BDI

INNONATION

POSITION | DIGITALISIERUNG | DATENSCHUTZ

Reformbedarf in der EU-Datenschutzgrundverordnung (DSGVO)

Forderungen der Industrie für mehr Ausgewogenheit und Innovationsfreundlichkeit im Datenschutzrecht

1. Oktober 2025

Vorbemerkung

In der heutigen Informationsgesellschaft ist die sichere und effiziente Verarbeitung personenbezogener Daten für die gesamte Industrie von zentraler Bedeutung. Ein einheitliches Datenschutzrecht, das gleichermaßen Vertrauen fördert und Innovationen ermöglicht, ist hierfür essenziell. Nach Einschätzung des BDI hat die Datenschutzgrundverordnung (DSGVO) mit den darauf basierenden nationalen Umsetzungsmaßnahmen maßgeblich zur Sensibilisierung für den Schutz personenbezogener Daten beigetragen. Nicht ohne Grund wurden die wesentlichen Grundzüge der DSGVO von Drittstaaten als Vorbild für eine Reform des Datenschutzrechts verwendet. Ein hohes Datenschutzniveau und damit verbunden ein festes Vertrauen in den Datenschutz ist nach der Überzeugung der deutschen Industrie eine wesentliche Voraussetzung für die erfolgreiche Entwicklung datenbasierter Geschäftsmodelle.

Für die Unternehmen ist die Umsetzung der DSGVO-Vorgaben in der Praxis jedoch mit einem enormen bürokratischen Aufwand und erheblichen Rechtsunsicherheiten verbunden, die den von der DSGVO auch bezweckten freien Datenfluss behindern und Innovationen hemmen. Nach einer vom BDI in Auftrag gegebenen Studie zur aktuellen Situation der Datenwirtschaft in Deutschland bezeichnen 85 Prozent der befragten Unternehmen „datenschutzrechtliche Grauzonen“ generell als Hemmnis für die wirtschaftliche Nutzung von Daten.[1] Zusätzlich erschwert wird die Umsetzung der Datenschutzregeln durch deren uneinheitliche Auslegung und Durchsetzung in den Mitgliedstaaten und auf nationaler Ebene sowie divergierende nationale Datenschutzgesetze. Diese Rechtsfragmentierung steht dem in der EU angestrebten Level Playing Field entgegen, was zu Standort- und Wettbewerbsnachteilen der Unternehmen in den Mitgliedstaaten führt. Darüber hinaus kann die DSGVO mit dem Inkrafttreten eines neuen und komplexen digitalen Regelwerks in der EU manchmal zu einer zusätzlichen regulatorischen Komplexität führen, ohne dass dies für die betroffenen Personen von Vorteil ist. Diese Komplexität droht die Ziele der Kommission zu behindern, die Wettbewerbsfähigkeit Europas zu stärken und Chancen, Innovation und Wachstum in der digitalen Wirtschaft der EU zu fördern. Um den freien Datenverkehr unter Wahrung der Grundrechte in der Praxis zu gewährleisten und zu fördern,

1 „Datenwirtschaft in Deutschland – Wo stehen die Unternehmen in der Datennutzung und was sind ihre größten Hemmnisse?“, IW-Studie im Auftrag des BDI, Februar 2021, abrufbar unter https://bdi.eu/media/publikationen/?publicationtyhttps://bdi.eu/media/publikationen/?publicationtype=Studien#/publikation/news/datenwirtschaft-in-deutschland/.

Dr. Michael Dose | Digitalisierung und Innovation | T: +49 30 2028-1560 | m.dose@bdi.eu | www.bdi.eu

sollten die Datenschutzregeln unter verstärkter Berücksichtigung des in der DSGVO verankerten risikobasierten Ansatzes und des Verhältnismäßigkeitsgrundsatzes kritisch überprüft sowie praxisgerecht angepasst und fortentwickelt werden. Viele Probleme in der Anwendungspraxis rühren tatsächlich von einer uneinheitlichen Interpretation und Durchsetzung der Datenschutzregeln durch die Aufsichtsbehörden. Diese können überwiegend durch homogene Leitlinien, Orientierungshilfen oder Verhaltenskodizes adäquat adressiert werden.

Die DSGVO weist jedoch selbst enorme Entwicklungs- und Erleichterungspotenziale auf, etwa bei den Erlaubnistatbeständen, Transparenzpflichten oder Anonymisierungskriterien, die allein durch untergesetzliche Maßnahmen nicht voll ausgeschöpft werden können. Der BDI begrüßt daher die Bestrebungen, die Anforderungen aus der DSGVO an die Industrie über die von der Europäischen Kommission am 21. Mai 2025 im Rahmen des sogenannten Omnibus-IV-Pakets vorgeschlagenen Änderungen der DSGVO für Small Mid-Caps (SMC) zu vereinfachen. Ziel der Reformen muss sein, einen effektiven Datenschutz herzustellen, ohne das Schutzniveau der DSGVO abzusenken oder den etablierten Ordnungsrahmen fundamental zu verändern.

Forderungen und Vorschläge des BDI

Die Vorschläge halten zwar das Schutzniveau der DSGVO aufrecht, werden den Bürokratieaufwand jedoch nur marginal reduzieren. Um die Unternehmen tatsächlich zu entlasten, sind weitergehende Anpassungen der DSGVO und ihrer Anwendung erforderlich. Insbesondere sind die folgenden Punkte reformbedürftig:

1. Reform der Grundsätze datenschutzrelevanter Verarbeitung

Der wesentliche Ansatzpunkt, die Unternehmen effektiv zu entlasten, ist eine Reform der Grundsätze datenschutzrelevanter Verarbeitungen. Zuvorderst sollte dazu der risikobasierte Ansatz als Leitprinzip der DSGVO verankert werden. Pflichten, die den Verantwortlichen aus der DSGVO erwachsen, würden so nicht pauschal und abstrakt auferlegt, sondern anhand des individuellen Schutzbedürfnisses eines konkreten Falls bestimmt. Stellt die Verarbeitung personenbezogener Daten etwa nur ein Nebenprodukt eines Verarbeitungsvorgangs dar oder steht allein die technische Information im Vordergrund, sollten keine umfangreichen Informationspflichten oder Dokumentationspflichten zum Schutz der personenbezogenen Daten erforderlich sein. Dennoch muss aktuell die DSGVO vollumfänglich beachten werden, obwohl kein Risiko für die betroffene Person besteht. Dies bindet Ressourcen, verursacht Kosten und hemmt Innovation – ohne erkennbaren Mehrwert für den Datenschutz. Eine präzisere Definition des Begriffs „personenbezogenes Datum“ in Art. 4 Nr. 1 DSGVO würde ermöglichen, den Datenschutz dort zu konzentrieren, wo tatsächlich ein Schutzbedarf besteht. Gleichzeitig würden Unternehmen entlastet, deren Ziel nicht die Nutzung personenbezogener Informationen, sondern rein technischer Erkenntnisse ist. Eine solche Klarstellung wäre ein echter Beitrag zur Praxistauglichkeit und Effizienz der DSGVO.

Weitere Prinzipien des Datenschutzes sind modernisierungsbedürftig, um den technologischen Entwicklungen und modernen Methoden der Datenverarbeitung zu entsprechen. Dies gilt insbesondere für die Prinzipien der Zweckbindung, Speicherbegrenzung, Datenminimierung und der unbegrenzten Rechenschaftspflicht des Verantwortlichen, die zunehmend im Widerspruch zu den Verarbeitungen im Lichte von Big-Data, Künstlicher Intelligenz oder dem Internet-of-Things (IoT) stehen. Sie sollten technologieadäquat angepasst werden. In diesem Zusammenhang sollte auch der gewählte Ansatz, die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO grundsätzlich

einem Verarbeitungsverbot zu unterstellen, evaluiert werden. Für Datenübermittlung innerhalb einer Konzerngesellschaft sollte eine Ausnahme aufgenommen werden, wonach solche Datenübermittlungen nicht als Offenlegung gegenüber Dritten gilt, sondern als interne Verarbeitung eingestuft wird.

Die DSGVO enthält in ausgewählten Normen, insbesondere bei der Auswahl von Sicherheitsmaßnahmen und der Datenschutz-Folgenabschätzung, Elemente eines risikobasierten Ansatzes. Diese punktuelle Anwendung könnte weiterentwickelt werden, um spezifische Pflichten im Lichte konkreter Risiken stärker zu differenzieren. Nur durch eine adäquate Berücksichtigung des Schweregrads des Datenverarbeitungsrisikos für den Betroffenen, lassen sich sachgerechte Lösungen für die von der DSGVO geregelte Vielzahl unterschiedlicher Lebenssachverhalte finden. Gleichwohl wird der risikobasierte Ansatz in der aufsichtsbehördlichen Praxis nicht umfassend beachtet und umgesetzt. Eine stärkere Berücksichtigung der unterschiedlichen Risiken unterschiedlicher Datenverarbeitungsvorgänge bei der rechtlichen Bewertung datenschutzrelevanter Sachverhalte ist nach Überzeugung des BDI daher dringend erforderlich.

Erleichterungen für Unternehmen vorzusehen, deren Datenverarbeitungen keine erhebliche Datenschutzrisiken bergen, ist ein Ansatz, dem konsequent gefolgt werden sollte. Der im Grundsatz richtige Ansatz expliziter Privilegierungen für KMU und SMC in Bezug auf Ausnahmen von Dokumentationspflichten gem. Art. 30 Abs. 5 DSGVO sollte auf alle Unternehmen erweitert werden, solange deren Verarbeitungsvorgänge kein hohes Risiko für die Rechte und Freiheiten einer betroffenen Person darstellen. In diesem Zusammenhang sollte der Begriff eines „hohen Risikos“ klar definiert werden, da dieser für die Beschränkung der Ausnahme maßgeblich ist und eine divergierende Auslegung des Begriffs Rechtsunsicherheit erzeugen würde. Zudem sollte präzisiert werden, ob ein einzelner hochriskanter Verarbeitungsvorgang die Führung des gesamten Verarbeitungsverzeichnisses nach sich zieht, oder ob die spezifische Tätigkeit dokumentiert werden muss. Würde ein Verarbeitungsverzeichnis aller Verarbeitungstätigkeiten geführt werden müssen, droht der Vorschlag ins Leere zu laufen, da viele Unternehmen wohl einzelne Verarbeitungsprozesse haben, die sich einem „hohen Risiko“ subsumieren ließen.

Eine starre Anknüpfung der datenschutzrechtlichen Privilegierung an einer Mitarbeiteranzahl sieht der BDI nicht als sachgerecht an. Auch größere Unternehmen führen routinemäßige Datenverarbeitungen durch, die ein geringes Risiko für die Rechte und Freiheiten der betroffenen Personen bergen. Umgekehrt können Unternehmen mit wenig Mitarbeitern sehr sensible personenbezogene Daten in großem Umfang verarbeiten und damit hohe Risiken verursachen. Daher sollten administrative Compliance-Auflagen konsequent in Abhängigkeit der Risiken tatsächlicher Datenverarbeitungstätigkeiten entstehen.

Darüber hinaus stellt auch der bestehende Vorschlag eine Änderung dar, welcher KMU und SMC in der Praxis nur begrenzt entlasten wird. Größere Unternehmen, für die derzeit keine Erleichterungen vorgesehen sind, müssen in ihrer Rolle als Verantwortliche in komplexen Datenverarbeitungsnetzwerken (z. B. bei ausgelagerten Services oder Datenlieferketten) weiterhin von ihren Dienstleistern und Partnern, auch wenn diese unter die Schwelle fallen, eine umfassende Dokumentation fordern, um ihre eigene Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO erfüllen zu können. Entlastungen in der Praxis werden so nur in geringem Umfang ausfallen.

2. Reform und Erweiterung der Erlaubnistatbestände

Die praxisgerechte Ausgestaltung der Erlaubnistatbestände der DSGVO ist zentral, nicht nur für den Bestand und die Weiterentwicklung datenbasierter Geschäftsmodelle, sondern für jegliche

Geschäftstätigkeit in Zeiten der Digitalisierung. Derzeit stoßen die bestehenden Erlaubnistatbestände der DSGVO bei innovativen Technologien und datenintensiven Anwendungen jedoch zunehmend an ihre Grenzen und führen zu großen Rechtsunsicherheiten, die die weitere Entwicklung analoger und digitaler Geschäftsmodelle und Innovationen in Deutschland und der EU hemmen.

Obwohl die Erlaubnistatbestände für die Verarbeitung personenbezogener Daten in Art. 6 DSGVO gleichberechtigt nebeneinanderstehen, werden diese in der Praxis insbesondere seitens der Datenschutzbehörden unterschiedlich gewichtet, mit einer klaren Priorität auf der Einwilligung. Die Einwilligung der betroffenen Person ist zu einem Standardmechanismus für die Legitimierung von Datenverarbeitungen geworden. Sie ist jedoch nicht in jedem Fall rechtlich oder praktisch geeignet, den Datenschutz effektiv zu gewährleisten, beispielsweise in Konstellationen mit strukturellem Ungleichgewicht, komplexen oder fortlaufend veränderlichen Verarbeitungskontexten sowie bei nur gering eingriffsintensiven Datenverarbeitungen. Der Einsatzbereich der Einwilligung sollte angesichts ihrer Bedeutung realitätsnäher gestaltet und die Anforderungen an ihre Wirksamkeit klarer und praxisorientierter geregelt werden. Eine Differenzierung nach Verarbeitungsrisiko würde der tatsächlichen Schutzbedürftigkeit besser gerecht werden und zugleich eine bessere Balance zwischen Datenschutz und Datennutzbarkeit herstellen. Dazu wäre zum einen eine rechtliche Klarstellung für Einwilligungen nach Art. 9 Abs. 2 lit. a) DSGVO erforderlich, insbesondere durch die Einführung von Regelbeispielen zulässiger Verarbeitungszwecke. Zum anderen sollte geprüft werden, ob bestimmte Verarbeitungsaktivitäten mit geringem Risiko vollständig von den bestehenden Einwilligungsanforderungen ausgenommen werden können. Dies würde den Einsatz der Einwilligung nachvollziehbarer und rechtssicherer machen und zugleich für eine verhältnismäßige Anwendung der Vorgaben sorgen. Der BDI befürwortet ein konsequent risikobasiertes Einwilligungsmodell, das bei weniger sensiblen oder pseudonymisierten Daten – etwa im Rahmen von Forschungsvorhaben mit ethischer Kontrolle – niedrigere Anforderungen an Form und Tiefe der Einwilligung zulässt.

Neben der Einwilligung fordert der BDI auch neue Formen der Rechtsgrundlagen zu erwägen. Beispielsweise ließe sich „Broad Consent“ auch im allgemeinen Datenschutzrecht verankern. Erwägungsgrund 33 der DSGVO zeigt einen möglichen Weg auf, Einwilligungen für mehrere, noch nicht abschließend bestimmte, aber vereinbare Zwecke zu ermöglichen. Dies würde insbesondere forschungs- und innovationsgetriebene Datenverarbeitungen rechtssicherer und effizienter machen. Darüber hinaus sollte geprüft werden, wie die Voraussetzungen für eine legitime Verarbeitung der weniger eingriffsintensiven pseudonymisierten Daten erleichtert werden kann, sofern starke Schutzmaßnahmen (z. B. obligatorische DSFA), Transparenzpflichten sowie ein Widerspruchsrecht für Betroffene gegeben sind. Der bestehende Rahmen in Art. 6 Abs. 4 DSGVO bietet hier zwar Ansätze, bleibt aber durch seine Komplexität in der Abwägungspraxis schwer handhabbar.

Demgegenüber ist die sog. Interessenabwägungsklausel des Art. 6 Abs. 1 f) DSGVO als Rechtsgrundlage für die Datenverarbeitung für Unternehmen aller Branchen von großer Bedeutung. Gleichwohl gibt es seitens der Datenschutzaufsichtsbehörden Tendenzen, den Anwendungsbereich von Art. 6 Abs. 1 f) DSGVO unangemessen und rechtswidrig zu beschränken.[2] Überdies sind die Abwägungsfragen im Rahmen der Prüfung des berechtigten Interesses im Einzelfall in der Praxis mit großen Unsicherheiten behaftet, die Unternehmen im täglichen Geschäftsverkehr behindern und Innovationen hemmen. Um eine unangemessene Einschränkung des Anwendungsbereichs der

[2] In den Leitlinien der niederländischen Datenschutzbehörde (DDPA) zur Auslegung des berechtigten Interesses aus dem Jahr 2019 wird z.B. die Anwendung von Art. 6 Abs. 1 f) DSGVO für kommerzielle Zwecke grundsätzlich ausgeschlossen. Dies hat unmittelbare Auswirkungen auf datenbasiertes Marketing und Veröffentlichungen, die nach der DSGVO auf die Interessenabwägungsklausel gestützt werden können (vgl. auch EG 47, letzter Satz).

Interessenabwägungsklausel in der aufsichtsrechtlichen Praxis zu verhindern, sollte in ErwG 47 zusätzlich klargestellt werden, dass die Datenverarbeitung zu kommerziellen Zwecken der Annahme eines berechtigten Interesses grundsätzlich nicht entgegensteht und auch das Direktmarketing zur Neukundengewinnung ein berechtigtes Interesse darstellen kann.

Schließlich ist die Weiterverarbeitung von personenbezogenen Daten zu einem anderen als dem ursprünglich vereinbarten Zweck mit großer Rechtsunsicherheit für die Unternehmen verbunden. Gemäß Art. 6 Abs. 4 DSGVO soll deren Zulässigkeit grundsätzlich von der Kompatibilität des ursprünglichen mit dem Zweck der beabsichtigten Weiterverarbeitung abhängen. Inwieweit bei vorhandener Vereinbarkeit der Zwecke gleichwohl eine gesonderte Rechtsgrundlage für Weiterverarbeitung erforderlich ist, ist in der Praxis jedoch unklar und wird unterschiedlich bewertet. Auch die beabsichtigte Privilegierung der Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke (Art. 5 Abs. 1 b) 2. HS DSGVO führt bei den Unternehmen in der Praxis bisher nicht zu den entsprechenden angemessenen Erleichterungen. Hierfür fehlt es an Konkretisierungen, wann eine Weiterverarbeitung zu den vorgenannten Zwecken gemäß Art. 89 Abs. 1 DSGVO in Verbindung mit Art. 5 Abs. 1 b) DSGVO „nicht unvereinbar“ ist mit den ursprünglichen Zwecken. Diese Rechtsunsicherheit wirkt sich u.a. im Bereich der wissenschaftlichen Gesundheitsforschung als erheblicher Hemmschuh zu Lasten der Gesellschaft aus. Erforderlich sind deshalb klare Vorgaben, inwieweit bei vorhandener Vereinbarkeit des ursprünglichen Zwecks der Datenverarbeitung mit dem der Weiterverarbeitung gleichwohl eine gesonderte Rechtsgrundlage für die weitere Verarbeitung erforderlich ist. Für die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke sowie für wissenschaftliche oder historische Forschungszwecke müssen weitere Konkretisierungen zu den Voraussetzungen der privilegierenden Wirkung gemäß Art. 89 Abs. 1 DSGVO in Verbindung mit Art. 5 Abs. 1 b) DSGVO erfolgen. Insbesondere ist unklar, welche konkreten Maßnahmen „geeignete Garantien“ im Sinne von Art. 89 Abs. 1 darstellen.

Im Hinblick auf die Rechtsakte der EU-Digitalstrategie müssen möglicherweise Ausnahmen für bestimmte Verarbeitungstätigkeiten aufgenommen werden, etwa im Zusammenhang mit den Pflichten zur Datenweitergabe nach der EU-Datenverordnung.

3. Reform der Betroffenenrechte

Der BDI erkennt Transparenz in der Datenverarbeitung als elementare Voraussetzung zur Verbesserung der Datensouveränität der Bürger an. Gleichwohl gelten die Informations- und Auskunftspflichten von Art. 13, 14 und 15 DSGVO im Grundsatz unterschiedslos für alle Verantwortlichen sowie für sämtliche Verarbeitungssituationen. Eine spürbare Entlastung der Unternehmen erfordert insofern auch Möglichkeiten zur besseren Handhabung von Betroffenenrechten. Betroffenenanfragen zu bearbeiten, insbesondere solche nach Art. 15 DSGVO, ist für viele Unternehmen mit erheblichem Aufwand verbunden, der oft zu unverhältnismäßigen Belastungen führt, und dem vielfach kein Mehrwert auf der Seite der Betroffenen gegenübersteht: Ein Übermaß an Informationen geht grundsätzlich zulasten der Verständlichkeit und Übersichtlichkeit, so dass die Hinweise letztlich gar nicht zur Kenntnis genommen werden. So zeigen Studien, dass die Bereitschaft, Datenschutzerklärungen zu lesen, seit dem Anwendungsbeginn der DSGVO abnimmt.[3] Empfehlenswert wäre dabei die Entwicklung und Anerkennung von modularen Standard-Datenschutzerklärungen mit Piktogrammen, wie ursprünglich im Gesetzgebungsprozess angedacht (vgl. Erwägungsgrund 60 DSGVO).

[3] Vgl. Eurobarometer “Charter of fundamental rights and General Data Protection Regulation”, Mai 2019, abrufbar unter https://europa.eu/eurobarometer/surveys/detail/2222.

Möglichkeiten, den Umgang mit offenkundig unbegründeten oder exzessiven Anfragen zu erleichtern, ohne die Betroffenenrechte insgesamt zu schwächen, wären gesetzliche Klarstellungen, Fristen, Beschränkungen oder Standardprozesse. So sollte der Betroffene schon bei der ersten Anfrage verpflichtet werden, seinen Auskunftsanspruch dahingehend konkret zu präzisieren, auf welche Informationen und/oder Verarbeitungstätigkeiten sich das Auskunftsersuchen bezieht; pauschale Formulierungen sollten zu einer Zurückweisung führen können. Auch Informationspflichten sollten mit Blick auf eine ausgewogene Interessenabwägung zwischen Betroffenenrechten und administrativen Umsetzbarkeit in den Unternehmen überarbeitet werden.

Um eine angemessene Informationsvermittlung in der Praxis sicherzustellen, sollte deshalb hinsichtlich der Art und des Zeitpunkts der Informationsgabe ein gestuftes Verfahren gesetzlich verankert werden: Beim Einsatz von formal oder technisch beschränkten Informationsträgern (z. B. fernmündlicher Datenerhebung) sollte es rechtssicher möglich sein, dem Betroffenen zunächst nur zentrale Basisinformationen verfügbar zu machen. Weitere Informationen sollte der Verantwortliche mittels anderer Mittel und Wege (insb. elektronische Form) verfügbar machen dürfen, sofern der Betroffene bei der Datenerhebung deutlich darauf hingewiesen wird. Ein entsprechender differenzierter Ansatz findet sich bereits in EG 58 der DSGVO und in den Guidelines der Artikel 29-Gruppe zu Transparenz[4]. Da die Umsetzung in der Praxis jedoch uneinheitlich gehandhabt wird, ist eine gesetzliche Verankerung erforderlich, die z. B. durch einen Zusatz unmittelbar in Art. 12 DSGVO oder jedenfalls in EG 58 erfolgen könnte.

Darüber hinaus sollte Art. 13 DSGVO nach dem Vorbild von Art. 14 Abs. 5 b) DSGVO um den Ausnahmetatbestand des „unverhältnismäßigen Aufwands“ erweitert werden. Auch bei der Direkterhebung von personenbezogenen Daten existieren Konstellationen, in denen die Informationsgabe einen reinen Formalismus darstellt, der zu einem unverhältnismäßigen Aufwand beim Verantwortlichen führt, z. B. bei persönlichen oder telefonischen Kontakten im geschäftlichen Bereich.

Schließlich sollte klargestellt werden, dass das in Art. 15 Abs. 3 DSGVO normierte Recht auf Kopie nur die von der Verarbeitung betroffenen personenbezogenen Daten, nicht aber ganz allgemein Kopien von zugrundeliegenden Dokumenten oder Akten umfasst. Dabei sollten insbesondere die Herausgabe ganzer Kommunikationsthreads aus E-Mail- oder Chatnachrichten, in denen eine Person benannt wird, vom Anwendungsbereich des Art. 15 Abs. 3 DSGVO herausgenommen werden. Diese teilweise in der Rechtsprechung zu beobachtende Tendenz zur Ausweitung dieser Norm birgt nicht nur ein immenses organisatorisches sowie zeit- und kostenintensives Problem für die betroffenen Unternehmen, wenn sie entsprechende Informationen aussondern und bereitstellen müssen. Es erschwert auch in enormen Maßen die Möglichkeit, interne Compliance-Untersuchungen durchzuführen und die Pflicht zur Einhaltung der Anonymität der Hinweisgeber gem. § 8 des Hinweisgeberschutzgesetzes einzuhalten. Ebenfalls konterkariert diese weite Auslegung des Art. 15 Abs. 3 DSGVO die Einschränkung des Art. 15 Abs. 4 DSGVO – denn in solchen Fällen dürfte immer auch das Brief- und Fernmeldegeheimnis der an der Kommunikation beteiligten Personen tangiert sein.

Ebenfalls sollte vor dem Hintergrund der rasanten Entwicklung im Bereich der künstlichen Intelligenz („KI“) eine Reform des in Art. 22 DSGVO normierten Verbots der automatisierten Entscheidungen im Einzelfall erfolgen. In vielen Fällen ist die KI bereits in der Lage, Sachverhalte korrekt und einwandfrei zu beurteilen. Darüber hinaus adressiert der EU AI-Act durch seinen risikobasierten Ansatz bereits die dennoch bestehenden Probleme, die der Einsatz von KI mit sich bringt. Unternehmen, die den

[4] Vgl. Guidelines on transparency under Regulation 2016/679 2016/679 i.d.F. vom 11. April 2018, Rdnr. 38, abrufbar unter https://ec.europa.eu/newsroom/article29/items/622227/en.

entsprechenden Sorgfaltspflichten nachkommen, sollten auch in der Lage sein, Entscheidungen – auch mit Bezug auf Personen – auf die KI zu übertragen. Es ist nicht mit dem technologischen Fortschritt vereinbar, dass eine KI nicht in der Lage sein darf, in Rahmen eines Bewerbungsprozesses völlig ungeeignete Bewerbende auf eine Stelle auszusortieren – zum Beispiel, wenn ein Unternehmen eine Elektrofachkraft sucht und sich ein Arzt oder eine Anwältin ohne entsprechende weitere Ausbildung auf diese Stelle bewerben. Das könnte durch eine Ergänzung des Art. 22 Absatz 2 DSGVO um einen weiteren Rechtfertigungstatbestand bestehen, der auf die Einhaltungen der Sorgfaltspflichten des EU AI-Acts verweist und einen entsprechend konformen Einsatz im Rahmen einer Interessensabwägung analog Art. 6 Abs. 1 f) DSGVO ermöglicht.

4. Reform der Pflichten von Verantwortlichem und Auftragsverarbeiter

Zahlreiche Pflichten des Verantwortlichen und Auftragsverarbeiters berücksichtigen nicht ausreichend das Prinzip des risikobasierten Ansatzes bzw. der Verhältnismäßigkeit und bringen daher für viele Unternehmen einen erheblichen bürokratischen Aufwand mit sich, ohne dem Betroffenen zu nutzen. So sieht z. B. die Verzeichnispflicht gemäß Art. 30 Abs. 2 DSGVO für Auftragsverarbeiter vor, dass diese in einem Verzeichnis zu den Kategorien der Verarbeitung u. a. den Namen und die Kontaktdaten jedes Verantwortlichen aufführen müssen, für die sie personenbezogene Daten verarbeiten. Dies führt bei Massenmarktprodukten (z. B. Cloud-Lösungen für Geschäftskunden) dazu, dass trotz gleichbleibender Kategorie der Verarbeitung für jeden einzelnen Kunden ein separater Eintrag aufzunehmen ist, was für eine Verarbeitungskategorie schnell mehrere Tausend Einträge zur Folge haben kann, die wegen wechselnden Kundenbestands laufend angepasst werden müssen. Dies bedeutet neben den ohnehin von den Auftragsverarbeitern geführten Kundendatensystemen eine doppelte Datenverwaltung, die einen erheblichen bürokratischen Mehraufwand für die Unternehmen bedeutet. Hier sollte ein erleichterter Nachweis durch die Vorlage einer das Verarbeitungsverzeichnis ergänzenden vollständigen Liste der Namen und Kontaktdaten der Verantwortlichen auf Anforderung der Aufsichtsbehörde in angemessener Frist vorgesehen werden. Zudem sollte eine Ausnahme für standardisierte, gesetzlich vorgeschriebene Prozesse mit geringem Risiko für Betroffene (z. B. Heizkostenabrechnung, Energieausweis-Erstellung) geschaffen werden.

Überdies lassen die uneingeschränkt geregelten Pflichten von Verantwortlichem und Auftragsverarbeiter die technische Machbarkeit teilweise unberücksichtigt. Soweit bestimmte Pflichten im Einzelfall nicht umsetzbar sind (z. B. die Löschung oder Herausgabe der personenbezogenen Daten durch den Auftragsverarbeiter nach Wahl des Verantwortlichen, Art. 28 Abs. 3 g) DSGVO), müssen diese angemessen einschränkbar sein, indem die Pflicht, die Daten nach Beendigung des Vertrags nach Wahl des Verantwortlichen entweder zu löschen oder zurückzugeben, von der technischen Umsetzbarkeit im Einzelfall abhängig gemacht wird.

Im Hinblick auf die speziellen Pflichten von Verantwortlichem und Auftragsverarbeiter zur Gewährleistung der Sicherheit personenbezogener Daten erweist sich insbesondere die in Art. 33 Abs. 1 DSGVO vorgesehene Meldepflicht von Datenschutzverletzungen in der Praxis als problematisch: Aufgrund der weiten gesetzlichen Definition der „Verletzung des Schutzes personenbezogener Daten“ und dem hohem Bußgeldrahmen bei Verstößen gegen die Meldepflicht, ist die Zahl der Meldungen bei den Aufsichtsbehörden nach dem Anwendungsbeginn der DSGVO stark gestiegen[5]. Die in Art. 33 Abs. 1 DSGVO vorgesehene Ausnahme von der Meldepflicht für Fälle, bei denen die Verletzung des

[5] Beim LfDI Baden-Württemberg etwa hatten sich die Meldungen im ersten Jahr seit dem Anwendungsbeginn der DSGVO im Mai 2018 verzehnfacht: https://www.haufe.de/compliance/recht-politik/zahl-der-gemeldeten-datenpannen-stieg-nach-dsgvo-start-stark-an_230132_496562.html.

Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, ist derart unbestimmt, dass die Verantwortlichen zur Vermeidung von bußgeldbewehrten Fehleinschätzungen im Zweifel sämtliche Datenpannen melden, unabhängig vom Risiko im Einzelfall. Deshalb sollte die Meldepflicht für Datenschutzverletzungen durch eine Erheblichkeitsschwelle angemessen begrenzt werden. Hierfür ist in ErwG 85 klarzustellen, dass von einem Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen nur dann ausgegangen werden kann, wenn bestimmte Kategorien personenbezogener Daten von der Datenschutzverletzung betroffen sind. Diese sollten durch Regelbeispiele veranschaulicht werden (z. B. besondere Datenkategorien; Daten, die einem Berufsgeheimnis unterliegen; personenbezogene Daten, die sich auf strafbare Handlungen beziehen; Passwörter etc.).

5. 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 branchenübergreifende, datengetriebene Geschäftsmodelle 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 Unternehmen jedoch vor der Herausforderung, dass weder klare rechtliche Vorgaben noch einheitliche technische Standards und Methoden für eine De-Personalisierung von Daten existieren, was eine Vielzahl als Hürde für die wirtschaftliche Datennutzung identifiziert[6]. 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, sondern auch die vertragliche Ausgestaltung von Auftragsverarbeitungen. Um die bestehende Rechtsunsicherheit zu beheben, braucht es deshalb konkret anwendbare Kriterien (wie Mindestgrößen von Aggregaten, Schwellenwerte etc.)und europaweit anerkannte Verfahren.

Erforderlich sind Präzisierungen zur rechtlichen Qualifikation einer Anonymisierung und deren Anforderungen unter Ergänzung gesetzlicher Vermutungstatbestände für eine rechtswirksame Anonymisierung, um hier ein größeres Maß an Rechtssicherheit zu schaffen. Hierzu gehört eine Klarstellung, dass es sich bei der Anonymisierung von personenbezogenen Daten nicht um eine Verarbeitung im Sinne von Art. 4 Ziff. 2 DSGVO handelt. Weder der Wortlaut noch die Systematik oder der Sinn und Zweck der DSGVO gebieten zwingend eine derartige Auslegung. Vielmehr handelt es sich hierbei nach Ansicht des BDI bei der Anonymisierung personenbezogener Daten nicht um einen datenschutzrelevanten Vorgang, da er durch die DSGVO privilegiert ist und somit nicht den Anforderungen der DSGVO unterfällt. In jedem Fall sollte klargestellt werden, dass bei einer kompatiblen, zweckändernden Weiterverarbeitung nach Art. 6 Abs. 4 DSGVO – auch bei der Verarbeitung besonderer Datenkategorien gemäß Art. 9 DSGVO – die die ursprüngliche Verarbeitung legitimierende Rechtsgrundlage zum Zuge kommt, wobei eine Anonymisierung unabhängig vom ursprünglichen Zweck der Datenerhebung stets als datenschutzkonform anzusehen ist: Der Zweck der Anonymisierung liegt in der Entfernung des Personenbezugs, womit die der DSGVO zugrundeliegenden Prinzipien der Datenminimierung und Speicherbegrenzung zum Schutz der Privatsphäre der Betroffenen umgesetzt werden. Dies stellt stets

[6] 73 Prozent der befragten Unternehmen bezeichnen Rechtsunsicherheit bei Datenanonymisierung als Hemmnis für wirtschaftliche Datennutzung, IW-Studie im Auftrag des BDI, a.a.O.

eine legitime Zweckänderung dar, so dass hier eine Kompatibilitätsprüfung im Einzelfall nicht erforderlich ist.

Daneben sind genehmigte Verhaltenskodizes gemäß Art. 40 DSGVO wichtige Instrumente für einen praxisgerechten, flexiblen, innovationsfreundlichen und rechtssicheren Datentransfer. Trotz dieser zahlreichen Vorteile existieren in der Praxis jedoch bislang nur sehr wenige von der EU-Kommission genehmigte Verhaltenskodizes. Um dem in der DSGVO angelegten Transferinstrument der Verhaltenskodizes in der Praxis zu mehr Geltung zu verhelfen, sollte daher kritisch überprüft werden, ob und inwieweit die umfangreichen Voraussetzungen für die Genehmigung und Überprüfung der Kodizes zumindest in der Auslegungspraxis der Datenschutzbehörden Potenzial für Erleichterungen bietet.

Um das Vertrauen der Bürger und Geschäftspartner in die Datenschutzkonformität von verantwortlichen Unternehmen und Auftragsverarbeiter zu erhöhen, sollten außerdem Zertifizierungsprozesse nach Art. 42 DSGVO beschleunigt und bei den Anforderungen für Zertifizierungen unter Berücksichtigung des risikobasierten Ansatzes angemessen differenziert werden.

6. Reform der Datenschutzdurchsetzung

Im Zuge einer Reform der Datenschutzdurchsetzung sollten zunächst die Aufgaben der Datenschutzbehörden zeitgemäß weiterentwickelt werden. Neben dem Schutz personenbezogener Daten sollten zukünftig auch der freie Datenverkehr innerhalb – und unter Zusicherung entsprechender Garantien – auch außerhalb der EU, die Wettbewerbsfähigkeit datenverarbeitender Unternehmen sowie die Förderung von Innovationen in der Digitalwirtschaft stärker berücksichtigt werden. Ein entsprechend erweitertes und ausbalanciertes Behördenmandat würde es ermöglichen, dass ein Gleichgewicht zwischen dem Datenschutz und Freiheitsrechten gewährleistet wird. Die Datenaufsichtsbehörden könnten dazu nach Art. 57 Abs. 1 lit. e) und f) DSGVO nicht nur zur Unterstützung betroffener Personen verpflichtet werden, sondern auch zur Beratung der Verantwortlichen und Auftragsverarbeiter.

Weiterhin sollte die Rolle des Europäischen Datenschutzausschusses (EDSA) weiterentwickelt werden. Insbesondere in Ermangelung einer gefestigten höchstrichterlichen Rechtsprechung zu zentralen Fragen der DSGVO sind die Stellungnahmen und Leitlinien des EDSA von großer Bedeutung für eine praxisnahe und wirtschaftsfreundliche Anwendung der DSGVO. Derzeit sind die Entscheidungsprozesse jedoch in hohem Maße intransparent. Häufig fehlt es an einer systematischen und breiten Beteiligung von Interessengruppen an Entscheidungsprozessen der Datenschutzaufsichtsbehörden, was dem in Art. 41 EU-Grundrechtecharta (GRCh) verankerten Recht auf gute Verwaltung widerspricht.

Um zukünftig mehr Transparenz sicherzustellen, muss das Verfahren zur Erstellung von Leitlinien, Stellungnahmen und Empfehlungen dahingehend modifiziert werden, dass Stakeholder zwingend vor der Erstellung von Textentwürfen einzubeziehen sind – etwa durch öffentliche Konsultationen oder Expertengespräche. Dadurch würde die Qualität der Dokumente gesteigert, die Umsetzbarkeit verbessert und die Akzeptanz erhöht werden. Darüber hinaus sollte die Rolle des EDSA, von einem primär ex-post agierenden Gremium hin zu einem kooperativen Innovationsbegleiter ausgeweitet werden, der offen, dialogorientiert und praxisnah arbeitet. Dies ließe sich etwa durch ein „EDSA Innovation Forum“ erreichen, das Unternehmen, Forschungseinrichtungen und Aufsichtsbehörden institutionalisiert in den Austausch bringt, um rechtskonforme Innovationen frühzeitig zu ermöglichen und neue Technologien regulatorisch zu begleiten.

Zu diesem Zweck schlagen wir gezielte Änderungen an Artikel 70 Absatz 4 DSGVO sowie die Hinzufügung eines neuen Artikels 58 Absatz 3 Buchstabe k vor:

Artikel 70 Absatz 4:

„Der Ausschuss konsultiert gegebenenfalls die betroffenen Parteien und gibt ihnen Gelegenheit, innerhalb einer angemessenen Frist Stellung zu nehmen. Diese Konsultation ist vor der Verabschiedung von Stellungnahmen, Leitlinien, Empfehlungen und bewährten Verfahren obligatorisch. Der Ausschuss berücksichtigt diese Konsultationen gebührend und veröffentlicht, unbeschadet des Artikels 76, die Ergebnisse des Konsultationsverfahrens, einschließlich einer Zusammenfassung der Ergebnisse aller vom Ausschuss durchgeführten Konsultationen und einer Erläuterung, wie der Ausschuss diese Ergebnisse berücksichtigt hat."

Artikel 58 Absatz 3 Buchstabe k:

„k) auf eigene Initiative oder auf Antrag Leitlinien, Empfehlungen und bewährte Verfahren dazu zu verabschieden, wie die Verantwortlichen und Auftragsverarbeiter ihren Verpflichtungen aus der DSGVO nachkommen können. Vor der Verabschiedung solcher Leitlinien, Empfehlungen oder bewährten Verfahren konsultiert die Aufsichtsbehörde die betroffenen Parteien und berücksichtigt deren Standpunkte umfassend."

Artikel 58 Absatz 3A:

„Bei der Ausübung der in Absatz 3 genannten Befugnisse berücksichtigt die Aufsichtsbehörde sämtliche Entscheidungen aus Rechtsprechung sowie die Auslegungen dieser Verordnung durch die Organe und Einrichtungen der Union."

7. Rolle der EU-Kommission für mehr Kohärenz im Datenschutz

Die DSGVO ist zwar technologieneutral ausgestaltet, gleichwohl erweist sie sich in der Praxis als nicht flexibel genug, um den datenschutzrechtlichen Spezifika und Bedürfnissen neuer technologischer Entwicklungen angemessen Rechnung zu tragen. Um Innovationen und neue Technologien zu fördern, muss die DSGVO technologieoffener ausgestaltet werden. So sollten z. B. mit Blick auf KI, Big Data oder Blockchain die Verarbeitungsgrundsätze der Datenminimierung und der Zweck- und Speicherbegrenzung (Art. 5 Abs. 1 b), c), e) DSGVO) kritisch überprüft und technologieadäquat konkretisiert werden.

Schließlich ist die Rolle der EU-Kommission zur Lösung bestehender Durchsetzungsprobleme, vor allem bei grenzüberschreitenden Fällen, zu stärken. Es muss eine verstärkte Aufgabe der EU-Kommission sein, für eine einheitliche, konsistente, ausgewogene und wirtschaftsfreundliche Datenschutzpolitik zu sorgen. Neben einer größeren Transparenz und Einbeziehung der Industriepositionen bei der Erarbeitung von DSGVO-Leitlinien sollte die EU-Kommission künftig auch selbst verbindliche Regeln in Form von Durchführungsrechtsakten erlassen oder auch Standard- Auftragsverarbeitungsvertragsmuster einführen dürfen. Die EU-Kommission sollte zudem für die Koordinierung der Harmonisierung und Rechtsanwendung der verschiedenen Rechtsakte im Zuge der EU-Digitalstrategie, die bislang nicht hinreichend aufeinander abgestimmt sind, eine stärkere Rolle übernehmen – etwa durch die Einrichtung einer zentralen Koordinationsstelle für Digitalrechtsakte, die auf Unionsebene Leitlinien oder Orientierungshilfen zum Zusammenspiel der Rechtsakte bereitstellt.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Redaktion
Dr. Michael Dose
Referent Digitalisierung und Innovation
T: +49 30 2028-1560
m.dose@bdi.eu

Florian Pühl
Studentische Hilfskraft für Digitalisierung und Innovation
T: +49 30 2028-1603
f.puehl@ifg.bdi.eu

Lobbyregisternummer: R000534

BDI Dokumentennummer: 2163