Erwartungen deutscher Unternehmen an die europäische Digitalregulierung

Was die Wirtschaft braucht, um die Chancen der Digitalisierung besser zu nutzen

Juni 2024

Centres for European Policy Network
FREIBURG | BERLIN | PARIS | ROMA

Building a better working world

INHALTSVERZEICHNIS

EXECUTIVE SUMMARY

In an era of global data flows and a race for technological dominance, European businesses must not only remain competitive but also comply with the European Union's (EU) strict data protection standards. To help domestic companies meet this challenge, the EU is pursuing a dedicated data strategy, including the Data Act's provisions on data sharing and interoperability of cloud solutions. But are these policy ideas being translated into business practice? To get to the bottom of this question, EY and the Centre for European Policy (cep) conducted a comprehensive survey of nearly 1,000 European businesses in the spring of 2024. The aim was to gain insights into the use of cloud services, data sharing and the associated legal and technological challenges, as well as to explore companies' attitudes towards current EU digital regulation.

The figures clearly show that European businesses still face a number of obstacles, ranging from data protection concerns and legal uncertainties to technological barriers. At the same time, businesses recognise the potential of EU initiatives to strengthen the digital single market and improve data protection – but the new requirements are too complex, their interaction is still unclear or there is scepticism about whether they will solve the problems. Shortly after the European elections in 2024, the message to policymakers is therefore clear: To manage the digital transformation and strengthen European sovereignty, domestic companies urgently need more legal certainty and a more innovation-friendly approach to the General Data Protection Regulation (GDPR), for example, when trading or transferring data internationally and in general with regard to the interaction of data protection rules with the new EU digital regulation. Our analysis suggests some targeted actions for the next Commission to make better use of the opportunities offered by digitalisation. These can be grouped under four themes.

First, further facilitating cloud switching through consistent application of the Data Act to make it easier to switch between data processing services. Open and interoperable standards can facilitate data exchange and reduce dependence on single dominant US providers. In addition, European cloud providers should be promoted through targeted measures to provide a real alternative to US services and reduce dependency on them. Timely publication by the Commission of market-relevant and workable standard contractual clauses for cloud computing contracts before the Data Act starts to apply can provide support and legal certainty to businesses. Still, further exploration of competition and industrial policy interventions may be necessary to weaken the market dominance of large cloud providers and strengthen the bargaining power of small and medium-sized enterprises.

Second, create long-term legal certainty for data transfers, in particular by promoting international agreements to regulate access to data for national security purposes. This is a necessity, given the risk of the US adequacy decision being overturned. Alternatively, targeted promotion of fiduciary cloud solutions – where European trustees ensure that no data is flowing to the US – could be helpful to allow European businesses to use economically indispensable functionalities of US cloud providers.

Thirdly, there is an urgent need for a legally secure, innovation-friendly approach to the GDPR and more support for businesses in complying with data protection regulation. Greater legal certainty can be achieved, for example, through the more flexible provision of interpretation tools and practical, clear guidance that not only identifies conflicts but also proposes solutions. Faster agreement on data protection guidelines within the European Data Protection Board is likewise required. For example, there is a need to clarify how synthetic data can be used in a legally secure manner and when data may be considered anonymised, e.g. by developing and defining uniform and workable standards, compliance with which will be presumed to provide a sufficient degree of anonymisation. More generally, the conflict between the principle of data minimisation and big data needs to be resolved in a legally secure manner. Wherever possible, new avenues for an innovation-friendly interpretation and application of the GDPR should be explored.

Fourth, the complex EU digital regulation that has been the focus of attention over the past decade needs to be made clearer and better implemented. For example, all digital legislation should be brought together in a single set of EU rules and their interaction with each other and with the GDPR should be explained. Any remaining ambiguities in individual EU digital laws must be clarified and these laws better harmonised with the GDPR. In addition to EU-wide guidelines and interpretation aids, training programmes should be implemented to achieve a better understanding and correct application of the digital acts by businesses.

EINLEITUNG

In Zeiten zunehmend globaler Datenströme und eines sicherheitspolitischen Wettrennens um Technologiesouveränität muss die europäische Wirtschaft nicht nur wettbewerbsfähig bleiben, sondern auch die strengen Datenschutzstandards der Europäischen Union (EU) einhalten. Um heimische Unternehmen bei der Bewältigung dieser Herausforderung zu unterstützen, verfolgt die EU eine dezidierte Datenstrategie, zu der insbesondere die Vorgaben des Data Act zur Teilung von Daten und zur Wechselbarkeit von Cloud-Lösungen gehören. Hoffnungen liegen zudem auf der jüngsten Angemessenheitsentscheidung der Europäischen Kommission zum transatlantischen Datentransfer. Insgesamt sehen sich europäische Unternehmen einem Paradigmenwechsel in der EU-Digitalpolitik gegenüber, der den technischen Fortschritt und die Marktrealität in Hinblick auf Daten anerkennt, aber gleichzeitig praxisnäher regulieren möchte. Doch kommen diese politischen Vorstellungen in der unternehmerischen Praxis an?

Um dieser Frage auf den Grund zu gehen, haben EY und das Centrum für Europäische Politik (cep) im Frühjahr 2024 eine umfassende Umfrage unter rund 1.000 europäischen Unternehmen durchgeführt. Ziel war es, Einblicke in die Nutzung von Cloud-Diensten, das Teilen von Daten und die damit verbundenen rechtlichen und technologischen Herausforderungen zu gewinnen sowie die Einstellung der Unternehmen zur aktuellen EU-Digitalregulierung zu erfragen. Aus den Zahlen wird deutlich: **Europäische Unternehmen sehen sich noch immer mit einer Vielzahl von Hemmnissen konfrontiert, die von Datenschutzbedenken über rechtliche Unsicherheiten bis hin zu technologischen Barrieren reichen.** Gleichzeitig erkennen die Unternehmen das Potenzial der EU-Initiativen zur Stärkung des digitalen Binnenmarkts und zur Verbesserung des Datenschutzes an – aber die neuen Vorgaben sind zu komplex, ihr Zusammenspiel noch zu unklar, oder es herrscht Skepsis, ob sie die Probleme lösen werden.

Kurz nach der Europawahl 2024 ist die Botschaft an die Politik klar: **Um die digitale Transformation zu meistern, die europäische Souveränität zu stärken und global wettbewerbsfähig zu bleiben, brauchen heimische Unternehmen dringend mehr Rechtssicherheit** und einen **innovationsfreundlicheren Umgang** mit der Datenschutzgrundverordnung (DSGVO), etwa beim Handel mit oder beim internationalen Transfer von Daten sowie generell in Bezug auf das Zusammenspiel der Datenschutzregeln mit der neuen EU-Digitalregulierung. Dies gilt gerade mit Blick auf die wachsende Bedeutung Künstlicher Intelligenz (KI) und datenbasierter Geschäftsmodelle. Damit europäische Unternehmen ihre Chance auf eine Führungsrolle in diesen Bereichen wahren können, muss geklärt werden, wie sie potenziell innovationshemmende Konflikte mit der DSGVO lösen oder von vornherein vermeiden können. Dabei geht es nicht um einen Verzicht auf Datenschutz, sondern um die weitestmögliche und rechtssichere Minimierung von Datenschutzrisiken, etwa – wo immer möglich – durch verstärkte Nutzung anonymisierter oder synthetischer Daten, etwa für KI-Training. Denn auf anonymisierte Daten finden die Regeln der DSGVO keine Anwendung. Hier muss jedoch klargestellt werden, ab wann **Daten als anonymisiert gelten**. Ein internationales Abkommen über Datenzugriffe zu Zwecken der nationalen Sicherheit könnte Unternehmen langfristig von der Fessel drohender datenschutzrechtlicher Illegalität bei transatlantischen Datentransfers befreien. Angesichts der oligopolistischen Struktur des derzeitigen Cloud-Markts und der steigenden Bedeutung von Cloud-Lösungen für Datenwirtschaft und KI-Entwicklung muss die EU darüber hinaus **europäische Cloud-Anbieter** als Alternativen zu US-Diensten besser fördern und so **mehr Wettbewerb** schaffen. Hierzu muss der **Data Act konsequent umgesetzt** und der Wechsel zwischen Datenverarbeitungsdiensten weiter erleichtert werden. Darüber hinaus sind **wettbewerbs- und industriepolitische Maßnahmen** erforderlich, um die Marktdominanz der großen Cloud-Anbieter perspektivisch zu verringern.

PROFIL DER BEFRAGTEN UNTERNEHMEN

Die große Mehrheit der befragten Unternehmen (92,05%) ist überwiegend im europäischen Wirtschaftsraum (EWR) tätig und wurde von Entscheidungsträgern als auch Einflussnehmern auf Compliance- und Datenschutzstrategien vertreten. Bemerkenswert ist, dass 37,57% der Befragten aus dem Management stammen, was auf die strategische Bedeutung von Daten und Cloud-Lösungen für heutige unternehmerische Aktivitäten hinweist.[1] Bei der Branchenverteilung zeigt sich eine breite Streuung über Industrie- und Dienstleistungssektoren. Die starke Vertretung von Unternehmen aus der Industrie (17,68%) und dem Dienstleistungssektor (15,58%) sowie aus dem Finanz- und IT-Sektor legt nahe, dass die genannten Probleme ein breites Spektrum von Branchen betreffen. Dass 30,31% der Befragten in Unternehmen mit mehr als 5.000 Mitarbeitern, gut ein Drittel (34,85%) in Unternehmen mit weniger als 5.000, aber mehr als 250 Mitarbeitern und ein weiteres Drittel (34,85%) in Unternehmen mit weniger als 250 Mitarbeitern tätig sind, lässt darauf schließen, **dass die EU-Digitalregulierung – von Regelungen zum Cloud-Wechsel und zum B2B-Datenaustausch bis hin zur DSGVO und dem transatlantischen Datentransfer – nicht nur wenige „Global Player", sondern das Rückgrat der europäischen Wirtschaft betrifft**.

[1] Darüber hinaus deutet der sehr hohe Anteil von Teilnehmern, die ihre Rolle im Unternehmen trotz der angebotenen detaillierten Klassifizierung unter „sonstige Funktionen" einordnen (35,87%), die vielfältigen Rollen an, innerhalb derer daten- und datenschutzbezogene Themen mittlerweile innerhalb eines Unternehmens von Bedeutung sind.

CLOUD-SWITCHING

DOMINANTE US-CLOUD ANBIETER, FEHLENDE EUROPÄISCHE ALTERNATIVEN

Die überwiegende Mehrheit der befragten Unternehmen nutzt Cloud-Dienste, wobei 44,81% europäische und 35,66% US-amerikanische Anbieter einsetzen. Die Präferenz der Unternehmen für Microsoft O365/Azure, Amazon Web Services und Google Cloud Plattform unterstreicht die zentrale Rolle, die diese drei Anbieter in der heutigen digitalen Infrastruktur europäischer Unternehmen spielen. Mehr als die Hälfte der Befragten, die US-Anbieter nutzen, setzen auf Microsoft-Dienste. Das Antwortenprofil suggeriert jedoch, dass zahlreiche Unternehmen mehrere der genannten US-Dienste parallel nutzen. Deswegen verwundert es kaum, dass Interoperabilität zwischen verschiedenen Cloud-Diensten von fast der Hälfte der Befragten als „sehr wichtig" und nur von 5,23% der Unternehmen als „nicht wichtig" eingestuft wird. Zudem zeigen die Daten, dass mindestens 42,96% der Unternehmen die Vertragsbedingungen für Cloud-Dienste nicht individuell aushandeln konnten, was ebenfalls das ungleiche **Kräfteverhältnis zwischen dominanten US-Cloud-Anbietern und europäischen Nutzern** spiegelt. Blendet man die 42,6% „weiß nicht"-Antworten auf diese Frage aus, sind es sogar fast 75% der Unternehmen, die laut ihren Angaben keine Möglichkeit zur individuellen Verhandlung der Vertragsbedingungen hatten.

Die Ergebnisse legen zudem nahe, dass die Mehrheit der befragten Unternehmen bislang keine Erfahrungen mit einem Wechsel ihres Cloud-Anbieters hat.[2] Betrachtet man ausschließlich diejenigen Unternehmen, die Bedarf für einen Wechsel sahen, beklagt hiervon fast ein Fünftel (17,22%) zu hohe Migrationskosten und fast ein Drittel (32,05%) sah bzw. sieht sich explizit durch sonstige Lock-in-Effekte wie etwa Interoperabilitätsprobleme beim Cloudwechsel behindert. Diese Ergebnisse bestätigen, was zugleich zentraler Beweggrund für die Aufnahme von Regelungen zum Cloud-Switching in das neue EU-Datengesetz (Data Act) war: **die für die innovative Tätigkeit der Unternehmen essentielle unkomplizierte Wechselbarkeit des Anbieters wird derzeit massiv behindert, unter anderem durch technische und vertragliche Lock-in-Effekte**.[3] Die neuen Regeln des Data Act zum Cloud-Switching sollen diese Hürden beseitigen. So legt der Data Act an Stelle der bisher geltenden Selbstregulierung zwingende, harmonisierte Regeln für den Wechsel zwischen Datenverarbeitungsdiensten[4] fest und gibt unter anderem vor, dass Anbieter ihren Kunden den Wechsel ermöglichen und welche Anforderungen ihre Vertragsklauseln über den Wechsel erfüllen müssen. Zudem soll der Data Act Wechselentgelte schrittweise abschaffen und die

[2] Obwohl die Mehrheit (64,4%) der Unternehmen angeben, bislang keinen Bedarf für einen Wechsel des Cloud-Anbieters gehabt zu haben, lässt sich daraus nicht schließen, dass diese Unternehmen mit ihrem bisherigen Anbieter zufrieden sind. Die Gründe für den mangelnden Wechselbedarf können vielschichtig sein und von purer Bequemlichkeit über wirtschaftliche Vorteile der bestehenden Lösung bis hin zum Fehlen eines adäquaten Alternativanbieters reichen. Nur bei gut einem Viertel der Unternehmen lässt sich der fehlende Bedarf für einen Wechsel klar darauf zurückführen, dass diese Unternehmen überhaupt keine Cloud-Dienste nutzen.

[3] Laut der Folgenabschätzung der EU-Kommission zum Entwurf des Data Act hindern vor allem vertragliche, wirtschaftliche und technische Hürden die Nutzer daran, von einem Anbieter zu einem anderen zu wechseln und führen daher zu einem Vendor-lock-in, vgl. European Commission, Impact Assessment Report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 23/02/2022, SWD (2022) 34 final, S. 19f., abrufbar unter https://digital-strategy.ec.europa.eu/en/library/impact-assessment-report-and-support-studies-accompanying-proposal-data-act.
Als wichtigste technische Ursache für die Anbieterbindung bei Cloud- und Edge-Diensten wird dort die mangelnde Interoperabilität bzw. das Fehlen gemeinsamer Standards genannt, insbesondere bei PaaS und Saas-Diensten, die über die einfache Speicherung hinausgehen (S. 22).

[4] Unter die Definition der Datenverarbeitungsdienste im Data Act fallen Cloud- und Edge-Dienste, insbesondere Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS), aber auch neuere Variationen wie Storage-as-a-Service und Database-as-a-Service, vgl. EG 78 S.1, 80 S. 10, 81 Data Act.

Interoperabilität von Datenverarbeitungsdiensten verbessern.[5] Letzteres soll Nutzern nicht nur den (einmaligen) Wechsel des Anbieters, sondern auch die parallele Nutzung mehrerer Datenverarbeitungsdienste (Multi-Cloud) erleichtern, um einander ergänzende Funktionen verschiedener Dienste besser nutzen zu können.[6] Schließlich soll die Kommission bis zum Beginn der Anwendbarkeit des Data Act am 12. September 2025 allgemeine, zunächst unverbindliche Mustervertragsklauseln („Standardvertragsklauseln") für Cloud-Verträge entwickeln, die ihre Vorstellungen für „faire" Vertragsbedingungen widerspiegeln.

Soweit die Theorie, doch wie sieht es in der Praxis aus? Nur gut ein Fünftel (21,72%) der befragten Unternehmen glaubt, dass der Data Act den Wechsel von Cloud-Diensten maßgeblich erleichtern wird, während gut ein Viertel (26,7%) dies nicht erwartet und 47,06% hierzu keine Angabe machen. Es besteht also weiterhin eine erhebliche Unsicherheit: fast die Hälfte der Befragten hat keine klare Meinung zu diesem Thema. Die Kommentare einiger Befragter bestätigen, dass **die Hindernisse für den Wechsel zu Cloud-Diensten vielfältig und nicht ausschließlich rechtlicher Natur sind**. Auch IT-Prozesse, wirtschaftliche und technologische Faktoren spielen eine wichtige Rolle. Ebenfalls wurde betont, dass die effektive Anwendung des Data Act auch von seiner pragmatischen Durchsetzung durch die Datenschutzaufsichtsbehörden unter fairer Abwägung der widerstreitenden Werte und Interessen abhängt. Die Befürchtung einiger Unternehmen, dass die Regulierung nicht greifen wird, solange große Cloud-Anbieter weiterhin über erhebliche Marktmacht verfügen und außerhalb der EU agieren, verdeutlicht die Grenzen europäischer Gesetzgebung.

Was folgt daraus? Die Europäische Union muss die **Regeln des Data Act zur Erleichterung des Wechsels zwischen Cloud-Diensten konsequent durchsetzen und, falls nötig, auch wettbewerbsrechtliche Maßnahmen ergreifen**, um die Marktmacht der großen Cloud-Anbieter stärker zu regulieren und die Verhandlungsmacht der Unternehmen gegenüber diesen Anbietern zu stärken. Dies wird in Zukunft umso wichtiger, weil Cloud- und Edge-Dienste für die wachsende Zahl an daten- und KI-basierten Geschäftsmodellen nahezu unverzichtbar sind und daher noch mehr an Bedeutung gewinnen werden.

Die Kommission sollte die **Standardvertragsklauseln für Verträge über Cloud Computing so schnell wie möglich veröffentlichen, und zwar – anders als gesetzlich vorgesehen – bereits deutlich vor dem Anwendungsbeginn des Data Act am 12. September 2025**[7] , damit die Unternehmen sich darauf einstellen und die Klauseln ggf. noch rechtzeitig für ihre Zwecke anpassen können. Zudem muss die Kommission sicherstellen, dass ihre Klauseln für möglichst viele Branchen[8] marktrelevant und praxistauglich sind, und hierzu alle relevanten Stakeholder bei ihrer Entwicklung einbeziehen. Ob die marktmächtigen Anbieter allerdings bereit sein werden, die aus Sicht der Kommission „fairen" – aber unverbindlichen – Bedingungen zu akzeptieren und ihre Verträge entsprechend anzupassen, ist gleichwohl offen.[9] Sollten die großen Anbieter die Bedingungen nicht übernehmen, könnte die Kommission erwägen, weitere Schritte zu ergreifen, um die oligopolistische Struktur des Cloud-Marktes aufzubrechen.[10] Wie unsere Daten zudem zeigen, werden eine verbesserte Interoperabilität und reduzierte Wechselkosten – wie sie der EU Data Act einführen möchte – allein nicht ausreichen, um die Abhängigkeit von US-Anbietern zu reduzieren. Vielmehr muss die EU über die Regelungen des Data Act hinaus die Schaffung adäquater Alternativen zu US-Clouds – auch auf der Basis von Open-Source-Software – innerhalb der EU noch viel stärker unterstützen und EU-Clouds weiter fördern, um für echten Wettbewerb zu sorgen.

[5] Vgl. Art. 35 Data Act.

[6] Vgl. Art. 34 Data Act.

[7] Vgl. Art. 41 Data Act.

[8] Daher sind ggf. verschiedene Klauselvarianten wünschenswert.

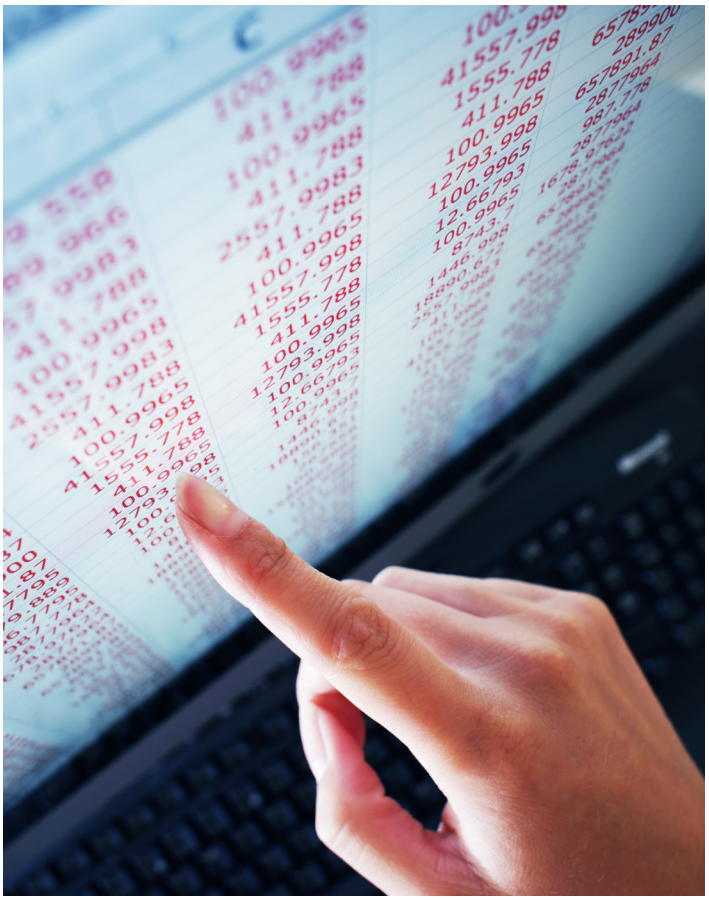
[9] Zweifelnd, was der Ansatz des Data Act angesichts der Marktverhältnisse bewirken wird, insoweit Staudenmayer, NJW 2024, S. 1377ff., Rn. 42. Sattler, Computer und Recht 2024, S. 213 (214) sieht die Klauseln als Test für die Bereitschaft der marktmächtigen Anbieter zur Übernahme der Bedingungen der Kommission.

[10] Näher hierzu Sattler, Computer und Recht 2024, S. 213 (214).

DATENTRANSFERS

TREND ZUR DATENLOKALISIERUNG SETZT SICH TROTZ ANGEMESSENHEITSBESCHLUSSES FORT

Die Dominanz der US-Cloud-Anbieter stellt die europäischen Unternehmen auch unter datenschutzrechtlichen Aspekten vor enorme Probleme. Denn für in der EU niedergelassene Unternehmen, die als Verantwortliche oder Auftragsverarbeiter personenbezogene Daten im Rahmen der Tätigkeit ihrer Niederlassung verarbeiten, gilt die DSGVO unabhängig davon, wo die Datenverarbeitung stattfindet.[11] Cloud-Dienstleistungen sind typischerweise Auftragsverarbeitungen, bei denen Daten im Auftrag des datenschutzrechtlich verantwortlichen Unternehmens verarbeitet (gespeichert) werden. Nutzt ein in der EU ansässiges Unternehmen die Dienste eines US-amerikanischen Cloud-Anbieters und werden deshalb personenbezogene Daten in die USA übermittelt, unterliegen diese Transfers den strengen Regeln der DSGVO über den internationalen Datentransfer in ihrer Auslegung durch den Europäischen Gerichtshof (EuGH). Der EuGH hat die Zulässigkeit der Datentransfers in die USA in seinen Urteilen Schrems I (2015) und Schrems II[12] (2020) wiederholt in Frage gestellt. Unsere Umfrage bestätigt deren hohen Bekanntheitsgrad – nur 10,16% der befragten Unternehmen geben an, die Schrems-Urteile nicht zu kennen. Vor diesem Hintergrund wirft die starke Nutzung von Cloud-Diensten mit US-Bezug durch europäische Unternehmen wichtige Fragen hinsichtlich der Datensicherheit und der Einhaltung der DSGVO auf.



Einem weltweiten Trend hin zu mehr „Datenlokalisierung“ folgend wird die Datenverarbeitung innerhalb Europas auch hierzulande zunehmend wichtig – nicht nur juristisch, sondern auch aus Reputationsgründen. Die weit überwiegende Mehrheit von über 85% der Befragten gibt an, dass es für ihr Unternehmen sehr wichtig ist, dass ihr Cloud-Anbieter die Datenverarbeitung innerhalb der EU bzw. des Europäischen Wirtschaftsraums (EWR) sicherstellt. 63,10% begründen ihre Antwort damit, dass dies zunehmend eine Voraussetzung für die Zusammenarbeit mit Kunden sei. Weitere 22,76% betonen die Wichtigkeit aus Gründen wie den rechtlichen Anforderungen zur Einhaltung der DSGVO.

Das deutet darauf hin, dass die Schrems-Urteile zu einer **hohen Sensibilität bei der Nutzung von US-amerikanischen Cloud-Diensten geführt haben** – eine Vermutung, die sich im Laufe der Umfrage erhärtet. Dennoch nutzen 15,45% der Befragten aufgrund wirtschaftlicher Vorteile weiterhin US-amerikanische Dienste, während 20,12% keine adäquaten Alternativen innerhalb des EWR gefunden haben. **Europäische Unternehmen stehen daher oftmals vor einem Dilemma zwischen wirtschaftlicher Effizienz und rechtlicher Konformität.**

[11] Art. 3 Abs. 1 DSGVO.

[12] EuGH, Urteil vom 16. Juli 2020, Rs. C-311/18 (Data Protection Officer/Facebook Ireland Ltd und Maximilian Schrems), ECLI:EU:C:2020:559, nachfolgend abgekürzt als „Schrems II“-Urteil bezeichnet.

Dass die Forderung nach einem Verbleib der Daten in der EU für die Unternehmen eine derart hohe Wichtigkeit erreicht hat, verwundert im Zuge der aktuellen Diskussionen um „souveräne Clouds" wenig. So sind Anbietersitz und Datenverarbeitung im EWR etwa aus der Sicht der deutschen Datenschutzbehörden ein „Muss"-Kriterium für „souveräne Clouds".[13] Dies bedeutet zugleich, dass die Plattformen der großen US-basierten Anbieter aus Sicht der DSK nicht als „souveräne Clouds" gelten.[14] Allerdings geht die Forderung nach souveränen Clouds weit über die Datenschutzkonformität hinaus.

Dieser Trend zur Datenlokalisierung ist kritisch zu sehen. Zum einen kann Datenlokalisierung Folgeprobleme nach sich ziehen[15], etwa zu ökonomischen Ineffizienzen führen. Zum anderen beseitigt allein die Speicherung der Daten auf Servern in der EU die Probleme nicht in allen Fällen (vollständig). Dies gilt jedenfalls dann, wenn EU-Unternehmen US-Cloud-Anbieter oder europäische Cloud-Anbieter mit Verbindungen zu den USA einsetzen – was bei Microsoft, AWS oder Google jedoch gerade der Fall ist. Denn die datenschutzrechtlichen Rechtsunsicherheiten sind zu einem großen Teil auf die Datenzugriffsmöglichkeiten der US-Behörden und Geheimdienste zurückzuführen, die US-Gesetze[16] diesen Behörden verleihen.

Allein die Speicherung von Daten auf EU-Territorium schließt derartige Zugriffe jedoch nicht rechtssicher aus. Auch wenn aktiv keine Daten (mehr) in die USA übermittelt werden[17], ist zu beachten, dass Cloud-Anbieter mit Verbindungen zu den USA auch dann, wenn sie in der EU ansässig sind, dem US CLOUD Act[18] unterliegen können und somit auf dessen Grundlage ggf. Daten an US-Behörden herausgeben müssen, die sich unter ihrer Kontrolle befinden.[19]

Soweit (noch) Daten in die USA übermittelt werden, bleibt das Risiko bestehen, dass US-Behörden auf diese Daten zugreifen. Solche Datentransfers erfolgen nicht nur bei der Nutzung von Clouds, die auf Servern in den USA gehostet werden, sondern werden – in geringerem Umfang – auch von Anbietern vorgenommen, die Daten grundsätzlich innerhalb der EU verarbeiten[20]. Beispielsweise werden auch bei der Nutzung von Cloud-Produkten wie Microsoft 365 Daten in die USA gesendet, weshalb die datenschutzkonforme Nutzbarkeit dieser Lösung in Frage gestellt wurde und weiterhin diskutiert wird.

[13] Deutsche Datenschutzkonferenz (DSK), Kriterien für Souveräne Clouds, Positionspapier der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 11. Mai 2023, Ziffer 2.6, abrufbar unter https://www.datenschutzkonferenz-online.de/media/weitere_dokumente/2023-05-11_DSK-Positionspapier_Kritierien-Souv-Clouds.pdf.

[14] Sieger, H., Digitale Souveränität: Warum auch die Selbstbestimmung dazu gehört, 7. Juni 2023, abrufbar unter https://www.digitalbusiness-cloud.de/digitale-souveraenitaet-warum-auch-die-selbstbestimmung-dazu-gehoert-a-08e4a0d4f1527c2f9b3a949db429617d/.

[15] Näher dazu Chander, A., Is Data Localization a Solution for Schrems II?, 27. Juli 2020, abrufbar unter https://scholarship.law.georgetown.edu/facpub/2300/.

[16] So etwa der Abschnitt 702 des US Foreign Intelligence Surveillance Act oder Executive Order 12333: United States Intelligence Activities, U.S. Federal Register Vol. 40, No 235 oder der US CLOUD Act [Gesetz über die Klarstellung der Nutzung von Daten im Ausland (US Clarifying Lawful Overseas Use of Data Act), H.R. 4943, abrufbar unter https://www.congress.gov/bill/115th-congress/house-bill/4943/text.

[17] Allein die bloße Gefahr, dass ein EWR-Unternehmen aus einem Drittland angewiesen werden könnte, personenbezogene Daten dorthin zu übermitteln, stellt noch keine Übermittlung dar, vgl. den Beschluss der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) vom 31. Januar 2023, Ziffer 1., abrufbar unter https://www.datenschutzkonferenz-online.de/media/dskb/20230206_DSK_Beschluss_Extraterritoriale_Zugriffe.pdf?trk=article-ssr-frontend-pulse_little-text-block. Sie kann aber dazu führen, dass der Cloud-Anbieter als Auftragsverarbeiter als unzuverlässig gilt und so für den Verantwortlichen ein erhöhtes Haftungsrisiko besteht, sofern nicht geeignete technische und organisatorische Maßnahmen zum Ausschluss solcher Übermittlungen ergriffen werden.

[18] US Clarifying Lawful Overseas Use of Data Act, a.a.O.

[19] So etwa bei Nutzung der „EU Data Boundary" für die Microsoft-Cloud, die eine weitgehende Datenspeicherung und -verarbeitung innerhalb der Länder der Europäischen Union (EU) und der Europäischen Freihandelsassoziation (EFTA) gewährleisten soll, vgl. hierzu die Antwort auf die 14. Frage der Q&A von Microsoft: "If compelled to disclose or give access to any customer's data, Microsoft will, if possible, promptly notify the customer and provide a copy of the demand unless legally prohibited from doing so", abrufbar unter https://techcommunity.microsoft.com/t5/security-compliance-and-identity/eu-data-boundary-for-the-microsoft-cloud-frequently-asked/ba-p/2329098.

[20] So werden etwa auch bei der Verarbeitung von Daten in der Microsoft Data Boundary (https://www.microsoft.com/de-de/trust-center/privacy/european-data-boundary-eudb) noch Daten in die USA gesendet, vgl. etwa Microsoft, What is the Data Boundary, 1. Februar 2024, abrufbar unter https://learn.microsoft.com/en-us/privacy/eudb/eu-data-boundary-learn: "The EU Data Boundary is a geographically defined boundary within which Microsoft has committed to store and process Customer Data and personal data for our Microsoft enterprise online services, including Azure, Dynamics 365, Power Platform, and Microsoft 365, subject to limited circumstances where Customer Data and personal data will continue to be transferred outside the EU Data Boundary".

All dies sorgt offenbar bei vielen Unternehmen noch immer für Rechtsunsicherheit, obwohl die EU-Kommission als Reaktion auf die Schrems-Urteile am 10. Juli 2023 einen neuen Angemessenheitsbeschluss[21] erlassen hat, um eine weitere Rechtsgrundlage für die Übermittlung personenbezogener Daten in die USA zu schaffen. Dieser Beschluss soll Datentransfers an Empfänger in den USA legitimieren, die sich im Wege der Selbstzertifizierung an das neue „EU-U.S. Data Privacy Framework" binden. So hat beispielsweise Microsoft in seinem Data Processing Addendum[22] vom November 2023 klargestellt, dass es nach dem EU-US Privacy Framework zertifiziert ist. Datentransfers in die USA bei der Nutzung von Microsoft 365 können daher auf den Angemessenheitsbeschluss gestützt werden, womit ein wesentlicher Kritikpunkt[23] an der Nutzung von Office 365 – zumindest vorübergehend – an Gewicht verloren hat.

Doch **gerade die Unsicherheit bezüglich des Fortbestehens des Angemessenheitsbeschlusses scheint das Vertrauen in diesen Beschluss bislang zu untergraben**. Denn nur 13,67% der befragten Unternehmen stützen ihre Nutzung von Public Cloud Computing oder SaaS-Lösungen allein auf den Angemessenheitsbeschluss. Weitere 10,72% greifen parallel auf alternative Transfergrundlagen wie die EU-Standardvertragsklauseln und Binding Corporate Rules zurück und haben somit bürokratischen Mehraufwand. Insgesamt glauben fast 16% der Unternehmensvertreter nicht an das langfristige Fortbestehen des Beschlusses. Allerdings herrscht bei zahlreichen Entscheidungsträgern, die an der Umfrage teilgenommen haben, Unkenntnis: Fast die Hälfte der Befragten (49,33%) sagen, dass sie nicht wissen, ob sich ihr Unternehmen auf den Angemessenheitsbeschluss stützt. Weitere 16,35% transferieren keine Daten in die USA. Blendet man die beiden letztgenannten Antwortgruppen aus und betrachtet ausschließlich diejenigen Unternehmen, die inhaltlich geantwortet haben und auch tatsächlich Daten transferieren, wird das oben gezeichnete Bild noch deutlicher: Zwar stützen sich über 71% dieser Unternehmen auf den neuen Angemessenheitsbeschluss; gleichzeitig gehen aber über 46% davon aus, dass der Beschluss nicht langfristig gelten wird, und stützen sich daher zumindest auch auf alternative Transfergrundlagen.

In der Summe suggerieren die verschiedenen Angaben, **dass trotz des Angemessenheitsbeschlusses erhebliche Skepsis hinsichtlich der Dauerhaftigkeit und Verlässlichkeit des neuen Kompromisses bestehen.** Dahinter verbirgt sich offenkundig die Angst der Unternehmen, der EuGH könnte auch diesen Angemessenheitsbeschluss in einem „Schrems III"-Urteil erneut zu Fall bringen. **Diese Angst ist nicht unbegründet,** da einige rechtliche „Grauzonen" trotz des Angemessenheitsbeschlusses fortbestehen und entsprechende Verfahren bereits beim Gerichtshof anhängig sind. Der EuGH muss insbesondere entscheiden, ob Datenzugriffe der US-Behörden auf übermittelte Daten unter der geänderten Rechtslage[24] auf ein verhältnismäßiges Maß reduziert wurden und der neue Rechtsbehelfsmechanismus EU-Bürgern hinreichenden Schutz gegen solche Zugriffe bietet. Viele Unternehmen befürchten, dass die Regelungen des Angemessenheitsbeschlusses nicht ausreichen, um langfristige Rechtssicherheit zu gewährleisten, und nutzen daher weiterhin (parallel) Standardvertragsklauseln und weitere Maßnahmen wie Verschlüsselung und „bring your own key", um ihre Daten zu schützen. Aus all dem lässt sich schließen, dass der Angemessenheitsbeschluss aus der Sicht erheblicher Teile der Wirtschaft bislang nicht die erhoffte wesentliche – sondern allenfalls eine vorübergehende – Entlastung gebracht hat.

ÜBER 46%* DERJENIGEN UNTERNEHMEN, DIE EINE ANGABE MACHTEN UND TATSÄCHLICH DATEN AN US-CLOUD-ANBIETER TRANSFERIEREN, GEHEN DAVON AUS, DASS DER ANGEMESSENHEITSBESCHLUSS KEINEN LANGFRISTIGEN BESTAND HAT.

*KNAPP 16% DER BEFRAGTEN UNTERNEHMEN (FAST 50% DER UNTERNEHMEN MACHTEN KEINE ANGABE).

[21] Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10.7.2023 gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates über die Angemessenheit des Schutzniveaus für personenbezogene Daten nach dem Datenschutzrahmen EU-USA, C(2023) 4745, abrufbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32023D1795.

[22] Datenschutznachtrag zu den Produkten und Services von Microsoft, zuletzt aktualisiert am 2. Januar 2024, S. 10, abrufbar unter https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA.

[23] Über die Datenübermittlungsproblematik hinaus wird Microsoft 365 unter weiteren Aspekten als datenschutzwidrig kritisiert, etwa aufgrund mangelnder Datenminimierung und Transparenz, wie welche Daten verarbeitet werden, vgl. Schonschek, O., Das Data Privacy Framework allein reicht nicht! Was Datenschützer bei Microsoft 365 kritisch sehen, 19.04.2024, abrufbar unter https://www.security-insider.de/eu-kommission-verstoss-datenschutz-microsoft-365-a-91a5761878506a02d5d421b768084acb/?cflt=rdt.

[24] Relevant sind insoweit insbesondere die Regelungen der „Executive Order on Enhancing Safeguards for U.S. Signals Intelligence Activities" des US-Präsidenten Joe Biden vom 7. Oktober 2022, abrufbar unter https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities.

Was folgt daraus? Angesichts fortbestehender Möglichkeiten der US-Behörden, Zugang zu personenbezogenen Daten von EU-Bürgern zu erhalten, besteht die Gefahr, dass auch der neue Angemessenheitsbeschluss für die USA langfristig keinen Bestand haben wird. Sofern die Verarbeitung anonymisierter Daten nicht in Betracht kommt (siehe dazu unten), weil die Cloud-Anbieter Zugriff auf die Daten im Klartext benötigen, müssen andere Lösungen gefunden werden. Es gilt, personenbezogene Daten so weit wie möglich vor Datenzugriffen durch US- und andere Drittlandsbehörden zu schützen und der europäischen Wirtschaft dennoch die Nutzung derjenigen Cloud-Lösungen zu ermöglichen, die sie für ihre erfolgreiche Innovationstätigkeit benötigt.[25] Eine solche Möglichkeit könnte der **Abschluss eines internationalen Abkommens zwischen den EU-Mitgliedstaaten und den USA bieten, das gegenseitige Datenzugriffe (insbesondere durch Geheimdienste) zu Zwecken der nationalen Sicherheit regelt**, legitimiert und so weit wie möglich auf das notwendige Maß begrenzt.

Hierfür muss das gegenseitige transatlantische Vertrauen gestärkt werden, wozu auch die in jüngster Zeit regelmäßig abgehaltenen Treffen des EU-US Trade and Technology Council (TTC) beitragen könnten. **Der EU-US TTC sollte daher nach den anstehenden Wahlen in der EU und den USA unbedingt fortgeführt werden.** Allerdings erscheint eine weitere Begrenzung der US-Überwachungsbefugnisse angesichts der gestiegenen globalen Bedrohungen für die nationale Sicherheit derzeit politisch wenig wahrscheinlich. Trotzdem müssen weitere Schritte unternommen werden, um EU-Unternehmen, die für den Erhalt ihrer Wettbewerbsfähigkeit auf die Nutzung von US-Cloud-Lösungen und -Produkten angewiesen sind, auch langfristig von der investitionshemmenden Rechtsunsicherheit oder gar datenschutzrechtlichen Illegalität ihres Handelns zu befreien. Würden Datenzugriffe und -weitergaben an Drittlandsbehörden, die zum Schutz der nationalen Sicherheit unverzichtbar sind, durch internationale Abkommen wechselseitig legitimiert, handelten Unternehmen, die solchen rechtlich zulässigen Ersuchen von Drittlandsbehörden nachkommen, datenschutzrechtlich legal. Solange kein derartiges Abkommen existiert, ist für Unternehmen, die nicht auf die Funktionalitäten der Cloud-Lösungen von US-Anbietern verzichten können oder wollen, die Nutzung von Treuhandlösungen am rechtssichersten, bei denen europäische Treuhänder sicherstellen, dass keine Daten in die USA fließen.[26] Diese sollen es ermöglichen, die Vorzüge der US-Clouds (weiter) zu nutzen und zugleich die Defizite der US-Clouds zu vermeiden.[27] Bei der Auswahl ihres Cloud-Anbieters sollten sich Cloud-Nutzer jedoch nicht allein auf den Marketingbegriff „souveräne Cloud“ verlassen, sondern Angebote konkret hinterfragen und genau prüfen.

[25] Gleiches gilt, um europäischen Unternehmen sonstige Datenübermittlungen zum Zweck des internationalen Handels zu ermöglichen.

[26] Derartige Angebote entstehen bereits (wieder), so etwa die T-Systems Sovereign Cloud in Zusammenarbeit mit Google (https://www.t-systems.com/de/de/souveraene-cloud/loesungen/sovereign-cloud-powered-by-google-cloud) oder die Delos Cloud von SAP und Microsoft für den öffentlichen Dienst (https://www.deloscloud.de/index.html). Bei beiden handelt es sich um Kooperationen europäischer Cloud-Anbieter mit US-Anbietern, bei denen die „Europäer“ bzw. die deutschen Tochterunternehmen (in den zuvor genannten Beispielen die deutschen Tochterunternehmen von T-Systems und SAP) die alleinige Kontrolle über die Daten und die Schlüssel für die Entschlüsselung innehaben. Siehe zu der Problematik bereits Hoffmann, A., Unzulässigkeit der Datenübermittlung in die USA, cepStudie vom 26.01.2021, S. III, 43, 57, abrufbar unter https://www.cep.eu/de/eu-themen/details/unzulaessigkeit-der-datenuebermittlung-in-die-usa-cepstudie.html.

[27] Sieger, H., Digitale Souveränität: Warum auch die Selbstbestimmung dazu gehört, 7. Juni 2023, abrufbar unter https://www.digitalbusiness-cloud.de/digitale-souveraenitaet-warum-auch-die-selbstbestimmung-dazu-gehoert-a-08e4a0d4f1527c2f9b3a949db429617d/.

DSGVO

RECHTSUNSICHERHEIT ALS HEMMSCHUH FÜR DEN B2B-DATENAUSTAUSCH UND DIE DIGITALISIERUNG

Datenschutzbedenken (20,42%) und Rechtsunsicherheit (14,03%) sind die von den Unternehmen am häufigsten genannten Hindernisse für den vom Data Act angestrebten Austausch von Daten, die von vernetzten Produkten wie intelligenten Industriemaschinen erzeugt werden, zwischen Geschäftspartnern. Weitere Probleme sind neben dem (noch) fehlenden Zugang zu vom Hersteller kontrollierten Daten der unzureichende Schutz von Geschäftsgeheimnissen und die mangelnde Interoperabilität von Daten und Anwendungen. Bemerkenswerterweise gab ein Drittel (33,49%) der Befragten auf die Frage nach dem Bedarf an weiteren Regelungen an, dass die Entwicklung von Standards oder Lösungen erforderlich ist, die die Anwendung der DSGVO ausschließen, wie etwa Anonymisierung und Nutzung synthetischer Daten. Auch die Forderung nach verbesserten Interoperabilitätsregeln auch für Daten und Anwendungen (28,47%) unterstreicht die Notwendigkeit, technische und regulatorische Barrieren abzubauen, um den Zugang zu und die (gemeinsame) Nutzung von Daten über verschiedene Plattformen und Systeme hinweg zu gewährleisten.

Insgesamt sind die Reaktionen der Befragten auf aktuelle EU-Initiativen wie den Data Act und den Data Governance Act gemischt. Während die Hälfte der Befragten angibt, dass diese zumindest teilweise (41,21%) zur Stärkung des B2B-Datenaustauschs beitragen werden, bleibt ein großer Teil (35,73%) unsicher über die Auswirkungen dieser Regelungen. Hierbei zeigt sich eine interessante sektorale Differenzierung (Abbildung 1). Am optimistischsten, was das Potenzial der aktuellen Initiativen der EU zu Datenaustausch und Datenwirtschaft angeht, sind **Banken, Software-Entwickler sowie Vertreter der Gesundheitsbranche** [letztere vermutlich aufgrund des geplanten Europäischen Gesundheitsdatenraums (EHDS)[28]]. Vergleichsweise **skeptisch sind hingegen Unternehmen aus den Branchen Medien und Dienstleistungen und dem öffentlichen Sektor.**

Werden die aktuellen EU-Initiativen den B2B-Datenaustausch stärken?

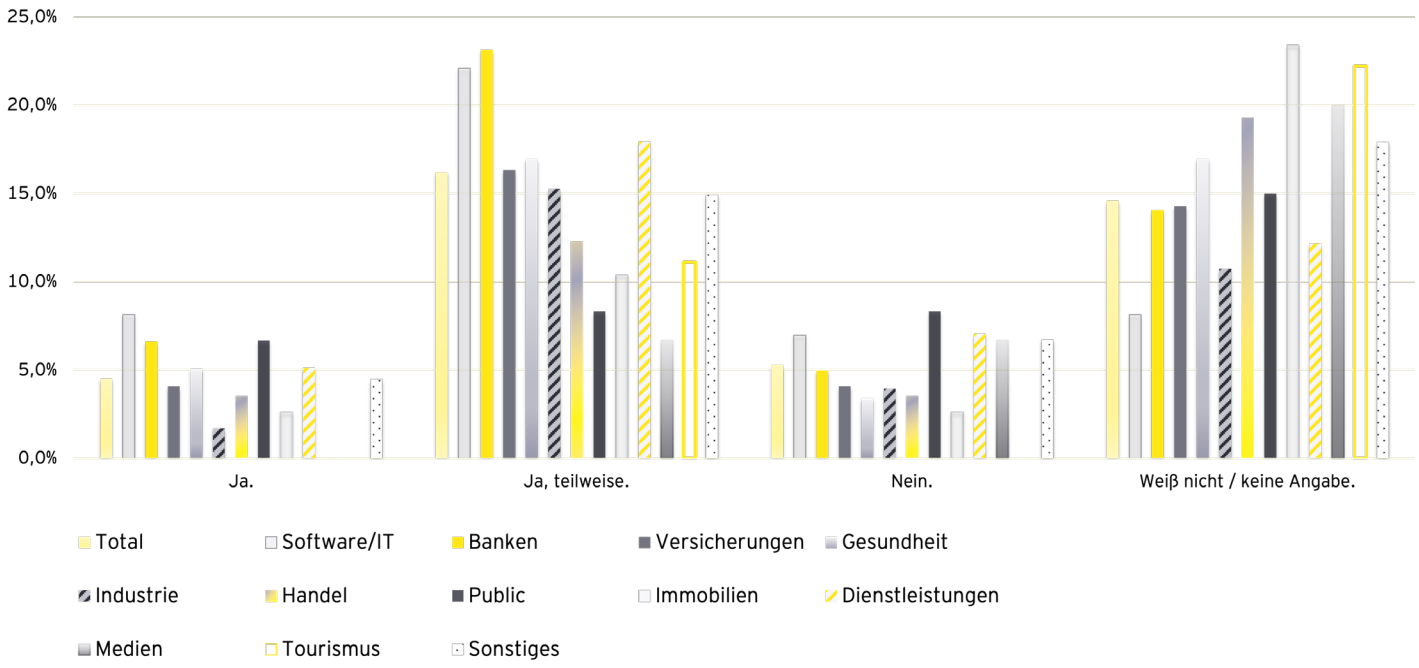


ABBILDUNG 1

[28] Vgl. etwa https://health.ec.europa.eu/ehealth-digital-health-and-care/european-health-data-space_en.

Insgesamt zeigen diese Umfrageergebnisse, dass sich viele europäische Unternehmen generell durch die DSGVO und die hierzu ergangenen Gerichtsentscheidungen wie die Schrems-Urteile stark belastet fühlen. 12,48% halten die Vorgaben der DSGVO generell für zu streng, 22,6% für nicht praxistauglich. Für 15,73% ist das Zusammenspiel der DSGVO mit der EU-Digitalregulierung zu unklar und für 13,02% ist die Rechtsunsicherheit in Bezug auf Datentransfers eine große Belastung. Lediglich 2,71% der Unternehmen geben an, dass ihnen die DSGVO sogar eine Chance, etwa einen Wettbewerbsvorteil, biete. Positiv zu sehen ist, dass sich 11,57% mittlerweile ganz gut auf die Anforderungen der DSGVO eingestellt haben. 9,22% sind sogar der Meinung, dass die DSGVO häufig zu Unrecht als Problem dargestellt wird. Klar ist: **die Unternehmen möchten durchaus datenschutzfreundliche Technologien einsetzen, die dennoch einen effizienten Datenaustausch ermöglichen – aber wissen nicht genau, wie ihnen diese Quadratur des Kreises gelingen soll**.

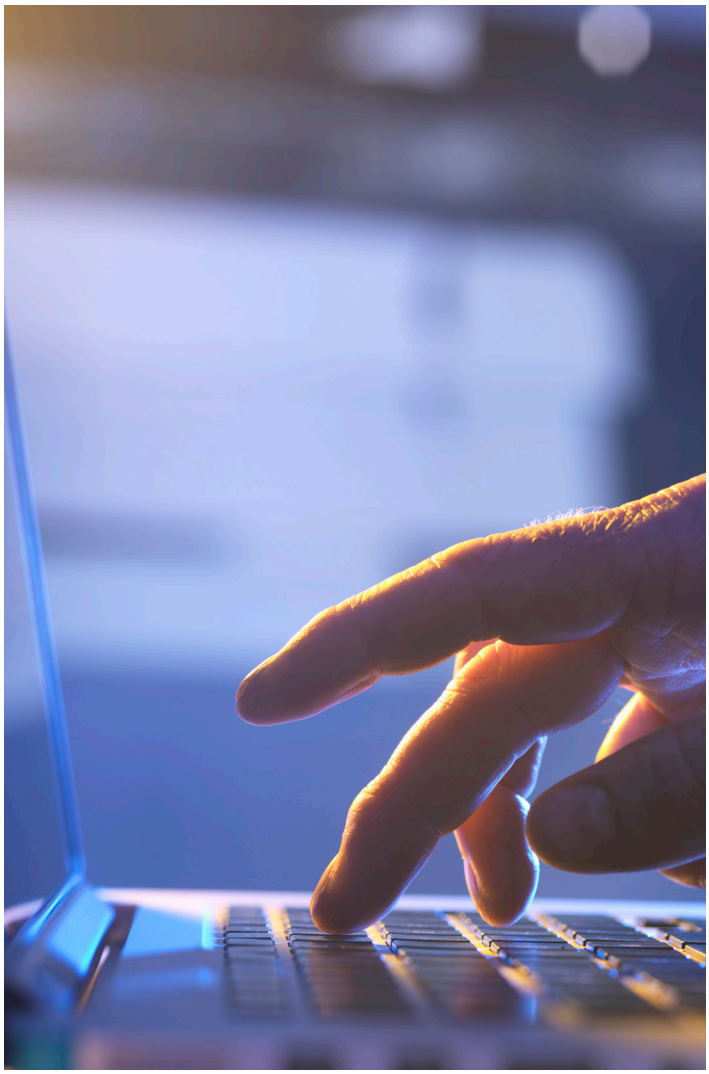
Dass die DSGVO den Datenschutz in Europa verbessert und einheitlicher gestaltet hat und anderen Regionen der Welt mittlerweile als Vorbild dient, ist unbestreitbar, aber unsere Umfrageergebnisse deuten darauf hin, dass **gewisse negative wirtschaftliche Folgewirkungen des strengen Datenschutzniveaus möglicherweise unbeabsichtigt unterschätzt wurden.** Dies steht im Einklang mit der jüngsten ökonomischen Forschung, die gezeigt hat, dass die durch die Verordnung verursachten höheren Kosten für Entwickler einige Unternehmen zum Marktaustritt verleitet und die Entwicklung neuer wertvoller Anwendungen verhindert haben.[29] Diesen Berechnungen zufolge stieg die Quote der Marktaustritte von App-Entwicklern nach der Einführung der Datenschutz-Grundverordnung um mehr als ein Drittel, während die Quote der Markteintritte um 47,2% zurückging. Andere Untersuchungen zeigen, dass EU-Firmen als Reaktion auf die DSGVO ihre Datenspeicherung um 26% und ihre Datenverarbeitung um 15% gegenüber vergleichbaren US-Firmen verringert haben und damit weniger „datenintensiv" geworden sind[30] – dies könnte sich im Zeitalter von Big Data-basierter Künstlicher Intelligenz rächen. Unabhängig von den Vorteilen, die die DSGVO mit sich bringt, verursacht sie in ihrer aktuellen Form offenbar erhebliche Kosten für Unternehmen.

Was folgt daraus? Die EU muss schnellstmöglich Initiativen ergreifen, um Rechtsunsicherheiten im Zusammenhang mit der DSGVO zeitnah zu beseitigen oder zumindest deutlich zu verringern und so drohenden Wettbewerbsnachteilen für europäische Unternehmen entgegenzuwirken. Datenschutzaufsichtsbehörden und die Kommission müssen die Unternehmen noch stärker bei der Einhaltung der Anforderungen der DSGVO unterstützen, insbesondere durch praxisorientierte und klare Leitlinien und Auslegungshilfen. Die EU-Mitgliedstaaten müssen dafür Sorge tragen, dass sich ihre nationalen Datenschutzbehörden im Europäischen Datenschutzausschuss schneller als bislang auf einheitliche Leitlinien und Empfehlungen einigen. Denn eine flexiblere Entwicklung von Leitlinien für die Rechtsanwendung ist unabdingbar, um schnell auf technologische Entwicklungen wie generative KI reagieren zu können. **Leitlinien und „Orientierungshilfen" sollten generell aber nicht lediglich rechtliche Konflikte aufzeigen, sondern auch Ansätze zu ihrer Lösung vorschlagen.**

[29] Janßen, R., Kesler, R., Kummer, M.E, und Waldfogel, J., GDPR and the Lost Generation of Innovative Apps, NBER Working Paper No. 30028, May 2022, abrufbar unter https://www.nber.org/system/files/working_papers/w30028/w30028.pdf.

[30] Demirer, M., Hernández, D., Li, D., und Peng, S., Firm Responses to the EU's Data Privacy Requirements, NBER Working Paper No. 32146, February 2024, abrufbar unter https://www.nber.org/papers/w32146.

Dass die genannten Unsicherheiten beseitigt werden müssen, wird besonders deutlich mit Blick auf den wachsenden Einfluss Künstlicher Intelligenz, welche ebenfalls an zahlreichen Stellen mit dem Datenschutz in Konflikt gerät. Europäische Unternehmen können im globalen Wettbewerb nur bestehen und ihre Chance auf eine Führungsrolle im Bereich KI wahren, wenn **ein rechtssicherer und innovationsfreundlicher Umgang mit der DSGVO entwickelt und ermöglicht wird**. Dies bedeutet nicht von vornherein einen Verzicht auf Datenschutz, sondern kann sogar – wie etwa bei der Nutzung anonymisierter oder synthetischer Daten – ein Plus an Privatsphäre bedeuten.



Unter anderem muss geklärt werden, wie Unternehmen mehr anonymisierte oder synthetische Daten nutzen können – etwa für das KI-Training – und mit aktuellen und künftigen Re-Identifizierungs- und damit Datenschutzrisiken[31] umzugehen haben. Anonymisierte Daten sind für Unternehmen besonders interessant, weil die Regeln der DSGVO mangels fortbestehenden Personenbezugs für diese Daten nicht gelten. **Es bedarf dringend einer Klarstellung, ab wann Daten als anonymisiert gelten, etwa durch Entwicklung und Festlegung einheitlicher und praktikabler Standards, bei deren Einhaltung ein hinreichender Anonymisierungsgrad vermutet wird.**[32]

Zudem muss der **Konflikt zwischen dem Grundsatz der Datensparsamkeit und dem für eine erfolgreiche Datenwirtschaft und für das adäquate Training einer qualitativ hochwertigen KI so wichtigen Datenreichtum rechtssicher aufgelöst werden**.[33] In diesem Zusammenhang ist der Ansatz der französischen Datenschutzbehörde CNIL zu begrüßen, die in ihren jüngsten Empfehlungen für die Entwicklung von KI-Systemen die Auffassung vertritt, dass das Prinzip der Datenminimierung es nicht verbietet, einen Algorithmus mit sehr großen Datenmengen zu trainieren, solange nur Daten verwendet und gesammelt werden, die für die Entwicklung des Systems nützlich sind.[34] **Wo immer praktikabel, sollten Kommission, Behörden und Gerichte Möglichkeiten einer derart innovationsfreundlichen Auslegung und Anwendung der DSGVO ausloten bzw. sich dieser nicht länger verschließen.** Soweit die Rechtsunsicherheit allein durch Leitlinien und Auslegungshilfen nicht beseitigt werden kann und eine zeitnahe Klärung durch den EuGH nicht aussichtsreich erscheint oder Innovationshemmnisse nicht anderweitig beseitigt werden können, sollten auch punktuelle Änderungen der DSGVO erwogen werden.

[31] Beduschi, A., Synthetic data protection: Towards a paradigm change in data regulation?, 14 February 2024, abrufbar unter https://journals.sagepub.com/doi/10.1177/20539517241231277.

[32] Vgl. etwa Specht-Riemenschneider, L., BT-Drs. 19/26450 et al., S. 5, 16f., abrufbar unter https://www.bundestag.de/resource/blob/823800/6f11b79c8288a181eaec827c4361825b/Stellungnahme-Specht-Riemenschneider-data.pdf.

[33] Der Grundsatz der Datensparsamkeit ist zwar wichtig für den Schutz der Privatsphäre, kann aber die Entwicklung und das Training leistungsfähiger KI-Systeme behindern, da diese oft große Datenmengen benötigen. Um europäische Unternehmen dabei zu unterstützen, im Bereich der KI führend zu werden, sollte die EU daher einen ausgewogeneren Ansatz verfolgen, der sowohl den Datenschutz stärkt als auch den Anforderungen der KI-Technologie gerecht wird.

[34] CNIL, Développement des systèmes d'IA : les recommandations de la CNIL pour respecter le RGPD, 8. April 2024, 5e étape, abrufbar unter https://www.cnil.fr/fr/developpement-des-systemes-dia-les-recommandations-de-la-cnil-pour-respecter-le-rgpd.

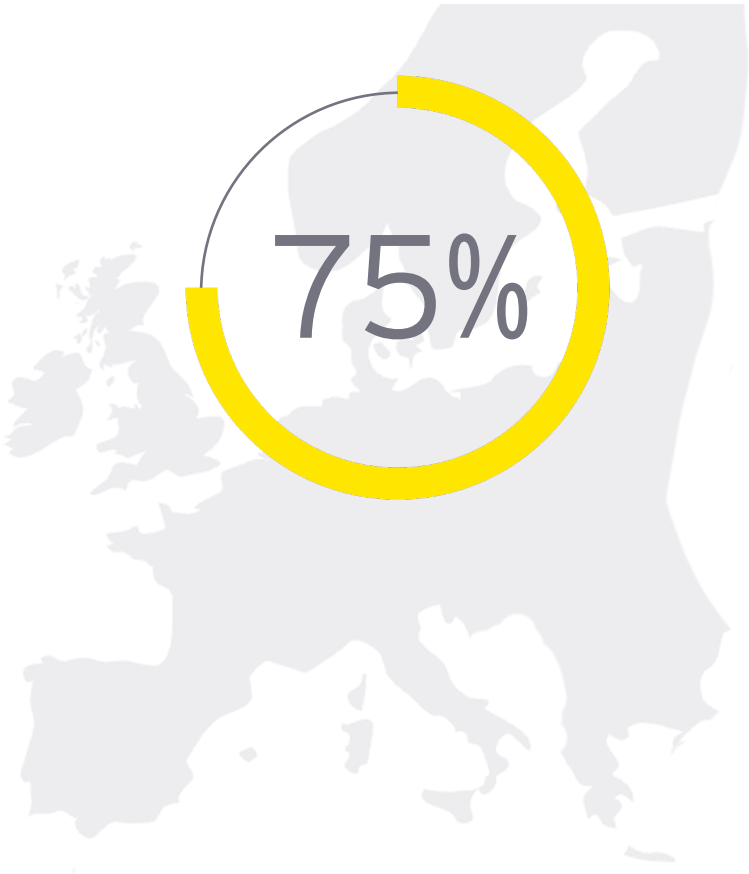
EU-DIGITALREGULIERUNG IN IHRER GÄNZE

UNVERSTÄNDLICHE, KOMPLEXE & VERSCHACHTELTE RECHTSLAGE

Die Umfrageergebnisse zeigen, dass der Bekanntheitsgrad der verschiedenen digitalen Regulierungsinitiativen der EU und ihre Relevanz für die Unternehmen recht unterschiedlich sind. Der AI Act und der Data Act sind am bekanntesten und werden als besonders relevant eingestuft, was wenig erstaunt, da diese Rechtsakte als horizontale Regelungen – im Gegensatz zur Regulierung einzelner Produkte oder Sektoren – erhebliche Auswirkungen auf die Geschäftstätigkeit vieler europäischer Unternehmen haben werden. Gleichwohl zeigt der niedrige Durchschnittswert für die Verständlichkeit der EU-Digitalregulierung in ihrer Gänze (Mittelwert 3,31 auf einer Skala von 10), **dass die Komplexität der Rechtsakte – und ihre teilweise Widersprüchlichkeit oder unbekannten Interdependenzen – für die Unternehmen eine erhebliche Hürde darstellt**. Auch dies verwundert nicht, da die in den letzten Jahren zahlreich erlassenen EU-Digitalgesetze in erheblicher Weise miteinander verzahnt sind und sich ihre Regelungen teilweise überlappen, etwa bestimmte Informations- und Dokumentationspflichten sowie die Portabilitätspflichten in DSGVO und im Data Act.

Die Chancen, die sich für die Unternehmen aus der EU-Digitalregulierung ergeben, werden von den Befragten mit einem Mittelwert von 5,19 auf einer Skala von 10 bewertet. Dies stärkt die Erkenntnis, dass die Unternehmen das Potenzial der digitalen Regulierung zwar sehen, aber noch Unsicherheiten über die konkreten Auswirkungen und Vorteile für ihr spezifisches Geschäft bestehen. Die Bereitschaft, digitale Lösungen in Unternehmen zu entwickeln oder einzusetzen, hängt stark von der Rechtssicherheit ab. **Eine überwältigende Mehrheit von mehr als 75 Prozent der Befragten gibt an, dass sie mehr digitale Lösungen entwickeln oder nutzen würden, wenn es mehr Rechtssicherheit gäbe**, wie dies im Einklang mit der DSGVO möglich ist („Ja, definitiv“: 45,13%; „Ja, aber nur geringfügig“: 30,26%).

> DIE MEHRHEIT DER BEFRAGTEN GIBT AN, DASS SIE MEHR DIGITALE LÖSUNGEN ENTWICKELN ODER NUTZEN WÜRDEN, WENN ES MEHR RECHTSSICHERHEIT GÄBE.



Was folgt daraus? Die Umfrageergebnisse zeigen, dass neben der nötigen Rechtssicherheit in puncto Datenschutz **auch ein verständliches Regelungsumfeld ein entscheidender – und bislang wohl zu sehr vernachlässigter – Faktor für die wettbewerbsfähige Innovation in europäischen Unternehmen ist**. Eine zu komplexe Rechtslage und Rechtsunsicherheiten machen häufig kostspielige Rechtsberatung und Rechtsstreitigkeiten erforderlich und behindern den technologischen Fortschritt, weil Unternehmen aus Angst vor unrechtmäßigem Handeln auf Innovationen verzichten. Die EU sollte daher über die oben genannten Empfehlungen hinaus weitere Maßnahmen ergreifen, um die Verständlichkeit ihrer Digitalregulierung zu verbessern und auch insoweit die Rechtssicherheit zu erhöhen. Um den „Dschungel" der EZ-Digitalregulierung zu lichten, **sollte die Kommission erstens alle EU Digitalrechtsakte in einem EU-Regelwerk zusammenfassen und ihr Zusammenspiel untereinander sowie mit der DSGVO erläutern**.

Hilfreich wären auch Hinweise, wie Unternehmen Synergien nutzen können, um ähnliche oder sich überschneidende Verpflichtungen (z.B. im AI Act und in der DSGVO) zu erfüllen. Zweitens müssen **fortbestehende Unklarheiten in den einzelnen EU-Rechtsakten aufgelöst** werden. Insbesondere müssen die **Digitalrechtsakte besser mit der DSGVO abgestimmt und geklärt werden, wie sie datenschutzkonform angewendet werden können**. Drittens sollten neben EU-weiten Leitlinien und Auslegungshilfen auch **spezifische Schulungen** für Unternehmen unterstützt werden, damit diese die einschlägigen Rechtsvorschriften verstehen und effektiv anwenden können. Nur so kann sichergestellt werden, dass Unternehmen die Vorteile eines einheitlichen europäischen Rechtsrahmens für die digitale Transformation ausschöpfen können.

SCHLUSSFOLGERUNG

DIE CHANCEN DER DIGITALISIERUNG BESSER NUTZEN

Die Ergebnisse unserer Umfrage zeigen deutlich, **dass mehr Wettbewerb im Cloud-Sektor und technologische Souveränität in Europa nicht allein durch Regulierung entstehen werden – die neuen Regeln müssen verstanden und rechtssicher in die Praxis umgesetzt werden können, damit heimische Unternehmen innovativ und wettbewerbsfähig agieren können**. Dies ist auch und gerade wichtig, damit europäische Unternehmen datenbasierte Geschäftsmodelle und Anwendungen künstlicher Intelligenz entwickeln und nutzen und ihre Chance auf eine Führungsrolle in diesen Bereichen wahren können. Unsere Analyse der Antworten von rund 1.000 Unternehmen legt einige gezielte Maßnahmen für die nächste Kommission nahe, um die Chancen der Digitalisierung besser zu nutzen.
Die folgenden Forderungen sollten von den politischen Entscheidungsträgern nach der Europawahl berücksichtigt werden:

1.

Cloud-Switching weiter erleichtern:

- **Konsequente Anwendung des Data Act,** um den Wechsel zwischen Datenverarbeitungsdiensten zu erleichtern. Offene und interoperable Standards können den Datenaustausch erleichtern und die Abhängigkeit von einzelnen dominanten Anbietern aus den USA verringern.
- **Förderung europäischer Cloud-Anbieter durch gezielte Maßnahmen**, um eine echte Alternative zu US-Diensten zu bieten und die Abhängigkeit von diesen zu reduzieren.
- **Rechtzeitige Veröffentlichung marktrelevanter und praxistauglicher Standardvertragsklauseln für Cloud-Computing-Verträge** durch die Kommission vor dem Anwendungsbeginn des Data Act, um Unternehmen Unterstützung und Rechtssicherheit zu bieten.
- **Zusätzliches Ausloten wettbewerbspolitischer und industriepolitischer Eingriffe**, um die Marktdominanz großer Cloud-Anbieter abzuschwächen und die Verhandlungsmacht kleiner und mittlerer Unternehmen zu stärken.

2.

Langfristige Rechtssicherheit bei Datentransfers schaffen:

- **Förderung internationaler Abkommen zur Regelung behördlicher Datenzugriffe zu Zwecken der nationalen Sicherheit** – aufgrund der Gefahr, dass der Angemessenheitsbeschluss für die USA aufgehoben wird, insbesondere zwischen den EU-Mitgliedstaaten und den USA.
- **Ersatzweise: Förderung von Treuhand-Cloud-Lösungen**, bei denen europäische Treuhänder sicherstellen, dass keine Daten in die USA fließen, um europäischen Unternehmen die Nutzung wirtschaftlich unverzichtbarer Funktionalitäten von US-Cloud-Anbietern zu ermöglichen.

3.

Einen rechtssicheren, innovationsfreundlichen Umgang mit der DSGVO ermöglichen:

- **Unternehmen noch stärker bei der Einhaltung der DSGVO unterstützen.**

- **Mehr Rechtssicherheit schaffen**, etwa durch flexiblere Bereitstellung von Auslegungshilfen und praxisorientierten, klaren Leitlinien, die nicht nur Konflikte aufzeigen, sondern auch Lösungsansätze vorschlagen. Eine schnellere Einigung auf Datenschutzleitlinien innerhalb des Europäischen Datenschutzausschusses sicherstellen.

- **Klarstellen, wie synthetische Daten rechtssicher genutzt werden können und ab wann Daten als anonymisiert gelten**, etwa durch Entwicklung und Festlegung einheitlicher und praktikabler Standards, bei deren Einhaltung ein hinreichender Anonymisierungsgrad vermutet wird.

- **Den Konflikt zwischen dem Grundsatz der Datensparsamkeit und Big Data rechtssicher auflösen.** Wo immer praktikabel, **Möglichkeiten einer innovationsfreundlichen Auslegung und Anwendung der DSGVO ausloten**.

4.

Komplexe EU-Digitalregulierung verständlich machen:

- Alle **Digitalrechtsakte in einem EU-Regelwerk zusammenfassen und ihr Zusammenspiel untereinander sowie mit der DSGVO erläutern.**
- **Fortbestehende Unklarheiten in den einzelnen EU-Digitalrechtsakten auflösen und diese besser mit der DSGVO abstimmen.**
- Neben **EU-weiten Leitlinien und Auslegungshilfen** auch **Schulungsprogramme** implementieren, um ein besseres Verständnis und eine korrekte Anwendung der Digitalrechtsakte durch die Unternehmen zu erreichen.

EY UND CEP

IHRE ANSPRECHPARTNER:INNEN

AUTOR:IN

Dr. Anja Hoffmann, LL.M. Eur., cep,
Wissenschaftliche Referentin

Dr. Anselm Küsters, LL.M., cep,
Fachbereichsleiter Digitalisierung
und Neue Technologien

MITWIRKENDE

IN ALPHABETISCHER REIHENFOLGE

- Christian Alfter, EY
- Hermann Gauß, EY
- Dr. Cornelia Kindler, EY
- Jürgen Obal, EY
- Faezeh Shokrian, EY
- Prof. Dr. Henning Vöpel, cep

IMPRESSUM

Herausgeber

EY GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft

cep | Centrum für Europäische Politik

Bildquelle

Getty Images International

Design

Enablement & Communication | Assurance Research & Development
EY GmbH & Co. KG
Wirtschaftsprüfungsgesellschaft

WEBLINKS

cep Centrum für Europäische Politik

https://www.cep.eu/

EY Building a better working world

https://www.ey.com/de_de
https://www.ey.com/de_de/public-policy

EY | Building a better working world

Mit unserer Arbeit setzen wir uns für eine besser funktionierende Welt ein. Wir helfen unseren Kunden, Mitarbeitenden und der Gesellschaft, langfristige Werte zu schaffen und das Vertrauen in die Kapitalmärkte zu stärken.

In mehr als 150 Ländern unterstützen wir unsere Kunden, verantwortungsvoll zu wachsen und den digitalen Wandel zu gestalten. Dabei setzen wir auf Diversität im Team sowie Daten und modernste Technologien in unseren Dienstleistungen.

Ob Assurance, Tax & Law, Strategy and Transactions oder Consulting: Unsere Teams stellen bessere Fragen, um neue und bessere Antworten auf die komplexen Herausforderungen unserer Zeit geben zu können.

In Deutschland finden Sie uns an 20 Standorten.

ey.com