wissenschaftliches institut für die
digitalisierung der arbeitswelt

Strategische Überlegungen zur Zukunft der europäischen Datenschutzaufsicht

- unter besonderer Berücksichtigung der Aufsicht in Deutschland -

erstellt auf Ansuchen von
Europäischen und US-amerikanischen Unternehmen

von
Dr. Stefan Brink
Geschäftsführender Direktor
des Wissenschaftlichen Instituts für die Digitalisierung der Arbeitswelt / Berlin
Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg (a.D.)

Juni 2025

Gegenwart und Zukunft der europäischen Datenschutzaufsicht unter der DS-GVO: Strategische Überlegungen

Zusammenfassung

Die europäische Datenschutzlandschaft befindet sich an einem kritischen Punkt, da die EU-Datenschutz-Grundverordnung (DS-GVO) bei ihrer Umsetzung vor erheblichen Herausforderungen steht. Trotz ihrer Zielsetzung, das Vertrauen in die digitale Wirtschaft zu fördern, wird die DS-GVO wegen ihrer mangelnden Klarheit, ihrer uneinheitlichen und teilweise unausgewogenen Durchsetzung und unzureichenden Koordinierung zwischen den nationalen Behörden und der Europäischen Kommission kritisiert, auch im Hinblick auf das neuen EU-Datenrecht (DSA/DA/AI Act). Dies hat zu Unsicherheiten und Hindernissen für Unternehmen geführt, insbesondere für kleine und mittlere Unternehmen (KMU).

Die derzeitige Durchsetzung der DS-GVO ist gekennzeichnet durch eine Politisierung und Radikalisierung der Aufsicht und einen Wettlauf der Aufsichtsbehörden um die strengste Position. Dies führt zu einem „Datenschutz-Absolutismus“, bei dem gegenläufige Interessen und Grundprinzipien gegenüber dem Datenschutz nicht mehr angemessen wahrgenommen werden. Der Mangel an Verantwortlichkeit, Transparenz und Kohärenz in den Entscheidungsprozessen hat zu einer Kultur der Vorsicht bei den Unternehmen geführt, welche Innovationen erstickt und das Wachstumspotenzial begrenzt.

Die Ursachen für diese negativen Entwicklungen lassen sich auf die Mängel der Datenschutz-Grundverordnung selbst zurückführen, einschließlich ihres restriktiven Ansatzes bei der Datenverarbeitung, und der Zuweisung einer zentralen Machtposition an unabhängige Institutionen, die einseitig die ihnen anvertrauten Interessen begünstigen. Darüber hinaus hat die mangelhafte Struktur des Europäischen Datenschutzausschusses (EDSA) diese Probleme noch verschärft.

In Deutschland wird diese schwierige Situation von vier weiteren Faktoren beeinflusst: von der Sonderstellung, die sich deutsche Aufsichtsbehörden im europäischen Verbund zuordnen, von den zwei grundlegend unterschiedlichen Datenschutzkulturen in Deutschland, von der föderalen Struktur der Datenschutzaufsicht (Vielfalt und Konkurrenz) und von der äußerst unterschiedlichen Ausstattung der Landesdatenschutzbehörden.

Um diese Herausforderungen zu bewältigen, ist ein vielschichtiger Ansatz erforderlich, der sowohl kurzfristige als auch mittel- bis langfristige Lösungen umfasst. Zu den kurzfristigen Maßnahmen gehören die Erhöhung der Transparenz und Vorhersehbarkeit von Entscheidungsprozessen, die Sicherstellung, dass Innovation und Wettbewerbsfähigkeit in das Mandat der Aufsichtsbehörden aufgenommen werden, und die Verbesserung der Zusammenarbeit zwischen föderalen Regulierungsbehörden.

Mittel- bis langfristig sind substanziellere Reformen erforderlich, einschließlich der Annahme zusätzlicher Verfahrensregeln für die Durchsetzung der Datenschutz-Grundverordnung (abweichend vom aktuellen Vorschlag der Kommission), die Stärkung der Verantwortlichkeit der Datenschutzbehörden, ein angemessenes Verhältnis zwischen dem Datenschutz und anderen Grundrechten und die Einführung einer stärkeren Rolle für einen differenzierten und flexibleren risikobasierten Ansatz.

Letztlich ist die Stärkung der Position der EU-Kommission entscheidend für die Lösung des Durchsetzungsproblems. Die Zuweisung einer führenden Position an die Kommission im EDSA, möglicherweise auch in Form einer Europäischen Digitalisierungsbehörde, würde einen effektiveren und ausgewogeneren Ansatz für die künftige Datenschutzregulierung bieten.

Durch die Bewältigung dieser Herausforderungen und die Übernahme eines differenzierteren Ansatzes für den Datenschutz kann die EU eine Kultur der Innovation und des Wachstums fördern und dabei gleichzeitig die Rechte und Freiheiten des Einzelnen auf vorbildliche Weise schützen.

Einführung

Die Datenschutz-Grundverordnung (DS-GVO) ist ein Meilenstein in der Geschichte des Datenschutzes, sie schützt die personenbezogenen Daten von Einzelpersonen innerhalb der Europäischen Union (EU) auf einem weltweit einzigartigen Niveau. Im siebten Jahr der DS-GVO hat sich die Verordnung weit über die EU hinaus etabliert, doch ihre Durchsetzung wird zunehmend als problematisch und geschäfts- und technologiefeindlich wahrgenommen. Derzeit findet auf nationaler und europäischer Ebene eine intensive Debatte über die Rolle der DS-GVO für Innovation und Wettbewerbsfähigkeit in der EU statt.
Diese Analyse wird den aktuellen Stand der europäischen Datenschutzaufsicht und -regulierung untersuchen, Fehlentwicklungen aufzeigen, die Kernpunkte der Datenschutz-Grundverordnung beleuchten sowie mögliche Lösungen skizzieren.

Aktueller Stand der Europäischen Datenschutz-Grundverordnung

Die europäische Datenschutzlandschaft befindet sich an einem kritischen Punkt. Immer mehr Stimmen aus Wirtschaft und Politik fordern ein Überdenken der derzeitigen Umsetzung der DS-GVO. Angesichts der rasanten Entwicklung der globalen digitalen Wirtschaft mehren sich die Bedenken, dass die DS-GVO in ihrer derzeitigen Form ihrer Anwendung Europas Wettbewerbsfähigkeit und Innovation eher behindert als fördert. Vor diesem Hintergrund haben mehrere einflussreiche Berichte die Notwendigkeit eines ausgewogeneren Ansatzes für den Datenschutz hervorgehoben, der das komplexe Zusammenspiel von Verbraucherrechten, Geschäftsanforderungen und technologischem Fortschritt berücksichtigt.

Der Enrico-Letta-Bericht "Viel mehr als ein Markt" hebt die Bedeutung der DS-GVO für die Förderung des Vertrauens in die digitale Wirtschaft hervor. Er zeigt jedoch auch erhebliche Herausforderungen bei der Umsetzung auf, darunter eine uneinheitliche Durchsetzung, mangelnde Klarheit und eine unzureichende Koordinierung zwischen den nationalen Behörden und der Europäischen Kommission. Diese Probleme begrenzen die Entfaltung des vollen Potenzials der DS-GVO und schaffen Unsicherheit und Hindernisse für Unternehmen aller

Größen. Um diese Hindernisse auszuräumen, ist laut diesem Bericht eine Korrektur erforderlich, um die Durchsetzung zu verbessern, klarere Leitlinien bereitzustellen und die internationale Zusammenarbeit zu verstärken - um letztendlich sicherzustellen, dass die DS-GVO ihre beabsichtigten Ziele der Förderung von Vertrauen, Innovation und Wachstum in der digitalen Wirtschaft tatsächlich erreicht.

Der zweite Bericht der Europäischen Kommission über die Anwendung der Datenschutz-Grundverordnung (DSGVO) zeigt erhebliche Herausforderungen auf, die eine Korrektur ihrer Umsetzung erforderlich machen. Der Bericht zeigt, dass die DS-GVO, obwohl seit 2018 in Kraft, weiterhin mit einer uneinheitlichen Durchsetzung, unzureichenden Ressourcen für die Datenschutzbehörden und einer mangelnden Harmonisierung zwischen den Mitgliedstaaten zu kämpfen hat. Die Europäische Kommission identifiziert zu Recht unterschiedliche Auslegungen der DS-GVO durch nationale Aufsichtsbehörden als Haupthindernis für die einheitliche Anwendung der DS-GVO in der EU. Darüber hinaus stellen die Komplexität und der bürokratische Aufwand der Verordnung ein Hindernis für kleine und mittlere Unternehmen dar, während das Bewusstsein der Bürger über ihre Rechte im Rahmen der DS-GVO nach wie vor gering ausgeprägt ist. Darüber hinaus gibt die rasche Entwicklung von Technologien wie der künstlichen Intelligenz Anlass zur Sorge hinsichtlich der Wirksamkeit der DS-GVO bei der Bewältigung dieser aktuellen Probleme und dringenden sozialen und wirtschaftlichen Bedürfnisse. Um diese Herausforderungen zu bewältigen und sicherzustellen, dass die DS-GVO wirksam und relevant bleibt, hält es die EU-Kommission insbesondere für notwendig, ihre ordnungsgemäße Umsetzung zu verbessern und einen kohärenteren und harmonisierten Ansatz für den Datenschutz in der gesamten EU zu fördern, der den freien Verkehr personenbezogener Daten und eine Kohärenz mit der digitalen Strategie der EU ermöglicht.

Der Bericht über die Wettbewerbsfähigkeit der EU, den der ehemalige Präsident der Europäischen Zentralbank Mario Draghi im Auftrag des Präsidenten der EU-Kommission verfasst hat, bewertet die DS-GVO als zweischneidiges Schwert für die europäische Wirtschaft. Während der Bericht die Vorzüge der DS-GVO bei der Stärkung der Privatsphäre und des Vertrauens der Verbraucher anerkennt, unterstreicht er die Notwendigkeit eines ausgewogeneren Ansatzes für den Datenschutz und betont die Bedeutung der datengesteuerten Innovation für die EU-Wirtschaft. In dem Bericht wird auf die erheblichen Kosten hingewiesen, welche die DS-GVO vor allem für Start-ups und kleine bis mittlere Unternehmen (KMU) mit sich bringt[1]. Der Bericht beklagt, dass diese Belastungen Innovation und Wachstum behindern und es europäischen Unternehmen erschweren, auf dem globalen Markt zu konkurrieren[2]. Der Bericht kommt zu dem Schluss, dass diese Kosten die Innovation einschränken und ausländische Investitionen abschrecken können, da die Unternehmen mit den komplexen Vorschriften nicht zurechtkommen.[3] Draghi warnt vor einer allgemeinen Risikoscheu der Regulierungsbehörden und insbesondere vor den Folgen der **Komplexität** der DS-GVO **und ihrer fragmentierten Umsetzung,** welche, wenn sie nicht angegangen werden, Auswirkungen auf die Wettbewerbslandschaft haben und Europas Fähigkeit behindern werden, bei neuen

[1] Die Kosten für die Einhaltung von Vorschriften können für europäische Start-ups und kleine bis mittlere Unternehmen (KMU) unerschwinglich sein, da sie im Durchschnitt 12 % ihres Umsatzes ausmachen, verglichen mit nur 5 % in den USA.

[2] So sind beispielsweise die (US-amerikanischen) Hyperscaler inzwischen weggezogen und können nicht mehr eingeholt werden, und in der EU sind Investitionen in Höhe von 800 Milliarden Euro erforderlich, um die Wettbewerbsfähigkeit zu erhalten.

[3] Als weiteres Beispiel für die Folgen eines innovationsfeindlichen Umfelds in der EU hebt Draghi hervor, dass von den 141 "Einhörnern" (die zwischen 2008 und 2021 in Europa gegründet wurden) 40 ihren Sitz ins Ausland verlegt haben.

Technologien führend zu sein, was sich letztlich auf das Wachstum und die wirtschaftliche Dynamik auswirke.

Im Gegensatz zur aktuellen Debatte über die Notwendigkeit einer Neuregelung des Datenschutzrahmens **scheint** die **Rechtslage derzeit** durch die DS-GVO **zementiert zu sein**, die Europäische Kommission scheint angesichts der Schlussfolgerungen in ihrem jüngsten Bericht derzeit keinerlei Änderungen des Rechtstextes zu beabsichtigen. Die umfangreichen politischen Initiativen der EU-Kommission mit neuen Datenregelungen (DA/DSA/KI-Verordnung) stehen in krassem Gegensatz zu der bis heute unveränderten, aber dominierenden DS-GVO. Damit werden weithin geteilte Bedenken und Entwicklungen im Hinblick auf verankerte zentrale Defizite der DS-GVO außer Acht gelassen, insbesondere

- die Aufsicht in die Hände von mehr als 27 völlig unabhängigen Aufsichtsbehörden (allein in Deutschland gibt es 17 Landesbehörden) zu legen, die keine politische Verantwortung für die Entscheidungsfindung tragen und die wirtschaftliche Daten-Regulierung allein aus der Perspektive des Schutzes des Einzelnen verfolgen, wobei sie dazu neigen, die DS-GVO sehr restriktiv und isoliert auszulegen. **Die Beauftragung unabhängiger Institutionen mit einem einseitigen Mandat zur Regulierung von neuen Märkten ist ein außergewöhnliches und riskantes Experiment.**
- die grundsätzliche Entscheidung, jede Verarbeitung personenbezogener Daten als Verbot mit Erlaubnisvorbehalt, d.h. als rechtfertigungsbedürftige Ausnahme, einzustufen, statt nur besonders risikoreiche Datenverarbeitungen zu regulieren. **Damit erhält das Recht auf informationelle Selbstbestimmung einen ungerechtfertigten systematischen Vorrang vor konkurrierenden Rechten bzw. Interessen.**

Abgesehen von der problematischen Rechtslage, die ohne den politischen Willen der Regierungen der Mitgliedstaaten nur schwer zu ändern ist, führen die Besonderheiten der Rechtsdurchsetzung im Bereich des Datenschutzes zu zusätzlichen Problemen. Wir sehen personell und materiell unzureichend ausgestattete Aufsichtsbehörden, die in ihren Entscheidungen weder den freien Verkehr personenbezogener Daten (Art. 1 Abs. 3 DS-GVO) noch den risikobasierten Ansatz (Art. 25, 32, 35 DS-GVO) angemessen berücksichtigen und andere Rechte und Interessen nur unzureichend abwägen (Erwägungsgrund 4 DS-GVO).

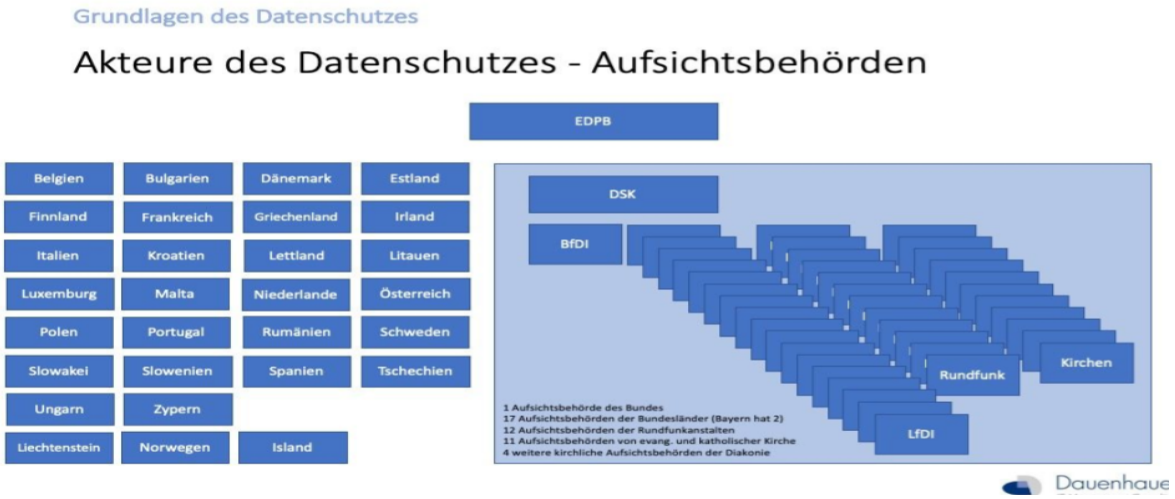
Darüber hinaus wird immer deutlicher, dass die Aufsicht über die DS-GVO mit einem schlecht funktionierenden One-Stop-Shop und einem EDSA, der als Mitregulierer und Quasi-Gesetzgeber fungiert, ohne die erforderliche Verantwortlichkeit, Transparenz und Verfahrensgarantien nicht funktioniert.

Mangelnde Verantwortlichkeit für behördliche Eingriffe in internetbasierte Geschäftsmodelle findet sich nämlich nicht nur bei den nationalen Aufsichtsbehörden, sondern auch bei ihrer Koordinations- und Kohärenzstelle, dem EDSA (vgl. Art. 68 DS-GVO): Der EDSA besitzt eine eigene Rechtspersönlichkeit (Art. 68 Abs. 1 DS-GVO) und seine Entscheidungen entfalten verbindliche Wirkung gegenüber den nationalen Aufsichtsbehörden (vgl. dazu Art. 65 und 66 DS-GVO), trotzdem ist umstritten, ob seine Entscheidungen unmittelbar gerichtlich angreifbar sind. Obwohl die ausschlaggebende Entscheidungsmacht beim EDSA liegt, trägt er keine klare

Verantwortung für sein Tun. Nach vertretener Auffassung sind erst die umsetzenden Entscheidung der nationalen Aufsichtsbehörden Gegenstand gerichtlicher Überprüfung. Dies entspricht etwa der Ansicht des Europäischen Gerichts 1. Instanz[4], wonach Entscheidungen des EDSA keine Außenwirkung hätten, da sie förmlich von der federführenden Aufsichtsbehörde umgesetzt werden müssen. Hat die Entscheidung des Gerichts 1. Instanz Bestand,[5] kann nur die federführende Aufsichtsbehörde einer gerichtlichen Kontrolle unterworfen werden.

Diese „Unverantwortlichkeit“ des EDSA hat zahlreiche negative Konsequenzen: Sie macht den EDSA „ungehemmter“ bei seiner Entscheidungsfindung und nachlässiger, was die Wahrung verfahrensmäßiger Rechte wie das Anhörungsrecht Beteiligter angeht. Da die Entscheidung des EDSA auch von ihm selbst als rein interner und vorbereitender Akt aufgefasst werden, kommen Beteiligungsrechte und Begründungspflichten systematisch zu kurz. Gleichzeitig sehen sich die mitgliedstaatlichen Aufsichtsbehörden wegen ihrer Bindung an die EDSA-Entscheidung als weniger verantwortlich, das macht sie weniger verantwortungsbewusst und damit viel eingriffsfreudiger. Auch für Betroffene und Verantwortliche bringt diese in der DS-GVO angelegte Rollenverteilung erhebliche Nachteile mit sich: mangels direkter gerichtlicher Überprüfung der EDSA-Vorgabe ist zunächst der nationale Instanzenzug zu absolvieren, was erhebliche Kosten, langdauernde Rechtsunsicherheit und ein mögliches Versanden der Rechtsfrage in den mitgliedstaatlichen Instanzen bedeutet.

Hinzu kommen die Kosten eines komplexen und ineffizienten EU-Aufsichtssystems, die durch nationale Besonderheiten wie den deutschen Föderalismus mit 17 Landesaufsichtsbehörden, welche die Aktivitäten auf EU-, Bundes- und Landesebene koordinieren müssen und die sehr unterschiedliche Kapazitäten und Datenschutzverständnisse haben, noch weiter erhöht werden.



Überblick über die fragmentierte Datenschutz-Aufsichtsstruktur in der EU und in Deutschland. N.B. Die Vielzahl der Aufsichtsbehörden für den Schutz der Privatsphäre in der elektronischen Kommunikation und andere Rechtsakte mit datenschutzrechtlichen Auswirkungen sind in dieser Übersicht nicht enthalten.

[4] https://curia.europa.eu/juris/liste.jsf?num=T-709/21
[5] Es ist Gegenstand einer Beschwerde beim EuGH

Erste Ergebnisse und illustrative Beispiele

Der derzeitige Stand der Durchsetzung der DS-GVO hat tatsächlich negative Auswirkungen und Folgen für die Rechtssicherheit, die Harmonisierung und die gesamte digitale Wirtschaft in der EU. Diese Folgen sind in ganz Europa die gleichen: Geschäftsmodelle, die auf der Monetarisierung personenbezogener Daten basieren, werden in der EU weder entwickelt noch zugelassen; bestenfalls wird die EU zu einem Absatzmarkt für Produkte, die außerhalb Europas entwickelt und betrieben werden. Zu den Kosten der Über- und Fehlregulierung gehören ein innovationsfeindliches Klima und - langfristig gesehen - die Gefahr der Deindustrialisierung.

Die folgenden **drei Beispiele** sollen helfen, die inhärenten Probleme der Datenschutzregulierung und ihre höchst problematischen Folgen zu veranschaulichen:

Beispiel 1: Stellungnahme des EDSA zum Thema "Pay or Consent"
Die Stellungnahme 08/2024 des Europäischen Datenschutzausschusses (EDSA) zum Thema "Pay or Consent" ist ein Beispiel für die Unvorhersehbarkeit, mangelnde Ausgewogenheit und teilweise Willkür, welche die Auslegung der DS-GVO auszeichnen. Diese Stellungnahme verdeutlicht die Herausforderungen, mit denen Unternehmen konfrontiert sind, wenn sie sich in der sich ständig verändernden Landschaft der Datenschutzvorschriften in Bezug auf verhaltensbezogene Werbung zurechtfinden müssen, in der sinnvolle und praktische Optionen für die Datenverarbeitung grundsätzlich abgelehnt werden und sogar die Verwendung personenbezogener Daten als Grundlage für Geschäftsmodelle in Frage gestellt wird. Die Stellungnahme verdeutlicht weiter die Komplexität und den Mangel an Sicherheit der geltenden DS-GVO mit sich ständig weiterentwickelnden regulatorischen Anforderungen, unklaren Grenzen und mangelnder Klarheit über Schlüsselkonzepte wie "Einwilligung". Darüber hinaus wird die Fragmentierung und der unausgewogene Ansatz bei der Überwachung der DS-GVO verdeutlicht, mit unterschiedlichen Regulierungsansätzen, einer unausgewogenen Durchsetzung und einem Mangel an Harmonisierung zwischen den Mitgliedstaaten. Dieser radikale Ansatz der Stellungnahme 08/2024 spiegelt die explizit unternehmensschädlichen Positionen des EDSA wider, welche die Bestimmungen der DS-GVO und den EU-Acquis missachten; er wirft die Frage auf, ob personenbezogene Daten überhaupt Gegenstand eines wirtschaftlichen Austauschs sein können. Der EDSA überschreitet dabei den Anwendungsbereich der DS-GVO mit möglicherweise erheblichen Folgen für Unternehmen, Verbraucher und die Wirtschaft insgesamt sowie für das freie und offene Internet, das durch werbefinanzierte Geschäftsmodelle weitgehend erst ermöglicht wird. Dass die erwartete allgemeine Stellungnahme des EDSA, die auch jenseits großer Online-Plattformen regulierend wirken soll, von diesen Ansätzen Abstand nimmt, steht nicht zu erwarten. Letztlich unterstreicht diese Stellungnahme die Notwendigkeit klarerer Grenzen und entsprechender Leitlinien, einer stärkeren Harmonisierung und eines ausgewogeneren Ansatzes für die Regulierung der DS-GVO unter Berücksichtigung des EU-Acquis.

Beispiel 2: AI-Modell-Training

Die DS-GVO hat eine komplexe Landschaft für in der EU tätige Unternehmen geschaffen, insbesondere wenn es um die Verwendung personenbezogener Daten für das Training von Modellen der künstlichen Intelligenz (KI) geht. Die sechs Rechtsgrundlagen der Verordnung für die Verarbeitung personenbezogener Daten wurden von den verschiedenen europäischen Datenschutzbehörden unterschiedlich ausgelegt, was zu Verwirrung und Unsicherheit für Unternehmen geführt hat.

Einige Datenschutzbehörden nehmen beispielsweise eine restriktivere Haltung ein und verlangen die Zustimmung von Einzelpersonen für das Training mit KI-Modellen und verweigern Unternehmen die Möglichkeit, sich auf ihre berechtigten Interessen zu berufen. Im Gegensatz dazu haben andere Datenschutzbehörden einen nuancierteren Ansatz gewählt und erlauben das Training von KI-Modellen auf der Grundlage berechtigter Interessen. Das Erfordernis einer Zustimmung, wie es von einigen Datenschutzbehörden befürwortet wird, würde es schwierig machen, effektive KI-Modelle zu trainieren, was letztendlich die Wettbewerbsfähigkeit der europäischen KI-Industrie beeinträchtigt. Gleichzeitig nehmen deutsche Regulierungsbehörden nun Positionen ein, die nicht mehr mit rechtlichen Grundsätzen übereinstimmen - so wird beispielsweise behauptet, dass das unrechtmäßige Training von KI-Modellen die Nutzung von KI-Systemen beeinträchtigen und damit auch die Anwendungsebene "infizieren" könnte. Dafür gibt es jedoch keine rechtlichen Argumente - dennoch ist dies die aktuelle Verhandlungsposition der Mehrheit der deutschen Aufsichtsbehörden. Diese extremen und abweichenden Ansätze schaffen erhebliche Hürden und Unsicherheiten für Unternehmen, die in der EU tätig sind, und entsprechende Investitionen, was es schwierig macht, wirksame KI-Modelle zu trainieren oder einzusetzen, und die Wettbewerbsfähigkeit der europäischen KI-Branche ernsthaft zu beeinträchtigen droht. Die Industrie und die politischen Entscheidungsträger erkennen die Notwendigkeit von Klarheit und Konsistenz bei der Anwendung der DS-GVO-Vorschriften durchaus an, betonen aber die Bedeutung des Trainings von KI mit spezifischen und differenzierten personenbezogenen Daten. Das derzeitige regulatorische Umfeld schafft jedoch erhebliche Unsicherheiten für Unternehmen und unterstreicht die Notwendigkeit eines nuancierteren und ausgewogeneren Ansatzes für die DS-GVO. Seit dem 17.12.2024 liegt die Opinion 28/2024 des EDSA vor, anstatt Rechtssicherheit zu schaffen bleiben wesentliche Fragen, etwa nach dem Personenbezug von KI-Modellen oder der Verarbeitung von Art. 9-Daten weiter offen.

Beispiel 3: Die Datentransfer-Odyssee

Die Geschichte von Datenübertragungen zwischen der EU und den USA dient als Paradebeispiel für die außergewöhnliche Komplexität, den Mangel an Sicherheit und die Fragmentierung, die der DS-GVO-Aufsicht innewohnen. Eine seit 2016 fortlaufende Reihe von Ereignissen und Entwicklungen verdeutlicht die Herausforderungen, vor denen die Europäische Kommission, die Aufsichtsbehörden und der Europäische Gerichtshof (EuGH) bei der Schaffung einer zuverlässigen und einheitlichen Grundlage für Datenübermittlungen zwischen hoch entwickelten Rechtsstaaten stehen.

Die Geschichte dieser Datentransfers ist gekennzeichnet durch eine sich ständig verändernde Regulierungslandschaft, uneinheitliche Auslegungen und einen Mangel an klaren Richtlinien und Standards für die Datenübermittlung. Dies hat ein komplexes Umfeld geschaffen, das es schwierig bis unmöglich für Organisationen macht, die Einhaltung der DS-GVO-Anforderungen zu gewährleisten. Darüber hinaus haben die unterschiedlichen nationalen Ansätze zur Umsetzung der DS-GVO, die ungleiche Verteilung der Befugnisse und die unausgewogene Durchsetzung zu Unsicherheit und Verwirrung bei Organisationen und Personen geführt, die an grenzüberschreitenden Datenübertragungen beteiligt sind. Dies ging zu Lasten transatlantischer Geschäftstransaktionen und war für die EU-Wirtschaft mit erheblichen Kosten und Nachteilen verbunden. Selbst der EU-Kommission wurde die Transfer-Problematik jüngst zum Verhängnis: Mit Urteil des Europäischen Gerichts 1. Instanz (Rechtssache T-354/22 | Bindl / Kommission) vom 8.1.2025 wurde sie wegen eines Hyperlinks in die USA zu Schadenersatz in Höhe von 400 € verurteilt.

Letztlich unterstreicht dieses Beispiel die Notwendigkeit eines stärker harmonisierten, risikobasierten und ausgewogenen Ansatzes für die Datenschutzregulierung, der die unterschiedlichen Bedürfnisse und Interessen aller beteiligten Akteure berücksichtigt. Ein kohärenterer und wirksamerer Rahmen für Datenübermittlungen ist notwendig, um den freien Datenverkehr zu gewährleisten und gleichzeitig die Rechte und Freiheiten des Einzelnen zu schützen.

Nachteilige Entwicklungen bei der Auslegung der DS-GVO

Diese prekäre Situation verdient eine tiefere Analyse ihrer Ursachen und Bedingungen: Die derzeitige Durchsetzungspraxis der DS-GVO ist durch ein komplexes Zusammenspiel von Faktoren gekennzeichnet, die zu einer **Politisierung der Aufsichtsbehörden** geführt haben, zu einem **radikalisierten Datenschutzverständnis und zu einem Wettlauf um die strengste Position** unter den Aufsichtsbehörden.

Im Kern ist die europäische Datenschutzlandschaft durch das One-Stop-Shop-Prinzip und den Europäischen Datenschutzausschuss geprägt, der sich aus den 27 Datenschutzbehörden der EU-Mitgliedstaaten zusammensetzt und in einem hohen Maß unabhängig arbeitet.

Der EDSA wurde zwar eingerichtet, um die Kohärenz und Konsistenz zwischen den Datenschutzbehörden zu gewährleisten, seine Struktur und Mechanismen haben jedoch unbeabsichtigt ein Umfeld geschaffen, das den Wettbewerb und den Konkurrenzkampf zwischen den Aufsichtsbehörden fördert. Für die Datenschutzbehörden gibt es Anreize, ihr Engagement für den Datenschutz zu demonstrieren, indem sie die denkbar strengsten

Positionen einnehmen, was zu einer Politisierung und Radikalisierung einiger Aufsichtsbehörden geführt hat. Dieses Phänomen wird durch den Mangel an Verantwortlichkeit und Transparenz in den Entscheidungsprozessen der Datenschutzbehörden noch verschärft, was es ihnen ermöglicht, relativ ungestraft zu agieren - die Verteilung und der Mangel an Verantwortung führen manchmal zu Nachlässigkeiten bei der Ausübung von Macht.

Darüber hinaus wurden die vom EDSA geschaffenen Kohärenzmechanismen, wie das Kohärenzverfahren und das Streitbeilegungsverfahren, genutzt und als Instrument eingesetzt, um den für die Verarbeitung Verantwortlichen in anderen Mitgliedstaaten strengere Vorschriften aufzuerlegen. Anstatt für Kohärenz und Zusammenarbeit zwischen den Datenschutzbehörden zu sorgen, sind diese Mechanismen zu Instrumenten geworden, mit denen die nationalen Behörden übergangen und den Unternehmen strengere Anforderungen auferlegt werden können. Dies hat zu einer weiteren Aushöhlung des One-Stop-Shop-Prinzips geführt und eine Kultur des Regulierungswettbewerbs geschaffen, in der die Datenschutzbehörden einen Anreiz haben, möglichst extreme Positionen einzunehmen, um ihr Engagement für den Datenschutz zu demonstrieren.

Die Struktur des EDSA, die eine Entscheidungsfindung hinter verschlossenen Türen und ohne umfassende öffentliche Konsultation ermöglicht, hat ebenfalls zu diesem Problem beigetragen. Das Fehlen von Expertenbeiträgen aus der Praxis und die unzureichende Berücksichtigung anderer Vorschriften, Rechte und Interessen führt nicht selten zu negativen Ergebnissen für die Rechtssicherheit und Kohärenz. Darüber hinaus ermöglicht der Mangel an Transparenz und Rechenschaftspflicht es den Datenschutzbehörden, Kritik an ihren Entscheidungen auf ein Mehrheitsvotum des EDSA zu verschieben, anstatt die Verantwortung für ihre Handlungen und Positionen zu übernehmen.

Diese Entwicklung hat auch in den Mitgliedsstaaten erhebliche Konsequenzen. In Deutschland beispielsweise geraten die Aufsichtsbehörden zunehmend unter Druck, weil die Datenschutzpraxis als innovations- und wirtschaftsfeindlich wahrgenommen wird. Infolgedessen werden neue Aufsichtsaufgaben, beispielsweise im Bereich der KI-Überwachung, an andere Institutionen übertragen. Diese politischen und institutionellen Reaktionen auf wahrgenommene Durchsetzungsprobleme führen jedoch nicht zu einer Selbstreflexion der Datenschutzbehörden, sondern vielmehr zu einer weiteren Radikalisierung der Positionen der Aufsichtsbehörden. Diese Radikalisierung beschränkt sich nicht nur auf den Inhalt ihrer Positionen, sondern erstreckt sich auch auf deren Politisierung und betrifft letztlich die rechtlichen Verpflichtungen dieser staatlichen Organe als Rechtssubjekte.

Zurück zur europäischen Ebene: Die Art und Weise, wie der Europäische Datenschutzausschuss aufgebaut ist, ermöglicht eine einseitige Entscheidungsfindung und begründet keine ausreichende Verantwortlichkeit für seine Entscheidungen. Dies hat dazu geführt, dass die Aufsichtsbehörden immer ruppiger miteinander umgehen und die Zuständigkeitskonzentration des One-Stop-Shops immer weniger respektiert wird. Die EU-Kommission und andere Institutionen, wie z. B. die Wettbewerbsbehörden, befinden sich zudem in einem Wettlauf um eine noch strengere Datenschutzposition, was das Problem weiter verschärft.

Die Folgen dieser Schieflage

Die derzeitige Durchsetzungspraxis der DS-GVO hat zu einem besorgniserregenden Trend des „Absolutismus“ in Bezug auf den Schutz der informationellen Selbstbestimmung gegenüber anderen legitimen Interessen und Rechten, zu mangelnder Ausgewogenheit bei der Lösung von Interessenkonflikten und zu einem Null-Risiko-Ansatz bei den Datenschutzbehörden geführt. Dieses Phänomen ist nicht das Ergebnis einer Überregulierung, sondern eher einer Fehlregulierung, bei der die Datenschutzbehörden von der ursprünglichen Absicht der DS-GVO abgewichen sind.

Die Datenschutz-Grundverordnung wurde als zukunftsweisender, grundsätzlich risikobasierter und technologieneutraler Rahmen konzipiert, der die Datenschutzbehörden ermächtigt, in Fällen einzugreifen, in denen personenbezogene Daten ein erhebliches Risiko für die informationelle Selbstbestimmung der Nutzerinnen und Nutzer in der EU darstellen. In der Praxis haben sich die Datenschutzbehörden jedoch von diesem risikobasierten Ansatz entfernt und es versäumt, das notwendige Gleichgewicht zwischen den verschiedenen Grundrechten herzustellen. Insbesondere fällt es ihnen schwer, die wirtschaftlichen und gesellschaftlichen Vorteile des technologischen Fortschritts gegen potenzielle Risiken abzuwägen, das Recht auf Datenschutz mit anderen Grundrechten und -freiheiten, einschließlich der unternehmerischen Freiheit, in Einklang zu bringen und eine faktengestützte Position zu den wahrgenommenen Risikofaktoren einzunehmen.

Infolgedessen neigen Datenschutzbehörden dazu, auf sehr restriktive Maßnahmen zurückzugreifen, wie z. B. die Einschränkung von Datenübertragungen, personalisierter Werbung und KI-Training, die zwar leichter durchzusetzen sind, aber letztlich Rechtsunsicherheit fördern und Handel, Innovation und Fortschritt behindern.

Dieser Ansatz ist aus mehreren Gründen problematisch. Erstens lässt er die umfassenderen gesellschaftlichen und wirtschaftlichen Auswirkungen des technologischen Fortschritts außer Acht und führt zu einem engen Fokus auf den Datenschutz auf Kosten anderer wichtiger Interessen. Zweitens schafft er eine Kultur der Angst und Vorsicht, in der Unternehmen aufgrund der Ungewissheit und des Risikos von Regulierungsmaßnahmen zögern, in neue Technologien zu investieren oder Innovationen vorzunehmen.

Außerdem untergräbt dieser Ansatz das ursprüngliche Ziel der DS-GVO, einen Beitrag zum Datenbinnenmarkt zu leisten. Durch die Verabschiedung übermäßig restriktiver Maßnahmen schaffen die Datenschutzbehörden eine fragmentierte Regulierungslandschaft, die den freien grenzüberschreitenden Datenverkehr behindert. Der Mangel an Kapazitäten und Verlässlichkeit unter den nationalen Aufsichtsbehörden hat zu einer uneinheitlichen Rechtsdurchsetzung geführt, was bei den Unternehmen zu Unsicherheit oder gar Verwirrung führt. Dies wiederum kann zu einem Verlust an Wettbewerbsfähigkeit für europäische Unternehmen führen, da sie Mühe haben, mit ihren globalen Konkurrenten Schritt zu halten.

Zudem ist der von den Datenschutzbehörden verfolgte Null-Risiko-Ansatz unrealistisch und unerreichbar - und rechtlich nicht erforderlich. Es ist unmöglich, alle Risiken im Zusammenhang mit der Verwendung personenbezogener Daten auszuschalten, und der Versuch, dies zu tun, kann zu unbeabsichtigten Folgen führen, wie z. B. einer Überregulierung und dem Abwürgen von Innovationen. Ein ausgewogenerer Ansatz würde anerkennen, dass

jede Tätigkeit, die mit personenbezogenen Daten verbunden ist, ein gewisses Risiko birgt, und versuchen, diese Risiken durch verhältnismäßige und wirksame Maßnahmen zu mindern.

Zusammenfassend lässt sich sagen, dass die derzeitige DS-GVO-Durchsetzung ein Umfeld geschaffen hat, das **Politisierung, Radikalisierung und einen Wettlauf um die strengste Position unter den Aufsichtsbehörden** begünstigt. Der Mangel an Rechenschaftspflicht, Transparenz und Kohärenz in den Entscheidungsprozessen der Datenschutzbehörden in Verbindung mit der unangemessenen Nutzung von Kohärenzmechanismen und der Struktur des EDSA haben zu diesem Phänomen beigetragen. Gleichzeitig hat die derzeitige Durchsetzungspolitik der DS-GVO zu einem besorgniserregenden **Trend zu Datenschutz-Absolutismus, mangelnder Ausgewogenheit und einem Null-Risiko-Ansatz bei den Datenschutzbehörden** geführt. Dieser Ansatz ist fehlgeleitet und kann schwerwiegende Folgen für Handel, Innovation und Fortschritt haben.

Grundlegende Ursachen für diese ungünstigen Entwicklungen

Die Ursachen für die negativen Entwicklungen in der europäischen Datenschutzlandschaft lassen sich auf zwei Hauptfaktoren zurückführen: die Mängel der DS-GVO selbst und die mangelhafte Governance-Struktur und -Praxis bei der Durchsetzung des Datenschutzes.

Erstens hat das Verbot mit Erlaubnisvorbehalt in der DS-GVO zu einem Richtungswechsel hin zu einer gebremsten Innovation in der Datenwirtschaft geführt. Artikel 6 der DS-GVO, der die Grundsätze für die rechtmäßige Verarbeitung personenbezogener Daten festlegt, wurde als restriktiv ausgelegt und der informationellen Selbstbestimmung des Einzelnen Vorrang vor anderen Rechten und wirtschaftlichen Interessen einräumt. Durch die Einstufung der gesamten Verarbeitung personenbezogener Daten als verboten (mit Erlaubnisvorbehalt) wird eine Kultur der Vorsicht geschaffen, in der Unternehmen der Wahrung des Status Quo Vorrang vor Innovation einräumen, was sie anfällig bei disruptiven Entwicklungen macht. Die Annahme der Rechtswidrigkeit jeder Datenverarbeitung und die angedrohten drakonischen Strafen führen zu einem unangemessenen Wirtschaftsverhalten, das Innovation erstickt und Wachstum einschränkt, was letztlich die Wettbewerbsfähigkeit der europäischen Unternehmen in der globalen Wirtschaft gefährdet. Ein nuancierterer Ansatz ist erforderlich und durch den Grundsatz der Verhältnismäßigkeit sogar gefordert: Die Regulierung muss sich auf besonders risikoreiche Datenverarbeitungstätigkeiten konzentrieren und klare Leitlinien für die Einhaltung der Vorschriften vorgeben, um ein Gleichgewicht zwischen Datenschutz und Innovation herzustellen. Der risikoaverse Ansatz stellt ein erhebliches wirtschaftliches Risiko für Unternehmen dar, die im digitalen Raum innovativ tätig sind, und hat zu einer Kultur der Vorsicht geführt: Unternehmen zögern die aufgrund der Unsicherheit und des Risikos von Aufsichtsmaßnahmen, in neue Technologien zu investieren oder Innovationen vorzunehmen.

Darüber hinaus hat die Zuweisung zentraler Machtpositionen an unabhängige Institutionen ohne Kontrolle und Gegengewicht, wie z.B. an die Datenschutzaufsichtsbehörden, zu einem Ungleichgewicht geführt. Diese Behörden wurden eingerichtet, um die informationelle Selbstbestimmung des Einzelnen zu schützen und zu stärken, aber sie haben es versäumt, eine ausgewogene Position einzunehmen, die auch das Gemeinwohl einbezieht und fördert und andere Rechte und Interessen berücksichtigt. Die Rechtsprechung des Europäischen Gerichtshofs (EuGH) zur DS-GVO hat dieses einseitige Verständnis bekräftigt, indem dieses

feststellte, dass "das hohe Niveau des Datenschutzes" das Leitprinzip der Rechtsauslegung sein sollte. Infolgedessen haben sich die Aufsichtsbehörden einseitig auf die Seite der betroffenen Personen gestellt und ihre Verantwortung für eine ausgewogene Regulierung vernachlässigt.

Auch die Bestimmungen der DS-GVO über die Zusammenarbeit der Aufsichtsbehörden und über das Kohärenzverfahren (die fast die Hälfte der DS-GVO ausmachen) erweisen sich als systematisches Hindernis: Die zuständigen Aufsichtsbehörden (One-Stop-Shop) werden dadurch in ihrem Rollenverständnis eingeschränkt, sie treffen letztlich nur Vorentscheidungen, bis der EDSA das letzte Wort gesprochen hat. Dies führt zu einer zögerlichen Positionierung seitens der federführenden Aufsichtsbehörde - und zu offensiven und überzogenen Positionen seitens der betroffenen Aufsichtsbehörden. Dieser Mangel an Legitimität führt zu einem übermäßig aktiven EDSA, der die Entscheidungsfähigkeit der federführenden Aufsichtsbehörde weiter bremst. Dies wiederum hat zur Folge, dass die für die Verarbeitung Verantwortlichen noch weniger Rechtssicherheit haben, da sie es letztlich mit den Mitgliedern des EDSA zu tun haben und nicht mit einer einzigen Aufsichtsbehörde.

Darüber hinaus hat die Selbstwahrnehmung der Aufsichtsbehörden als „Gegenspieler der datenverarbeitenden Industrie“ zu einem konfrontativen Ansatz geführt, bei dem sie eher versuchen, die Datenwirtschaft einzuschränken als einen fairen Interessenausgleich zu schaffen. Diese kontradiktorische Denkweise hat ein toxisches Umfeld geschaffen, in dem Unternehmen eher als Gegner denn als verantwortliche Beteiligte bei der Sicherstellung einer vernünftigen Nutzung personenbezogener Daten angesehen werden.

Der besondere Blick auf Deutschland

In Deutschland wird diese schwierige Situation von vier weiteren Faktoren beeinflusst: von der Sonderstellung, die sich deutsche Aufsichtsbehörden im europäischen Verbund zuordnen, von den zwei grundlegend unterschiedlichen Datenschutzkulturen in Deutschland, von der föderalen Struktur der Datenschutzaufsicht (Vielfalt und Konkurrenz) und von der äußerst unterschiedlichen Ausstattung der Landesdatenschutzbehörden.

Die Sonderstellung deutscher Aufsichtsbehörden im europäischen Verbund?

Aus Sicht der deutschen Aufsichtsbehörden kommt dem deutschen Datenschutz aus zwei Gründen einen Sonderstellung im europäischen Verbundsystem der Aufsicht zu: aus historischen und aus Kapazitätsgründen.

Zwar ist der Datenschutz sicherlich keine deutsche „Erfindung", doch fand die Idee, den technologischen Fortschritt der Digitalisierung mit eigenen gesetzgeberischen Antworten zu versehen, seinen Ursprung in Deutschland. Es war im deutschen Land Hessen, dass das Landesparlament auf die wachsenden Datenverarbeitungskapazitäten der Regierung 1970 mit einem Datenschutzgesetz reagierte, dass den Abgeordneten neue Informations- und Kontrollrechte gegenüber der digital gestärkten Landesregierung einräumte und zugleich den BürgerInnen erstmals Rechte gegenüber der datenverarbeitenden öffentlichen Hand gewährte. Damals waren es die Großrechner der Sozialversicherer und des Sicherheitsbereichs, welche in Deutschland Ängste vor einer Übermacht der Landesexekutive aufkommen ließen und nach neuen Institutionen zum Schutz der Bürgerrechte – den Datenschutzbeauftragten – verlangten. Bereits 1977 zog die Bundesebene mit dem Bundesdatenschutzgesetz nach und nahm nun auch die datenverarbeitende Wirtschaft mit in den Fokus.

Hieraus leitet sich in Deutschland ein gewisses Selbstverständnis ab, den Datenschutz grundlegend entwickelt und geprägt zu haben – was für Institutionen wie die staatlichen und betrieblichen Datenschutzbeauftragten sicherlich auch zutrifft, auf das umfassende Auskunftsrecht, die Datenschutzfolgenabschätzung (bzw. Vorabkontrolle) oder das Verfahrensverzeichnis (heute: Verzeichnis der Verarbeitungstätigkeiten).

Zum anderen verfügt der Mitgliedsstaat Deutschland über das meiste Personal bei staatlichen Aufsichtsbehörden. Durch die Kombination von Bundes- und Länderbehörden sind aktuell mehr als 1.000 Beschäftigte für den Datenschutz (und die Informationsfreiheit) tätig. Die BfDI verfügt derzeit über 263 Beschäftigte, die deutschen Länder zusammen über ca. 800 Beschäftigte (größte Landesbehörde Baden-Württemberg mit 85, kleinste das Saarland mit 12 Mitarbeitern). Das dürfte das Personal in anderen europäischen Aufsichtsbehörden deutlich übertreffen.

Allerdings scheiterten bislang die Versuche deutscher Aufsichtsbehörden, aus dieser historischen und zahlenmäßigen Position Vorteile im EDSA zu schlagen. Frühe Versuche, kleinere Aufsichtsbehörden im EDSA zu dominieren oder eine Führungsposition einzunehmen, trugen bislang keine Früchte.

Die zwei grundlegend unterschiedlichen Datenschutzkulturen in Deutschland

Trotz der langen, mittlerweile mehr als 50 Jahre dauernden gemeinsamen Geschichte der deutschen Aufsichtsbehörden sind ihre Positionierungen nach wie vor sehr unterschiedlich. Dies hängt weniger mit den unterschiedlichen Landes-Datenschutzgesetzen zusammen, welche die jeweiligen regionalen Aufsichtsbehörden regulieren, als mit zwei grundlegend unterschiedlichen Datenschutzkulturen, die in Deutschland seit den 70er Jahren gewachsen sind: Während der norddeutsche Datenschutz sich als Verteidiger von Betroffenenrechten versteht und trotz seiner staatlichen Stellung einseitig gegen die Interessen der Datenverarbeiter Front macht, zeichnet sich der süddeutsche Datenschutz durch eine ausgewogener und neutralere Verortung aus; hier werden Betroffenenrechte zwar auch durchgesetzt, allerdings ist man offen für Beratungsgespräche mit Verantwortlichen und tritt insbesondere kleineren Verantwortlichen (Vereine, Handwerker) helfend zur Seite. Diese Zweiteilung hängt stark mit dem behördlichen Selbstverständnis in den deutsche Ländern zusammen, in Süddeutschland stand der Servicegedanke schon immer im Vordergrund, während sich norddeutsche Verwaltung eher um Transparenz bemüht.

Diese gegenläufigen Datenschutzkulturen prallen seit mehr als 50 Jahren in der deutschen Datenschutzkonferenz (DSK) aufeinander und haben nicht selten gemeinsame Beschlussfassungen zu Themen des öffentlichen wie nicht-öffentlichen Datenschutzes verhindert. Zwar bemüht man sich inzwischen stärker um gemeinsame Positionierungen (gerade mit Blick auf europäische Verfahren), die Grundhaltungen schlagen aber bis heute immer noch erkennbar durch und nähren das Bild der „uneinheitlichen“ deutschen Datenschützer.

Die föderale Struktur der deutschen Datenschutzaufsicht (Vielfalt und Konkurrenz inkl. BfDI)

In der Kritik steht schon lange – in Deutschland seit der wenig folgenreichen Föderalismusreform 2009, von Brüssel her hinter vorgehaltener Hand, da die EU sich nicht in „innere Angelegenheiten“ der Mitgliedstaaten einmischen darf – die föderale Struktur der Bundesrepublik, die sich auch bei der Verteilung der Aufgaben und Kompetenzen beim Datenschutz deutlich bemerkbar macht. Das Grundgesetz von 1949 ist, auch als Konsequenz des 3. Reiches, von den deutschen Ländern her gedacht: Dort liegt die ursprüngliche Gesetzgebungs- und Verwaltungskompetenz (Art. 70 und 83 Grundgesetz), die Staatsgewalt liegt unveränderlich (Art. 79 Abs. 3 GG) bei den Ländern und einem nur subsidiär tätigen Bund. Zwar wurde diese Gewichtung schon in den 60er Jahren insbesondere im Bereich der Finanz- und Steuerhoheit unterlaufen, doch gerade im Bereich der Exekutive haben die Länder nach wie vor das Schwergewicht – auch bei den Datenschutz-Aufsichtsbehörden, welche in den Ländern gebildet werden. Der Bundesbeauftragten für den Datenschutz kommt nur eine sehr eingeschränkte Funktion im privaten Sektor zu, sie wird schwerpunktmäßig gegenüber Bundesbehörden tätig und vertritt, was seit 2018 von strategischer Bedeutung ist, Deutschland im EDSA.

Im Bereich des Datenschutzes wird die föderale Struktur allerdings ebenso wenig genutzt wie auch in der übrigen Staatsverwaltung, anstatt im Wettbewerb um die beste

Verwaltungslösung zu stehen überwiegen Koordinationsbemühungen (etwa in der Konferenz der Datenschutzaufsichtsbehörden der Länder und des Bundes DSK) nach dem nivellierenden und ausbremsenden Geleitzugprinzip. Gleichzeitig fokussiert sich die öffentliche (und vor allem wirtschaftlich getriebene) Debatte zum Datenschutz auf eine Vielfältigkeit und Uneinheitlichkeit der Rechtspositionen zur DS-GVO in den föderalen Aufsichtsbehörden, obwohl diese Vielfalt als Ausgangspunkt durchaus positiv zu bewerten und wegen der Verlagerung der Entscheidungskompetenzen auf EU-Ebene auch völlig überbewertet ist. Ängstliche Verantwortliche sehen sich durch die wahrnehmbare Diskutierfreudigkeit der deutschen Aufsichtsbehörden eher bedroht, als dass sie die darin liegenden Chancen erblicken. So wird von den föderalen Behörden das erwartet, was letztlich nur der EDSA und der EuGH liefern können. Die hieraus abgeleitete Zentralisierungsdebatte (Verlagerung der Aufsicht über den privaten Sektor zur BfDI) geht daher objektiv an den Bedürfnissen der Wirtschaft vorbei und ist zeitlich schon lange überholt. Dennoch wird die Frage einer Verschlankung des Verwaltungsaufbaus im Bereich des Datenschutzes auf der Agenda der nächsten Bundesregierung stehen.

Die Ausstattungsdivergenzen der Landesdatenschutzbehörden

Ebenso maßgeblich wie die unterschiedlichen Datenschutzkulturen in Deutschland ist die höchst unterschiedliche personelle und sächliche Ausstattung der Landesdatenschutzbehörden: Während die größeren Aufsichtsbehörden (BaWü/Bayern/NRW/Nds/Hessen/HH) mit einem Personalbestand von bis zu 85 Vollzeitstellen die Herausforderungen der DS-GVO einschließlich einer substanziellen Beteiligung am europäischen Koordinations- und Kohärenzmechanismus durchaus bewältigen können, sieht dies für die Vielzahl kleinerer Aufsichtsbehörden (Bremen/Saar/Bbg/Sachsen/Sa-Anh/Thür/MeckP) deutlich anders aus: Mit weniger als 15 Mitarbeitern kann eine Erfüllung der Aufgaben nach Art. 57 DS-GVO und den jeweiligen Landes-Datenschutzgesetzen nicht gelingen. Indikator dafür ist etwa, dass Beratungsaufgaben gegenüber Verantwortlichen nicht mehr wahrgenommen werden oder sogar der turnusmäßige Vorsitz in der DSK angelehnt wird. Diese Unterausstattung ist auch ein Grund dafür, warum die Landesbehörden selbst in zentralen Fragestellungen unterschiedlich votieren. Die soeben erörterte Frage einer Zentralisierung der Datenschutzaufsicht auf Bundesebene wird von einer Mehrheit der Landesbehörden nicht als Beschneidung der Kompetenzen, sondern als willkommene Entlastung betrachtet.

Insgesamt stellt die deutsche Datenschutzaufsicht daher einen „Sonderfall“ in der EU dar: lange Datenschutztradition, vergleichsweise aktive Aufsichtsbehörden mit allerdings divergenter Aufsichtskultur und erheblichen Ausstattungsunterschieden. Sucht man einen Einstieg in die europäische Datenschutzszene, kann sich der Weg zu den (gut ausgestatteten und wirtschaftsoffenen) Aufsichtsbehörden lohnen – jedenfalls als Sparringspartner sind einige der deutschen Datenschutzbehörden gut zu nutzen. Der deutsche Einfluss im EDSA ist zwar begrenzt, allerdings wird die deutsche Stimme immer angehört und gegen diese wird nur selten agiert.

Verbesserung des Systems zur Durchsetzung der DS-GVO: Chancen und Lösungsmöglichkeiten

Um der Politisierung, der Radikalisierung und dem Wettlauf um die strengste Position unter den Aufsichtsbehörden sowie dem Problem des Absolutismus des Datenschutzes gegenüber anderen legitimen Interessen und Rechten, der mangelnden Ausgewogenheit und dem Null-Risiko-Ansatz unter den Datenschutzbehörden zu begegnen, ist ein vielschichtiger Ansatz erforderlich, der sowohl kurzfristige als auch mittel- bis langfristige Lösungen beinhaltet.

Kurzfristige Lösungen

Kurzfristig können mehrere Maßnahmen ergriffen werden, um die derzeitigen Probleme zu lösen. Erstens ist es entscheidend, **die Transparenz und Vorhersehbarkeit** der Entscheidungsprozesse auf EU-Ebene **zu erhöhen**. Dies kann durch eine größere Offenheit der Verfahren erreicht werden, z. B. durch eine **systematische und breitere Beteiligung von Interessengruppen** im Vorfeld von EDSA-Entscheidungen. Die frühzeitige Einbeziehung von betroffenen Akteuren aus Wirtschaft, Wissenschaft und von Verbraucherseite sollte als rechtliche Verpflichtung verstanden werden und nicht dem Ermessen des Ausschusses überlassen bleiben.

Zweitens sollte die **Gewährleistung von Innovation und Wettbewerbsfähigkeit in das Mandat der Aufsichtsbehörden aufgenommen** werden, etwa im Sinne der Zielsetzung der französischen CNIL, Innovation zu fördern. Ein angepasstes Behördenmandat, das ausdrücklich den freien Datenverkehr, den digitalen Binnenmarkt, die Wettbewerbsfähigkeit und die Innovation einschließt, würde dazu beitragen, ein besseres Gleichgewicht zwischen dem Datenschutz und anderen Grundrechten und Interessen herzustellen.

Drittens müssen die Aufsichtsbehörden einen **strukturierten Dialog und einen regelmäßigen Austausch mit Wirtschaft, Politik und Zivilgesellschaft** etablieren, wie in Artikel 70 Absatz 4 DS-GVO vorgesehen.

Eine verbesserte Zusammenarbeit zwischen den föderalen Aufsichtsbehörden in den Mitgliedstaaten kann zu mehr Professionalität und Vorhersehbarkeit führen, was durch Verfahrensänderungen wie die Abkehr vom (deutschen) Einstimmigkeitsprinzip und die Verbindlichkeit von Mehrheitsentscheidungen für alle Regulierungsbehörden erreicht werden kann.

Mittel- bis langfristige Lösungen

Mittel- bis langfristig sind substanziellere Reformen erforderlich, um die Ursachen der aktuellen Probleme zu beseitigen. Erstens sollte der Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung **zusätzlicher Verfahrensregeln für die Durchsetzung der Datenschutz-Grundverordnung** genutzt werden, um einen solideren Rahmen für die Gewährleistung der Kohärenz und Zusammenarbeit zwischen den Aufsichtsbehörden, der Verantwortlichkeit für ihre Entscheidungen und der Sicherheit sowie

wirksame Verfahrensrechte für die Verantwortlichen zu schaffen. **Dies würde allerdings erfordern, dass die derzeitigen Trilog-Texte neu bewertet und überdacht werden.**

Da bei politischer Betrachtung die Verantwortung für seine Entscheidungen beim EDSA liegt, sollten diese – auch aus zeitlichen Gründen und wegen der bis dahin bestehenden Rechtsunsicherheit – direkt vor dem EuG/EuGH angegriffen werden können. Vorbild dafür kann die europagerichtliche Angreifbarkeit von Entscheidungen der EU-Kommission im Beihilfe-, Biozid- bzw. Bankenrecht sein. Zwischenzeitlich wird der EuGH die Möglichkeit haben, die direkte Anfechtbarkeit von EDPB-Entscheidungen durch Unternehmen/andere Dritte vor den EU-Gerichten zu bestätigen.[6]

Zweitens muss ein **angemessenes Verhältnis zwischen dem Datenschutz und anderen Grundrechten**, wie der unternehmerischen Freiheit, hergestellt werden. Dies erfordert einen nuancierteren Ansatz, der das komplexe Zusammenspiel zwischen verschiedenen Grundrechten und Interessen berücksichtigt.

Drittens sollte **dem risikobasierten Ansatz eine größere Bedeutung beigemessen** werden, insbesondere bei den Fragen Personenbezug/Anonymisierung, Datenübermittlung und sensible Daten. Dies würde einen ausgewogeneren Ansatz ermöglichen, der die spezifischen Risiken und Vorteile berücksichtigt, die mit den verschiedenen Arten der Datenverarbeitung verbunden sind.

Stärkung der Position der EU-Kommission

Letztlich kann das Durchsetzungsproblem nur durch eine **Stärkung der Position der EU-Kommission bei der Auslegung der DS-GVO und der grenzüberschreitenden Durchsetzung** überzeugend gelöst werden. Die Kommission ist am besten in der Lage, eine einheitliche, konsistente und nicht einseitig auf den Datenschutz fixierte Position zu entwickeln und zu vertreten. Um dies zu erreichen, könnte der Kommission eine führende Position im EDSA zugewiesen werden, möglicherweise in Form einer Europäischen Digitalisierungsbehörde, wobei **den nationalen Aufsichtsbehörden eine beratende Rolle zukäme**. Dies würde die historische Schieflage korrigieren und einen effektiveren und ausgewogeneren Ansatz für die Datenschutzregulierung bieten. Als einzig Zuständiger für grenzüberschreitende Datenverarbeitungen wäre die Kommission auch auf der richtigen Ebene legitimiert und würde eine Diffusion der Verantwortung verhindern.

[6] Siehe auch den Mlex-Artikel zur Anhörung *C-97/23 P – WhatsApp Ireland gegen EDPB*: „WhatsApp argues for direct challenge of EU privacy watchdogs“ (26. November 2024). Abgerufen über *https://www.mlex.com/mlex/articles/2265801?scroll=1&related=1*

Schlussfolgerung

Zusammenfassend lässt sich sagen, dass sich die europäische Datenschutzlandschaft an einem kritischen Punkt befindet und die DS-GVO bei ihrer Umsetzung vor erheblichen Herausforderungen steht. Die derzeitige Durchsetzung der DS-GVO ist gekennzeichnet durch Politisierung, Radikalisierung und einen Wettlauf um die strengste Position unter den Aufsichtsbehörden, was zu einem „Absolutismus des Datenschutzes“ gegenüber anderen legitimen Interessen und Rechten und zu einem Mangel an Ausgewogenheit führt. Dies hat zu Unsicherheit und Hindernissen für Unternehmen geführt, insbesondere für kleine und mittlere Unternehmen (KMU), und hat Innovation und Wachstum behindert.

Um diese Herausforderungen zu bewältigen, ist ein vielschichtiger Ansatz erforderlich, der sowohl kurzfristige als auch mittel- bis langfristige Lösungen umfasst. Zu den kurzfristigen Maßnahmen gehören die Erhöhung der Transparenz und Vorhersehbarkeit von Entscheidungsprozessen, die Sicherstellung, dass Innovation und Wettbewerbsfähigkeit in das Mandat der Aufsichtsbehörden aufgenommen werden, und die Verbesserung der Zusammenarbeit zwischen den (föderalen) Aufsichtsbehörden.

Mittel- bis langfristig sind substanziellere Reformen erforderlich, einschließlich der Verabschiedung zusätzlicher Verfahrensregeln für die Durchsetzung der DS-GVO, der Schaffung eines angemessenen Verhältnisses zwischen Datenschutz und anderen Grundrechten und der Einführung einer stärkeren Rolle für den risikobasierten Ansatz.

Letztlich ist die Stärkung der Position der EU-Kommission entscheidend für die Lösung des Durchsetzungsproblems. Die Zuweisung einer führenden Position an die Kommission im EDSA, möglicherweise in Form einer Europäischen Digitalisierungsbehörde, würde einen effektiveren und ausgewogeneren Ansatz für die Datenschutzregulierung bieten.

Durch einen nuancierteren Ansatz beim Datenschutz kann die EU eine Kultur der Innovation und des Wachstums fördern und gleichzeitig die Rechte und Freiheiten des Einzelnen in vorbildlicher Weise schützen.

Es ist von entscheidender Bedeutung, dass politische Entscheidungs- und Interessenträger zusammenarbeiten, um die Herausforderungen der DS-GVO zu bewältigen und sicherzustellen, dass sie ein relevanter und wirksamer Rahmen für die Regulierung des Datenschutzes im digitalen Zeitalter bleibt.

Dr. Stefan Brink

Geschäftsführender Direktor
des wissenschaftlichen Instituts für die Digitalisierung der Arbeitswelt / Berlin
Landesbeauftragter für den Datenschutz und die Informationsfreiheit Baden-Württemberg a.D.