STIFTUNG DATENSCHUTZ

White Paper

WIRTSCHAFTSVORTEIL DATENSCHUTZ

Warum DSGVO-Standards Unternehmen resilient und erfolgreich für die Zukunft aufstellen

Inhaltsverzeichnis

Einleitung

Datenschutz wird fälschlicherweise häufig als Innovationsbremse dargestellt. Unternehmen geben ihm die Schuld am mangelnden Fortschritt oder werfen ihm vor, Entwicklungen zu blockieren. Dabei ist das Gegenteil der Fall. Bei zielgerichteter Interpretation und Anwendung ist Datenschutz ein entscheidender Standort- und Wettbewerbsvorteil, denn er schafft die wichtigste Währung der digitalen Welt: Vertrauen. Geschäftsmodelle, die Datenschutz beherzigen und Grundrechte respektieren, handeln zum einen ethisch und sind zum anderen wirtschaftlich nachhaltiger sowie zukunftsfester.

Die gesetzliche Verpflichtung zu „Datenschutz durch Technikgestaltung“ (das sogenannte Prinzip „Data Privacy by Design and Default“) soll Unternehmen zur Entwicklung smarter und effizienter Lösungen anspornen. Es zwingt zur Konzentration auf das Wesentliche und verhindert den Einsatz von riskanten „Black-Box“-Anwendungen, bei denen niemand genau weiß, wer Zugriff auf die Daten hat oder wie die Algorithmen funktionieren. Damit dieser gute Gestaltungsgrundsatz optimale Wirkung entfalten kann, sollte er auch für Hersteller und Anbieter digitaler Werkzeuge gelten. Die europäische Datenschutzgrundverordnung (DSGVO) gilt mittlerweile in großen Teilen der Welt als Vorbild. Für eine Exportnation wie Deutschland liegt hierin eine riesige Chance. So wie „Made in Germany“ für Ingenieurskunst und hohe Qualitätsstandards steht, kann Datenschutz-Know-how zu einem weltweit anerkannten Qualitätsmerkmal für digitale Produkte und Dienstleistungen werden. Ein treffsicherer Datenschutz schafft das Fundament, das es braucht, um digitale Innovationen erfolgreich zu machen und unsere Wirtschaft im globalen Wettbewerb zu stärken.

Summary

Das vorliegende White Paper zeigt anhand von vier zentralen Fakten, dass der Datenschutz weit über Compliance hinaus ein bedeutender wirtschaftlicher Standortvorteil für Unternehmen sein kann. Mit der fortwährenden Digitalisierung nahezu aller gesellschaftlicher und wirtschaftlicher Bereiche wird deutlich, dass in einer verantwortungsvollen Datenverarbeitung nicht nur ein Schutzmechanismus steckt, sondern ein strategisches Potenzial: Datenschutz stärkt gesellschaftliche Grundwerte und kann gleichzeitig ökonomischen Nutzen erzeugen.

Anhand aktueller Studien und Forschungsergebnisse wird aufgezeigt, dass Datenschutz eine entscheidende Komponente für das Vertrauen in Marken oder Unternehmen ist und somit unmittelbar auf den Unternehmenserfolg wirkt. Darüber hinaus wird deutlich: Eine frühzeitige systematische Implementierung von Datenschutzmaßnahmen verhilft zu präventivem Risikomanagement und einer effektiveren Datenverarbeitung. Das Paper erläutert, wie professionell umgesetzter Datenschutz in Unternehmen immaterielle Vermögenswerte schützen kann und die Cybersicherheit stärkt.

Hintergrund: Warum wurde die DSGVO eingeführt?

Datenschutz entwickelte sich als Reaktion auf weitreichende technologische Veränderungen: Mit dem Aufkommen neuer Computertechniken und staatlicher Datensammlungen ging es zunächst um Regelungen für den Umgang mit personenbezogenen Daten in staatlichen Einrichtungen.[1] Fast zeitgleich mussten Gesetzgeber und Aufsichtsbehörden auf weitere Entwicklungen reagieren – das aufkommende Internet, einsetzender E-Commerce sowie zunehmend vernetzte Datensammlungen stellten neue Anforderungen an den Schutz personenbezogener Daten. Für diese brauchte es ebenfalls konkrete Regeln, die den Umgang mit einem rasant wachsenden digitalen Datenvolumen definieren und begrenzen.

So wurde 1995 die Europäische Datenschutzrichtlinie erlassen, deren Grundsätze dafür sorgen sollten, dass Unternehmen verantwortungsvoll mit personenbezogenen Informationen umgehen und diese nicht länger als notwendig aufbewahren (Speicherbegrenzung) oder unnötig sammeln (Datenminimierung); 2018 wurde die Richtlinie durch die Datenschutzgrundverordnung aktualisiert und vereinheitlicht.

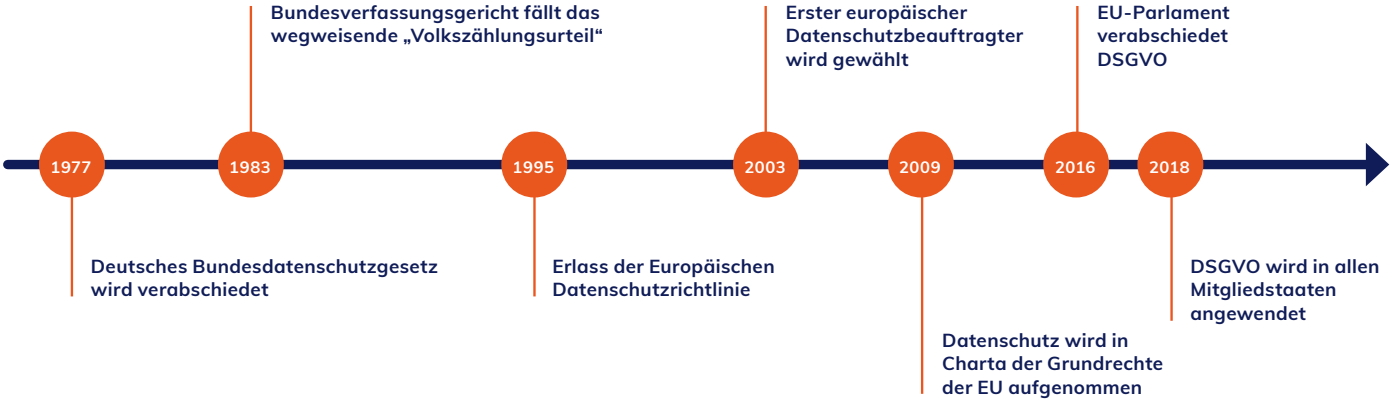
Das primäre Ziel der DSGVO: Die Etablierung eines einheitlichen Datenschutzniveaus für die europäischen Staaten. Diese gemeinschaftlichen Regeln sollen besonders für international tätige Unternehmen gelten. Die DSGVO verhilft nicht nur zu einer steigenden Verantwortung von Unternehmensseite, Compliance sorgt gleichzeitig auch für gleichmäßige Marktchancen. Denn durch die DSGVO wurden nationale Besonderheiten eingeschränkt, die seitdem nur noch in bestimmten Bereichen zulässig sind. Zudem wurde die Kontrolle der Bürger*innen über ihre persönlichen Daten gestärkt, indem Unternehmen transparente und verständliche Informationspflichten auferlegt wurden.

Datenschutz beginnt mit Verantwortung

Ende 2025 machten zwei internationale Fälle Schlagzeilen: der spektakuläre Kunstraub im Pariser Louvre, eines der bekanntesten Museen weltweit, sowie Flugausfälle und Chaos an vier internationalen Flughäfen, weil die Firma, deren Software das Einchecken steuerte, Opfer einer Cyberattacke wurde.

Ob Kunstschätze oder Passagierdaten – in beiden Fällen waren leicht zu erratene Standardpasswörter die Sicherheitslücke im System. In beiden Fällen fehlte das Bewusstsein dafür, wie wichtig klare Zuständigkeiten sowie technische und organisatorische Maßnahmen sind.

Diese Beispiele sind keine Einzelfälle und machen deutlich: Wer Risikoprävention nur als gesetzliche Pflicht betrachtet, übersieht, dass jede Sicherheitslücke eine offene Einladung ist. Datenschutz und IT-Compliance sind wichtige Grundpfeiler. Dabei kommt Datenschutzbeauftragten eine wichtige Rolle zu: Sie beraten die Geschäftsführung und sorgen beispielsweise für ein sicheres Passwort-, Rollen- und Zugangsmanagement. Ihre Kenntnisse wirken sich unmittelbar auf die Sicherheitsarchitektur der Unternehmen aus – ein Gewinn für alle.



Die DSGVO als Umsetzung der Charta der Grundrechte

In der Charta der Grundrechte der Europäischen Union ist ausdrücklich der Schutz personenbezogener Daten festgeschrieben. Daten dürfen nach Art. 8 der EU-Charta nur für festgelegte, legitime Zwecke verwendet werden. Die DSGVO setzt dieses Recht somit auf Nationalstaatsebene um.[2] Dementsprechend werden in der DSGVO die Rechte der betroffenen Personen – wie Löschungspflichten ihrer Daten, das „Recht auf Vergessenwerden“ und das Recht auf Datenportabilität – gestärkt, was insgesamt eine bessere Kontrolle über eigene Daten ermöglicht. Durch die DSGVO erhielt somit das Grundrecht auf Datenschutz mehr Aufmerksamkeit in der Breite, und es wurde die Bedeutung des verantwortungsbewussten Umgangs mit personenbezogenen Daten betont.

Woher kommt der Gedanke, dass Datenschutz Unternehmen vor allem ausbremst?

Auch wenn schon bei der Einführung der DSGVO deutlich wurde, dass sich mithilfe verbesserter Datenorganisation im Rahmen der Regelung durchaus wirtschaftliche Vorteile ergeben können, prägt die historische Genese bis heute die Wahrnehmung von Datenschutz. Immer noch wird er häufig weniger als aktives Gestaltungsmittel für digitale Geschäftsmodelle verstanden, sondern primär als Abwehrrecht, das Einschränkungen und vor allem Pflichten für Unternehmen mit sich bringt. Grund dieses diffusen Ablehnungsgefühls ist in den meisten Fällen eine Unkenntnis des tatsächlichen Regelwerks oder fehlendes Verständnis für dessen Bedeutung. Diesem Empfinden lässt sich schwer konkret begegnen.

Hinzu kommt die finanzielle Ebene: Für Unternehmen, die sich erst im späteren Prozess mit Datenschutz befassen und diesen nicht systematisch von Beginn an in ihrer Unternehmensstrategie mitdenken („Privacy by Design“), sind Schritte zur Anpassung an die aktuellen Regeln oftmals mit Arbeit und Ressourcenaufwand verbunden – und somit zunächst mit plötzlich entstehenden Kosten. Verkannt wird dabei jedoch, dass zum einen vor allem die nachträgliche Compliance höhere Kosten verursachen kann und andererseits die Integration der Datenschutzrichtlinien auf lange Sicht gesehen Kosten einzusparen hilft.

Wie stark Datenschutz tatsächlich als Standortvorteil dienen kann und warum es sich – nicht nur – im unternehmerischen Sinne lohnt, ihn aktiv zu fördern, wird im weiteren Verlauf des White Papers diskutiert.

Strategischer Erfolgsfaktor Datenschutz

Deutschland profitiert von einem hohen Datenschutzstandard. Die Grundsätze der DSGVO ermöglichen Unternehmen eine kosteneffektive Planung und Ausrichtung ihrer Systeme sowie Prozesse und unterstützen so ein solides Risikomanagement. Wird Datenschutz nicht als Hürde, sondern als wichtiger Baustein der Unternehmensstrategie begriffen, können daraus reelle Wettbewerbsvorteile entstehen.

Die folgenden vier Themenbereiche verdeutlichen, welche tatsächliche Wirkung Datenschutz entwickeln kann – von der Vertrauensbildung mit Kund*innen bis hin zur Stärkung der unternehmerischen Governance.

1. Vertrauensstärkung und Reputationsaufbau

Datenschutz schafft Glaubwürdigkeit und schützt Unternehmen vor Reputationsverlusten bei Verbraucher*innen, Kund*innen und Investor*innen.

2. Gestärkte Marktposition

DSGVO-konforme Geschäftsmodelle sichern eine stabile Marktposition, weil das europäische Regelwerk den globalen Standard im Datenschutz setzt.

3. Risikominderung und finanzieller Vorteil

Professionell umgesetzte Datenschutzmaßnahmen erhöhen die unternehmerische Resilienz und mindern das Risiko, von wirtschaftlichen Einbußen, Betriebsausfällen oder von Sanktionen betroffen zu sein.

4. Datenschutz als Bestandteil der Corporate Governance

Eine gute Datenschutz-Governance schützt automatisch auch interne Geschäftsgeheimnisse, Know-how und den USP.

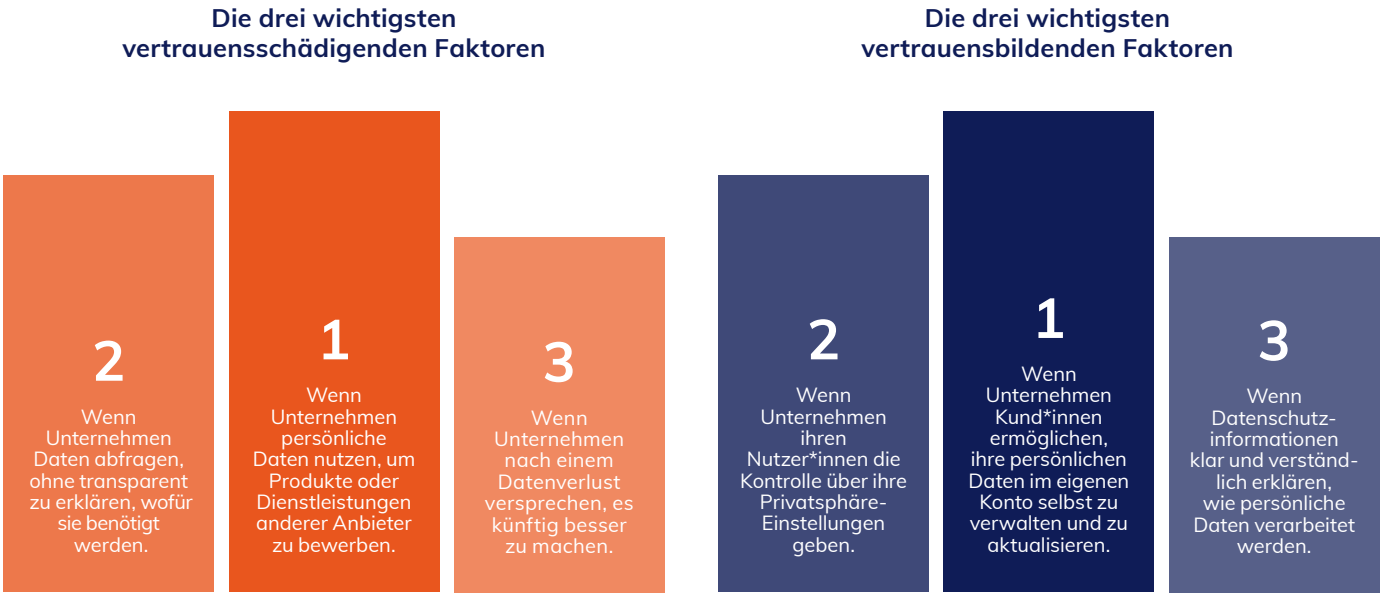
1. Vertrauensstärkung und Reputationsaufbau

Datenschutz ist in einer datengetriebenen Wirtschaft ein strategischer Erfolgsfaktor, der weit über die bloße Erfüllung gesetzlicher Vorgaben hinausgeht. Professionell implementierte Datenschutzmaßnahmen in einem Unternehmen reduzieren zum einen unmittelbare Risiken und stärken zum anderen nachweislich das Vertrauen von Kund*innen, Partner*innen und Investor*innen. Das wiederum wirkt sich positiv auf Kaufentscheidungen und in diesem Zuge gewinnbringend für das Unternehmen aus.

Obwohl die Datenschutzgrundverordnung (DSGVO) häufig nur als Herausforderung wahrgenommen wird, bietet sie auch Chancen zur Professionalisierung datenbasierter Geschäftsmodelle. Sie setzt international geschätzte Standards und ermöglicht Unternehmen, sich durch ein hohes Schutzniveau zu differenzieren. Vertrauen entsteht nicht allein durch Rechtskonformität: Unternehmen müssen Verantwortung im digitalen Raum sichtbar wahrnehmen. Hier rückt der Ansatz der „Corporate Digital Responsibility (CDR)" in den Vordergrund, der über gesetzliche Mindeststandards hinausgeht und Datenschutz als Bestandteil verantwortungsvoller Unternehmensführung begreift.[3]

Die ökonomische Relevanz zeigt die Intuit-Mailchimp-Studie 2025: Der Umgang mit personenbezogenen Daten ist ein zentraler Treiber für Markenvertrauen. Franz Riedl, bei Intuit Mailchimp zuständig für den deutschsprachigen Raum[4], betont, dass ein Unternehmen bei deutschen Verbraucher*innen nur Vertrauen aufbauen kann, wenn es sich ernsthaft und transparent mit Datenschutzanforderungen auseinandersetzt.[5] So erwarten 77 Prozent der Befragten 2025 von Unternehmen einen verantwortungsbewussten Umgang mit ihren Daten – gegenüber 70 Prozent im Vorjahr.[6] Eine im Dezember 2025 vorgestellte Onlinestudie des Verbraucherzentrale Bundesverbands e.V. liefert ähnliche Ergebnisse. Demnach haben 63 Prozent der befragten Verbraucher*innen deutlich mehr oder zumindest etwas mehr Vertrauen in den Umgang mit persönlichen Daten bei Unternehmen, wenn diese der DSGVO unterliegen. Außerdem finden 87 Prozent der Befragten es sehr oder eher wichtig, dass sie Unternehmen im Umgang mit ihren persönlichen Daten vertrauen können, bevor sie deren Angebote nutzen.[7] Diese Entwicklungen zeigen, dass Datenschutz messbar auf Konsum- und Investitionsentscheidungen wirkt.

Unternehmensverhalten, das Vertrauen stärkt oder schwächt



Basis: Umfrage Konsument*innen in 19 Ländern (n=5.000) | Quelle: IAAP Privacy and Consumer Trust in Germany 2023

Diese Einschätzung deckt sich auch mit Ergebnissen der *IAAP (International Association of Privacy Professionals)*: Weltweit äußern 68 Prozent der Verbraucher*innen substanzielle Sorgen hinsichtlich ihrer digitalen Identität.[8] Solche Bedenken beeinflussen direkt das Verhalten: Nutzer*innen deinstallieren Apps, verweigern Dateneingaben oder vermeiden Käufe, wenn sie die Datennutzung nicht einschätzen können.[9] Laut den Erkenntnissen einer Umfrage der französische Datenschutzaufsichtsbehörde CNIL ist nicht nur das Bewusstsein für Datenschutz und informationelle Selbstbestimmung bei Kund*innen gestiegen, sondern auch die Bereitschaft für digitale Dienste wie Apps zu bezahlen, um personenbezogene Daten besser geschützt zu wissen. Dabei benannten 51 Prozent der Befragten Datenschutz als eines der drei wichtigsten Kriterien bei der Auswahl eines digitalen Dienstes.[10]

Ein weiterer relevanter Faktor ist die Wechselwirkung zwischen Datenschutz, Cybersicherheit und Markentreue. Eine Mehrheit der Verbraucher*innen weltweit gibt an, bereits von Datenverstößen betroffen gewesen zu sein. Mehr als 80 Prozent der betroffenen Verbraucher*innen gaben an, dass sie wahrscheinlich künftig keine Geschäfte mehr mit einem Unternehmen tätigen würden, nachdem es Opfer eines Cyberangriffs wurde.[11] Für Unternehmen bedeutet dies unmittelbare wirtschaftliche Konsequenzen: Umsatzrückgänge, Verluste von Kund*innen, beeinträchtigte Wachstumsperspektiven. Gleichzeitig erkennen immer mehr Unternehmen, insbesondere in technologieaffinen Branchen, den Mehrwert robuster Datenschutz- sowie Sicherheitskonzepte für ihre wirtschaftliche Existenz und kommunizieren aktiv die Vorteile des Datenschutzes.[12]

Eine strategische Perspektive, in der Datenschutz und Informationssicherheit gleichermaßen eine Rolle spielen, geben die Expert*innen der CNIL: Sie empfehlen Unternehmen, Datenschutz nicht als operative Pflicht, sondern als „strategische Architekturaufgabe“ zu begreifen.[13] Das bedeutet, dass Unternehmen eine genau zu ihren spezifischen Geschäftsprozessen passende IT-Infrastruktur aufbauen sollten, die zudem mit einem ganzheitlichen Sicherheitskonzept verbunden ist. Dieses prüft regelmäßig die Angemessenheit und Wirksamkeit des Datenschutzmanagements, umfasst kontinuierliche Risikoanalysen und das Monitoring von Bedrohungslagen – zentrale Voraussetzungen für Resilienz und Zukunftsfähigkeit.

In der betriebswirtschaftlichen Konsequenz ergibt sich daraus ein klares Bild: Datenschutz und Informationssicherheit sind keine statischen Zustände, sondern ein Prozess fortlaufender Organisationsaufgaben, der Ressourcen, Expertise und Managementaufmerksamkeit erfordert. Unternehmen, die Datenschutz als Bestandteil ihrer Wertschöpfungsstrategie verstehen, stärken ihre eigene Marktposition und die Kundenbindung. Die Intuit-Studie 2025 empfiehlt Unternehmen explizit sicherzustellen, dass interne Prozesse sowie genutzte Tools und Plattformen den Datenschutzanforderungen entsprechen.[14] Erst so wird eine transparente und glaubwürdige Kommunikation möglich – ein entscheidender Faktor für nachhaltiges Vertrauen.

Kirsten Bock

Wissenschaftliche Leiterin der Stiftung Datenschutz

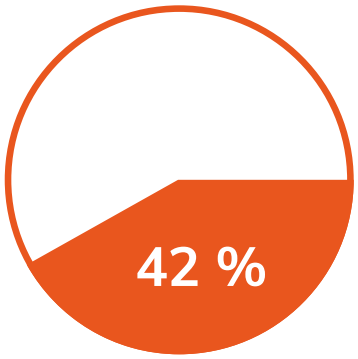
„Ein Investment in Kund*innenvertrauen als Alleinstellungsmerkmal für Unternehmen aus Deutschland und der EU kann sich langfristig lohnen. Da das europäische Datenschutzrecht als Vorbild in vielen Teilen der Welt wahrgenommen wird, sollten Unternehmen diesen Ruf nicht verspielen, sondern für sich zum Vorteil nutzen. Unternehmen haben dadurch nicht nur einen individuellen Wirtschaftsvorteil, sondern tragen gleichzeitig zur Attraktivität des Wirtschaftsstandorts Deutschland bei.“

2. Gestärkte Marktposition

Datenschutz kann zum zentralen Wettbewerbsvorteil werden. Die Kombination aus international anerkannter Regelkonformität, gestärktem Markenvertrauen für Verbraucher*innen, besserer Kapitalmarktbewertung und einer möglichen Neuausrichtung der Innovationskraft macht eine solide Datenschutzpraxis zu einem entscheidenden Erfolgsfaktor. Darüber hinaus sichert Datenschutz unsere demokratischen Prozesse und fördert den gesellschaftlichen Zusammenhalt, was sich wiederum positiv auf unser Vertrauen in digitale Wirtschaft und Verwaltung auswirkt. So trägt guter Datenschutz dazu bei, Deutschland weiterhin als attraktiven und zukunftssicheren Standort zu positionieren.

Die DSGVO der Europäischen Union verlangt von Unternehmen weltweit, die Daten von Verbraucher*innen nur auf Basis einer Rechtsgrundlage zu verwenden und dazu die betroffenen Personen auch umfassend zu informieren. Seit ihrer Einführung im Jahr 2018 hat sich dieses Gesetz von einer zunächst in Deutschland sehr kritisch betrachteten Regelung zu einem globalen Standardinstrument für den Datenschutz entwickelt. Und Unternehmen, die die Datenschutzgrundsätze beachten und implementieren, sichern sich dadurch eine stabile und nachhaltige Marktposition. Mittlerweile dient das europäische Datenschutzregelwerk als Referenz für zahlreiche nationale Datenschutzgesetze. So orientieren sich unter anderem in Brasilien, China, Indien und sogar in Teilen der USA Gesetzgeber an der DSGVO – ein Beleg dafür, dass das grundrechtebasierte europäische Datenschutzmodell zum globalen Standard avanciert ist. Diese internationale Adaption der Regeln bietet wiederum europäischen Unternehmen einen klaren Wettbewerbsvorteil: Wer die Anforderungen der DSGVO bereits erfüllt, ist bestens gerüstet für die Markterschließung in Drittländern, in denen ähnliche Datenschutzstandards gelten. So entsteht kein Mehraufwand, sondern Effizienz und Vertrauen durch normierte Prozesse und bewährte Strukturen.

Darüber hinaus ist Datenschutz nicht nur eine Pflicht, sondern gleichzeitig ein strategischer Wettbewerbsvorteil im Bereich Governance. Unternehmen, die dokumentierte Privacy- und Security-Standards nachweisen können, gelten bei Investor*innen, ESG-Ratingagenturen oder im Rahmen von M&A-Due-Diligence-Prüfungen als deutlich risikoärmer und wertstabiler. Transparente Datenschutzmechanismen stärken das Vertrauen von Kapitalgebern und erhöhen die Bewertung solcher Unternehmen. Gleichzeitig ist auch eine signifikant höhere Auftragsquote bei öffentlichen Ausschreibungen nachgewiesen, wenn Unternehmen eine*n Datenschutzbeauftragte*n beschäftigen[15] – ein konkreter, messbarer ökonomischer Benefit.



der Datenschutzbeauftragten gaben an, dass Unternehmen nach der Einführung einer Strategie zur Förderung der Compliance die Chancen, Ausschreibungen zu gewinnen, um die Hälfte steigern können.

Quelle: „Quels bénéfices économiques du DPO en entreprise ?“ CNIL, 2025

Datenschutz stärkt Demokratie und Gesellschaft

Zudem birgt ein fairer Umgang mit personenbezogenen Daten ein häufig unterschätztes Potenzial: Neben Kund*innenvertrauen sichert und fördert er auch unsere gesellschaftlich-demokratischen Werte. Denn Datenschutz beinhaltet deutlich mehr als nur die Einhaltung technischer Regelungen. Er fördert grundlegende gesellschaftliche Güter wie Vertraulichkeit, Integrität, Fairness und Respekt. Sie stellen die Grundlage unseres gesellschaftlichen Zusammenlebens und stärken das Vertrauen in digitale Wirtschaft und Verwaltung. Kirsten Bock, wissenschaftliche Leiterin der Stiftung Datenschutz, fordert deshalb ein Grundrecht auf digitale Unversehrtheit, um Menschen vor unerwünschten Auswirkungen der Datenverarbeitung zu schützen. Ein solches Grundrecht könnte das in Deutschland bereits bestehende Grundrecht auf Unverletzlichkeit digitaler Systeme[16] maßgeblich ergänzen: Während das bestehende unsere digitalen Systeme vor Überwachung oder heimlichen Zugriffen schützt, würde ein weiter gefasstes Recht auf digitale Integrität den Schutz personenbezogener Daten auf eine fundamentale Ebene heben.

Damit dieses Recht wirksam wird, braucht es systemisch verankerte Garantien: Technologien und Dienste müssen Datenschutz von Anfang an berücksichtigen – das Prinzip „Data Protection by Design and by Default“.[17] Diese Verankerung hilft Unternehmen, Datenschutz nicht als Bremse, sondern als Innovationsmotor wahrzunehmen, um smarte und nachhaltige Lösungen zu entwickeln.

Frederick Richter

Vorstand der Stiftung Datenschutz

„Um die globale Wettbewerbsposition der europäischen Wirtschaft zu stärken, sollte das EU-Datenschutzrecht modifiziert werden. Der 2025 von der Europäischen Kommission angestoßene Reformprozess kann dafür klug genutzt werden. Allerdings gilt es, einen wirksamen Grundrechtsschutz als oberstes Ziel im Auge zu behalten. Es sollte möglich sein, die wirtschaftsseitig geforderte Bürokratieentlastung zu schaffen, ohne die Rechte der Betroffenen einzuschränken. So muss beispielsweise geprüft werden, welche der bislang umfangreichen Dokumentationspflichten für KMU ohne datenintensives risikoreiches Geschäftsmodell wirklich nötig sind. Gleichzeitig darf der Schutzstandard für die Menschen nicht sinken."

Die Stiftung Datenschutz zu den geplanten Reformen beim europäischen Digitalrecht

Damit Datenschutz sein Potenzial als Standortfaktor voll entfalten kann, braucht es eine gute Umsetzung in der Praxis. Es braucht aber auch eine bessere Orientierung für diese Unternehmenspraxis. Die beiden derzeit im Raum stehenden Reformvorhaben auf europäischer Ebene und in Deutschland könnten genau auf diese notwendige Orientierung und Klarheit unterstützend hinwirken.

So ist von der Europäischen Kommission ein Maßnahmenpaket zum bestehenden Datenrecht geplant, welches deutliche Vereinfachungen vorsieht und damit den Verwaltungsaufwand gerade für kleinere Unternehmen reduzieren will. Wird das europäische Datenschutzrecht durch diese Reform treffsicherer, hilft es, die europäische Wirtschaft global zu stärken.

Die Stiftung Datenschutz hofft dabei auf eine ausgewogene Initiative, die nur solche Anpassungen an der DSGVO vornimmt, die den Grundrechtsschutz nicht schwächen. Denn dieser hat gerade für Minderheiten eine hohe Bedeutung. Zwar braucht es beispielsweise mehr Klarheit über Rechtsgrundlagen für das KI-Training und mehr Praktikabilität bei Cookies und Einwilligungsverwaltung. Die Änderungen dürfen aber nicht zu Lasten eines sinkenden Schutzstandards für die Menschen hinsichtlich ihrer (sensiblen) Daten gehen.

Der Gesetzgeber in Deutschland muss zudem rasch die Reform der Datenschutzaufsicht voranbringen. Eine danach einheitlichere Beratung durch die Datenschutzbehörden von Bund und Ländern könnte manche Unsicherheit bei der Gesetzesauslegung in Unternehmen vermeiden. Gelingt die Vereinheitlichung der Aufsichten, gewinnen alle Seiten: Die Unternehmen, die klarere Orientierung zur Rechtsumsetzung erlangen, und auch die Aufsichtsbehörden, die ihre knappen Ressourcen besser konzentrieren und arbeitsteiliger einsetzen können.

Zum aktuellen Stand der Reformen im europäischen Digitalrecht und Datenschutz können Sie sich in der regelmäßigen DatenschutzWoche der Stiftung informieren.

3. Risikominderung und finanzieller Vorteil

Professionell umgesetzte Datenschutzmaßnahmen erhöhen die unternehmerische Resilienz und mindern das Risiko kostspieliger Sicherheitsvorfälle. Entscheidend ist dabei weniger die Vermeidung formaler DSGVO-Sanktionen als die Fähigkeit eines Unternehmens, seine Datenbestände zu kennen und zu kontrollieren – eine Grundlage, um Cyberangriffe frühzeitig zu identifizieren und Angriffsflächen zu reduzieren. Ein Unternehmen, das seine Datenflüsse kennt, entwickelt strukturelle Robustheit und erlangt damit einen klaren Vorteil.

Schäden durch Sicherheitsvorfälle

Ein Großteil der Schadenskosten entsteht durch Cyberattacken

Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=868) | Quelle: Bitkom Research 2025

Zwar müssen Unternehmen zur Erfüllung der DSGVO-Grundsätze von Rechtmäßigkeit über Speicherbegrenzung bis hin zur Rechenschaftspflicht Zeit und Ressourcen investieren. Doch diese Investitionen führen zu deutlichen Effizienzgewinnen: Eine strukturierte Dateninventarisierung und regelmäßige Überprüfung von Datenbeständen sorgen für geringere Speicherlast und damit für niedrigere Infrastruktur- und Energiekosten. Darauf weist bereits die Cisco-Studie von 2019 hin, die Datenmanagement als kontinuierlichen Prozess beschreibt, der im besten Fall sogar Energieeinsparungen auf Servern schafft.[18]

Eine zentrale Rolle in diesem Prozess spielen betriebliche Datenschutzbeauftragte (DSB). Ihre gesetzlich verankerte Aufgabe, bei der Dokumentation von Datenverarbeitungen und bei der Festlegung von Verantwortlichkeiten zu beraten und interne Abläufe zu koordinieren, sorgt für eine präzise Kenntnis der Informationsressourcen im Unternehmen. Untersuchungen zeigen, dass Organisationen mit DSB weniger redundante Daten, weniger Datensilos und eine insgesamt effizientere Nutzung ihrer Informationsbestände aufweisen.[19] Diese strukturierte Datenlandschaft reduziert nicht nur Verwaltungsaufwand, sondern erleichtert auch die schnelle Identifikation von Schwachstellen und damit eine zügigere Reaktion im Ernstfall.

Wie wichtig das ist, zeigen aktuelle Zahlen: Der IBM Cost of a Data Breach Report weist durchschnittliche Kosten von rund 4,88 Mio. USD pro Sicherheitsvorfall aus. Kostensteigernde Faktoren sind vor allem verzögerte Erkennung, mangelnde Verschlüsselung oder unkontrollierte KI-Nutzung.[20] Das belegt deutliche ökonomische Folgen von Vorfällen, die Datenschutzmaßnahmen verhindern helfen können. Ergänzend dokumentiert die European Union Agency for Cybersecurity, dass Organisationen mit strukturiertem Datenmanagement – oftmals ein direktes Ergebnis professioneller Datenschutzpraxis – Sicherheitsvorfälle im Schnitt 20 bis 30 Prozent schneller eindämmen.[21] Kürzere Reaktionszeiten verringern Ausfälle, begrenzen Wiederherstellungskosten und verhindern größeren Datenabfluss.

Neben Datenschutzvorfällen sind vor allem Cyberangriffe auf Firmen ein aktuelles und zunehmendes Problem. Laut der Bitkom-Studie Wirtschaftsschutz 2025 rechnet mehr als ein Drittel der befragten Unternehmen mit einer deutlichen Zunahme von Angriffen in den kommenden Jahren. Das hat große finanzielle Auswirkungen: Über 202 Milliarden Euro Schadenskosten entstanden allein 2025 durch Cyberangriffe.[22] Rechnet man analoge Angriffstypen hinzu, steigt der Betrag auf über 289 Milliarden Euro.[23] Darin enthalten sind nicht nur die direkten Kosten, etwa für Betriebsausfälle, Ersatzmaßnahmen, Erpressungen oder Rechtsstreitigkeiten. Es werden auch Umsatzeinbußen durch den Verlust von Wettbewerbsvorteilen oder Plagiaten hinzugerechnet. Unternehmen empfinden dies zurecht als existenzbedrohend. Vor diesem Hintergrund wird Datenschutz zu einem zentralen Baustein der Cybersicherheitsstrategie. Denn sowohl personenbezogene Daten als auch Unternehmensdaten müssen strukturiert, sicher und nachvollziehbar verarbeitet werden. Der Cybersecurity Readiness Index 2025 zeigt, dass Unternehmen mit etablierten Datenschutzprozessen widerstandsfähiger gegenüber Cyberangriffen sind.[24]

Insgesamt ist ein differenzierter Blick notwendig: Kurzfristig kann erhöhter Datenschutz für datenintensive Unternehmen zusätzliche Kosten bedeuten. Langfristig jedoch schafft er Märkte mit höherem Vertrauen, klareren Regeln und einer robusteren digitalen Infrastruktur. Effektiver Datenschutz ist damit sowohl Compliance als auch eine Risikomanagementmaßnahme mit wertschöpfendem Potenzial – und somit unmittelbar ein wirtschaftlicher Vorteil.[25]

Kirsten Bock

Wissenschaftliche Leiterin der Stiftung Datenschutz

„Die Integration von Datenschutzbestimmungen hat bei vielen Unternehmen zu Unrecht einen schlechten Ruf. Oftmals werden zum Beispiel Einwilligungen verlangt, die gar nicht erforderlich sind. Das schafft Aufwand, der bei einem guten Datenschutzmanagement vermeidbar ist. Die Komplexität des Datenschutzrechts lässt sich reduzieren und dadurch das Risikomanagement besser durchführen. Nicht durch Wegfall von Regelungen, sondern durch eine systematische Anwendung der Datenschutzgrundsätze. Das ist oft leichter als gedacht: Das Standard-Datenschutzmodell liefert einen systematischen Ansatz, der sich leicht auf die individuellen Bedarfe von Unternehmen skalieren lässt."

Das Standard-Datenschutzmodell (SDM) bietet Unternehmen eine praxisorientierte und rechtssichere Methode, mit der sich Datenschutzvorgaben systematisch in konkrete technische und organisatorische Maßnahmen übersetzen lassen. Durch die Vorgehensweise (Modellierung der Verarbeitung, Identifikation von Risiken, Auswahl und Prüfung von Maßnahmen) erhalten Unternehmen einen klaren Ablauf – von der Anforderung bis zur Wirksamkeitskontrolle. Datenschutz wird so nicht nur formal dokumentiert, sondern in Abläufe und Systeme integriert und überprüft.

Das SDM ist daher eine empfehlenswerte Methode zur Planung, Einführung und Überprüfung von Datenschutzmaßnahmen, die auch die Kommunikation zwischen Unternehmen, Datenschutzbeauftragten und Aufsichtsbehörden erleichtern kann.

Weiterführende Links:

Zur Methode des SDM

Guide zur praktischen Einführung ins SDM

Tieferer Einblick für Jurist*innen

4. Datenschutz als Bestandteil der Daten-Governance

Eine moderne Daten-Governance – also die systematische Organisation, Speicherung, Steuerung und Kontrolle von Daten innerhalb eines Unternehmens – betrachtet Daten als strategische Ressource und verbindet technische, organisatorische und rechtliche Anforderungen zu einem konsistenten Steuerungsrahmen. Datenschutz nimmt darin eine Schlüsselrolle ein: Er strukturiert nicht nur den Umgang mit personenbezogenen Daten, sondern trägt maßgeblich auch zum Schutz unternehmerischer Informationen bei.

Unternehmen, die ihre Daten-Governance konsequent am Datenschutz ausrichten, stärken damit gleichzeitig ihre Wissensbasis, ihre Wettbewerbsfähigkeit und letztlich den wirtschaftlichen Standortvorteil.[26] Zentral ist dabei die Integration klar definierter Rollen- und Rechtskonzepte. Wer festlegt, welche Mitarbeitenden Zugriff auf welche Datentypen erhalten, schafft Transparenz, verhindert Datenmissbrauch und schützt gleichzeitig sensible Geschäftsgeheimnisse. Das betrifft beispielsweise Algorithmen, Produktentwicklungen oder strategische Marktinformationen. Eine stabile Datenschutzarchitektur ist damit auch ein Schutzschild für immaterielle Vermögenswerte und trägt direkt zur Stabilität unternehmerischer Wertschöpfung bei.

Technische Maßnahmen wie Verschlüsselung, Zugriffskontrollen, Netzwerksegmentierung, Logging oder Backup-Mechanismen erfüllen eine Doppelfunktion: Sie sind Kernbestandteile für die Sicherheit der Verarbeitung gemäß Art. 32 DSGVO und gleichzeitig „angemessene Geheimhaltungsmaßnahmen“ im Sinne des Geschäftsgeheimnisgesetz (GeschGehG, § 2 Abs. 1). Datenschutz und Geheimnisschutz wirken damit synergetisch.[28]

Aus ökonomischer Perspektive ist diese Verzahnung hoch relevant: Unternehmen mit etablierten Datenschutzprozessen verringern das Risiko interner Datenabflüsse erheblich. Studien zeigen, dass strukturierte Zugriffsberechtigungen, Audits und klare Policies das Risiko unbeabsichtigter oder vorsätzlicher Datenabflüsse deutlich reduzieren.[29] Datenschutz schützt folglich neben personenbezogenen Daten auch Prototypen, Quelltexte, Forschungsdaten oder Kundendatenbanken – und damit zentrale Wertträger des Unternehmens. Auch ökonomisch zeigt sich ein signifikanter Effekt: Unternehmen mit starker Datenschutz-Governance gelten Investor*innen und Geschäftspartner*innen als risikoärmer, da sie regulatorische Risiken beherrschen und geringere Ausfall- oder Sicherheitskosten erwarten lassen.[30]

Eine weitere Säule für eine gute Daten-Governance bildet „Data Privacy/Dataprotection by Design and by Default”, das die frühzeitige Integration von Datenschutz- und Sicherheitsanforderungen in Software- und Systemarchitekturen fordert (Art. 25 DSGVO). Vor allem im Kontext von Big-Data-Systemen kann eine frühzeitige Integration von konkreten technischen Ansätzen zur Datenschutzkonformität persönliche Daten schützen und Sicherheitsrisiken minimieren.[31] Forschende bestätigen, dass früh implementierte Sicherheitsmechanismen die Zahl schwerer Sicherheitslücken nachweislich senken.[32] „Privacy/Datenschutz by Design and Default” verhindert somit strukturelle Schwachstellen, reduziert langfristige Sicherheitskosten und stärkt die operative Resilienz.

Entgegen der verbreiteten Annahme, dass eine datenschutzsensible Daten-Governance vor allem Kosten und bürokratischen Aufwand verursache, belegen aktuelle Studien und Praxisbeispiele, dass sie Unternehmen rechtlich absichert und durch erhöhte Datensicherheit sowie effiziente Prozesse einen klar messbaren wirtschaftlichen Standortvorteil schafft – ein Signal für Professionalität, Nachhaltigkeit und digitale Reife.

Frederick Richter

Vorstand der Stiftung Datenschutz

„Gute Daten-Governance mit gewissenhaft umgesetztem Datenschutz ist mehr als bloße Compliance-Pflicht. Denn wer die Datenhaltung in seinem Haus besser überblickt und steuert, unterstützt damit nicht nur die Gesetzeseinhaltung. Wer im Griff hat, welche Daten wo in seinem Unternehmen wie eingesetzt werden, kann erreichen, dass nur genaue, konsistente und zuverlässige Daten genutzt werden. Die so erreichte Datenqualität erhöht die Effizienz – und unterstützt ganz nebenbei auch den Datenschutz.“

Fazit

Datenschutz nur als gesetzliche Pflicht wahrzunehmen, wird seiner Wichtigkeit in unserer heutigen Zeit nicht annähernd gerecht. Geschäftsmodelle, die Datenschutz beherzigen und Grundrechte respektieren, handeln zum einen ethisch und sind zum anderen wirtschaftlich nachhaltiger sowie zukunftsfester. Deshalb ist Datenschutz auf sehr unterschiedlichen Ebenen ein wichtiger Baustein für Unternehmen, um glaubwürdig und sicher zu agieren, wettbewerbsfähig zu bleiben sowie die eigene Compliance gewährleisten zu können.

Dieses White Paper zeigt auf, wie Datenschutz – neben einem klaren Wirtschaftsvorteil – auch digitale Integrität, Privatsphäre und demokratische Werte sichert. Denn professionell umgesetzte Datenschutzmaßnahmen erhöhen unternehmerische Resilienz und helfen dabei:

- mit Transparenz das Vertrauen von Kund*innen zu gewinnen und zu halten,
- eine starke Position im Wettbewerb auszubauen,
- ein robustes Risikomanagement zu betreiben
- vor Wirtschaftsspionage und Cyberangriffen zu schützen sowie
- eigene Unternehmensassets abzusichern.

Parallel zu den laufenden Reformbestrebungen wird deutlich, welches wirtschaftliche Potenzial die DSGVO bereits heute birgt. Geplante Entlastungen, etwa für kleine und mittelständische Unternehmen oder Ehrenamtliche, sowie eine Bündelung der Aufsicht für den privaten Sektor beim Bundesdatenschutzbeauftragten, können klare Vorteile bringen – sofern sie praxisorientiert umgesetzt werden.

Darüber hinaus gibt es zahlreiche Möglichkeiten, wie die Politik durch klare Rahmenbedingungen und gezielte Reformen unternehmerische Bemühungen zum Datenschutz unterstützen kann. Beispielsweise durch eine Vereinheitlichung der Datenschutzaufsichten: Wird das europäische Datenschutzrecht in allen Bundesländern konsistent interpretiert und durchgesetzt, entstehen für Unternehmen mehr Klarheit und bessere Voraussetzungen für rechtskonformes Wirtschaften. Ein Grund mehr, den eigenen unternehmerischen Datenschutz unter die Lupe zu nehmen und DSGVO-konform aufzustellen.

Die Stiftung Datenschutz hilft weiter

Neben juristischen Expert*innen beheimatet die Stiftung Datenschutz zahlreiche andere Datenschutzprofis. Sie bietet handfeste Lösungsansätze und spricht Empfehlungen für Politik, Wirtschaft und Gesellschaft aus. Im Hinblick auf die aktuelle Rechtslage gibt die Stiftung Datenschutz kleineren und mittelständischen Unternehmen rechtskonforme und praxisorientierte Hinweise, wie sie durch Datenschutzmaßnahmen ihre unternehmerische Resilienz erhöhen können.

Mit dem Portal Datenschutz für Kleinunternehmen bietet sie zudem Kleinstunternehmen und Selbstständigen eine Schritt-für-Schritt-Anleitung, um Datenschutzaufgaben unkompliziert und rechtssicher umzusetzen.

Es ist klar, dass der Datenschutz und die damit verbundenen Aufgaben für Unternehmen im ersten Moment überwältigend sein können. Die Stiftung Datenschutz bietet daher hilfreiches Wissen und eine Plattform für den praxisnahen Austausch.

Quellen

[1] Wichtiger Meilenstein dazu ist das Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahr 1983. Daraus ist für Deutschland das Grundrecht auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht und der Menschenwürde abgeleitet worden: BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983 - 1 BvR 209/83 -, Rn. 1-215, https://www.bverfg.de/e/rs19831215_1bvr020983, 20.11.2025;

[2] Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: https://www.bfdi.bund.de/DE/BfDI/Inhalte/Datenschutzpfad/Grundrecht-Datenschutz.html, 17.11.2025;

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI): Whitepaper des Digitalen Verbraucherschutzes #2: Corporate Digital Responsibility – Unternehmensverantwortung im Digitalen Verbraucherschutz 21.05.2025: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/whitepaper-cdr.html, 17.11.2025;

[4] Intuit Mailchimp ist momentan eine der führenden Marketingplattformen für kleine und mittelständische Unternehmen (KMU) weltweit.

[5] Intuit Mailchimp Studie 2025 zu Datenschutz und Kundenvertrauen (Juni 2025): https://mailchimp.com/de/newsroom/gdpr/, 19.12.2025;

[6] Im Vergleich dazu Intuit-Studie aus 2024: „Markenvertrauen im Zeitalter der Informationsflut" (Juni 2024): https://mailchimp.com/newsroom/brand-trust-global-report/, 19.12.2025;

[7] Onlinebefragung des vzbv im Rahmen der Stellungnahme zum Digitalen Omnibus der Europäischen Kommission (Dezember 2025): https://www.vzbv.de/pressemitteilungen/digital-omnibus-europaeische-kommission-setzt-vertrauen-der-verbraucherinnen, 19.12.2025;

[8] IAAP Privacy and Consumer Trust Report, 2023: https://iapp.org/resources/article/privacy-and-consumer-trust-summary/, 18.12.2025;

[9] Entscheidungen, wie die des OLG Stuttgart vom 23.09.2025 zur App „Lidl Plus" unterstützen diese Sorge: https://stiftungdatenschutz.org/veroeffentlichungen/datenschutz-im-fokus/datenschutz-im-fokus-detailansicht/olg-stuttgart-lidl-plus-darf-trotz-zahlung-mit-daten-als-kostenlose-app-beworben-werden-645, 17.11.2025;

[10] Commission nationale de l'informatique et des libertés (CNIL): „Are we ready to pay for online services without targeted advertising?" (Oktober 2025): https://www.cnil.fr/en/are-we-ready-pay-online-services-without-targeted-advertising, 04.12.2025;

[11] IAAP Privacy and Consumer Trust Report, 2023: https://iapp.org/resources/article/privacy-and-consumer-trust-summary/ , 07.01.2026;

[12] Wie z. B. die Vodafone GmbH in Bezug auf „Privacy by Design" in ihrem Unternehmensblog, 03.01.2025: https://www.vodafone.de/business/blog/privacy-by-design-20510/?utm_source=chatgpt.com, 19.11.2025;

[13] Französische Aufsichtsbehörde CNIL und Veranstaltung zu Wirtschaftlichen Auswirkungen der DSGVO: https://www.cnil.fr/fr/participez-levenement-rgpd-quel-impact-economique-le-20-mai-2025 , 19.11.2025;

[14] Intuit Mailchimp Studie 2025 zu Datenschutz und Kundenvertrauen, 2025: https://mailchimp.com/de/newsroom/gdpr/, 19.12.2025;

[15] Commission nationale de l'informatique et des libertés (CNIL): „What are the economic benefits of having a DPO for a company?": https://www.cnil.fr/en/what-are-economic-benefits-having-dpo-company, 19.12.2025;

[16] Wurde vom Bundesverfassungsgericht 2008 im Kontext von unverhältnismäßiger Überwachung entwickelt, um Lücken im Schutz des allgemeinen Persönlichkeitsrechts zu schließen: https://www.egovernment.de/was-ist-das-it-grundrecht-a-3caf4fe0310a003c7950e9aca8820434/, 19.11.2025;

[17] Die Begriffe „Data Privacy" und „Data Protection" werden synonym verwendet. Mit dem Prinzip „Data Protection by Design and Default" ist durch die DSGVO festgelegt, dass Datenschutzprinzipien schon in den Entwicklungsprozess einfließen müssen (by Design) und dass Voreinstellungen so datenschutzfreundlich wie möglich gestaltet werden (by Default).

[18] Studie Cisco zur Cybersicherheit 2019. Datenschutz 2019: Maximierung des Nutzens von Datenschutzinvestitionen. Benchmark-Studie zum Datenschutz, 2019: https://www.cisco.com/c/dam/global/de_de/products/security/pdfs/de-cybersecurityseries_priv.pdf, 04.12.2025;

[19] Commission nationale de l'informatique et des libertés (CNIL): What are the economic benefits of having a DPO for a company? https://www.cnil.fr/en/what-are-economic-benefits-having-dpo-company, 19.12.2025;

[20] IBM: Cost of a Data Breach Report 2024, https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financial-industry, 08.01.2026;

[21] ENISA Threat Landscape 2023/2024: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf, 08.01.2026;

[22] Presseinformation zur Studie von Bitkom e.V.: https://www.bitkom.org/Presse/Presseinformation/Russland-China-deutsche-Wirtschaft-Visier, 19.11.2025;

[23] Studie Wirtschaftsschutz 2025, Bitkom e.V.: https://www.bitkom.org/sites/main/files/2025-09/bitkom-pressekonferenz-wirtschaftsschutz-cybercrime.pdf, 18.11.2025;

[24] Cisco: Cybersecurity Readiness Index 2025: https://news-blogs.cisco.com/emea/de/2025/05/08/cisco-studie-unternehmen-in-deutschland-besser-auf-cybergefahren-vorbereitet-86-integrieren-ki-in-angriffserkennung/, 08.01.2026;

[25] Garrett Johnson 2022: „Economic Research on Privacy Regulation: Lessons from the GDPR and beyond"; https://www.nber.org/system/files/working_papers/w30705/w30705.pdf, 08.01.2026;

[26] Vgl. Engels, Barbara / Scheufen, Marc, 2020, Wettbewerbseffekte der Europäischen Datenschutzgrundverordnung – Eine Analyse basierend auf einer Befragung unter deutschen Unternehmen, IW-Report, Nr. 1, Köln sowie Joshi, The Role of Modern Data Governance in Enabling Reliable Analytics for Competitive Advantage (Journal of Economics Intelligence and Technology), 2025, https://sarcouncil.com/download-article/JEIT-2025-9-15.pdf?, 23.01.2026;

[28] Z. B. Kühling/Buchner, Kommentar zur DSGVO, 3. Auflage, 2020;

[29] Vgl. IBM: Cost of a Data Breach Report 2024, https://www.ibm.com/think/insights/cost-of-a-data-breach-2024-financialindustry, 08.01.2026 sowie Liu/Ali Baba: Corporate Cybersecurity Risk and Data Breaches: A Systematic Review of Empirical Research (SAGE Journals), 2024 https://journals.sagepub.com/doi/10.1177/03128962241293658?utm, 23.01.2026;

[30] Harvard Business Review, „The ROI of Privacy and Security Governance", 2021: https://hbr.org/sponsored/2021/03/is-your-privacy-governance-ready-for-ai, 2021; 08.01.2026;

[31] Vgl. Frauenhofer Institut für Sichere Informationstechnologie SIT, „Privacy und Big Data", Studie des Verbundprojekts „Cybersicherheit für die digitale Verwaltung", 2020: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Privacy_und_Big_Data.pdf?_=1610456196, 08.01.2026;

[32] MIT Sloan Cybersecurity Research Consortium, 2020: https://sloanreview.mit.edu/article/make-cybersecurity-a-strategic-asset/, 08.01.2026;

KONTAKT

Frederick Richter, Vorstand
richter@stiftungdatenschutz.org

Kirsten Bock, Wissenschaftliche Leitung
k.bock@stiftungdatenschutz.org

Theresa Wenzel, Pressesprecherin und Referentin Stiftungskommunikation
t.wenzel@stiftungdatenschutz.org
presse@stiftungdatenschutz.org
0151 1578 9431

stiftungdatenschutz.org

Mastodon: social.bund.de/@DS_Stiftung
Bluesky: bsky.app/profile/datenschutz.bsky.social
LinkedIn: linkedin.com/company/stiftungdatenschutz

Newsletter DatenschutzWoche

IMPRESSUM

Herausgeber:
Stiftung Datenschutz
Karl-Rothe-Straße 10-14, 04105 Leipzig
0341 / 5861 555-0
mail@stiftungdatenschutz.org
stiftungdatenschutz.org

Redaktion:
Hier Mittenmang GmbH / hier-mittenmang.de

Gestaltung:
I LIKE VISUALS GmbH / ilikevisuals.com

Stand: Januar 2026