Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Positionspapier

Überlegungen zur

Verbesserung und Vereinfachung der

EU-Datenschutzgrundverordnung (DSGVO)

Lobbyregister-Nr. R001459
EU-Transparenzregister-Nr. 52646912360-95

Kontakt:
Wulf Hartmann
Director
Telefon: +49 30 1663-3140
E-Mail: wulf.hartmann@bdb.de

Berlin, 29. Oktober 2025

Federführer:
Bundesverband deutscher Banken e. V.
Burgstraße 28 | 10178 Berlin
Telefon: +49 30 1663-0
https://die-dk.de

Inhalt

A. Allgemein

I. Evaluierung der DSGVO griff bisher zu kurz

Die EU-Datenschutzgrundverordnung (DSGVO) gilt seit dem 25. Mai 2018 unverändert. Sie bietet einen EU-weit geltenden einheitlichen Rechtsrahmen und gewährleistet ein hohes Datenschutzniveau. Auch aus Sicht der Deutschen Kreditwirtschaft (DK) ist die DSGVO grundsätzlich ein Meilenstein in der EU-Datenschutzgesetzgebung.

Die EU-Kommission hat die DSGVO zweimal evaluiert, zuletzt im Jahr 2024. Beide Male kam die EU-Kommission zu dem Schluss, dass kaum Verbesserungsbedarf bestehe und allenfalls Vollzugsdefizite festzustellen seien, obwohl u.a. aus der Wirtschaft ein solcher Bedarf geltend gemacht wurde.

II. Bürokratieentlastung als Ziel

Eine Kehrtwende hat die EU-Kommission nunmehr im Mai 2025 mit ihrem „vierten Omnibus-Paket" eingeleitet, um kleine und mittlere Unternehmen von Bürokratiekosten zu entlasten. Im Bereich des Datenschutzes schlägt die EU-Kommission insbesondere eine Änderung von Art. 30 DSGVO zur Führung eines „Verzeichnisses von Verarbeitungstätigkeiten" durch verantwortliche Stellen vor.

Wir begrüßen das übergeordnete Ziel der EU-Kommission, den Verwaltungsaufwand zu verringern und die regulatorische Kohärenz für EU-Unternehmen, einschließlich Kreditinstitute, zu optimieren. Der Vorschlag des Omnibus-IV-Pakets, Organisationen mit weniger als 750 Mitarbeitern von den Aufzeichnungspflichten gemäß Art. 30 Abs. 5 DSGVO zu befreien, ist ein Schritt in die richtige Richtung. Allerdings sollten sich die datenschutzrechtlichen Dokumentationspflichten auch an Art, Umfang und Risiko der Datenverarbeitung orientieren und nicht nur an Unternehmensgrößen. Im Rahmen der Risikogewichtung muss der Aspekt der Informationssicherheit stärker beachtet werden. Datentransfers innerhalb besonders gesicherter Systeme stellen für Betroffene ein deutlich geringeres Risiko dar. Soweit IT-Systeme bereits in anderen Bereichen als ausreichend sicher gegen bestimmte Risiken wie Cyberattacken gesehen werden, muss diese Wertung beachtet werden.

Auch reicht die Initiative der EU-Kommission zur Bürokratieentlastung nicht aus. Die DSGVO ließe sich noch in anderen Punkten vereinfachen und modernisieren. Die Akzeptanz des Datenschutzes bei Bürgern und Unternehmen würde gefördert, wenn die DSGVO von unverhältnismäßigem bürokratischem Aufwand befreit und das Datenschutzrecht in der Anwendung vereinfacht und der Fokus stärker auf risikoreichere Verarbeitungen gerichtet würde. Fraglich ist auch, ob aufgrund des Fortschreitens der technischen Entwicklungen (z. B. cloud-basierte Anwendungen, KI-gestützte Instrumente) die DSGVO hierfür noch die richtigen Antworten hat bzw. wie die Anforderungen der DSGVO hiermit in Einklang zu bringen sind.

B. Auswahl verbesserungsbedürftiger Regelungen

Die Kreditinstitute in Deutschland haben erhebliche Anstrengungen unternommen, die DSGVO sachgerecht umzusetzen. Aufgrund der inzwischen gesammelten Erfahrungen ist insbesondere der folgende Handlungsbedarf festzustellen:

I. Allgemein

1. Erweiterung des Verhältnismäßigkeitsgrundsatzes und der Risikoorientierung

Das Verhältnismäßigkeitsprinzip findet sich bereits in Art. 24 DSGVO. Auch die spezielleren Art. 25, 32 und 35 DSGVO eröffnen dem Verantwortlichen Abwägungsspielräume. Jedoch sollte sich die Umsetzung des Datenschutzes insgesamt am Verhältnismäßigkeitsgrundsatz orientieren. Daher ist die Notwendigkeit von Schutzmaßnahmen am jeweiligen Risiko der Datenverarbeitung auszurichten. Ebenso sollten Einwilligungs- und Zweckbindungsanforderungen einer praxisnahen Überprüfung unterzogen werden, insbesondere mit Blick auf neue, innovative Nutzungen (z. B. KI-Trainingsdaten). Für nicht sensible Bereiche könnten flexiblere Widerspruchslösungen (Opt-out) geprüft werden. Zudem sollte eine unionsweit einheitliche Definition für „risikoarme" Verarbeitungen geschaffen und mit Positiv- bzw. Whitelists (z. B. für DSFA) unterlegt werden, um den Unternehmen mehr Rechtssicherheit zu geben. Soweit ein KI-Training durch einen sicheren IT-Rahmen und den Ausschluss der Datenextraktion von Trainingsdaten aus dem KI-Modell kein relevantes Risiko für Betroffene darstellt, sollte auch diese Art der Prozessoptimierung zulässig sein.

2. Rolle der Datenschutzaufsicht bei der Umsetzung der DSGVO

Bei der Umsetzung der DSGVO ist auch die Datenschutzaufsicht gefragt, die hierbei aber nicht die Rolle eines Ersatzgesetzgebers einnehmen darf. So können von der Datenschutzaufsicht entwickelte praxistaugliche Musterdokumente, aktuelle Checklisten und regelmäßig überarbeitete Orientierungshilfen eine wertvolle Hilfestellung nicht nur für kleinere Unternehmen sein. Dabei sollten die Aufsichtsbehörden aber ebenso den Verhältnismäßigkeitsgrundsatz berücksichtigen und nicht durch eine zu extensive Auslegung der DSGVO deren Anforderungen noch weiter nach oben schrauben. Hohe Umsetzungskosten durch immer neue Anforderungen verletzen den Verhältnismäßigkeitsgrundsatz. Gleichwohl sollte die einheitliche europäische Auslegung und Durchsetzung der DSGVO gestärkt werden. Unterschiedliche nationale Vollzugspraxen führen zu Fragmentierung und Wettbewerbsnachteilen. Kohärenz und Rechtsklarheit sollten in der gesamten EU gewährleistet sein.

II. Weiterentwicklung der DSGVO im Hinblick auf den Einsatz von Instrumenten der Künstlichen Intelligenz (KI)

1. Allgemein

Die zunehmende Verbreitung und Relevanz von KI-Technologien stellt das bestehende Datenschutzrecht vor strukturelle und normative Herausforderungen. Die DSGVO bietet zwar einen europaweit einheitlichen Rahmen für den Schutz personenbezogener Daten, ist jedoch aufgrund ihrer Entstehung vor einem Jahrzehnt bislang nicht in allen Aspekten auf die besonderen technischen und funktionalen Eigenheiten von KI-Systemen ausgerichtet. Im Zusammenspiel mit der Verordnung (EU) 2024/1689 des Europäischen Parlaments und des Rates vom 13. Juni 2024 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (KI-Verordnung) stellen sich in der Praxis eine Vielzahl von Einzelfragen, insbesondere zur Anonymisierung und Pseudonymisierung von Daten, zu einschlägigen Rechtsgrundlagen, zu Zweckänderungsgesichtspunkten, zur Verarbeitung von sensiblen personenbezogenen Daten und zur automatisierten Entscheidungsfindung mit Hilfe von KI. Es besteht daher ein erhöhter Bedarf an klarstellenden Regelungen und an einer kohärenten Verzahnung der datenschutzrechtlichen Anforderungen mit den regulatorischen Vorgaben der KI-Verordnung.

Ziel muss es sein, einerseits den effektiven Schutz personenbezogener Daten sowie die Sicherung der Grundrechte auch im Kontext datengetriebener KI-Anwendungen uneingeschränkt zu gewährleisten. Gleichzeitig gilt es, innovationsfreundliche Rahmenbedingungen zu schaffen, die die technologische Wettbewerbsfähigkeit und die Entwicklung vertrauenswürdiger KI-Systeme sowohl auf nationaler als auch auf europäischer Ebene nachhaltig fördern. Eine präzisierende Fortentwicklung der DSGVO in zentralen Anwendungsfeldern erscheint daher erforderlich, um regulatorische Klarheit zu schaffen und rechtssichere sowie verantwortungsvolle KI-Anwendungen zu ermöglichen. Zwar versuchen die Datenschutzaufsichtsbehörden bereits Unterstützung zu Auslegungsfragen zu geben[1], doch besteht hier weiterer Unterstützungs- und Klärungsbedarf durch den Gesetzgeber und die nach der KI-Verordnung und DSGVO zuständigen Aufsichtsbehörden. Sowohl die gesetzlichen Vorgaben als auch die Aufsichtspraxis sollten einen widerspruchsfreien Handlungsrahmen bilden.

2. Art. 6 DSGVO – Mehr Rechtssicherheit für die Verarbeitung personenbezogener Daten durch KI-Systeme

Im Falle der Verarbeitung personenbezogener Daten durch KI-Systeme hält es der EU-Datenschutzausschuss für erforderlich, für jede Phase des Lebenszyklus des KI-Systems/-Modells eine geeignete Rechtsgrundlage für die Verarbeitung zu ermitteln, wobei unter bestimmten Bedingungen, die einer spezifischen Abwägungsprüfung unterliegen, die Verwendung des berechtigten Interesses bevorzugt wird.[2] Dieser Ansatz ist übermäßig komplex, zumal die

[1] Vgl. u.a. https://www.datenschutzkonferenz-online.de/media/oh/20240506_DSK_Orientierungshilfe_KI_und_Datenschutz.pdf

[2] Vgl. https://www.edpb.europa.eu/system/files/2025-05/edpb_opinion_202428_ai-models_de.pdf

Interessenabwägung nach Art. 6 Abs. 1 lit. f DSGVO individuell vorzunehmen ist. Um mehr Rechtssicherheit für die Verarbeitung personenbezogener Daten durch KI-Systeme zu erreichen, sollte erwogen werden, Art. 6 DSGVO diesbezüglich zu überarbeiten. So könnte z. B. die Verarbeitung personenbezogener Daten im KI-Zusammenhang in der Trainingsphase von Modellen sowie der Anwendung von KI-Modellen auf eine rechtssichere Grundlage gestellt werden, ohne dass auf das berechtigte Interesse zurückgegriffen werden muss. Auch könnten spezielle Rahmenbedingungen für General Purpose AI (GPAI) geschaffen werden, d. h. in Fällen, in denen die Zwecke des Modells vielfältig und nicht vorab festgelegt sein können, da es sich um ein Modell für allgemeine Zwecke handelt.

3. Art. 15 DSGVO – Betroffenenrechte anpassen

Im Kontext automatisierter Trainingsprozesse innerhalb von KI-Systemen stellt sich die Frage, inwieweit klassische Betroffenenrechte – etwa auf Auskunft oder Löschung gemäß Art. 15 ff. DSGVO – von der verantwortlichen Stelle überhaupt sinnvoll und verhältnismäßig umgesetzt werden können. Denn KI-Modelle verarbeiten Trainingsdaten in der Regel nicht in einer Weise, die eine nachträgliche personenbezogene Rückverfolgbarkeit ohne erhebliche Zusatzinformationen ermöglicht oder bei denen eine nachträgliche Löschung oder Auskunftserteilung über personenbezogene Daten technisch überhaupt möglich ist. In Konstellationen, in denen ein Rückschluss auf identifizierbare Personen für andere Verantwortliche als die Inhaber der Trainingsdaten praktisch ausgeschlossen ist, sollte geprüft werden, inwieweit sich Betroffenenrechte sachgerecht anpassen lassen, um eine funktionale Umsetzung von KI-Anwendungen nicht unverhältnismäßig zu erschweren.

4. Art. 22 DSGVO – Konzept des Verbots automatisierter Entscheidungsfindungen im Lichte der KI-Verordnung überdenken

Die Digitalisierung und der Einsatz von KI werden zu einer stärkeren Automatisierung der Entscheidungsfindung führen. Art. 22 DSGVO sieht das Recht vor, keiner automatisierten individuellen Entscheidungsfindung unterworfen zu werden. Der EuGH interpretiert dies in seiner Rechtsprechung (Urteil vom 7. Dezember 2023 – Rs. C-634/21) als „grundsätzliches Verbot" und erweitert mit dem Merkmal der „Maßgeblichkeit" sogar den Anwendungsbereich der Vorschrift, die eigentlich nur für ausschließlich automatisierte Entscheidungen gilt. Dies dürfte jedoch im Widerspruch zum Ziel der Europäischen Kommission stehen, den Einsatz und die Entwicklung neuer Technologien zu fördern, die zu einer genaueren Entscheidungsfindung beitragen können. Ein solcher Ansatz erscheint nicht nur anachronistisch, sondern untergräbt auch die Richtung, die die EU mit ihrer digitalen Gesetzgebung einschlägt, insbesondere die Stärkung ihrer digitalen Strategie und Datenwirtschaft. Eine Überarbeitung von Art. 22 DSGVO wäre daher zu begrüßen, um eine ausgewogene Lösung zur Wahrung von Datenschutzrechten der Betroffenen einerseits und dem rechtssicheren Einsatz von KI-Instrumenten andererseits zu erreichen. Um mehr Rechtssicherheit zu schaffen, sollte der Gesetzgeber zudem die Transparenzanforderungen in der DSGVO (u. a. Art. 15 Abs. 1h) und der KI-Verordnung (u. a. Art. 86) synchronisieren.

5. Art. 35 DSGVO - Datenschutzfolgenabschätzung nach DSGVO und Grundrechtsfolgenabschätzung nach KI-Verordnung synchronisieren

Die Datenschutzfolgenabschätzung nach Art. 35 DSGVO sowie die Grundrechtsfolgenabschätzung für Hochrisiko-KI-Systeme nach Art. 27 KI-Verordnung verfolgen übereinstimmend das Ziel, potenzielle Risiken für die Rechte und Freiheiten natürlicher Personen im Vorfeld technischer Systementwicklungen systematisch zu identifizieren, zu bewerten und – soweit möglich – zu minimieren. Beide Instrumente beruhen auf dem präventiven Risikomanagementansatz des europäischen Grundrechtsschutzes, sind bislang jedoch weder inhaltlich noch methodisch aufeinander abgestimmt.

Vor diesem Hintergrund erscheint eine systematische Koordinierung beider Prüfregime geboten. Die gegenwärtige Parallelität der Anforderungen birgt das Risiko redundanter Prüfprozesse auch in ggf. unterschiedlichen Fachbereichen aufgrund Zuständigkeitsverteilungen sowie potenziell widersprüchlicher Wertungen in Bezug auf die Schutzbedürftigkeit betroffener Rechtsgüter. Zur Vermeidung doppelten Verwaltungsaufwands und zur Steigerung der rechtspraktischen Kohärenz ist eine stärkere inhaltliche und strukturelle Verzahnung von Datenschutzfolgenabschätzung und Grundrechtsfolgenabschätzung erforderlich.

III. Verarbeitung personenbezogener Daten

1. Art. 4 DSGVO – Rechtssicherheit bei Anonymisierung und Pseudonymisierung schaffen

Eine verstärkte innovative und zugleich verantwortungsvolle Datennutzung erfordert einheitliche und rechtssichere Standards für eine wirksame Anonymisierung personenbezogener Daten. Die rechtssichere Anonymisierung personenbezogener Daten ist eine Kernvoraussetzung für datengetriebene Geschäftsmodelle (u. a. bei KI-Anwendungen) und für die Verfügbarkeit qualitativ hochwertiger Daten. Zugleich werden hierdurch ein hohes Datenschutzniveau und das Vertrauen der Betroffenen in den Schutz ihrer personenbezogenen Daten gewährleistet. In der Praxis stehen die Kreditinstitute jedoch vor der Herausforderung, dass weder klare rechtliche Vorgaben noch einheitliche technische Standards und Methoden für eine De-Personalisierung von Daten existieren. Die DSGVO enthält weder eine Legaldefinition von „Anonymisierung" noch einen Mindeststandard, ab wann die Identifizierbarkeit einer Person ausgeschlossen ist. Ebenso fehlen praxistaugliche Vorgaben für eine dauerhafte Pseudonymisierung – insbesondere bei älteren Bestandsdaten, für die keine Einwilligung nach heutigen Standards vorliegt. Dies erschwert nicht nur die Nutzung bestehender Datenbestände (u. a. bei KI-Anwendungen), sondern auch die vertragliche Ausgestaltung von Auftragsverarbeitungen. Erforderlich sind klare Regelungen, wann eine Anonymisierung vorliegt. Auch sollte gesetzlich unterstrichen werden, dass sowohl die Anonymisierung als auch die Pseudonymisierung von Daten durch die verantwortliche Stelle in der Regel zulässig ist und eine gesonderte Erfüllung der Erlaubnistatbestände nach Art. 6 DSGVO nicht erforderlich ist. Dies ließe sich beispielsweise systematisch umsetzen, indem man Art. 6 Abs. 4 DSGVO zur Zweckänderung dahingehend erweitert, dass

Anonymisierung und Pseudonymisierung als ausdrücklich erlaubte Weiterverarbeitungen stets von der Rechtsgrundlage der ursprünglichen Verarbeitung gedeckt sind.

2. Art. 5 Abs. 2 DSGVO - Nachweispflichten nach dem Verhältnismäßigkeitsgrundsatz aussteuern

Die sehr allgemein und abstrakt gefasste Nachweispflicht (accountability) in Art. 5 Abs. 2 DSGVO in Kombination mit dem übermäßigen Sanktionsregime in Art. 83 DSGVO hat zu einer enormen Bürokratisierung der unternehmensinternen Datenschutzkontrolle und zu einem gewaltigen Ausufern der Dokumentationspflichten in den Unternehmen geführt.

Gewiss ist eine ordnungsgemäße Dokumentation der Umsetzung der DSGVO sinnvoll, doch sollte diese sich auf das Erforderliche beschränken. Auch der Grad der Datenschutzrisiken sollte ausschlaggebend für den Umfang von Nachweispflichten sein. Eine automatische Verknüpfung eines etwaigen Dokumentationsdefizits mit dem strengen Sanktionsregime ist unverhältnismäßig. Hier sollte ein stärker risikobasierter Ansatz betont werden.

Wünschenswert wäre außerdem die Möglichkeit der Bezugnahme auf und der gegenseitigen Anerkennung von gesetzlich geforderten Dokumentationen (DSGVO, bankaufsichtsrechtlichen Regelungen zur Risikosteuerung [MaRisk], Digital Operational Resilience Act [DORA], bankaufsichtlichen Anforderungen an die IT [BAIT], gemeinsames Cybersicherheitsniveau [NIS2], ISO-Standards).

3. Art. 6 Abs. 1 lit. c, Abs. 2 und 3 DSGVO – DSGVO sollte Vorrang von Spezialgesetzen mit Datenschutzrelevanz deutlicher akzeptieren

Das Verhältnis der DSGVO zu anderen Rechtsvorschriften bereitet immer wieder Probleme in der Praxis. Gerade Kreditinstitute unterliegen vielen spezialgesetzlichen und bankaufsichtsbehördlichen Anforderungen zur Datenverarbeitung (in Deutschland z. B. MaRisk, BAIT, DORA). Diese spezialgesetzlichen Regelungen müssen die Leitlinie bilden und auch die damit verbundene Verarbeitung personenbezogener Daten rechtfertigen. Ein Unternehmen wäre völlig überfordert, die Kompatibilität der spezialgesetzlichen Regelungen mit der DSGVO eigenständig zu überprüfen. Dies ist allein Aufgabe des Gesetzgebers. Die DSGVO sollte daher deutlicher den sektorspezifischen Regelungen nachgeordnet werden, um Widersprüche zu vermeiden.

4. Art. 9 DSGVO - Anwendungsbereich besser abgrenzen und Vertrag als Erlaubnistatbestand ergänzen

Der Anwendungsbereich von Art. 9 Abs. 1 DSGVO wird vom EuGH regelmäßig sehr weit ausgelegt, was zur Folge hat, dass auch Daten, aus denen lediglich mittelbar Rückschlüsse auf sensible personenbezogene Daten gezogen werden können, als Daten i. S. v. Art. 9 Abs. 1 DSGVO betrachtet werden. Im Zahlungsverkehr betrifft dies häufig Umsatzdaten, die als sog. Mischdatensätze aufgrund ihres Empfängers oder Verwendungszwecks Rückschlüsse zulassen auf z. B. den Gesundheitszustand oder die Partei- oder Gewerkschaftszugehörigkeit des Zahlenden. Dies

hat zur Folge, dass Datenverarbeitungen sich regelmäßig an den strengeren Anforderungen von Art. 9 DSGVO messen lassen müssen und viele Rechtsgrundlagen aus Art. 6 DSGVO unanwendbar sind. Wir regen daher an, Art. 9 Abs. 1 DSGVO sachgerecht einzuschränken. Bei Mischdatensätzen, die lediglich mittelbar Rückschlüsse auf sensible personenbezogene Daten zulassen, die nicht den Schwerpunkt der Verarbeitungstätigkeit bilden, ist eine kontextabhängige Betrachtung erforderlich, welche sich (wie vielfach in der Literatur vertreten) an der Auswertungsabsicht des Verantwortlichen oder an einem Zu-Nutze-Machen des sensiblen Informationsgehalts durch den Verantwortlichen orientieren sollte.

In den täglichen Geschäftsbeziehungen zwischen Kunde und Bank kommt es zudem immer wieder vor, dass sensible personenbezogene Daten vom Betroffenen unaufgefordert an das Kreditinstitut übermittelt werden („aufgedrängte Daten"). Da Art. 9 Abs. 2 lit. a DSGVO jedoch keine konkludente Einwilligung gelten lässt und die Daten aufgrund des begrenzten Empfängerkreises auch nicht „offensichtlich öffentlich gemacht" wurden, dürfen sie nach derzeitiger Rechtslage nicht verarbeitet werden. Um den Kundeninteressen in solchen Fällen stärker Rechnung zu tragen, wird angeregt, die in Art. 9 Abs. 2 lit. e DSGVO normierte Verbotsausnahme tatbestandlich um personenbezogene Daten zu erweitern, die von der betroffenen Person freiwillig bereitgestellt wurden, ohne dass der Verantwortliche zu deren Bereitstellung aufgefordert hat.

Des Weiteren sollte in Art. 9 Abs. 2 DSGVO als neuer Erlaubnistatbestand die für den Abschluss und die Erfüllung eines Vertrags erforderlichen Verarbeitung sensibler Daten aufgenommen werden. Denn ist die Verarbeitung sensibler Daten für die Vertragsanbahnung und -erfüllung erforderlich, bedarf es nicht einer gesonderten Einwilligung des Betroffenen. Vielmehr ist dann der jeweilige Vertrag zugleich Rechtsgrundlage als auch Verbotsausnahme. Als Beispiel aus der Praxis ist die Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person zu nennen. Nach der EU-Zahlungsdiensterichtlinie (2015/2366) ist für Online-Transaktionen eine starke Kundenauthentifizierung vorzusehen, bei der auch biometrische Daten eingesetzt werden können. Haben Kunde und Kreditinstitut sich auf die Authentifizierung mittels biometrischer Daten vertraglich geeinigt, sollte dies sogleich auch nach Art. 9 DSGVO legitimiert sein.

IV. Rechte der Betroffenen

1. Art. 13 und 14 DSGVO - Zweistufenansatz bei Informationspflichten einführen

Die Informationspflichten für die verantwortliche Stelle in Art. 13 und 14 DSGVO sind zu detailliert und übermäßig. Sie sollten auf ein vernünftiges Maß beschränkt werden, um Betroffene nicht mit Informationen zu überfluten – weniger ist mehr. Vorzugswürdig wäre ein zweistufiger Ansatz, d. h. ein Überblick über wesentliche Aspekte der Datenverarbeitung bei der verantwortlichen Stelle auf erster Stufe und Detailinformationen zum Abruf/auf Nachfrage des Betroffenen auf zweiter Stufe. Dies würde Unternehmen und Betroffene entlasten und im Ergebnis für mehr Transparenz gegenüber den Betroffenen sorgen, da hinsichtlich wirklich relevanter Informationen fokussiert informiert würde. Auch ist es unverhältnismäßig, dass bereits ein

vergleichsweise kleines Informationsdefizit zu Sanktionen führen oder als Wettbewerbsverstoß eingeordnet werden kann (vgl. die zu weite Auslegung im Urteil des BGH v. 27. März 2025 – Az. I ZR 186/17).

2. Art. 15 DSGVO – Auskunftsrecht auf seinen Zweck zurückführen und Auskunftserteilung erleichtern

Das Auskunftsrecht des Betroffenen nach Art. 15 DSGVO ist ein Grundpfeiler des Datenschutzrechts, wie auch die Rechtsprechung des EuGH belegt. Doch zeigen die Praxis und die Rechtsprechung (vgl. EuGH, Urt. v. 26. Oktober 2023 – Rs. C-307/22, BGH, Urt. vom 5. März 2024 – Az. VI ZR 330/21), dass dieses Recht teilweise für datenschutzfremde Zwecke exzessiv instrumentalisiert wird (z. B. in arbeitsrechtlichen Beendigungsstreitigkeiten im Rahmen von Verhandlungen über Abfindungen). Deshalb sollte im Sinne des EG 63 S. 1 DSGVO klargestellt werden, dass das Auskunftsrecht ausschließlich dazu dienen darf, dass der Betroffene damit seine Datenschutzrechte und keine anderweitigen Zwecke verfolgt. Außerdem wäre wünschenswert, entweder in den Erwägungsgründen oder – bestenfalls – tatbestandlich klarer zu definieren, wann von einem offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Antrag ausgegangen werden kann, um den Verantwortlichen zur Verweigerung der Auskunftserteilung zu berechtigen (vgl. Art. 12 Abs. 5 S. 2 DSGVO).

Die Bearbeitung von Auskunftsersuchen durch die verantwortliche Stelle sollte dahingehend erleichtert werden, dass der Betroffene grundsätzlich darlegen sollte, auf welche konkreten Bereiche sich sein Auskunftsersuchen erstreckt. Insofern sollte EG 63 S. 7 DSGVO tatbestandlich Niederschlag finden.

Vom Auskunftsrecht sollten solche Daten ausgenommen sein, die der Verantwortliche dem Betroffenen in der Vergangenheit nachweislich bereits zur Verfügung gestellt hat oder die lediglich zur Erfüllung gesetzlicher Aufbewahrungspflichten vorgehalten werden, also nur noch zu Archivzwecken gespeichert sind.

Der Begriff der Kopie in Art. 15 Abs. 3 S. 1 DSGVO sollte klarer definiert werden. Zudem wäre es zu begrüßen, wenn deutlicher als bisher dargestellt würde, dass das Recht auf Erhalt einer Kopie Betroffenen kein Wahlrecht hinsichtlich der Form der Datenwiedergabe gewährt.

3. Art. 17 DSGVO - Sperrung von Daten als Alternative zur Löschung bei verfahrenstechnischen Grenzen

Das Löschen von Daten kann technisch anspruchsvoll bis faktisch oder rechtlich unmöglich sein, was zum Teil von den verantwortlichen Stellen gar nicht hinreichend beeinflussbar ist (Stichwort Wettbewerbsmacht einzelner Anbieter). Ist die verantwortliche Stelle auf einen externen Anbieter angewiesen, sollte dieser im Sinne einer „Anbieterhaftung" in die Pflicht genommen werden können (siehe auch Stellungnahme zu Art. 25 DSGVO).

Zudem sollte erwogen werden, die bestehenden hohen Löschanforderungen zu qualifizieren oder zu begrenzen, insbesondere durch eine stärkere Betonung der technischen Durchführbarkeit bei der Umsetzung von Löschungsanfragen und die Ermöglichung alternativer Schutzmaßnahmen in Fällen fehlender technischer Durchführbarkeit (z. B. Sperren der betroffenen Daten oder Zugriffseinschränkungen auf archivierte Daten). Überdies sollte anerkannt werden, dass ein Löschbegehren nach Art. 17 DSGVO auch stets durch Anonymisierung der Daten erfüllt werden kann.

Die Gleichbehandlung aller personenbezogenen Daten, unabhängig von ihrer Art, stellt insbesondere bei der Löschung von geschäftsbezogenen Dokumenten mit personenbezogenen Daten eine Herausforderung dar. Im B2B-Bereich sowie für Soloselbstständige und kleine Unternehmen sollten gezielte Vereinfachungen in Betracht gezogen werden, um unnötige Bürokratie abzubauen und den Schutz auf tatsächlich risikobehaftete Verarbeitungen zu konzentrieren.

Das Tatbestandsmerkmal der Erforderlichkeit in Art. 17 Abs. 3 lit. e DSGVO sollte konkretisiert werden. Nach derzeitiger Auslegungspraxis der Aufsichtsbehörden kann sich auf diese Regelung nur berufen, wer die konkrete Gefahr eines Rechtsstreites darlegen kann. Dies führte in der Vergangenheit wiederholt zur Löschung von Daten, die in einem späteren Rechtsstreit benötigt wurden. Hier sollte eine Datensperrung ausreichen.

V. Verantwortlicher und Auftragsverarbeiter

1. Art. 25 DSGVO – Einbeziehung von Herstellern

Der Adressatenkreis von Art. 25 DSGVO zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sollte auf Hersteller von Datenverarbeitungsprodukten ausgedehnt werden, denn diese sind die Produktverantwortlichen. Derzeit sind die Produktanwender gezwungen, von Herstellern erworbene Produkte vor deren Einsatz auf Datenschutzschwachstellen zu prüfen, was erheblichen Aufwand verursacht und bei der Nutzung komplexer Software wie bspw. KI-Anwendungen (technisch) nicht zu leisten ist. Auch lassen sich Produkte vom Anwender oft nicht anpassen. Die laufende Debatte über die datenschutzkonforme Nutzung von Microsoft 365-Produkten verdeutlicht dieses Problem. Hersteller sollten verpflichtet sein, datenschutzrechtliche Vorgaben bereits in der Produktentwicklung zu berücksichtigen und sich am Stand der Technik zu orientieren, um den Verantwortlichen bei Einsatz des Produkts die Erfüllung ihrer Verpflichtungen zu ermöglichen. Da Hersteller von Diensten, Produkten und Anwendungen gerade in Zeiten immer schnellerer technologischer Weiterentwicklung eine Schlüsselfunktion sowohl für Datenschutz als auch Datensicherheit einnehmen, sollte ihnen unter der DSGVO eine gesonderte Rolle (bspw. „produktverantwortliche Stelle") mit eigenständigen Pflichten (und Sanktionierungsmöglichkeiten) zugewiesen werden. Insbesondere sollten Hersteller in die Pflicht genommen werden, die Datenschutzkonformität ihrer Produkte entsprechend der Einsatzzwecke zu gewährleisten, wozu auch eine datenschutzkonforme Grundeinstellung für die öffentlich beworbene Standardnutzung gehören sollte.

2. Art. 26 DSGVO – Ansatz der gemeinsamen Verantwortung bedarf Überarbeitung

Das Merkmal der „gemeinsamen Bestimmung über die Mittel und Zwecke" zur Einstufung als „gemeinsame Verantwortung" in Art. 26 DSGVO ist sehr generisch. Es wird daher vorgeschlagen, die Fallgruppen der gemeinsamen Verarbeitung klarer zu definieren, indem man über das allgemeine Merkmal der gemeinsamen Bestimmung über die Mittel und Zwecke hinausgeht. Der Aufwand für die Ausgestaltung der gemeinsamen Verarbeitung im horizontalen Verhältnis zwischen den Verarbeitern und im vertikalen Verhältnis zu den Betroffenen steht in vielen Fällen nicht in einem angemessenen Verhältnis zum datenschutzrechtlichen Mehrwert für die Betroffenen. Die gesamtschuldnerische Haftung ist in der Praxis oft unverhältnismäßig, selbst unter Berücksichtigung des Einblicks und der Einflussnahme auf die Datenverarbeitung der jeweils anderen Partei. Daher wird eine angemessene Begrenzung der gemeinsamen Haftung im Außenverhältnis empfohlen. Außerdem sollte allein die sachnächste Aufsichtsbehörde zuständig sein, um widersprüchliche aufsichtsbehördliche Entscheidungen zu vermeiden.

3. Art. 33 und 34 DSGVO – Meldepflichten bei Datenpannen vereinfachen

Zur Meldung von Datenschutzvorfällen wünschen wir uns einfachere Verfahren. Die Meldepflicht sollte nur gelten, wenn von der verantwortlichen Stelle ein voraussichtlich hohes Risiko für die Rechte und Freiheiten festgestellt worden ist. Der aktuelle Zeitrahmen für Meldungen erscheint zu knapp, insbesondere bei Vorfällen vor Feiertagen oder an Freitagen. Wochenenden und Feiertage sollten bei der Fristberechnung ausgeschlossen sein, um den rechtlichen Anforderungen gerecht zu werden und die Fallbearbeitung auch qualitativ gut bewältigen zu können. Zum Teil nehmen die Sachverhaltsermittlung und nötige Aufklärungen mehr Zeit in Anspruch, was an Freitagen oder vor Feiertagen in der Praxis oft zu Schwierigkeiten und ggf. zu unvollständigen oder unbegründeten Meldungen führt, nur um die 72-Stunden-Frist einhalten zu können. Als Lösung bietet sich in Anlehnung an den Arbeitstagesansatz in Art. 3 Abs. 3 und 5 der Verordnung Nr. 1182/71 des Rates zur Festlegung der Regeln für die Fristen, Daten und Termine an, die Fristbemessung in Art. 33 Abs. 1 S. 2 DSGVO von „72 Stunden" auf „drei Arbeitstage" umzustellen.

VI. Art. 44 ff. DSGVO – Drittstaatendatentransfer rechtssicher gestalten

Um den Drittstaatendatentransfer sicherer und einheitlicher zu gestalten, schlagen wir vor, dass die EU-Kommission kontinuierlich Kriterien für ein Transfer Impact Assessment (TIA) überprüft. Diese Kriterien sollten nicht nur bestimmte Datenempfänger, sondern auch den allgemeinen rechtlichen Rahmen und Datenschutzstandards in diesen Ländern berücksichtigen. Darüber hinaus sollten Transfer Impact Assessments für Übertragungen in Drittländer öffentlich über Datenschutzaufsichtsbehörden zugänglich sein, um Unternehmen bei individuellen Bewertungen zu unterstützen, Transparenz zu fördern und Ressourcen zu sparen.