmenbedingungen für datengetriebene Innovationen schaffen.

Insgesamt zeigen die Studienergebnisse:

Die DS-GVO hat Datenschutz in der deutschen Wirtschaft fest verankert. Sie hat aber nicht zu weniger Aufwand, mehr Klarheit oder einfacheren Prozessen geführt. Unternehmen akzeptieren Datenschutz als wichtigen Rahmen für Vertrauen in die digitale Wirtschaft, fordern aber eine praxistauglichere und stärker risikobasierte Anwendung. Zehn Jahre nach ihrem in Kraft treten steht die DS-GVO damit vor der nächsten Etappe. Sie muss wirksamen Grundrechtsschutz sichern und zugleich Innovation, KI-Entwicklung und internationale Wettbewerbsfähigkeit ermöglichen.

Zentrale Wegmarken

Von der Datenschutzrichtlinie zur DS-GVO

1995

Europäische Datenschutzrichtlinie

Mit der Richtlinie 95/46/EG schafft die EU erstmals einen gemeinsamen Rahmen für den Schutz personenbezogener Daten und den freien Datenverkehr im Binnenmarkt. Sie bildet die Grundlage des europäischen Datenschutzrechts vor der DS-GVO.

2012

Vorschlag für eine Datenschutzreform

Die Europäische Kommission legt den Entwurf der Datenschutz-Grundverordnung (DS-GVO) vor. Ziel ist ein einheitlicher, unmittelbar geltender Rechtsrahmen für eine zunehmend digitale und datengetriebene Wirtschaft.

2016

Verabschiedung der DS-GVO

EU-Parlament und Rat beschließen die DS-GVO. Sie wird am 4. Mai 2016 im Amtsblatt veröffentlicht und tritt am 24. Mai 2016 in Kraft. Unternehmen erhalten eine zweijährige Übergangsfrist bis zur Anwendbarkeit.

25. Mai 2018

Die DS-GVO wird anwendbar

Die DS-GVO gilt unmittelbar in allen EU-Mitgliedstaaten. Unternehmen müssen Datenschutzprozesse, Dokumentation, Rechtsgrundlagen. Betroffenenrechte, Auftragsverarbeitung und Governance-Strukturen umfassend überprüfen und anpassen.

2019/2020

Einwilligung und Cookies rücken in den Fokus

Mit der Planet49-Entscheidung konkretisiert der EuGH die Anforderungen an wirksame Cookie-Einwilligungen. In Deutschland schafft das TTDSG, heute TDDDG, einen eigenständigen Rechtsrahmen für den Schutz der Privatsphäre in Telekommunikation und digitalen Diensten.

2020

Schrems II und internationale Datentransfers

Der EuGH erklärt den EU-US Privacy Shield für ungültig. Unternehmen müssen internationale Datenübermittlungen, insbesondere an US-Dienstleister, neu bewerten und zusätzliche Schutzmaßnahmen prüfen.

2021

Neue Standardvertragsklauseln

Die EU-Kommission veröffentlicht modernisierte Standardvertragsklauseln für Drittlandtransfers. Sie werden zum zentralen Instrument für viele internationale Datenübermittlungen nach Schrems II.

2023

EU-US Data Privacy Framework

Die EU beschließt eine neue Rechtsgrundlage für Datentransfers in die USA. Gleichzeitig prägen generative KI und neue Digitalgesetze die Datenschutzdebatte.

seit 2024

Datenschutz im Kontext neuer Digitalregulierung

Mit dem Digital Services Act und der KI-Verordnung wird Datenschutz zunehmend Teil einer breiteren europäischen Digitalregulierung. Für Unternehmen verschiebt sich der Fokus von reiner DS-GVO-Compliance hin zu integrierter Daten-, Plattform- und KI-Governance.

Inhalt

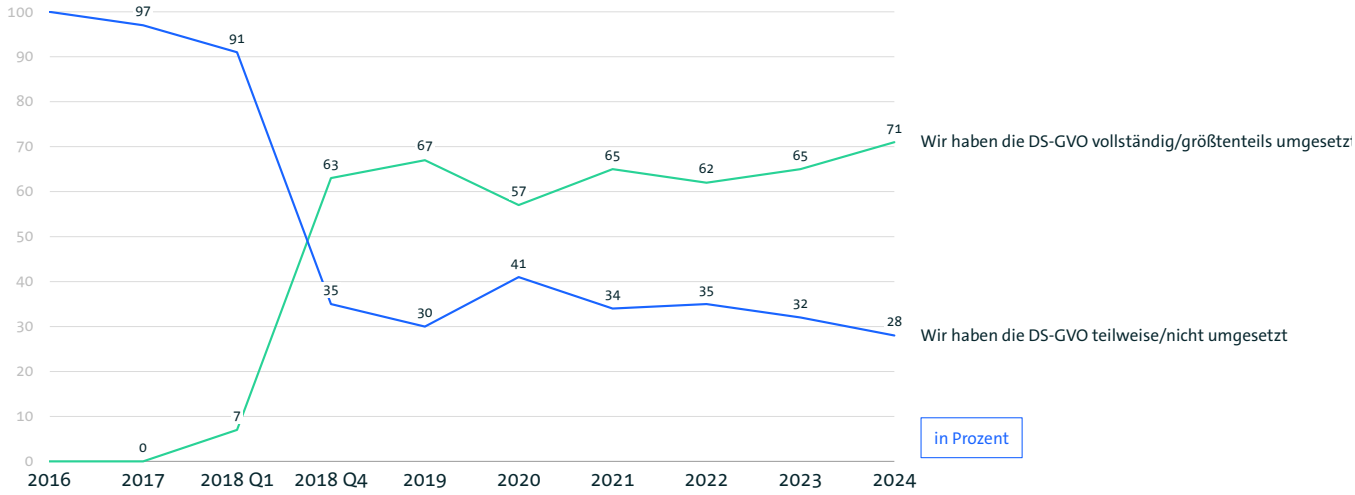
Abbildungen

1 Umsetzung & Belastung

1 Umsetzung & Belastung

1.1 Wie weit ist die DS-GVO in Unternehmen umgesetzt?

Wie weit sind Sie in Ihrem Unternehmen zum aktuellen Zeitpunkt mit der Umsetzung der DS-GVO?



Basis: Alle befragten Unternehmen ab 20 Beschäftigten | Abweichungen von 100 Prozent sind rundungsbedingt | Nicht dargestellt: »Weiß nicht/ keine Angabe« | Quelle: Bitkom Research

Abbildung 1: Umsetzungsstand der DS-GVO

Datenschutz ist angekommen – aber nicht abgeschlossen

Die DS-GVO hat sich in den Unternehmen fest etabliert. Vor ihrer Anwendbarkeit im Mai 2018 spielte eine vollständige oder weitgehende Umsetzung praktisch noch keine Rolle. 2016 und 2017 lag der Anteil bei 0 Prozent, im ersten Quartal 2018 erst bei 7 Prozent. Mit dem Start der Anwendbarkeit kam dann der deutliche Umsetzungsschub. Im vierten Quartal 2018 gaben 63 Prozent der Unternehmen an, die Vorgaben vollständig oder größtenteils umgesetzt zu haben. 2019 waren es 67 Prozent.

Der Rückgang im Jahr 2020 auf 57 Prozent zeigt jedoch, dass DS-GVO-Compliance kein einmaliges Umsetzungsprojekt ist. Neue rechtliche Anforderungen und Unsicherheiten – etwa rund um internationale Datentransfers infolge des Schrems-II-Urteils – dürften dazu beigetragen haben, dass Unternehmen ihren Umsetzungsstand neu und kritischer bewertet haben. Das Urteil des EuGH vom Juli 2020 erklärte das EU-US Privacy Shield für ungültig, in der Folge mussten Unternehmen bei Standardvertragsklauseln zusätzliche Prüfungen und gegebenenfalls ergänzende Schutzmaßnahmen berücksichtigen.

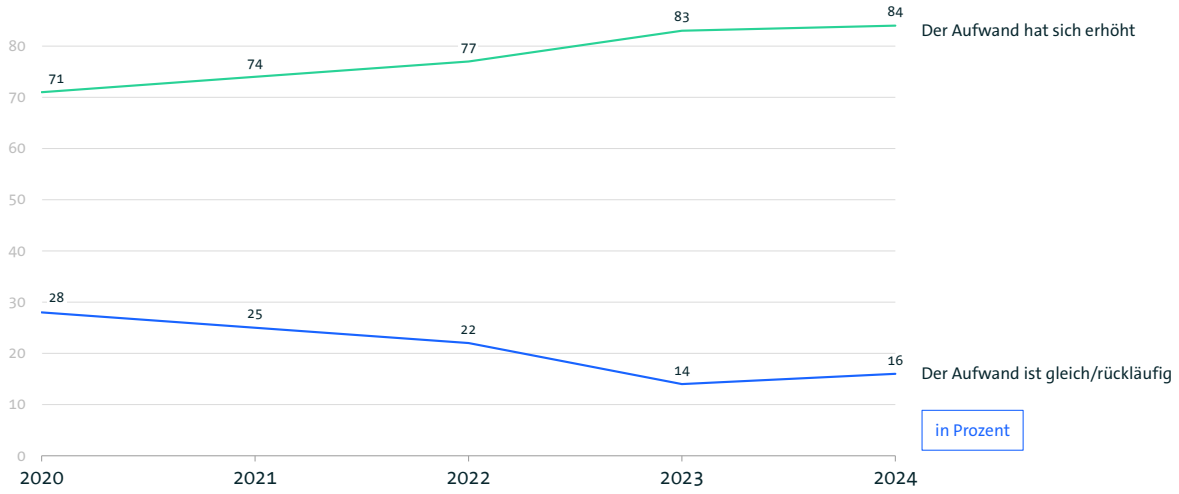
Auch die Entwicklung 2022 deutet darauf hin, dass Datenschutzmaßnahmen laufend nachjustiert werden müssen. So mussten bestehende Standardvertragsklauseln bis Ende Dezember 2022 auf die neuen EU-Standardvertragsklauseln umgestellt werden, was für viele Unternehmen zusätzlichen Anpassungsbedarf bedeutete.

2024 geben 71 Prozent der Unternehmen an, die DS-GVO vollständig oder größtenteils umgesetzt zu haben – der höchste Wert der Zeitreihe. Gleichzeitig sehen 28 Prozent die Vorgaben weiterhin nur teilweise oder noch nicht umgesetzt.

Die Zahlen zeigen damit zweierlei: Datenschutz ist in der Breite der Wirtschaft angekommen, bleibt aber auch zehn Jahre nach dem Inkrafttreten der DS-GVO eine dauerhafte Aufgabe.

1.2 Aufwand für den Datenschutz

Welche der folgenden Aussagen trifft auf Ihren Aufwand für den Datenschutz seit Einführung der DS-GVO im Jahr 2018 zu?



Basis: Alle befragten Unternehmen ab 20 Beschäftigten | Abweichungen von 100 Prozent sind rundungsbedingt | Nicht dargestellt: »Weiß nicht/ keine Angabe« | Quelle: Bitkom Research

Abbildung 2: Aufwand für den Datenschutz seit Einführung der DS-GVO

Mehr Reife, mehr Aufwand

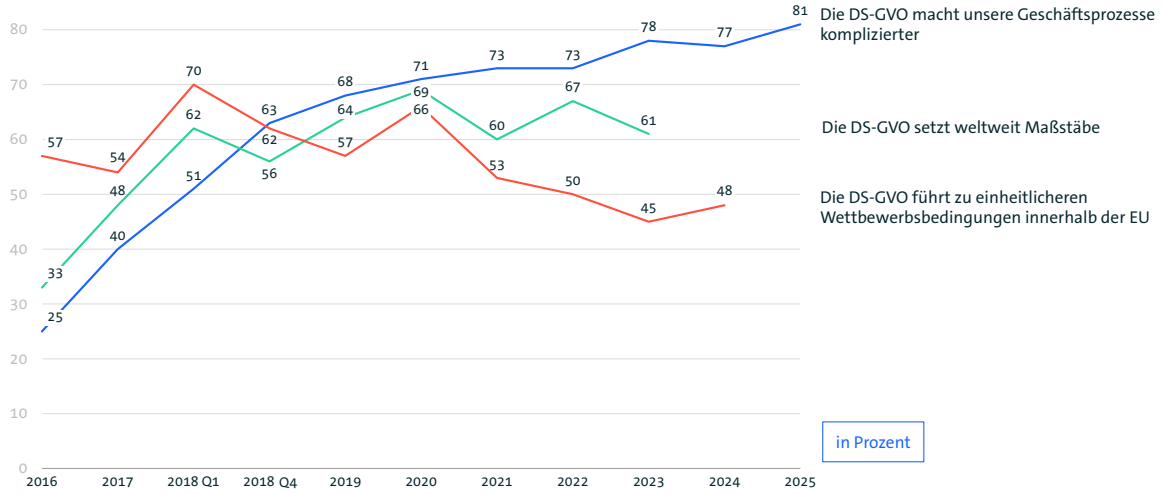
Die Umsetzung der DS-GVO ist für Unternehmen kein abgeschlossenes Projekt, sondern ein dauerhaftes Thema im Unternehmensalltag. Mit zunehmender Erfahrung im Datenschutz sinkt der wahrgenommene Aufwand nicht – im Gegenteil. Der Anteil der Unternehmen, die seit Einführung der DS-GVO einen höheren Aufwand feststellen, ist von 71 Prozent im Jahr 2020 auf 84 Prozent im Jahr 2024 gestiegen. Gleichzeitig ist der Anteil der Unternehmen, bei denen der Aufwand gleichgeblieben oder zurückgegangen ist, von 28 Prozent auf nur noch 16 Prozent gesunken.

Die Zahlen zeigen: Mehr Datenschutzreife führt nicht automatisch zu Entlastung. Vielmehr steigen mit der praktischen Umsetzung häufig auch die Anforderungen an Dokumentation, Prozesse, Verträge, technische und organisatorische Maßnahmen sowie die laufende Bewertung neuer rechtlicher und technologischer Entwicklungen. Datenschutz wird damit stärker professionalisiert, bleibt aber zugleich ressourcenintensiv.

Auch die aktuelle Bewertung des Datenschutzaufwands unterstreicht diese Entwicklung: 2025 bewerten insgesamt 97 Prozent der Unternehmen den Aufwand für Datenschutz als hoch, davon 44 Prozent als »sehr hoch« und 53 Prozent als »eher hoch« ↗Studienbericht »Datenschutz in der deutschen Wirtschaft«.

1.3 Einschätzungen zur DS-GVO seit 2016

Inwieweit treffen die folgenden Aussagen auf Ihr Unternehmen bzw. Ihrer Meinung nach zu?



Basis: Alle befragten Unternehmen ab 20 Beschäftigten | Angaben für »Trifft voll und ganz zu« und »Trifft eher zu« | Formulierung im Jahr 2016 und 2017: »(...) wird unsere Geschäftsprozesse komplizierter machen« | Item »DSGVO setzt weltweit Maßstäbe« 2024 & 2025 nicht erhoben; Item »einheitlichere Wettbewerbsbedingungen« 2025 nicht erhoben | Quelle: Bitkom Research

Abbildung 3: Aussagen zum Aufwand durch die DSGVO (2016-2025)

Datenschutz wird als Komplexitätsfaktor wahrgenommen

Die DS-GVO wird von Unternehmen immer stärker als Faktor wahrgenommen, der Geschäftsprozesse komplizierter macht. Bereits vor ihrer Anwendbarkeit erwartete ein wachsender Anteil der Unternehmen durch das neue Gesetz zusätzliche Komplexität. 2016 stimmten dieser Aussage 25 Prozent zu, im ersten Quartal 2018 bereits 51 Prozent. Mit Anwendbarkeit der DS-GVO im Mai 2018 stieg der Wert weiter deutlich an und lag im zweiten Quartal 2018 bei 63 Prozent. Seitdem hat sich diese Wahrnehmung weiter verfestigt. 2025 sagen 81 Prozent der Unternehmen, dass die DS-GVO ihre Geschäftsprozesse komplizierter macht.

Gleichzeitig wurde die DS-GVO über viele Jahre mehrheitlich als internationaler Maßstab gesehen. Zwischen 2018 und 2023 lag die Zustimmung zu dieser Aussage durchgehend bei mindestens 56 Prozent, mit einem Höchstwert von 69 Prozent im Jahr 2020. Die Unternehmen erkennen damit grundsätzlich die internationale Bedeutung der DS-GVO an.

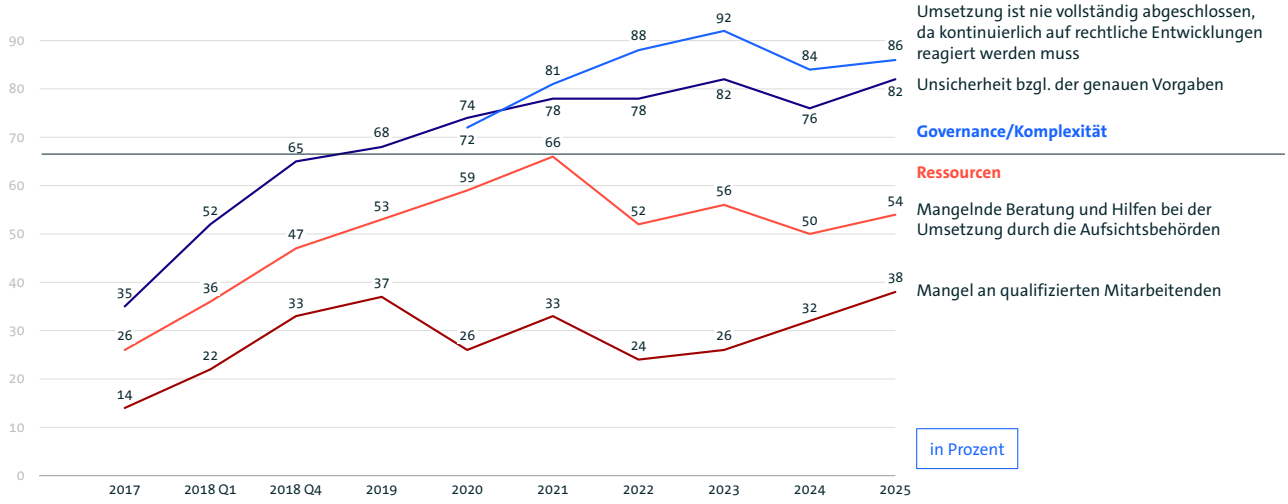
Ambivalenter fällt die Bewertung der Wirkung innerhalb der EU aus. Zwar wurde die DS-GVO anfangs mehrheitlich mit einheitlicheren Wettbewerbsbedingungen verbunden – 2018 stimmten im ersten Quartal 70 Prozent und im zweiten Quartal 63 Prozent dieser Aussage zu. In den Folgejahren ist die Zustimmung jedoch deutlich zurückgegangen und lag 2024 nur noch bei 48 Prozent. Das deutet darauf hin, dass Unternehmen den Anspruch die Vorteile eines einheitlichen europäischen Datenschutzrahmens zwar grundsätzlich sehen, in der praktischen Anwendung aber weiterhin Unterschiede, Unsicherheiten oder Umsetzungsaufwand wahrnehmen.

Insgesamt zeigt sich: Die DS-GVO bleibt aus Sicht vieler Unternehmen ein wichtiger regulatorischer Rahmen mit internationaler Strahlkraft. Zugleich wird sie im Unternehmensalltag immer stärker mit zusätzlicher Komplexität, aufwendigeren Prozessen und begrenzten Entlastungseffekten verbunden.

2 Herausforderungen bei der Umsetzung der DS-GVO

2 Herausforderungen bei der Umsetzung der DS-GVO

Was sind bzw. waren aus Ihrer Sicht die größten Herausforderungen bei der Umsetzung von Datenschutz-Vorgaben wie z. B. der DS-GVO in Ihrem Unternehmen?



Basis: Alle befragten Unternehmen ab 20 Beschäftigten | Items »Umsetzung nie vollständig abgeschlossen« 2017-2019 nicht erhoben | Mehrfachnennungen | Quelle: Bitkom Research

Abbildung 4: Größte Herausforderungen bei der Umsetzung von Datenschutz-Vorgaben

Komplexität bleibt hoch, Herausforderungen verschieben sich

Die größten Herausforderungen beim Datenschutz liegen für Unternehmen weiterhin in der Steuerung, Organisation und laufenden Anpassung ihrer Datenschutzprozesse. Besonders deutlich zeigt sich das bei der Einschätzung, dass die Umsetzung nie vollständig abgeschlossen ist, weil Unternehmen kontinuierlich auf technische und rechtliche Entwicklungen reagieren müssen. Dieser Wert lag bereits 2020 bei 72 Prozent, stieg bis 2023 auf 92 Prozent und bleibt auch 2025 mit 86 Prozent auf sehr hohem Niveau. Datenschutz wird damit klar als Daueraufgabe wahrgenommen – nicht als einmaliges Umsetzungsprojekt. Auch die Unsicherheit über die genauen Vorgaben bleibt ein zentrales Problem. Schon vor Anwendbarkeit der DS-GVO nahm diese Unsicherheit deutlich zu: von 35 Prozent im Jahr 2017 auf 65 Prozent im zweiten Quartal 2018. Seitdem bewegt sich der Wert dauerhaft auf hohem Niveau und erreicht 2025 erneut 82 Prozent. Das zeigt: Auch nach Jahren praktischer Erfahrung bestehen weiterhin erhebliche Auslegungs- und Anwendungsschwierigkeiten.

Parallel dazu verändern sich die Ressourcenprobleme. Fehlende Beratung und Hilfestellungen durch die Aufsichtsbehörden wurden insbesondere in den ersten Jahren nach Einführung der DS-GVO häufiger als Herausforderung genannt. Der Wert stieg von 26 Prozent im Jahr 2017 auf 66 Prozent im Jahr 2021. Seitdem ist er zurückgegangen, bleibt 2025 mit 54 Prozent aber weiterhin relevant.

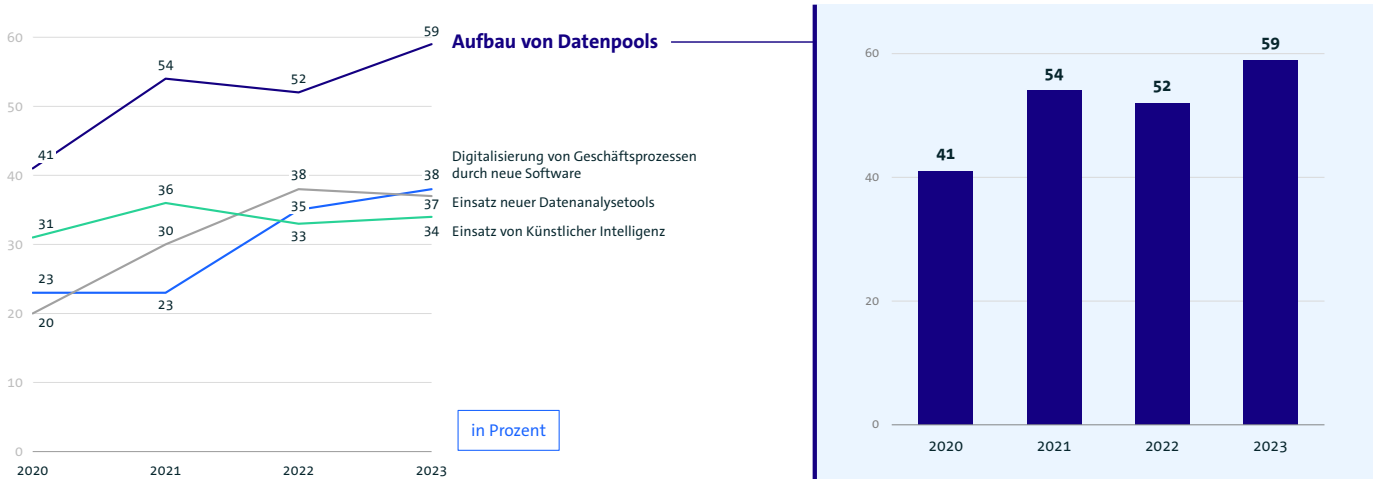
Zugleich gewinnt der Mangel an qualifizierten Mitarbeitenden wieder an Bedeutung. Nach schwankenden Werten in den Vorjahren nennen 2025 inzwischen 38 Prozent der Unternehmen fehlendes Fachpersonal als Herausforderung – der höchste Wert der Zeitreihe. Die Ergebnisse deuten damit auf eine Verschiebung hin. Neben externer Orientierung und klareren Vorgaben rücken zunehmend interne Ressourcen, Kompetenzen und Datenschutz-Know-how in den Fokus. Insgesamt zeigt sich: Die Herausforderungen im Datenschutz haben sich nicht erledigt, sondern verändert. Unternehmen müssen dauerhaft rechtliche Entwicklungen beobachten, Vorgaben auslegen, Prozesse anpassen und dafür ausreichend qualifiziertes Personal bereitstellen.

3 Innovation vs. Datenschutz

3 Innovation vs. Datenschutz

3.1 Datenschutzvorgaben und gescheiterte Innovationsprojekte

Ist es in den vergangenen 12 Monaten vorgekommen, dass in Ihrem Unternehmen innovative Projekte aufgrund von Datenschutzvorgaben gescheitert sind oder diese erst gar nicht in Angriff genommen wurden?



Basis: Alle befragten Unternehmen ab 20 Beschäftigten | Angaben für »Ja - aufgrund konkreter Vorgaben der DS-GVO« und »Ja - aufgrund von Unklarheiten im Umgang mit den Vorgaben der DS-GVO« | Quelle: Bitkom Research

Abbildung 5: Scheitern innovativer Projekte aufgrund von Datenschutzvorgaben

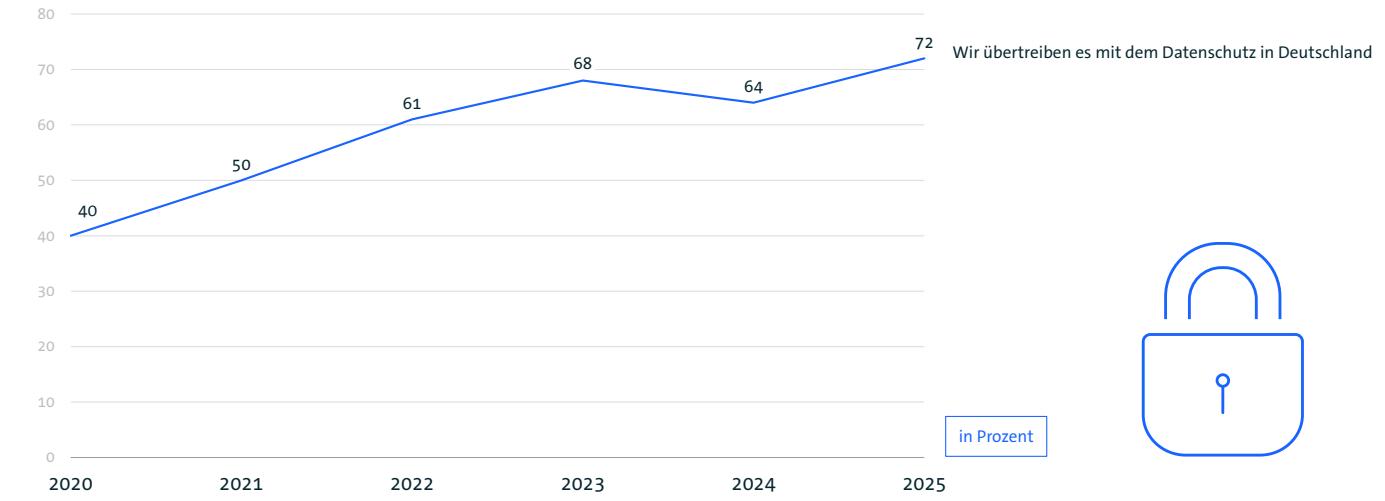
Datenschutzvorgaben werden für viele Unternehmen zunehmend zu einer Hürde bei datengetriebenen Innovationsprojekten. Besonders deutlich zeigt sich dies beim Aufbau von Datenpools. 2020 berichteten 41 Prozent der Unternehmen, dass entsprechende Projekte aufgrund von Datenschutzvorgaben gescheitert sind oder gar nicht erst in Angriff genommen wurden. 2025 liegt dieser Anteil bereits bei 59 Prozent. Auch bei weiteren digitalen und datenbasierten Vorhaben bleibt der Anteil betroffener Unternehmen hoch. Bei der Digitalisierung von Geschäftsprozessen durch neue Software ist der Wert von 23 Prozent in den Jahren 2020 und 2021 auf 38 Prozent im Jahr 2023 gestiegen. Beim Einsatz neuer Datenanalysetools zeigt sich ebenfalls ein deutlicher Anstieg – von 20 Prozent im Jahr 2020 auf 37 Prozent im Jahr 2023. Beim Einsatz von Künstlicher Intelligenz bewegt sich der Anteil seit 2020 durchgehend auf einem hohen Niveau zwischen 31 und 36 Prozent. Die Ergebnisse zeigen: Datenschutz wird besonders dort als Innovationshemmnis wahrgenommen, wo neue Geschäftsmodelle, effizientere Prozesse oder KI-Anwendungen auf die umfassende Nutzung von Daten angewiesen sind. Dabei geht es weniger um einzelne Projektarten als um ein strukturelles Spannungsfeld. Unternehmen wollen Daten stärker nutzen, stoßen aber in der praktischen Umsetzung häufig auf rechtliche Unsicherheiten, Dokumentationspflichten oder hohe Anforderungen an Einwilligungen, Zweckbindung und Datenminimierung.

Damit wird Datenschutz zunehmend zu einem Wettbewerbs- und Innovationsfaktor. Je stärker wirtschaftliche Wertschöpfung auf Daten basiert, desto entscheidender wird es, Datenschutzanforderungen rechtssicher, praxistauglich und innovationsfreundlich umzusetzen.

3.2 Mehrheit sieht Überregulierung beim Datenschutz

Inwieweit treffen die folgenden Aussagen Ihrer Meinung nach zu?

»Wir übertreiben es mit dem Datenschutz in Deutschland«



Basis: Alle befragten Unternehmen ab 20 Beschäftigten | Angaben für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research

Abbildung 6: Wahrnehmung von Datenschutzregulierung

Die Wahrnehmung, dass Datenschutz in Deutschland überreguliert ist, hat in den vergangenen Jahren deutlich zugenommen. 2020 stimmten 40 Prozent der Unternehmen der Aussage zu, dass »wir es mit dem Datenschutz in Deutschland übertreiben«. 2025 liegt dieser Anteil bei 72 Prozent – und damit auf dem höchsten Wert der Zeitreihe.

Besonders auffällig ist der starke Anstieg zwischen 2020 und 2023. Innerhalb von drei Jahren wuchs die Zustimmung von 40 auf 68 Prozent. Nach einem leichten Rückgang im Jahr 2024 auf 64 Prozent steigt der Wert 2025 erneut deutlich an. Damit hat sich die Einschätzung, dass Datenschutz in Deutschland zu weit geht, nicht nur verfestigt, sondern weiter zugespitzt.

Der Befund fügt sich in das Gesamtbild der vorangegangenen Ergebnisse ein: Unternehmen nehmen Datenschutz zunehmend als komplex, aufwendig und innovationshemmend wahr. Die hohe Zustimmung zur Aussage über übertriebenen Datenschutz deutet daher weniger auf eine grundsätzliche Ablehnung von Datenschutz hin, sondern auf wachsende Kritik an der praktischen Ausgestaltung, Auslegung und Umsetzung der Vorgaben in Deutschland.

4 Aufsichtsbehörden

4 Aufsichtsbehörden

Die Aufsichtsbehörden spielen für Unternehmen eine wichtige Rolle bei der praktischen Umsetzung von Datenschutzvorgaben.

Die Nutzung bzw. Anfrage von Hilfestellungen bleibt seit Jahren auf einem hohen Niveau. 2022 und 2023 gaben jeweils 82 Prozent der Unternehmen an, Hilfestellungen der Aufsichtsbehörden genutzt oder angefragt zu haben, 2024 waren es 80 Prozent. Das zeigt: Der Bedarf an Orientierung, Auslegungshilfen und praktischer Unterstützung ist weiterhin groß und die Behörden werden als wichtige Anlaufstelle wahrgenommen.

Gleichzeitig fällt die Bewertung der erhaltenen Hilfestellungen kritisch aus. Nur 36 Prozent der Unternehmen waren 2023 mit den genutzten Hilfestellungen zufrieden, während 63 Prozent unzufrieden waren. Auch in den Vorjahren überwog die Unzufriedenheit deutlich: 2021 lag sie bei 66 Prozent, 2022 bei 56 Prozent. Die stärkere Nutzung der Behördenangebote geht also nicht automatisch mit einer höheren Zufriedenheit einher. Vielmehr zeigt sich ein Spannungsverhältnis: Unternehmen suchen verstärkt Unterstützung, erleben diese aber häufig nicht als ausreichend hilfreich für die konkrete Umsetzung.

Ein Blick auf die Bewertung einzelner Aspekte verdeutlicht dieses Bild. Positiv fällt auf, dass die Beratung überwiegend als freundlich wahrgenommen wird. 2023 stimmten 59 Prozent der Unternehmen dieser Aussage zu, 2022 waren es sogar 65 Prozent. Auch die Bearbeitungsgeschwindigkeit hat sich im Vergleich zu 2021 verbessert. Damals gaben 29 Prozent an, ihre Anfrage sei schnell bearbeitet worden; 2023 waren es 41 Prozent. Dennoch bleiben die Werte insgesamt verhalten. Besonders kritisch ist, dass der Anteil der Unternehmen, die in der Aufsichtsbehörde einen kompetenten Ansprechpartner hatten, von 47 Prozent im Jahr 2021 auf 38 Prozent im Jahr 2023 zurückgegangen ist.

Für datengetriebene Innovationen leisten die Hilfestellungen der Behörden offenbar nur begrenzt Unterstützung. 2023 gaben 34 Prozent der Unternehmen an, innovative, datengetriebene Projekte mit Hilfe der Aufsichtsbehörden schneller umgesetzt zu haben. Das ist zwar mehr als 2021 mit 27 Prozent, liegt aber unter dem Wert von 2022 mit 40 Prozent. Gerade vor dem Hintergrund, dass Datenschutz zunehmend als Hürde für Datenpools, Datenanalysen oder KI-Projekte wahrgenommen wird, deutet dieser Befund darauf hin, dass Unternehmen von den Behörden noch stärker praxisnahe, innovationsfreundliche Orientierung erwarten.

Auch die Gründe, aus denen Unternehmen keine Hilfestellungen nutzen oder anfragen, haben sich verändert. Klassische Zugangshürden verlieren an Bedeutung. Der Anteil der Unternehmen, denen nicht bekannt war, dass es Hilfestellungen gibt, sank von 26 Prozent im Jahr 2021 auf nur noch 7 Prozent im Jahr 2024. Auch die Angst vor Behörden ging deutlich zurück – von 18 Prozent im Jahr 2021 auf 8 Prozent im Jahr 2024. Das spricht dafür, dass die Sichtbarkeit der Angebote gestiegen ist und grundsätzliche Berührungsängste abnehmen. An ihre Stelle treten jedoch stärker qualitative Vorbehalte. Der Anteil der Unternehmen, die die Qualität der Hilfestellungen als nicht gut bewerten, ist von 25 Prozent im Jahr 2021 auf 44 Prozent im Jahr 2024 gestiegen. Gleichzeitig berichten 25 Prozent der Unternehmen 2024, andere Unternehmen hätten ihnen von schlechten Erfahrungen berichtet, der höchste Wert der Zeitreihe.

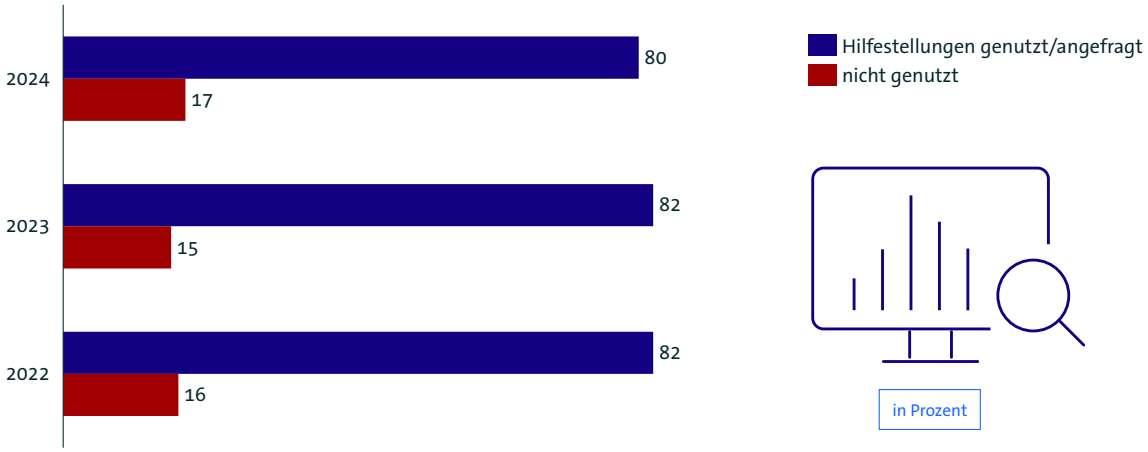
Zwar ist der Eindruck, Aufsichtsbehörden seien nicht an Problemlösungen interessiert, von 34 Prozent im Jahr 2021 auf 24 Prozent im Jahr 2024 zurückgegangen. Dennoch bleibt ein relevanter Teil der Unternehmen skeptisch gegenüber dem konkreten Nutzen der Unterstützung.

Insgesamt zeigen die Ergebnisse ein ambivalentes Bild: Die Aufsichtsbehörden werden häufiger als Unterstützungsinstanz genutzt, ihre Hilfestellungen erfüllen aber aus Sicht vieler Unternehmen nicht die Erwartungen. Nicht mangelnde Bekanntheit oder Angst vor Behörden stehen zunehmend im Vordergrund, sondern Zweifel an Qualität, Praxisnähe und Problemlösungsorientierung.

Für die weitere Umsetzung der DS-GVO und insbesondere für datengetriebene Innovationen kommt es daher darauf an, dass Aufsichtsbehörden nicht nur kontrollieren, sondern stärker als verlässliche, kompetente und praxisnahe Orientierungspartner wahrgenommen werden.

4.1 Nutzung von Hilfestellungen der Aufsichtsbehörden

Haben Sie in den vergangenen Jahren Hilfestellungen der Aufsichtsbehörden für die Umsetzungen der Datenschutzvorgaben genutzt oder angefragt?

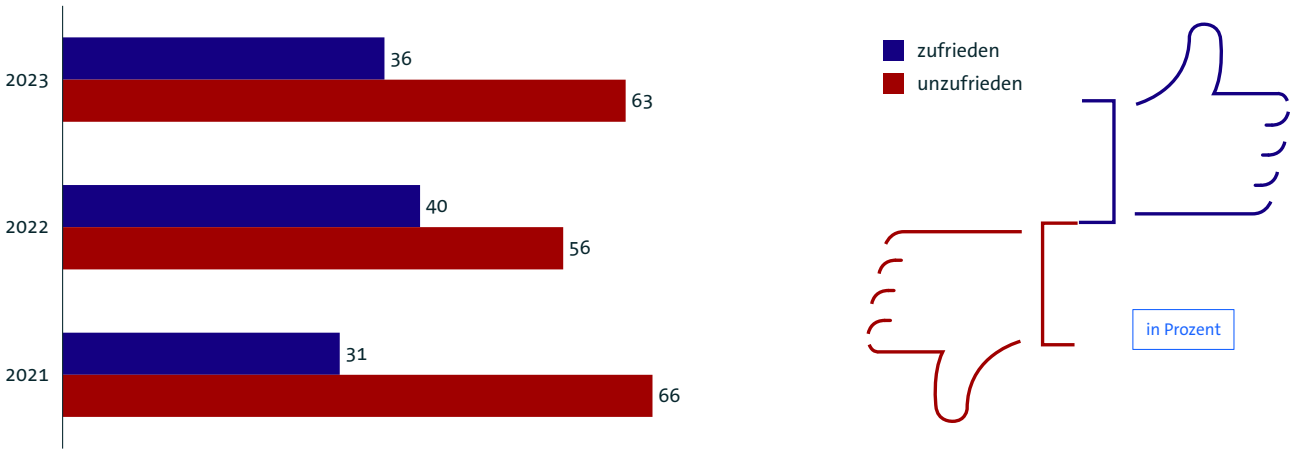


Basis: Alle befragten Unternehmen ab 20 Beschäftigten | Quelle: Bitkom Research

Abbildung 7: Nutzung von Hilfestellungen der Aufsichtsbehörden

4.2 Zufriedenheit mit Hilfestellungen der Aufsichtsbehörden

Wie zufrieden sind Sie mit den Hilfestellungen, die Ihr Unternehmen genutzt hat?

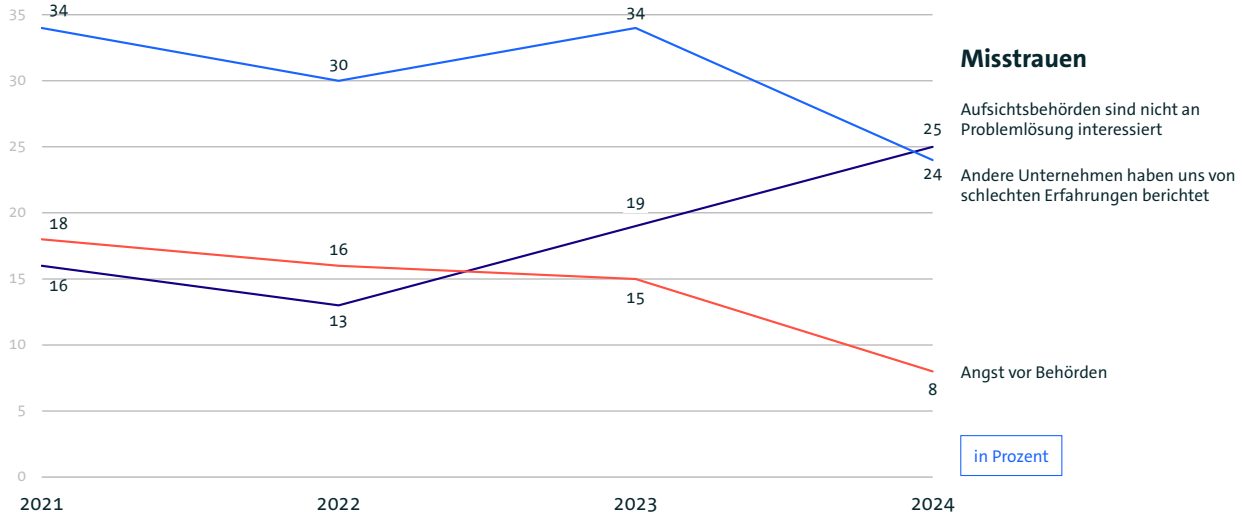


Basis: Befragte Unternehmen ab 20 Beschäftigten, die Hilfestellung in Anspruch genommen haben | Abweichungen von 100 Prozent sind rundungsbedingt | Nicht dargestellt: »Weiß nicht/ keine Angabe« | Quelle: Bitkom Research

Abbildung 8: Zufriedenheit mit Hilfestellungen der Aufsichtsbehörden

4.3 Misstrauen gegenüber Aufsichtsbehörden

Warum haben Sie keine Hilfestellungen der Aufsichtsbehörden genutzt bzw. angefragt?

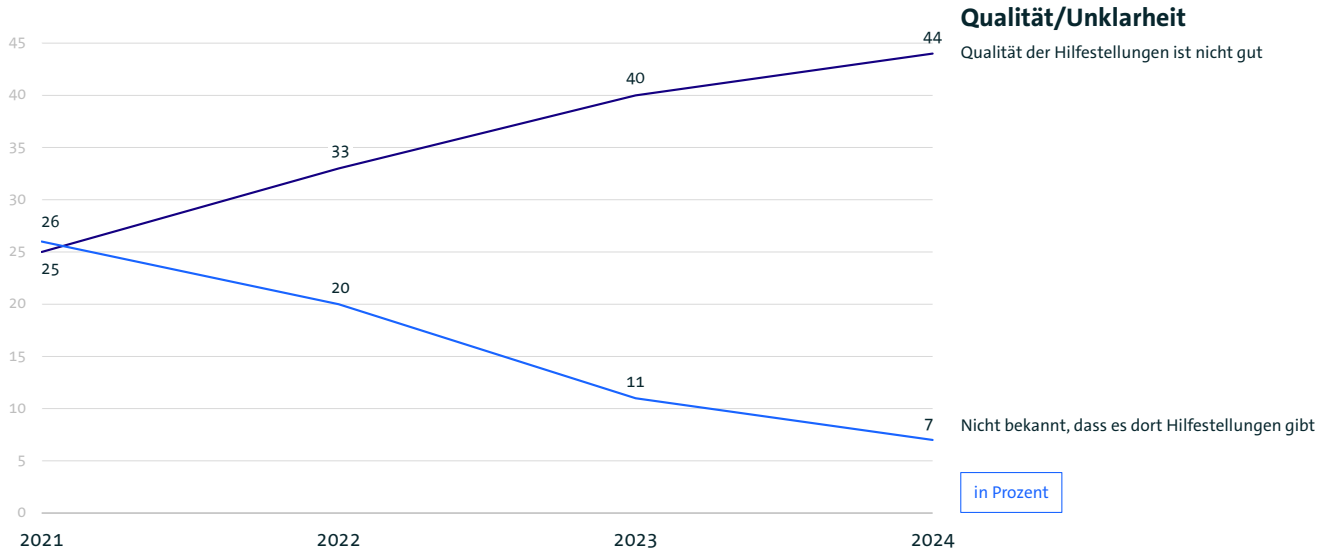


Basis: Befragte Unternehmen ab 20 Beschäftigten, die keine Hilfestellung in Anspruch genommen haben | Mehrfachnennungen | Quelle: Bitkom Research

Abbildung 9: Gründe für die Nicht-Nutzung von Hilfestellungen: Misstrauen

4.4 Aufsichtsbehörden: Qualität und Unklarheit

Warum haben Sie keine Hilfestellungen der Aufsichtsbehörden genutzt bzw. angefragt?

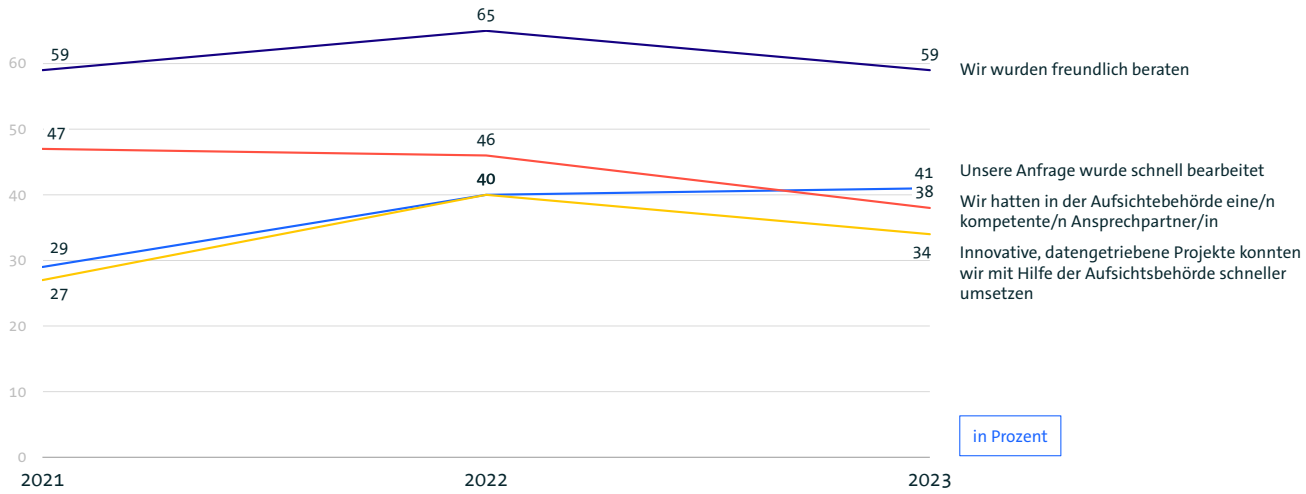


Basis: Befragte Unternehmen ab 20 Beschäftigten, die keine Hilfestellung in Anspruch genommen haben | Mehrfachnennungen | Quelle: Bitkom Research

Abbildung 10: Gründe für die Nicht-Nutzung von Hilfestellungen: Qualität/Unklarheit

4.5 Bewertung der Hilfestellungen der Aufsichtsbehörden

Inwiefern treffen die folgenden Aussagen auf die von Ihrem Unternehmen in Anspruch genommenen Hilfestellungen zu?



Basis: Befragte Unternehmen ab 20 Beschäftigten, die Hilfestellung in Anspruch genommen haben | Angaben für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research

Abbildung 11: Bewertung der Hilfestellungen der Aufsichtsbehörden

5 Internationale Datentransfers

5 Internationale Datentransfers

Internationale Datentransfers sind für viele Unternehmen weiterhin fester Bestandteil ihrer Geschäftsprozesse.

Besonders deutlich zeigt sich dies bei den USA. 2021 übermittelten 52 Prozent der Unternehmen personenbezogene Daten dorthin, 2023 waren es 64 Prozent und 2025 weiterhin 61 Prozent. Die USA bleiben damit mit Abstand das wichtigste Drittland für personenbezogene Datentransfers außerhalb der EU.

Auch Großbritannien gewinnt nach dem Brexit als Drittland an Bedeutung. Der Anteil steigt von 35 Prozent im Jahr 2021 auf 43 Prozent im Jahr 2025. Bei Indien zeigt sich ebenfalls ein klarer Zuwachs, von 13 Prozent in den Jahren 2021 und 2022 auf 24 Prozent im Jahr 2025.

Die Ergebnisse zeigen: Trotz Souveränitätsdebatte und rechtlicher Unsicherheiten nehmen internationale Datenflüsse nicht ab. Unternehmen sind in global vernetzte Wertschöpfungsketten, Cloud-Infrastrukturen, Softwarelösungen und Dienstleistungsbeziehungen eingebunden. Gerade deshalb wächst der Bedarf an verlässlichen, rechtssicheren und zugleich praxistauglichen Regelungen für internationale Datentransfers.

Bei den Rechtsgrundlagen für Datentransfers in die USA bleiben Standardvertragsklauseln das zentrale Instrument. Seit 2016 liegen sie durchgehend auf sehr hohem Niveau und werden auch 2025 von 80 Prozent der Unternehmen genutzt. Zwar ist der Wert gegenüber 2023 gesunken, als 94 Prozent Standardvertragsklauseln nutzten. Dennoch bleiben sie mit deutlichem Abstand die wichtigste Grundlage für US-Transfers. Das passt zur Rolle der Standardvertragsklauseln als vorab genehmigtes Instrument für Transfers in Länder außerhalb des Europäischen Wirtschaftsraums.

Das EU-US Data Privacy Framework hat 2025 zwar eine neue Grundlage für Transfers in die USA geschaffen, erreicht aber bislang nicht die praktische Bedeutung des früheren Privacy Shield. Während das Privacy Shield 2019 von 42 Prozent der Unternehmen genutzt wurde, liegt das Data Privacy Framework 2025 bei 21 Prozent. Das deutet darauf hin, dass viele Unternehmen trotz neuer Angemessenheitsentscheidung weiterhin auf etablierte Instrumente wie Standardvertragsklauseln setzen – möglicherweise auch, weil das Framework nur für teilnehmende bzw. zertifizierte US-Unternehmen gilt. Auch andere Rechtsgrundlagen spielen eine Rolle, bleiben aber deutlich dahinter zurück.

Binding Corporate Rules werden 2025 von 23 Prozent der Unternehmen genutzt und liegen damit unter den Werten früherer Jahre. Einwilligungen werden 2025 von 12 Prozent genannt und bewegen sich damit wieder etwa auf dem Niveau von 2021. Insgesamt zeigt sich: Die Rechtsgrundlagen für US-Transfers bleiben fragmentiert. Unternehmen kombinieren unterschiedliche Instrumente, Standardvertragsklauseln bleiben aber das Rückgrat der Praxis.

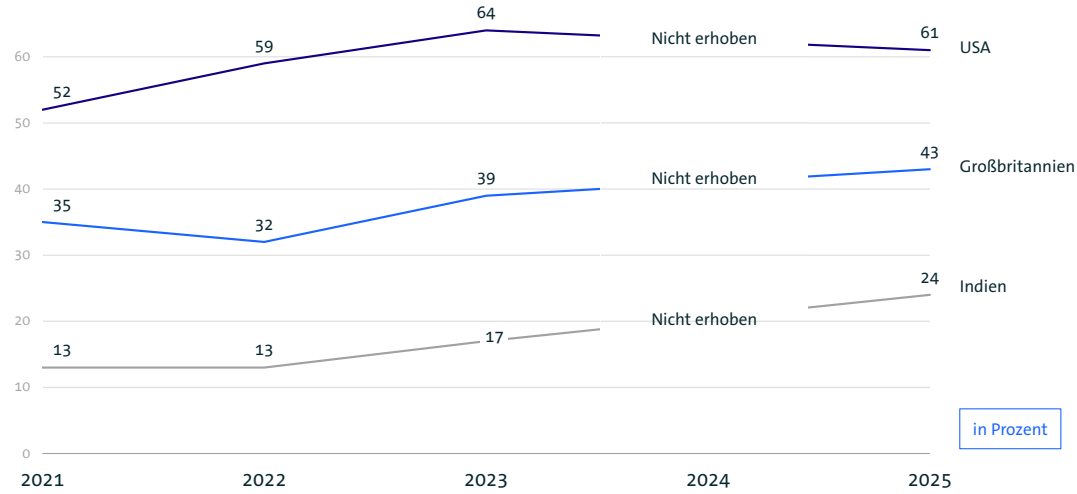
Parallel steigt der politische Handlungsdruck deutlich. Der Anteil der Unternehmen, die sich von der Politik die Durchsetzung politischer Lösungen für internationale Datentransfers wünschen, ist von 32 Prozent im Jahr 2021 auf 71 Prozent im Jahr 2025 gestiegen.

Unternehmen sehen internationale Datentransfers zunehmend nicht nur als Compliance-Frage, sondern als strategische Standort- und Wettbewerbsfrage.

Insgesamt zeigen die Zahlen ein klares Spannungsfeld. Internationale Datenflüsse bleiben für die Wirtschaft unverzichtbar, ihre rechtliche Absicherung aber aufwendig und unsicher.

5.1 Internationale Datentransfers außerhalb der EU

In welche Länder, außerhalb der EU, werden die personenbezogenen Daten Ihres Unternehmens transferiert?

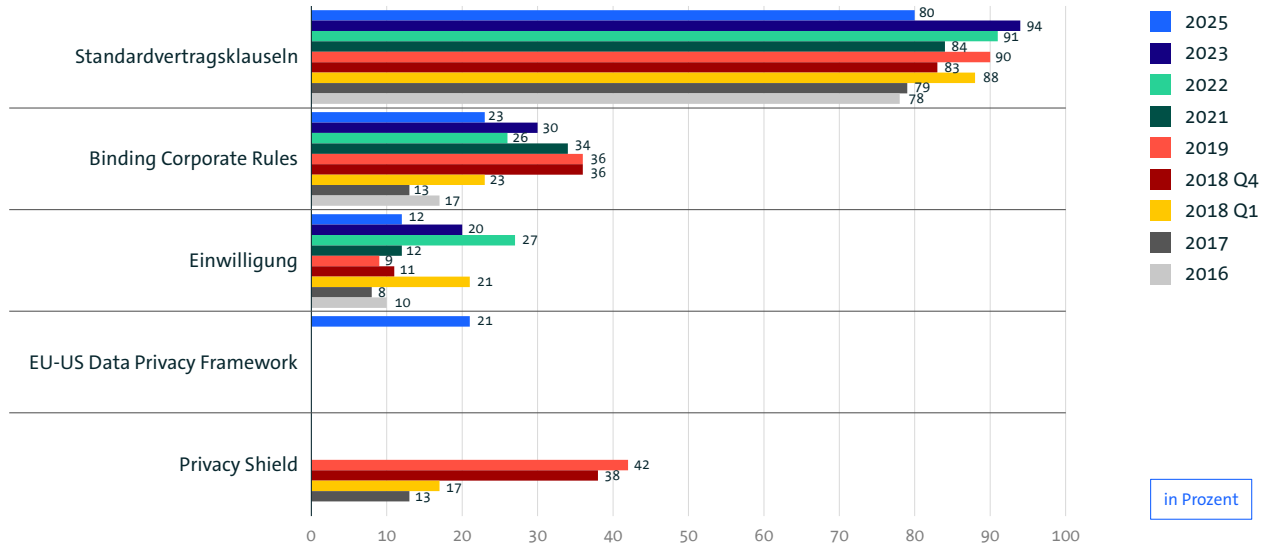


Basis: Befragte Unternehmen ab 20 Beschäftigten, die personenbezogene Daten außerhalb der EU transferieren | Mehrfachnennungen | Quelle: Bitkom Research

Abbildung 12: Internationale Datentransfers außerhalb der EU

5.2 Rechtsgrundlagen für Datentransfers in die USA

Auf welcher Rechtsgrundlage übermittelt Ihr Unternehmen aktuell personenbezogene Daten in die USA?

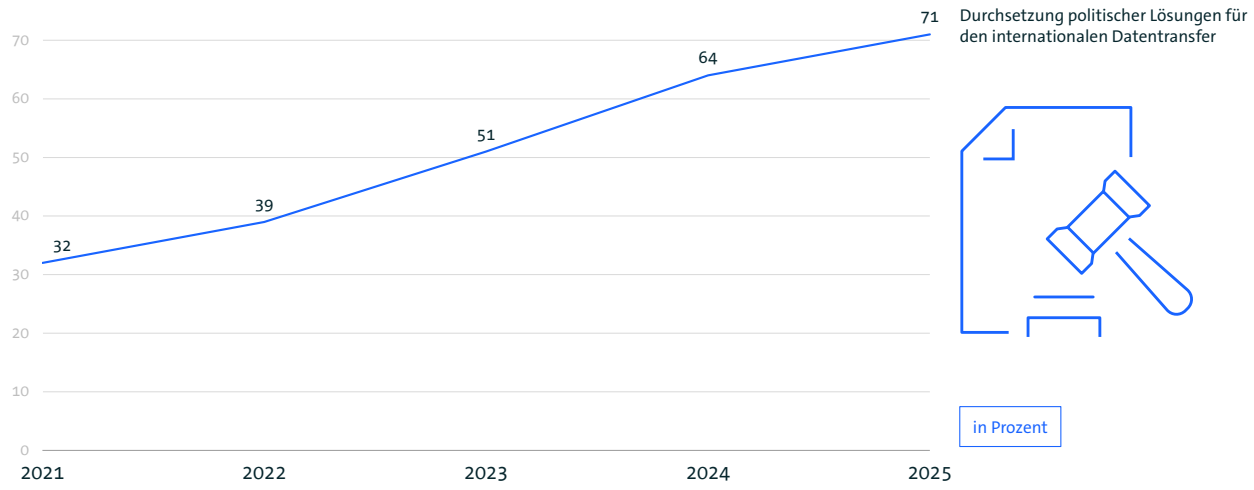


Basis: Befragte Unternehmen ab 20 Beschäftigten, die personenbezogenen Daten in die USA transferieren | Mehrfachnennungen | Quelle: Bitkom Research

Abbildung 13: Rechtsgrundlagen für Datentransfers in die USA

5.3 Internationaler Datentransfer: Erwartungen an die Politik

Welche Maßnahmen wünschen Sie sich von der Politik beim Thema Datenschutz?



Basis: Befragte Unternehmen ab 20 Beschäftigten | Mehrfachnennungen | Quelle: Bitkom Research

Abbildung 14: Erwartungen an die Politik hinsichtlich des internationalen Datentransfers

6 DS-GVO und Künstliche Intelligenz

6 DS-GVO und Künstliche Intelligenz

Europäischer Datenschutz gilt als Vorteil – erschwert aber die KI-Praxis. Beim Verhältnis von Datenschutz und Künstlicher Intelligenz zeigt sich ein ambivalentes Bild.

Einerseits bewerten immer mehr Unternehmen den europäischen Datenschutz im internationalen Vergleich als Vorteil für die Entwicklung von KI in Deutschland und Europa. Der Anteil steigt von 48 Prozent im Jahr 2023 auf 53 Prozent im Jahr 2024 und 59 Prozent im Jahr 2025.

Gleichzeitig geht der Anteil der Unternehmen, die den europäischen Datenschutz als Nachteil sehen, von 46 Prozent im Jahr 2023 auf 36 Prozent im Jahr 2025 zurück.

Auf den ersten Blick deutet dies darauf hin, dass Unternehmen im europäischen Datenschutz zunehmend ein Differenzierungsmerkmal sehen. Datenschutz kann Vertrauen schaffen, Akzeptanz für KI-Anwendungen erhöhen und zu einem Qualitätsversprechen für europäische KI werden. Gerade bei sensiblen Daten, in regulierten Branchen oder im B2B-Kontext kann ein hoher Datenschutzstandard ein Standortvorteil sein.

Gleichzeitig zeigen die weiteren Ergebnisse, dass dieser potenzielle Vorteil in der praktischen Umsetzung bislang nur begrenzt eingelöst wird.

2025 sagen 69 Prozent der Unternehmen, Datenschutz erschwere es, KI-Modelle mit genügend Daten zu trainieren, ein deutlicher Anstieg gegenüber 42 Prozent im Jahr 2023 und 50 Prozent im Jahr 2024.

Auch die Sorge um Standortnachteile bleibt hoch: 63 Prozent sind 2025 der Ansicht, Datenschutz vertreibe Unternehmen, die KI entwickeln, aus der EU. Zudem sagen 57 Prozent, Datenschutz sorge dafür, dass die Anwendung von KI in der EU eingeschränkt werde. Der scheinbare Widerspruch lässt sich daher als Spannungsverhältnis zwischen Anspruch und Umsetzung verstehen.

Viele Unternehmen sehen im europäischen Datenschutz offenbar grundsätzlich das Potenzial für einen internationalen Vorteil.

In der konkreten KI-Entwicklung erleben sie Datenschutzvorgaben jedoch häufig als Hürde – etwa beim Zugang zu Trainingsdaten, bei der rechtssicheren Nutzung großer Datenbestände oder bei der Entwicklung datenintensiver Geschäftsmodelle.

Bemerkenswert ist zugleich, dass der Datenschutz auch bei der Rechtssicherheit besser bewertet wird. Der Anteil der Unternehmen, die sagen, Datenschutz schaffe Rechtssicherheit bei der Entwicklung von KI-Anwendungen, steigt von 44 Prozent im Jahr 2023 auf 58 Prozent im Jahr 2025. Datenschutz wird also nicht nur als Belastung gesehen, sondern auch als Orientierungsrahmen.

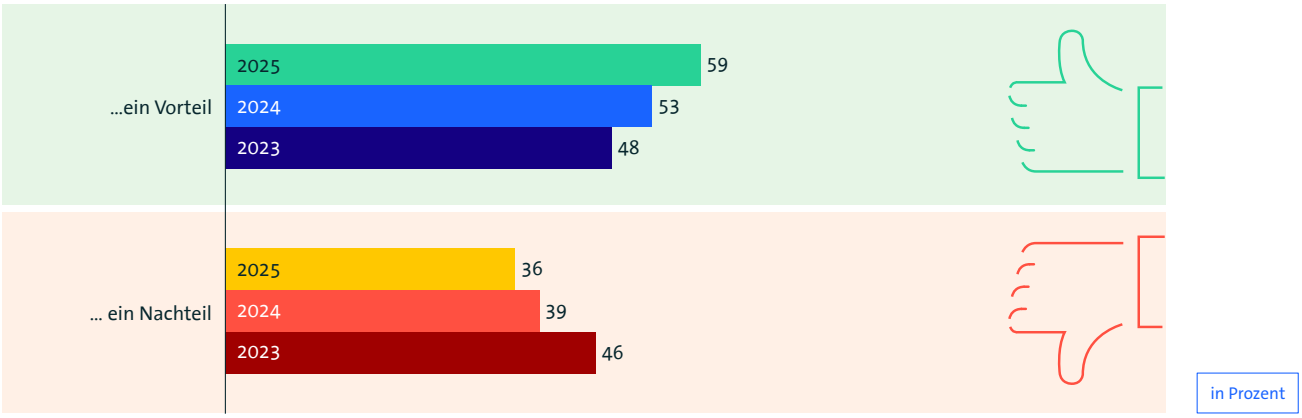
Genau darin liegt die Ambivalenz: Datenschutz kann Vertrauen und Rechtssicherheit schaffen, wird aber zugleich als Bremsfaktor für Datenverfügbarkeit, Skalierung und internationale Wettbewerbsfähigkeit wahrgenommen.

Insgesamt zeigen die Ergebnisse:

Europäischer Datenschutz ist aus Sicht der befragten Unternehmen für KI weder eindeutig Standortvorteil noch eindeutig Standortnachteil. Er wird zunehmend als strategisches Qualitätsversprechen gesehen, bleibt in der praktischen Anwendung aber ein erheblicher Wettbewerbsfaktor.

6.1 KI-Entwicklung und europäischer Datenschutz

Für die Entwicklung von KI in Deutschland und Europa ist der europäische Datenschutz im internationalen Vergleich...

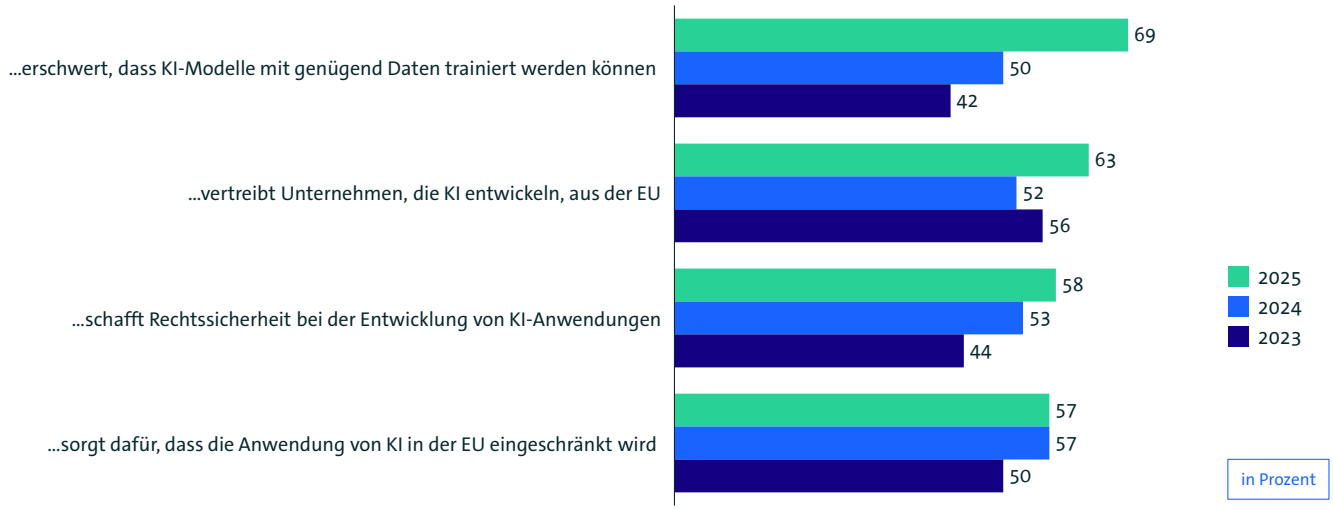


Basis: Befragte Unternehmen ab 20 Beschäftigten | Abweichungen von 100 Prozent sind rundungsbedingt | Nicht dargestellt: »Weiß nicht/ keine Angabe« | Quelle: Bitkom Research

Abbildung 15: KI-Entwicklung und europäischer Datenschutz

6.2 Auswirkungen von Datenschutzvorgaben auf KI-Entwicklung

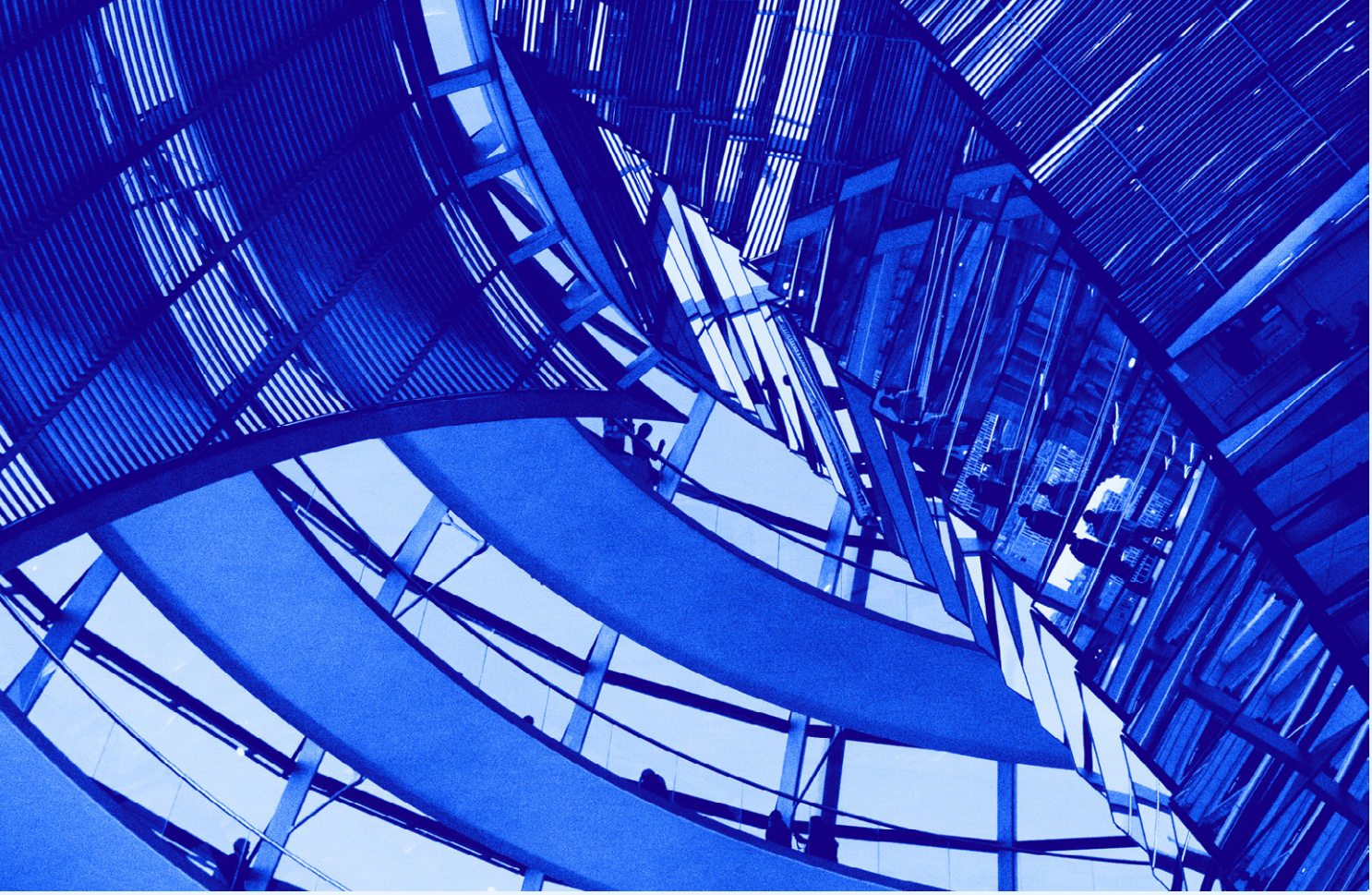
Inwieweit treffen die folgenden Aussagen auf Ihr Unternehmen bzw. Ihrer Meinung nach zu? Datenschutz...



Basis: Alle befragten Unternehmen ab 20 Beschäftigten | Angaben für »Trifft voll und ganz zu« und »Trifft eher zu« | Quelle: Bitkom Research

Abbildung 16: Auswirkungen von Datenschutzvorgaben auf die KI-Entwicklung

7 Reform der DS-GVO



7 Reform der DS-GVO

Datenschutz wirksam machen, Unternehmen entlasten, Innovation ermöglichen

Zehn Jahre nach ihrer Verabschiedung ist die DS-GVO in den Unternehmen angekommen – aber sie ist für viele weiterhin keine abgeschlossene Aufgabe.

Zwar geben 2024 inzwischen 71 Prozent der Unternehmen an, die Vorgaben vollständig oder größtenteils umgesetzt zu haben. Gleichzeitig zeigt der Blick auf Aufwand, Komplexität und Innovationshemmnisse deutlich. Die praktische Anwendung der DS-GVO bleibt für die Wirtschaft eine dauerhafte Herausforderung.

Der Reformbedarf ergibt sich dabei nicht aus einem einzelnen Befund, sondern aus dem Zusammenspiel mehrerer Entwicklungen. Der Datenschutzaufwand ist seit Einführung der DS-GVO weiter gestiegen, Geschäftsprozesse werden zunehmend als komplizierter wahrgenommen, die Auslegung der Vorgaben bleibt für viele Unternehmen unsicher und datengetriebene Innovationen werden in der Praxis häufig erschwert. Die Befragungsergebnisse zeigen damit, an welchen Stellen eine Reform ansetzen sollte. Insbesondere bei mehr Rechtssicherheit, stärkerer Risikoorientierung, weniger formalen Pflichten bei risikoarmen Verarbeitungen, besseren Rahmenbedingungen für datengetriebene Innovationen und einer einheitlicheren Anwendung der Vorgaben in Europa.

Es geht dabei nicht darum, Datenschutz als Grundrecht zu schwächen. Im Gegenteil, Datenschutz bleibt eine zentrale Voraussetzung für Vertrauen in die digitale Wirtschaft. Damit Datenschutz aber auch künftig wirksam bleibt, muss er praxistauglicher, risikobasierter und innovationsfreundlicher werden. Eine Reform sollte daher dort entlasten, wo formale Anforderungen keinen zusätzlichen Schutzgewinn bringen und zugleich dort klare Schutzstandards sichern, wo tatsächlich hohe Risiken für Betroffene entstehen.

Der aktuelle Reformansatz im Rahmen des Digitalomnibus setzt aus Sicht des Bitkom an wichtigen Stellen an. Richtig ist insbesondere, bestehende Anwendungsprobleme gezielt zu beheben, ohne die DS-GVO insgesamt neu zu öffnen.

Die Vorschläge können zu mehr Rechtssicherheit, stärkerer Harmonisierung und einer risikobasierteren Anwendung des Datenschutzrechts beitragen. Entscheidend ist jedoch, dass die Reform im weiteren Verfahren konsequent nachgeschärft wird – damit Entlastungen in der Praxis tatsächlich ankommen und nicht durch unbestimmte Begriffe, Rückausnahmen oder neue Dokumentationspflichten entwertet werden.

Ein zentraler Reformbedarf liegt in der **konsequenten Risikoorientierung**.

Die DS-GVO enthält zwar bereits risikobasierte Elemente, in der praktischen Anwendung gelten viele Pflichten aber weitgehend unabhängig davon, ob eine Verarbeitung tatsächlich ein hohes Risiko für Betroffene darstellt. Das betrifft insbesondere Dokumentations- und Nachweispflichten, Informationspflichten, oder interne Prüfprozesse.

Für Unternehmen bedeutet das:

Auch risikoarme Standardprozesse verursachen erheblichen formalen Aufwand. Eine moderne DS-GVO sollte Umfang und Tiefe solcher Pflichten stärker am tatsächlichen Risiko ausrichten. Das würde Ressourcen auf die Fälle lenken, in denen Datenschutz wirklich entscheidend ist.

Diese Ableitung wird durch die Studienergebnisse gestützt. Wenn 84 Prozent der Unternehmen angeben,dass sich ihr Datenschutzaufwand seit Einführung der DGSVO erhöht hat und 86 Prozent die Umsetzung als nie vollständig abgeschlossen ansehen, spricht das für eine strukturelle Dauerbelastung. Reformen sollten daher nicht nur einzelne Pflichten anpassen, sondern systematisch prüfen, ob Aufwand und Schutzwirkung in einem angemessenen Verhältnis stehen.

Besonders deutlich wird der Reformbedarf bei datengetriebenen Innovationen und Künstlicher Intelligenz. Unternehmen sehen europäischen Datenschutz zwar zunehmend als potenziellen Vorteil im internationalen Wettbewerb. 2025 sagen 59 Prozent, Datenschutz sei für die KI-Entwicklung in Deutschland und Europa ein Vorteil. Gleichzeitig berichten 69 Prozent, dass Datenschutz erschwert, KI-Modelle mit genügend Daten zu trainieren. 63 Prozent meinen sogar, Datenschutz vertreibe Unternehmen, die KI entwickeln, aus der EU.

Dieses Spannungsverhältnis zeigt: Der Anspruch, mit hohen Datenschutzstandards Vertrauen und Wettbewerbsvorteile zu schaffen, wird in der Praxis noch nicht ausreichend eingelöst.

> Datenschutz kann ein Qualitätsmerkmal europäischer KI sein, aber nur, wenn Unternehmen zugleich rechtssichere und praxistaugliche Möglichkeiten erhalten, Daten für Training, Entwicklung und Anwendung von KI zu nutzen.

Deshalb braucht es **rechtssichere Grundlagen für datengetriebene Innovationen**. Die vorgesehene Klarstellung, dass Entwicklung und Betrieb von KI-Systemen grundsätzlich auf berechtigte Interessen gestützt werden können, ist ein wichtiger Schritt. Sie sollte jedoch unionsweit einheitlich gelten, nicht durch nationale Sonderregeln oder zusätzliche Einwilligungspflichten ausgehöhlt werden und technologieoffen ausgestaltet sein. Denn datenintensive Innovationen beschränken sich nicht auf heutige KI-Systeme. Auch in Bereichen wie Medizin, Mobilität, Energie, Cybersicherheit, Verwaltung oder Produktentwicklung entstehen datenbasierte Anwendungen, die einen klaren und verlässlichen Rechtsrahmen benötigen.

Auch beim **Personenbezug von Daten** braucht es mehr Klarheit. In der Praxis besteht häufig Unsicherheit, ob Daten für einen konkreten Empfänger tatsächlich personenbezogen sind oder ob eine Identifizierung nur theoretisch durch andere Akteure möglich wäre. Eine **präzisere, kontextbezogene Definition personenbezogener Daten** kann Unternehmen entlasten und zugleich den Schutz auf reale Risiken konzentrieren.

Ergänzend sollten Anonymisierung, Pseudonymisierung und moderne Privacy-Enhancing-Technologies stärker rechtlich anerkannt werden. Das würde Anreize schaffen, mehr Daten zu anonymisieren oder zu pseudonymisieren und damit Datenschutz technisch wirksamer umzusetzen. Solche Verfahren können Risiken für Betroffene deutlich reduzieren, sind für Unternehmen aber mit erheblichem technischen, organisatorischen und rechtlichem Aufwand verbunden. Damit sich dieser Aufwand lohnt, brauchen Unternehmen verlässliche Kriterien, wann Daten als anonym gelten, wann Pseudonymisierung risikomindernd berücksichtigt wird und welche Verfahren rechtssicher eingesetzt werden können.

Eine stärkere rechtliche Anerkennung solcher Schutzmaßnahmen würde daher nicht Datenschutz abbauen, sondern im Gegenteil wirksameren Datenschutz fördern. Unternehmen hätten einen klaren Anreiz, Datenverarbeitungen datenschutzfreundlicher zu gestalten, wenn dies zugleich zu mehr Rechtssicherheit und angemessenen Erleichterungen bei Folgepflichten führt.

Ein weiterer zentraler Reformbereich ist das **Cookie- und Endgerätezugriffsregime**. Die heutige Praxis führt zu massenhaften Einwilligungsabfragen, ohne dass dadurch automatisch mehr Datenschutz entsteht. Vielmehr erleben Nutzerinnen und Nutzer Consent Fatigue, während Unternehmen erhebliche Compliance-Aufwände tragen. Hier bietet die Zusammenführung von DS-GVO und ePrivacy-Regeln die Chance, das System grundlegend zu vereinfachen.

Risikoarme Verarbeitungen wie Reichweitenmessung, Betrugsprävention, IT-Sicherheit oder kontextbezogene Werbung sollten nicht pauschal einer Einwilligungspflicht unterliegen, sondern – wie andere Datenverarbeitungen auch – auf geeignete Rechtsgrundlagen wie berechtigte Interessen gestützt werden können.

Maschinenlesbare Präferenzsignale lösen dieses Grundproblem nicht, sondern drohen zusätzliche technische und rechtliche Komplexität zu schaffen.

Auch internationale Datentransfers bleiben ein politischer Dauerbrenner. Die USA sind weiterhin das wichtigste Drittland für personenbezogene Datentransfers außerhalb der EU; 2025 übermitteln 61 Prozent der Unternehmen personenbezogene Daten dorthin. Gleichzeitig wünschen sich 71 Prozent der Unternehmen von der Politik die Durchsetzung tragfähiger Lösungen für internationale Datentransfers.

Das zeigt: Globale Datenflüsse sind wirtschaftliche Realität, ihre rechtliche Absicherung bleibt aber aufwendig und unsicher. Eine Reform muss daher politische Lösungen stärken, die Datenschutzstandards sichern und zugleich internationale Zusammenarbeit, Cloud-Nutzung und digitale Geschäftsmodelle ermöglichen.

Schließlich braucht es mehr **Harmonisierung und eine stärkere Praxisorientierung der Aufsicht**.

Unternehmen nutzen Hilfestellungen der Datenschutzaufsichtsbehörden inzwischen sehr häufig. 2024 haben 86 Prozent solche Hilfestellungen genutzt oder angefragt. Gleichzeitig zeigen die Befunde, dass die Zufriedenheit begrenzt bleibt und Zweifel an Qualität und Praxisnähe bestehen.

Eine Reform sollte daher nicht nur materielle Regeln anpassen, sondern auch ihre Anwendung vereinheitlichen. EU-weit einheitliche Kriterien für Datenschutz-Folgenabschätzungen, Meldeformate bei Datenschutzverletzungen und klarere Leitlinien können helfen – sofern sie knapp, verständlich, praxisnah und nicht als zusätzliche Bürokratie ausgestaltet werden.

Aus den Befragungsergebnissen lassen sich damit mehrere **konkrete Reformansätze** ableiten.

- Erstens braucht es eine konsequentere Risikoorientierung, damit risikoarme Verarbeitungen nicht denselben formalen Aufwand auslösen wie Hochrisiko-Verarbeitungen.
- Zweitens braucht es klarere und einheitlichere Vorgaben, um Auslegungsunsicherheit zu reduzieren.
- Drittens müssen datengetriebene Innovationen und KI rechtssicher ermöglicht werden.
- Viertens sollten technische Schutzmaßnahmen wie Anonymisierung und Pseudonymisierung stärker honoriert werden.
- Fünftens braucht es eine harmonisierte, praxisnahe Aufsicht sowie tragfähige politische Lösungen für internationale Datentransfers.

Insgesamt zeigen die Studienergebnisse: Die DS-GVO hat Datenschutz in der Wirtschaft verankert, aber sie hat ihn nicht einfacher gemacht. Viele Unternehmen akzeptieren Datenschutz als wichtigen Rahmen, erleben die konkrete Umsetzung aber als zu komplex, zu unsicher und zu aufwendig.

72 Prozent sagen 2025, dass »wir es mit dem Datenschutz in Deutschland übertreiben«. Diese Kritik richtet sich nicht gegen Datenschutz an sich, sondern gegen eine Anwendungspraxis, die zu häufig formale Anforderungen über tatsächliche Risiken stellt. Eine Reform der DS-GVO sollte daher drei Ziele verfolgen:

- mehr Rechtssicherheit,
- mehr Risikoorientierung und
- mehr Innovationsfähigkeit.

Datenschutz muss dort stark sein, wo durch Datenverarbeitung hohe Risiken für die Privatsphäre und die informationelle Selbstbestimmung von Menschen entstehen. Wo Verarbeitungen risikoarm, gesellschaftlich nützlich oder wirtschaftlich notwendig sind, braucht es praxistaugliche Spielräume.

Nur so kann die DS-GVO auch in den kommenden zehn Jahren Vertrauen schaffen – und zugleich digitale Wertschöpfung, KI-Entwicklung und internationale Wettbewerbsfähigkeit in Europa ermöglichen.

8 Methodik

Befragungen 2016-2025 | Gesamtwirtschaft

Auftraggeber	Bitkom
Methodik	Computergestützte telefonische Befragung/ Computer Assisted Telephone Interview (CATI)
Grundgesamtheit	Unternehmen in Deutschland mit mindestens 20 Beschäftigten
Zielpersonen	Geschäftsführung, Vorstand, Chief Information Officers bzw. Datenschutzbeauftragte, Leitung der Rechtsabteilung, Justiziare oder Compliance-Beauftragte
Stichprobengröße	n=509 (2016); n=507 (2017); n=505 (2018 Q1); n=505 (2018 Q4); n=502 (2019); n=504 (2020); n=502 (2021); n=503 (2022); n=502 (2023); n=605 (2024); n=603 (2025)
Befragungszeitraum	↗Dataverse
Gewichtung	Repräsentative Gewichtung des Datensatzes auf Grundlage des aktuellen Unternehmensregisters des Statistischen Bundesamtes
Statistische Fehlertoleranz	+/- 5 Prozent bzw. +/- 4 Prozent (ab 2024)

Susanne Dehmel
Mitglied der Geschäftsleitung
Recht & Sicherheit
susanne.dehmel@bitkom.org
↗ LinkedIn

Isabelle Stroot
Bereichsleiterin
Datenschutzrecht & -politik
i.stroot@bitkom.org
↗ LinkedIn

Herausgeber
Bitkom e.V.
Albrechtstr. 10 | 10117 Berlin
bitkom.org

Wissenschaftliche Leitung
Bettina Lange

Ansprechpartner
Susanne Dehmel
Isabelle Stroot
Elena Kouremenou

Redaktion
Alissa Geffert

DOI
10.64022/2026-DSGVO

Zehn Jahre nach Beginn der DS-GVO-Vorbereitungen gehört Datenschutz fest zum organisatorischen Alltag von Unternehmen. Gleichzeitig zeigen die Erhebungen von Bitkom Research der Jahre 2016 bis 2025: Der Aufwand bleibt hoch, Rechtsunsicherheiten bestehen fort und datengetriebene Innovationen geraten zunehmend unter Druck. Anlässlich des 10-jährigen Jubiläums der DS-GVO zieht der Bericht eine Zwischenbilanz der DS-GVO aus Sicht der Wirtschaft. Auf Basis von Langzeitdaten analysiert er die Entwicklung des Datenschutzes in Unternehmen – von der Umsetzung regulatorischer Vorgaben bis zu Auswirkungen auf Innovation, internationale Datentransfers und Künstliche Intelligenz.

DOI
10.64022/2026-DSGVO

bitkom