DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins vorbereitet durch den Ausschuss Informationsrecht

zum Vorschlag der EU-Kommission für eine Digital-Omnibus-Verordnung (COM (2025) 837 final)

Stellungnahme Nr.: 21/2026 Brüssel, im März 2026

Mitglieder des Ausschusses

- Rechtsanwalt Prof Niko Härting, Berlin (Vorsitzender, Berichterstatter)
- Rechtsanwalt Dr. Simon Assion, Frankfurt am Main (Berichterstatter)
- Rechtsanwältin Dr. Christiane Bierekoven, Düsseldorf (Berichterstatterin)
- Rechtsanwältin Isabell Conrad, München (Berichterstatterin)
- Rechtsanwalt Prof. Dr. Malte Grützmacher, LL.M., Hamburg (Berichterstatter)
- Rechtsanwalt Peter Huppertz, LL.M, Düsseldorf (Berichterstatter)
- Rechtsanwalt Dr. Helmut Redeker, Bonn (Berichterstatter)
- Rechtsanwältin Dr. Kristina Schreiber, Köln (Berichterstatterin)
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU), München (Berichterstatter)

Zuständig in der DAV-Geschäftsstelle

- Rechtsanwältin Nicole Narewski, Geschäftsführerin, Berlin

Ansprechpartner in Brüssel

- Rechtsanwältin Eva Schriever, LL.M., Geschäftsführerin
- Rechtsanwältin Dorothee Wildt, LL.M., stellv. Leiterin
- Myra Jockisch, LL.M., Referentin

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV versammelt mehr als 60.000 Rechtsanwältinnen und Rechtsanwälte sowie Anwaltsnotarinnen und Anwaltsnotare, die in 253 lokalen Anwaltvereinen im In- und Ausland organisiert sind. Er vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene. Der DAV ist im Lobbyregister für die Interessenvertretung gegenüber dem Deutschen Bundestag und der Bundesregierung zur Registernummer R000952 eingetragen.

Der Deutsche Anwaltsverein nimmt nachfolgend Stellung zu der Änderungsverordnung 2025/0360 (COD) aus dem Entwurf der EU-Kommission COM (2025) 837 final in seiner Fassung vom 19.11.2025.

I. Zusammenfassung

Die Umsetzung der Anforderungen der DSGVO, des Data Acts, der KI-Verordnung und anderer Datenrechtsakte fällt in der Praxis nicht immer leicht. Daher begrüßt der DAV den Versuch, durch zwei „Omnibus-Pakete“ einige der bestehenden Unklarheiten zu bereinigen und für mehr Rechtssicherheit zu sorgen. Dies ist gut für die Rechte der Bürgerinnen und Bürger, für die betroffenen Unternehmen und Einrichtungen und für die Behörden, die mit der Durchsetzung der Rechtsakte befasst sind.

Im Grundsatz begrüßt der DAV insbesondere auch den Versuch, durch Änderungen des Art. 9 DSGVO und einen neuen Art. 88c DSGVO die spezifischen datenschutzrechtlichen Fragen zu adressieren, die sich bei der Verwendung personenbezogener Daten zum Training und Betrieb von KI-Anwendungen stellen. Zu näheren Einzelheiten ist eine gesonderte Stellungnahme beabsichtigt.

- Auskunftsrechte: Der DAV begrüßt Modifizierungen bei den datenschutzrechtlichen Auskunftsrechten. Die Auskunftsrechte sind ein zentrales Instrument zur Verwirklichung der Datenschutzrechte der Bürgerinnen und Bürger. Diese Rechte dürfen durch eine missbräuchliche Geltendmachung weder zweckentfremdet noch ausgehöhlt werden. Zielführend dürfte eine Begründungspflicht bei Auskunftsanträgen sein, da ohne eine solche Begründung eine Missbrauchskontrolle oft kaum möglich sein wird.
- Meldepflichten: Der DAV begrüßt Modifikationen bei den Meldepflichten. Mit exzessiven Meldungen von Datenpannen, die behördlich nicht gründlich bearbeitet

werden können, ist niemandem gedient. Das Ziel einer einheitlichen Meldestelle und eines einheitlichen Meldewegs für Pannenmeldungen nach unterschiedlichen Rechtsakten verdient Unterstützung.

- Auch die Vorschläge zu ergänzenden Regelungen für Forschungsdaten, biometrische Daten und automatisierte Einzelfallentscheidungen verdienen – bei einiger Detailkritik – Unterstützung.
- Cookies: Neben dem Schutz personenbezogener Daten lässt sich unter den heutigen technischen Bedingungen kein gesondertes Bedürfnis des „Schutzes von Endgeräten vor Cookies“ mehr feststellen. Daher begrüßt der DAV, dass die lange schon geforderte Überführung datenschutzrechtlicher „Cookie“-Bestimmungen aus der ePrivacy-Richtlinie in die DSGVO geplant ist. Diese Überführung sollte durch eine vollständige Streichung der „Cookie“-Bestimmungen in der ePrivacy-Richtlinie flankiert werden.
- Personenbezug: Der DAV sieht keine zwingende Notwendigkeit, den Begriff des Personenbezugs in der DSGVO an neuere Rechtsprechung des EuGH anzupassen. Sollte es jedoch zu einer solchen Anpassung kommen, sollte deutlicher klargestellt werden, ob und inwieweit die Rechtsprechung des EuGH modifiziert werden soll.
- Pseudonymisierung: Der DAV begrüßt ergänzende Regelungen zur Pseudonymisierung, regt aber an, diese Regelungen durch Bestimmungen zur Anonymisierung zu ergänzen. Pseudonymisierung und Anonymisierung sind wichtige praktische Instrumente des Datenschutzes, die einer Stärkung bedürfen.
- Datengesetzbuch: Der DAV begrüßt das Bestreben, den Data Act zu vereinfachen und zu einem umfassenden Datengesetzbuch auszuweiten, sieht allerdings bei den Vorschlägen aus dem „Omnibus“ noch erheblichen Ergänzungsbedarf.

II. Änderungen bei den Betroffenenrechten

Das Ziel der Änderungsvorschläge zu Art. 12, 13 und 22 DSGVO ist es, eine bessere Balance und Verbesserung der praktischen Konkordanz zwischen den Grundrechten und Grundfreiheiten der Personen, denen Betroffenenrechte zustehen, und dem jeweiligen Verantwortlichen herbeizuführen. Diese Zielrichtung ist zu begrüßen. Dass dafür ein großes praktisches Bedürfnis besteht zeigt sich v.a. im Beschäftigungsverhältnis und im Bereich der Künstlichen Intelligenz.

Die geplanten Änderungen zu Art. 12, 13 und 22 DSGVO sowie die Entwürfe neuer Erwägungsgründe (35) bis (38) zeigen gute Ansätze, lassen sich aber noch präziseren, indem vermieden wird, klärungsbedürftige Begriffe einführen, die zu neuer Rechtsunsicherheit führen.

1. Änderungen in Art. 12 Abs. 5 DSGVO

Der Änderungsvorschlag der Kommission zu Art. 12 Abs. 5 DSGVO sieht vor:

> *Bei offenkundig unbegründeten oder – insbesondere im Fall von häufiger Wiederholung – exzessiven Anträgen einer betroffenen Person oder bei Anträgen nach Artikel 15 kann der Verantwortliche, wenn die betroffene Person die ihr durch diese Verordnung verliehenen Rechte zu anderen Zwecken als dem Schutz ihrer Daten missbraucht, entweder*
>
> *a) ein angemessenes Entgelt verlangen, bei dem die Verwaltungskosten für die Unterrichtung oder die Mitteilung oder die Durchführung der beantragten Maßnahme berücksichtigt werden, oder*
>
> *b) sich weigern, aufgrund des Antrags tätig zu werden. Der Verantwortliche hat nachzuweisen, dass der Antrag offenkundig unbegründet ist oder dass hinreichende Gründe für die Annahme bestehen, dass der Antrag exzessiv ist.*

2. Vorschlag zur Präzisierung des Begriffs der „Missbräuchlichkeit“

Das Verhältnis von „missbräuchlich“ zu „unbegründet“ und „exzessiv“ ist nicht klar. Daher sollte erwogen werden, in Art. 12 Abs. 5 DSGVO-E eine Klarstellung einzufügen, z.B. durch Einführung des Worts *„etwa“*:

> *„etwa wenn die betroffene Person die ihr durch diese Verordnung verliehenen Rechte zu anderen Zwecken als dem Schutz ihrer Daten missbraucht ….“.*

Soweit im Entwurf des Erwägungsgrunds (35) als Beispiel für missbräuchliche Anträge genannt wird, dass „[z]u weit gefasste und undifferenzierte Auskunftsverlangen […] ebenfalls als exzessiv anzusehen“ sind, ist dies zu begrüßen, da dies tatsächlich ein in der Praxis häufig vorkommender Fall ist. Aber das Beispiel sollte konkretisiert werden, weil nicht jeder unspezifische Auskunftsantrag exzessiv oder missbräuchlich ist, insbesondere wenn die Daten nicht direkt bei der betroffenen Person erhoben wurden.

3. Vorschlag einer Begründungspflicht bei Auskunftsanträgen

Damit die Änderungen in Art. 12 Abs. 5 DSGVO-E nicht ins Leere gehen, sollte hinsichtlich Art. 15 DSGVO eine Begründungspflicht für betroffene Personen geregelt werden, damit der Verantwortliche beurteilen kann, ob die betroffene Person missbräuchliche Absichten hat. Die Begründungspflicht kann auch helfen, dass Verantwortlicher und Antragsteller bei unspezifischen Auskunftsanträgen in einen Dialog über die Konkretisierung der zu liefernden Informationen und Kopien treten.

Eine Begründungspflicht erscheint notwendig, um dem Verantwortlichen die Beurteilung einer möglichen Missbräuchlichkeit eines Auskunftsantrags zu ermöglichen. Ohne eine solche Begründungspflicht könnten die vorgeschlagenen Änderungen des Art. 12 Abs. 5 DSGVO-E ins Leere laufen.

Ausweislich des bisherigen Erwägungsgrund 63 der DSGVO dient das Auskunftsrecht dazu, dass sich die betroffene Person „problemlos und in angemessenen Abständen“ „der Verarbeitung von Daten bewusst“ werden und „die Rechtmäßigkeit überprüfen“ kann. Nach EuGH (Urt. v. 26.10.2023 - C-307/22, Patientenakte) ist dies ohne Angabe von Gründen möglich.

Nach dem Entwurf der Änderung in Art. 12 Abs. 5 DSGVO soll das Auskunftsbegehren missbräuchlich sein, wenn es „zu anderen Zwecken als zum Schutz der Daten“ verlangt wird. Daraus ergeben sich mehrere praktische Schwierigkeiten in der Umsetzung:

- Wie kann der Verantwortliche beurteilen, ob die Auskunft nur zum Schutz der Daten verlangt wird, wenn die betroffene Person den Auskunftsantrag nicht begründen muss?
- Führt die Absicht des Betroffenen, bei aufgrund der Auskunft belegter rechtswidriger Datenverarbeitung und/oder bei Verweigerung oder offensichtlicher fehlerhafter Erfüllung von Betroffenenrechten eine Beschwerde nach Art. 77 DSGVO und Schadensersatz nach Art. 82 DSGVO geltend zu machen, bereits zu einem missbräuchlichen Auskunftsantrag? Oder sind alle diese Fälle von dem Zweck „Schutz der Daten“ umfasst?
- Häufig haben betroffene Personen mehrere Motive für einen Auskunftsantrag, die teilweise der Ausübung der DSGVO-Rechte dienen und gleichzeitig anderen Zwecken. Führen die Verärgerung über Werbeschreiben und Überprüfung des

Einklangs mit § 7 UWG oder ein laufender Kündigungsschutzprozess der betroffenen Person gegen den Verantwortlichen zur Missbräuchlichkeit des vom Betroffenen situationsbezogen gestellten Auskunftsantrag?

- Führt der Umstand, dass im Rahmen eines Rechtsstreits von mehreren Ansprüchen des Gläubigers auch ein Auskunftsantrag nach Art. 15 DSGVO nicht erledigt ist und der Gläubiger insoweit einen Vergleich mit Gesamterledigung anbietet per se dazu, dass der Auskunftsantrag missbräuchlich ist?
- Die Beispiele im Entwurf von Erwägungsgrund (35) lassen erkennen, dass es auf die Absichten der betroffenen Person ankommen soll, etwa wenn der Antrag mit der „alleinige Absicht [erfolgt], dem Verantwortlichen einen Schaden zuzufügen“. Wie aber soll eine solche „alleinige Absicht“ für den Verantwortlichen nachweisbar sein, selbst wenn die Nachweispflicht auf „hinreichende Gründe für die Annahme“ der Exzessivität beschränkt wird?
- Der vom Antragsteller verfolgte Zweck einer Auskunft kann sich auch ändern. In der Praxis kommt es häufig vor, dass im Rahmen der Beauskunftung ein Dialog zwischen Verantwortlichem und Antragsteller geführt wird. Beispielsweise stellt die betroffene Person zunächst einen unspezifischen Antrag, mit der sie sich über die Verarbeitung bewusst werden will (Erwägungsgrund 63 DSGVO) und nach einem ersten Auskunftsschreiben, des Verantwortlichen, das möglicherweise nicht hinreichend transparent ist, sendet die betroffene Person konkretisierte Nachfragen mit denen sie anderen Zwecke verfolgt (etwa Geltendmachung von Schadensersatzansprüchen wegen Falschberatung, für die sie durch die erste Auskunft Indizien erhält). Inwieweit liegt in solchen Fällen im Hinblick auf den Regelungsentwurf zu Art. 12 Abs. 5 DSGVO-E ein Missbrauch des Auskunftsrechts vor?
- Führt der Umstand, dass im Rahmen eines Rechtsstreits von mehreren Ansprüchen des Gläubigers auch ein Auskunftsantrag nach Art. 15 DSGVO nicht erledigt ist und der Gläubiger insoweit einen Vergleich mit Gesamterledigung anbietet per se dazu, dass der Auskunftsantrag missbräuchlich ist?

4. Vorschlag zur Einschränkung von Art. 15 Abs. 3 DSGVO

In Art. 15 Abs. 3 DSGVO sollte der häufige Fall ausdrücklich geregelt werden, dass ein Beschäftigter oder ehemaliger Beschäftigter mit mehrjähriger Zugehörigkeit zum Betrieb oder zur Dienststelle des Verantwortlichen (auch bei gesetzlichen Vertretern und Leitungspersonen wie Gesellschaftern, Organmitgliedern, Geschäftsführern u.ä.)

unspezifisch Auskunft begehrt und die Auskunft eine große Menge an Daten umfasst, die er größtenteils selbst erstellt hat (etwa E-Mail-Kommunikation). In einem solchen Fall sollte der Verantwortliche die Spezifizierung des Antrags verlangen können und Kopien verweigern dürfen, wenn eine Spezifizierung nicht erfolgt, es sei denn, es bestehen berechtigte Gründe der betroffenen Person, warum eine Spezifizierung nicht möglich oder nicht zumutbar ist.

Während bei missbräuchlicher Absicht die Auskunft insgesamt abzulehnen ist, ist bei „zu weit gefassten und undifferenzierten Auskunftsverlangen“ ggf. zu differenzieren zwischen den Informationen nach Art. 15 Abs. 1 und Abs. 2 DSGVO und dem aufwändigen Recht auf Kopien nach Art. 15 Abs. 3 DSGVO.

Nach der Rechtsprechung des EuGH (zuletzt im Urt. v. 04.09.2025 - C-413/23 P, SRB) sind üblicherweise Nachrichten/Stellungnahmen in ihrer Gesamtheit personenbezogene Daten des Verfassers. Da die E-Mails eines Beschäftigten regelmäßig in großem Umfang auch Rechte anderer Personen tangieren (personenbezogene Daten Dritter, ggf. auch Geschäftsgeheimnisse, Art. 15 Abs. 4 DSGVO), hat der Verantwortliche gerade bei langer Betriebszugehörigkeit des ehemaligen Beschäftigten enorme Aufwände zur Erstellung der Kopie und Prüfung/Durchführung von Schwärzungen.

Werden geschwärzte Kopien von E-Mails an einen (ehemaligen) Beschäftigten, der die Auskunft begehrt, übermittelt, dann wird dieser häufig mit seinem Zusatzwissen rekonstruieren können, z.B. welche Namen anderer Personen in der E-Mail-Kommunikation geschwärzt wurden. So gesehen stellt sich die Frage, inwieweit die Kopie von E-Mails wegen Art. 15 Abs. 4 DSGVO insgesamt oder in weiten Teilen versagt werden kann, was der Verantwortliche bislang aber im Hinblick auf einzelne E-Mails, also für jeden Einzelfall beurteilen muss.

Digitale Schwärzungen sind bei unstrukturierten Daten wie E-Mails kaum verlässlich automatisiert möglich und bergen zudem ein erhebliches Risiko, dass unkenntlich gemacht Informationen rekonstruiert werden können. In den letzten Jahren ist das Risiko durch KI-gestützte Analyse-Tools sehr gestiegen, mit denen geschwärzte Passagen teilweise vollständig rekonstruiert werden können. Dieses Risiko lässt sich auch durch Ausdruck und Wiedereinscannen (Roundtripping) nicht vollständig beseitigen, jedenfalls nicht bei größeren Datenmengen. Zudem ist der – neben dem Aufwand für die digitale Schwärzung – entstehende Zusatzaufwand für Scannen und Qualitätssicherung bei großen Mengen von geschwärzten Ausdrucken sehr groß. Insoweit kann Art. 15 Abs. 4 DSGVO bei

unspezifischen Auskunftsanträge unangemessen große Aufwände beim Verantwortlichen nicht verhindern, und diese Aufwände führen häufig nicht einmal zur gewünschten Rechtssicherheit.

5. Klarstellungsbedarf bei E-Mail-Kopien im Beschäftigungskontext

Art. 15 Abs. 3 DSGVO sollte auch dahingehend geändert werden, dass der Antragsteller verpflichtet ist, sein Kopiebegehren zu spezifizieren und einzugrenzen und zudem der Verantwortliche das Wahlrecht hat, inwieweit er die Kopie unter Berücksichtigung der Sicherheit der Daten elektronisch oder auf anderem Wege zur Verfügung stellt, wenn die Auskunft im Zusammenhang mit einem mindestens 12 Monate dauerndem Beschäftigungsverhältnis erfolgt und größere Mengen dienstlicher E-Mails des Antragstellers umfasst.

In der Praxis stellt sich häufig die Frage, ob bei digitaler Übermittlung der Kopie von großen Mengen (teils geschwärzter) dienstlicher E-Mails an die betroffene Person die Daten im Hinblick auf den Verbleib bei der betroffenen Person hinreichend sicher sind. Der Verantwortliche muss zwar für die Sicherheit des Übermittlungsweges sorgen. Aber für den Verbleib auf - meist privater - IT der betroffenen Person gibt es kein definiertes Sicherheitsniveau.

Daher stellt sich die Frage, ob der (ehemalige) Beschäftigte stets ein Wahlrecht haben soll, die elektronische Übermittlung der (unspezifizierten) Kopie zu verlangen (Art. 15 Abs. 3 S. 3 DSGVO) oder ob der Verantwortliche unter bestimmten Umständen die elektronische Übermittlung großer Mengen an geschwärzten E-Mails, jedenfalls soweit das Kopie-Begehren von der betroffenen Person nicht spezifiziert wurde, verweigern darf und z.B. durch Übersendung in Papierform die Kopiebereitstellung erfüllen kann.

6. Änderungen in Art. 13 DSGVO-E und Relevanz für Art. 14 und 15 DSGVO

Die geplanten Änderungen in Art. 13 (4) DSGVO-E werden voraussichtlich für größere Verantwortliche wenig Entlastung bringen, weil Art. 13 im Vergleich zu Art. 14 und Art. 15 DSGVO im Regelfall einfacher zu erfüllen ist. Für z.B. kleine Vereine und Handwerksbetriebe, die bisher durch Datenschutzinformationen insgesamt überfordert waren, könnte sich eine Erleichterung einstellen, sodass die geplanten Änderungen im Ergebnis zu begrüßen sind.

7. Vorschlag zu Präzisierungen in Art. 13 und 14 DSGVO-E

Es müssten die Begriffe „nicht datenintensive Tätigkeit“ und „klare und begrenzte Beziehung“ präzisiert werden, weil anderenfalls Rechtsunsicherheit und unterschiedliche Auslegung zu erwarten ist.

Die unscharfen Begriffe werden durch die Beispiele im zugehörigen Entwurf des Erwägungsgrunds (36) etwas klarer, werden dort aber nicht konsistent verwendet. Dort heißt es „wenn der Verantwortliche eine geringe Menge personenbezogener Daten auf nicht datenintensive und nicht komplexe Weise verarbeitet […]“, somit scheint sich „nicht datenintensiv“ auf die Qualität der Verarbeitung zu beziehen, allerdings nicht auf die Komplexität.

In Erwägungsgrund (36) heißt es aber weiter: „Die Tätigkeit des Verantwortlichen ist nicht datenintensiv, wenn er personenbezogene Daten in geringem Umfang erhebt und seine Verarbeitungsvorgänge nicht komplex sind, wie beispielsweise im Beschäftigungsbereich.“ Hiernach scheint die Quantität der Daten und der Umfang der Verarbeitung ausschlaggebend für „nicht datenintensiv“ zu sein. Warum Verarbeitungen ausgerechnet im Beschäftigungsbereich „in geringem Umfang und wenig komplex“ erfolgen, leuchtet angesichts von E-Recruiting, Zuverlässigkeitsprüfungen bei Beschäftigten etc. nicht ohne weiteres ein, es sei denn man stellt auf kleine Vereine und Kleinstunternehmen ab.

Wünschenswert gerade für Vereine und Kleinstunternehmen wäre die Klarstellung im Erwägungsgrund (36), dass die Änderung in Art. 13 Abs. 4 DSGVO-E auch Datenschutzerklärungen auf Webseiten umfassen kann, soweit dort keine Cookies oder andere Tracking-Mechanismen eingesetzt werden. Wenn diese Klarstellung nicht erfolgt, könnten neue Abmahnwellen im Hinblick auf fehlende Datenschutzinformationen auf Webseiten die Folge sein.

Ebenfalls sollte im Hinblick auf EuGH Urt. v. 04.09.2025 (C-413/23 P, SRB) klargestellt werden, dass die Ausnahme in Art. 13 Abs. 4 DSGVO-E auch Fälle umfassen kann, in denen der Verantwortliche Daten mit anonymisierender Wirkung pseudonymisiert und nur in dieser Form an Empfänger weitergibt.

Eine Erleichterung für die wissenschaftliche Forschung ist grundsätzlich wünschenswert. Allerdings stellt sich beim Entwurf des Art. 13 Abs. 5 DSGVO-E ein ähnliches Problem wie

bei Art. 14 Abs. 5 lit. b DSGVO, nämlich dass in der Praxis große Rechtsunsicherheit besteht, wann Unverhältnismäßigkeit vorliegt. Der in Erwägungsgrund (37) genannte Beispielsfall der Zweckänderung für Forschungszwecke, was bei der Erhebung noch nicht vorhersehbar war, ist hilfreich.

Allerdings sollte klargestellt werden, dass dieser Fall auch bei Art. 14 Abs. 5 lit. b DSGVO erfüllt. Zudem sollte das Verhältnis zur Unverhältnismäßigkeit der Auskunft nach Art. 15 DSGVO klargestellt werden.

Nicht ganz ausgewogen erscheint, dass sowohl bei Art. 13 (Informationspflicht bei Direkterhebung) und Art. 12 Abs. 5 DSGVO-E (Auskunft) Verhältnismäßigkeitsgesichtspunkte geschärft wurden, in Art. 14 DSGVO aber nicht, der in der Praxis häufig das größten Erschwernis darstellt, v.a. bei Training von KI, aber auch bei RAG-Systemen. Die dazu verwendeten Daten (bei Wissensdatenbanken von RAG-Systemen z.B. Dokumente mit Autorennamen) sind häufig im Internet frei zugänglich, stammen also aus allgemein zugänglichen Quellen.

Soweit die Verarbeitung aus allgemein zugänglichen Quellen stammenden Daten voraussichtlich zu keinem hohen Risiko für betroffene Personen führt, insbesondere wenn die betroffenen Personen die Daten selbst öffentlich gemacht hat, und wenn zudem die Informationspflicht wegen der Vielzahl an betroffenen Personen und ungewisser E-Mail-Kontaktmöglichkeit unverhältnismäßig ist, sollte die Informationspflicht nach Art. 14 DSGVO durch eine Veröffentlichung (wie Online-Stellen) erfüllt werden können.

III. Automatisierte Einzelfallentscheidungen, Forschungsdaten und biometrische Daten

1. Automatisierte Einzelfallentscheidungen, Art. 22 DSGVO

Dringend klarzustellen gerade vor dem Hintergrund von KI-Agenten und Automatisierung von Workflows ist der Begriff „notwendig“ im Entwurf des Art. 22 Abs. 1 lit. a DSGVO-E. Die Abgrenzung zum DSGVO-typischen Begriff „erforderlich“ erschließt sich aus dem Text der Norm nicht. Erst aus dem zugehörigen Erwägungsgrund (38) wird klar, was gemeint ist.

Eine Verankerung im Normtext erscheint wünschenswert:

> *„Notwendig“ bedeutet, dass die Tatsache, dass auch ein Mensch die Entscheidung treffen könnte, den Verantwortlichen nicht daran hindert, die Entscheidung nur mittels automatisierter Verarbeitung zu treffen*
>
> *Wenn mehrere gleich wirksame automatisierte Verarbeitungsmöglichkeiten gegeben sind, soll der Verantwortliche die weniger intrusive Lösung verwenden.“*

Durch die geplante Änderung wurden die bisherigen Absätze 1 und 2 von Art. 22 DSGVO-E zusammengezogen und die Norm zu Erlaubnistatbeständen statt bisher einem Betroffenenrecht umgewandelt. Das ist nachvollziehbar, allerdings scheint der Standort in „Kapitel III Betroffenenrechte“ nun nicht mehr ganz passend.

Die Relevanz von Art. 22 DSGVO-E für KI-gestützte Entscheidungsprozesse ist sehr groß. Das gilt selbst bei nicht-vollautomatisierten Prozessen unter Einbezug von Sachbearbeitern, wenn KI-Empfehlungen die Entscheidungen maßgeblich bestimmen, weil für den Menschen nicht ausreichend Einblick und Selbstbeurteilungsmöglichkeit besteht (EuGH Urt. v. 07.12.2023 - C-634/21, SCHUFA). Im Anwendungsbereich von Art. 22 DSGVO-E wurde „rechtliche Wirkung“ in „Rechtswirkung“ geändert. Eine inhaltliche Änderung ist damit wohl nicht beabsichtigt.

Die vorgeschlagene Klarstellung in der Neufassung von Art. 22 Abs. 1, a) DSGVO, dass es bei der Bewertung, ob eine Entscheidung für den Abschluss oder die Erfüllung eines Vertrags der betroffenen Person mit einem Verantwortlichen notwendig ist, nicht erforderlich ist, dass sich die Entscheidung ausschließlich durch automatisierte Verarbeitung treffen lässt, ist zu begrüßen. Letztendlich ermöglicht diese Klarstellung eine einfachere Umsetzung in der Praxis, ohne dass dadurch die relevanten Betroffenenrechte wesentlich eingeschränkt werden.

2. Forschungsdaten

Der Vorschlag, durch die Einführung von Art. 4 Nr. 38 DSGVO den Begriff der „wissenschaftlichen Forschung“ konkret zu definieren sowie durch die Neufassung von Art. 5 Abs.1 b) und die Ergänzung von Art. 13 Abs. 5 DSGVO klarzustellen, dass die weitere Datenverarbeitung für wissenschaftliche Zwecke mit dem ursprünglichen Verarbeitungszweck vereinbar ist und dass wissenschaftliche Forschung ein berechtigtes Interesse darstellt, ist im Grundsatz ebenso zu begrüßen. Insbesondere die Klarstellung, dass es nicht ausgeschlossen ist, dass die Forschung auch der Förderung eines

gewerblichen Interesses dienen kann, erscheint sinnvoll und praxisnah, zumal dies ein mit der Verordnung (EU) 2025/327 zum EU-Gesundheitsdatenraum gleichlaufendes Begriffsverständnis sicherstellt. Durch die Änderungen werden gemeinwohlorientierte Forschungs- und Innovationstätigkeiten, auch wenn diese ggf. datenintensiv sind, im Ergebnis privilegiert. Diese Zielsetzung, gerade im Hinblick auf eine gestärkte Innovationsförderung, ist sinnvoll. Sicherlich entsteht hierdurch auch ein gewisses Missbrauchspotenzial, da Unternehmen Forschungserklärungen abgeben können, ohne dass ihnen wissenschaftliche Methodik, systematische Erkenntnisorientierung oder qualitätsgesicherte Verfahren zugrunde liegen. Die Beurteilung, ob ein Missbrauch vorliegt, dürfte aufgrund der diversen unbestimmten Rechtsbegriffe auch schwierig und komplex sein. Andererseits spricht auch nichts dagegen, diese Klärung den Aufsichtsbehörden bzw. den Gerichten zu überlassen, zumal das Missbrauchspotenzial letztlich auch bisher schon gegeben war. Es erscheint hier wesentlicher, die Forschungsprivilegierung zu stärken und dann im Vollzug zu überprüfen, dass diese auch nur für tatsächliche Forschungsvorhaben im erforderlichen Umfang genutzt wird.

3. Biometrische Daten

Der Vorschlag durch die Ergänzung von Art. 9 Abs. 2, l) DSGVO eine Ausnahme vom allgemeinen Verbot der Verarbeitung biometrischer Daten für den Fall einzuführen, wenn die Verarbeitung zur Bestätigung der Identität der betroffenen Person erforderlich ist und wenn die Daten und Mittel für eine solche Überprüfung der alleinigen Kontrolle dieser Person unterliegen, ist grundsätzlich sinnvoll. Zu unbestimmt erscheint allerdings die Anknüpfung an „die alleinige Kontrolle“ des Betroffenen bezogen auf die Daten oder Mittel. Besser wäre es, wenn man stattdessen auf geeignete technische und organisatorische Maßnahmen abstellen würde:

> *„l) die Verarbeitung biometrischer Daten zum Zwecke der Bestätigung der Identität einer betroffenen Person (Überprüfung) ist erforderlich, sofern der Verantwortliche durch geeignete technische und organisatorische Maßnahmen sicherstellt, dass die Verarbeitung der biometrischen Daten auf den Überprüfungsprozess beschränkt und eine sonstige nachfolgende Verarbeitung, insbesondere eine Speicherung, ausgeschlossen ist.“*

In diese Richtung dürfte auch der Erwägungsgrund (34) zu verstehen sein, zumal dort ausdrücklich auf die Verschlüsselung der biometrischen Daten nach dem neuesten Stand der Technik abgestellt wird.

IV. Meldepflichten

Der DAV begrüßt ausdrücklich die im Vorschlag COM (2025) 837 final enthaltenen Änderungen zur Konsolidierung der Meldepflichten über eine zentrale Anlaufstelle bei der ENISA. Die Einführung des „report once, share many"-Prinzips stellt einen wesentlichen Fortschritt zur Reduzierung administrativer Belastungen dar. Da die Meldungen für die betroffenen Einrichtungen erheblich sensitive Informationen umfassen können, sollten die von der ENISA zu ergreifenden technischen, operativen und organisatorischen Maßnahmen nach Art. 23a Abs. 2 des Änderungsvorschlags zur NIS-2-Richtlinie nicht nur „geeignet und verhältnismäßig", sondern auch wirksam sein und dem Stand der Technik entsprechen. Der DAV hält es für essenziell, dass die ENISA als Treuhänder fungiert und ausschließlich die meldende Einrichtung über die Weitergabe der Informationen entscheidet. Art. 23a Abs. 4 der vorgeschlagenen Neuregelung sollte daher den Zugang der ENISA zu den übermittelten Meldungen generell ausschließen.

Ebenfalls positiv zu bewerten sind die Verlängerung der Meldefrist nach Art. 33 DSGVO auf 96 Stunden sowie das Anheben der Risikoschwelle mit Angleichung an Art. 34 DSGVO.

Allerdings sollten die Meldepflichten nach NIS2-Richtlinie, DORA, eIDAS-Verordnung und CER-Richtlinie ebenfalls durch ein Anheben der Frist entschärft werden, um ein konsistentes und praxisgerechtes Meldeverfahren zu gewährleisten.

V. Änderungsvorschläge zu Cookies

Die Änderung in Art. 5 des Vorschlag COM (2025) 837 final erscheint aus Sicht des DAV nicht sinnvoll. Sie droht, das ohnehin schon sehr komplexe Verhältnis zwischen DSGVO, ePrivacy-Richtlinie und Data Act noch komplizierter zu machen und vergrößert dadurch sowohl die Rechtsunsicherheit als auch die Compliance-Aufwände für alle Beteiligten. Wichtige innovationsgetriebene Sektoren wie das "Internet of Things" und damit verbundene Initiativen (z.B. Industrie 4.0 oder vernetztes Fahren) werden dadurch behindert.

Der DAV empfiehlt, jedenfalls auf die Neuregelung zum Anwendungsvorrang des neuen Art. 88a DSGVO zu verzichten, die der Omnibus-Vorschlag COM (2025) 837 final derzeit vorsieht (dazu VI.1.). Außerdem schlägt der DAV vor, Art. 5 Abs. 3 der ePrivacy-Richtlinie insgesamt zu streichen (dazu VI. 2.).

1. Neuregelung würde die bereits bestehende Rechtsunsicherheit nur vergrößern

Bereits bei aktueller Rechtslage müssen Unternehmen, die ein Geschäftsmodell rund um vernetzte Gegenstände bzw. den damit erzeugten Daten realisieren wollen, Compliance mit (mindestens) drei unterschiedlichen Regelungsakten herstellen:

- Data Act
- DSGVO
- Art. 5 Abs. 3 der ePrivacy-Richtlinie, bzw. deren nationale Umsetzungen

Die drei Gesetze regeln alle ein- und denselben Sachverhalt: Sie legen fest, ob bzw. unter welchen Bedingungen ein Unternehmen aus einem vernetzten Gegenstand Daten entnehmen bzw. auf diesen aufspielen kann. Alle drei Gesetze legen sich also wie "Regelungsschichten" über denselben Sachverhalt. Nur dann, wenn ein Unternehmen die Bedingungen aller drei "Schichten" erfüllt, kann es das Geschäftsmodell umsetzen. Es ist offensichtlich, dass mit jeder weiteren Schicht der Bürokratieaufwand größer wird, während Rechtsrisiken steigen und bestimmte (auch legitime) Möglichkeiten zur Erzielung von Erlösen wegfallen.

Problematisch ist dies vor allem dann, wenn die Regelungsakte zu einander widersprechenden Ergebnissen führen. Manche dieser "Problemstellen" bei aufeinandertreffenden Regelungsakten sind bereits jetzt für Unternehmen kaum mit Rechtssicherheit bewältigbar. Beispielsweise findet die einschlägige Regelung im Data Act (Art. 4 Nr. 13) nur auf nicht-personenbezogene Daten Anwendung – obwohl sich dies aus Sicht des jeweiligen Unternehmens in der Regel nicht rechtssicher feststellen lässt und sich auch nachträglich noch ändern kann.

Ein ähnliches Problem würde nun durch den vorgeschlagenen Unterabsatz unter Art. 5 Abs. 3 der ePrivacy-Richtlinie ausgelöst, der einen Regelungsvorrang des neuen Art. 88a DSGVO bewirken soll. Es ist in den meisten Fällen schlichtweg nicht möglich, abstrakt zu

entscheiden, ob ein bestimmtes Geschäftsmodell oder ein bestimmter Prozess personenbezogene Daten betrifft oder nicht. Dies kann sich kontextbezogen ändern, beispielsweise wenn Zusatzwissen hinzukommt oder wenn die Daten mit Dritten geteilt werden (vgl. die EuGH-Rechtsprechung zu SRB (Rs. C-413/23 P), OLAF (Rs. C-479/22 P), Gesamtverband Automobilteile-Handel (Rs. C-319/22)). Außerdem basiert bereits die Definition des Begriffs der personenbezogenen Daten auf dem sog. "Breyer-Test" (heute Erwägungsgrund 26 der DSGVO), laut dem es darauf ankommt, ob die betroffene Person "nach allgemeinem Ermessen wahrscheinlich" identifiziert werden kann. Dies sind unbestimmte Rechtsbegriffe, die einzelfallabhängig immer wieder neu bewertet werden müssen, und bei denen es nach praktischer Erfahrung auch häufig unterschiedliche Rechtsauffassungen gibt.

Innovationsgetriebene Sektoren brauchen Rechtssicherheit – oder, falls es keine Rechtssicherheit gibt, jedenfalls die Möglichkeit, bei vertretbaren Risiken innovative Geschäftsmodelle umzusetzen.

Regelungen wie die hier vorgeschlagene sind sprichwörtlich "Gift" für innovationsgetriebene Unternehmen, weil sie einerseits Rechtsunsicherheit schaffen und andererseits extreme Risiken bewirken – Verstöße gegen die DSGVO oder die nationalen Umsetzungsgesetze von Art. 5 Abs. 3 ePrivacy-Richtlinie können Bußgelder und Massen-Schadensersatzklagen in existenzbedrohender Höhe auslösen.

Die neu vorgeschlagene Regelung würde Unternehmen einerseits vor eine unlösbare Aufgabe stellen, nämlich mit Sicherheit vorherzusagen, wie eine Behörde oder ein Gericht in einem komplexen (Grenz-) Fall den Personenbezug der verarbeiteten Daten einstufen würde. Andererseits bleibt es bei den drakonischen Rechtsfolgen, falls sich die Rechtsauffassung des Unternehmens nachträglich als "falsch" herausstellt.

Hinzu kommt zuletzt, dass der neue Unterabsatz zu dem systematischen Widerspruch führt, dass eine Regelung, die nicht für personenbezogene Daten gilt, strengere Voraussetzungen hat als eine Regelung für personenbezogene Daten. Das ist systemwidrig.

Der DAV schlägt vor diesem Hintergrund vor, den neuen Unterabsatz unter Art. 5 Abs. 3 der ePrivacy-Richtlinie zu streichen.

2. Art. 5 Abs. 3 ePrivacy-RL ist insgesamt zu streichen

Anstelle des neuen Unterabsatzes sollte Art. 5 Abs. 3 der ePrivacy-Richtlinie insgesamt gestrichen werden.

Die Regelung ist ursprünglich (wohl) eingeführt worden, weil der EU-Gesetzgeber zur Zeit der Einführung der ePrivacy-Richtlinie erstmals mit Cookies zu tun hatte – also mit kleinen Textdateien, die von Webseiten-Anbietern auf Computern der Nutzer:innen abgelegt wurden, um dort Daten abzuspeichern und diese später wieder abzurufen. Der EU-Gesetzgeber hielt dies für so problematisch, dass er hieran eine Regelung anknüpfte, die das Setzen von Cookies unter ein Verbot mit Erlaubnisvorbehalt stellte.
Aufgrund des offenen Wortlauts der Vorschrift hat sie mittlerweile ein Eigenleben angenommen, der vom ursprünglichen Gesetzgeber nicht intendiert war. Sie wird mittlerweile nicht nur auf Cookies angewendet, sondern auf eine Vielzahl weiterer Technologien – beispielsweise das bereits oben erwähnte "Internet der Dinge", aber auch jede Form von Tracking im Internet bzw. über Online-Anwendungen. In der Literatur wird sogar diskutiert, ob sogar das Aufspielen von Software-Updates in den Anwendungsbereich der Regelung fällt - was vom Wortlaut her auch zu bejahen wäre.
Richtig wäre nach Auffassung des DAV, einmal neu zu prüfen, welchen Schutzzweck die Regelung eigentlich hat und ob sie diesen erreicht. Die Antwort hierauf fällt aus Sicht des DAV negativ aus.

Art. 5 Abs. 3 der ePrivacy-Richtlinie hat als privatsphären-schützende Regelung einen ganz ähnlichen Schutzzweck wie Art. 6 der DSGVO, unterscheidet sich von diesem aber maßgeblich in zwei Punkten:

- Anders als Art. 6 der DSGVO findet Art. 5 Abs. 3 der ePrivacy-RL auch auf nicht-personenbezogene Daten Anwendung. Im Anwendungsbereich sind alle Daten, die auf Endgeräten gespeichert sind oder dort gespeichert werden. Art. 5 Abs. 3 der ePrivacy-Richtlinie sieht nur drei mögliche Rechtfertigungen für das Speichern oder Abrufen der Daten vor: Zur Erbringung eines ausdrücklich gewünschten Dienstes der Informationsgesellschaft (und begrenzt auf die dafür unbedingt notwendige Verarbeitung); zur Übermittlung einer Nachricht in einem Telekommunikationsnetz; oder mit Einwilligung des Betroffenen.

Diese Kombination von sehr großem Anwendungsbereich mit sehr restriktiven Erlaubnissen hat in der Praxis zu starken negativen Effekten geführt: Im Ergebnis fehlt für viele Datenverarbeitungen eine andere Rechtsgrundlage als die Einwilligung. Das hat (vor allem, aber nicht nur) im Internet zu einer wahrhaften Flut von Einwilligungsbannern geführt hat, die Nutzer:innen im Internet als störend empfinden und in nahezu allen Fällen schlichtweg "weggeklickt" wird, also dazu führt, dass die Nutzer:innen unbesehen und ungeprüft eine Einwilligung abgeben. Die Folge ist die sprichwörtliche "consent fatigue": Die Schutz- und Warnfunktion, die die Einwilligung eigentlich haben sollte, geht verloren.
Der Zuschnitt des Art. 5 Abs. 3 führt außerdem auch zu Regelungswidersprüchen zu anderen Regelungen und zu nicht nachvollziehbaren Ergebnissen. Was, wenn ein Unternehmen auf Daten im Endgerät zugreifen muss, um z.B. eine Rechtspflicht zu erfüllen oder ein wichtiges Ziel im Allgemeininteresse zu erreichen (z.B. Gewährleistung von Cybersicherheit)? Die DSGVO adressiert solche Datenverarbeitungszwecke mit Art. 6 Abs. 1 lit. c, lit. d oder lit. f DSGVO. Art. 5 Abs. 3 der ePrivacy-Richtlinie enthält keine vergleichbaren Ausnahmen. Nähme man seinen Wortlaut ernst, würde er die Datenspeicherung oder -entnahme für solche Zwecke verbieten.

Außerdem ergeben sich auch Regelungswidersprüche zu den bereits vorgenannten Rechtsgrundlagen in Art. 6. Diese bringen zum Ausdruck, dass bestimmte Datenverarbeitungen nach dem Willen des EU-Gesetzgebers erlaubt sein sollen – beispielsweise dann, wenn dies einem legitimen Interesse dient und keine überwiegenden Gegeninteressen der Betroffenen bestehen (Art. 6 Abs. 1 lit. f DSGVO). Warum aber will die DSGVO solche Datenverarbeitungen erlauben – Art. 5 Abs. 3 DSGVO aber nicht? Der Schutzzweck beider Vorschriften ist weitgehend derselbe, eine Regelung ist aber deutlich strenger als die andere.

Hinzu kommt, dass aus rechtspolitischer Sicht der Schutzzweck von Art. 5 Abs. 3 der ePrivacy-Richtlinie kaum nachvollziehbar ist. Soweit es um "normalen" Datenschutz geht, ist der Schutz bereits durch die DSGVO gewährleistet. Diese regelt bereits, unter welchen Voraussetzungen der EU-Gesetzgeber Eingriffe in die Privatsphäre der Nutzer:innen als gerechtfertigt ansieht. Wenn der EU-Gesetzgeber diesen Schutz nicht als stark genug empfindet, sollte dies in der DSGVO adressiert werden, nicht systemfremd in der ePrivacy-Richtlinie.

Und soweit man in Art. 5 Abs. 3 der ePrivacy einen wirtschaftlichen Schutzzweck sehen wollte, so wäre dieser in der ePrivacy-Richtlinie systemfremd und außerdem in Art. 4 Nr. 13 des Data Acts bereits adressiert.

Als Schutzzweck verbleibt letztlich nur der Gedanke, dass Art. 5 Abs. 3 der ePrivacy-Richtlinie seine besondere Form der Privatsphäre schützen soll, nämlich die "informationelle Integrität des Endgeräts" – also eine Art Kontrollrecht des Nutzers, zu bestimmen, welche Informationen von außen sein Endgerät "betreten" und welche es "verlassen"; ähnlich dem Wohnungsgrundrecht.

Ein solcher Schutzzweck wirkt aber übertrieben und ist rechtspolitisch nicht sinnvoll. Kommunikations-Endgeräte sind dafür gebaut, Informationen zu empfangen und zu senden. Ausgerechnet dies unter ein Verbot mit Erlaubnisvorbehalt zu stellen, ist innovationsfeindlich und verursacht Bürokratie. Eine sinnvolle Regelung, die diesen Aspekt betrifft, sollte nicht das "ob" regeln, sondern das "wie". Denkbar sind z.B. Informations- und Transparenzpflichten, die Pflicht zur Abfrage von Voreinstellungen auf dem Endgerät oder einschränkende Regelungen bei bestimmten Praktiken der Datenerhebung (z.B. Profiling). Wichtig ist in einem solchen Fall aber, dass sie systematisch in das richtige Gesetz eingefügt werden – wenn es um personenbezogene Daten geht, z.B. in der DSGVO, oder wenn es um bestimmte als "unfair" empfundene Praktiken geht, z.B. in der UCP-Richtlinie.

VI. Definition personenbezogene Daten

Zu begrüßen ist der Ansatz, den Begriff der „personenbezogenen Daten“ in Art. 4 Nr. 1 DSGVO an die Rechtsprechung des EuGH anzupassen und hierdurch Klarheit zu schaffen. Geklärt wird hierdurch die Frage, ob zur Bestimmung des Personenbezugs nur die der jeweils verarbeitenden Stelle zur Verfügung stehenden Mittel zu berücksichtigen sind (relativer Begriff), oder ob es ausreicht, dass eine beliebige Einrichtung oder verarbeitende Stelle einen Personenbezug herstellen kann (absoluter Begriff).

Der Entwurf setzt die Rechtsprechung des EuGH jedoch nicht in allen Punkten um.

3. Problemstellung

a) Die jüngste Rechtsprechung des EuGH

In seinem SRB-Urteil vom 4.9.2025 hat der EuGH hinsichtlich des Personenbezugs pseudonymisierter Daten entschieden, dass die Existenz von zusätzlichen, die Identifizierung der betroffenen Personen ermöglichenden Informationen nicht bedeutet, dass pseudonymisierte Daten in jedem Fall und für jede Person personenbezogene Daten darstellen (EuGH, Urt. v. 4.9.2025, C-413/23 P, Rn. 82, 86). Vielmehr kann die Pseudonymisierung je nach den Umständen des Einzelfalles andere Personen an einer Identifizierung der betroffenen Person hindern, sodass diese Daten für andere Personen nicht oder nicht mehr personenbezogen sind (EuGH, Urt. v. 4.9.2025, C-413/23 P, Rn. 86f.).

Je nach den Umständen des Einzelfalles kann einerseits der Verantwortliche, der die Pseudonymisierung vorgenommen hat, über zusätzliche Informationen zur Zuordnung von Daten an betroffene Personen verfügen (EuGH, Urt. v. 4.9.2025, C-413/23 P, Rn. 76), andererseits ebenso der Dritte, an den die Daten vom Verantwortlichen übermittelt wurden, wenn dieser anhand dieser Mittel zur Identifizierung eine solche Zuordnung vornehmen kann (EuGH, Urt. v. 4.9.2025, C-413/23 P, Rn. 77).
Entsprechendes gilt nach dem EuGH, wenn der Verantwortliche pseudonymisierte Daten Dritten überlässt, die über Mittel verfügen, die die Identifizierung der betroffenen Personen ermöglichen können. In diesem Fall sind die Daten für den nicht nur für den Dritten personenbezogen, sondern auch für den Verantwortlichen („indirekt“, vgl. EuGH, Urt. v. 4.9.2025, C-413/23 P, Rn. 84). Mit dieser Regelung wird nach dem EuGH verhindert, dass pseudonymisierte Daten, die an sich keinen Personenbezug aufweisen, der jedoch von anderen Personen hergestellt werden kann, zu Unrecht vom Anwendungsbereich des Unionsrechts zum Schutz personenbezogener Daten ausgenommen werden (EuGH, Urt. v. 4.9.2025 – C-413/23 P SRB, Rn. 85).

Der EuGH bewertet den Personenbezug also einzelfallbezogen und stellt hinsichtlich der Bestimmbarkeit des Personenbezugs jeweils auf die Person, Einrichtung oder Stelle, einschließlich der Empfänger der Daten ab, die über Mittel verfügen, eine betroffene Person – auch bei pseudonymisierten Daten – zu identifizieren. Es kommt nicht darauf an, dass ein beliebiger Dritter, der nicht an der Verarbeitung der Daten beteiligt ist, und dem die Daten nicht übermittelt werden, einen Personenbezug herstellen kann. Der EuGH bestimmt den

Personenbezug damit relativ im Einzelfall und erteilt einer absoluten Sichtweise eine Absage.

b) Geplante Änderung des Art. 4 Nr. 1 DSGVO

Die geplante Änderung des Art. 4 Nr. 1 DSGVO weicht in Satz 3 von der Rechtsprechung des EuGH ab. Dort heißt es, dass Daten nicht allein deshalb als personenbezogen gelten, weil ein potenzieller späterer Empfänger über Mittel verfügt, die mit hinreichender Wahrscheinlichkeit zur Identifizierung der natürlichen Person, auf die sich die Angaben beziehen, verwendet werden können.

Der EuGH hat – wie bereits ausgeführt – ganz im Gegenteil (pseudonymisierte) Daten als („indirekt“) personenbezogen für die übermittelnde Stelle bezeichnet, wenn ein späterer Empfänger eine solche Identifizierung vornehmen konnte (EuGH, Urt. v. 4.9.2025 – C-413/23 P, SRB, Rn. 84 unter Verweis auf das Urt. v. 9.11.2023 - C 319/22, Gesamtverband Autoteile-Handel, Rn. 46 und 49 zum Personenbezug der FIN bei Übermittlung durch einen Fahrzeughersteller).

Nach Erwägungsgrund (27) des Vorschlages ist unter Beachtung der einschlägigen Rechtsprechung des EuGH zur Definition der personenbezogenen Daten eingehender zu klären, wann eine natürliche Person als identifizierbar gelten sollte. Dabei ist insbesondere klarzustellen, dass Informationen für eine bestimmte Einrichtung nicht als personenbezogene Daten gelten, wenn diese Einrichtung über keine Mittel verfügt, die mit hinreichender Wahrscheinlichkeit zur Identifizierung der natürlichen Person dienen, auf die sich die Informationen beziehen. Bei einer eventuellen späteren Übermittlung dieser Informationen an Dritte, die ihrerseits nach vernünftigem Ermessen über Mittel verfügen, um die natürliche Person, auf die sich die Informationen beziehen, zu identifizieren, etwa durch einen Abgleich mit anderen ihnen zur Verfügung stehenden Daten, werden diese Angaben nur für jene Dritten, die solche Mittel besitzen, zu personenbezogenen Daten. Dieser letzte Satz des Erwägungsgrundes weicht aus den genannten Gründen von der Rechtsprechung des EuGH ab.

4. Vorschlag

Art. 4 Nr. 1 Satz 3 DSGVO-E

Es sollte deswegen bei der Bezugnahme auf die einschlägige Rechtsprechung des EuGH entweder klargestellt werden, dass Art. 4 Nr. 1 Satz 3 DSGVO-E von dieser Rechtsprechung abweicht, oder es sollte eine Anpassung an die Rechtsprechung des EuGH erfolgen („indirekter Personenbezug“). Dabei ist allerdings zu bedenken, dass fraglich ist, ob es überhaupt einer Änderung des Art. 4 Nr. 1 DSGVO bedarf, wenn die Rechtsprechung des EuGH zur Definition der personenbezogenen Daten lediglich festgeschrieben werden soll. In diesem Fall würde auch ohne eine Änderung des Art. 4 Abs. 1 DSGVO die bisherige Rechtsprechung des EuGH fortgelten und die Weiterentwicklung auf neue, insb. KI-getriebene Datenmodelle dieser Rechtsprechung überlassen bleiben. Dies böte den Vorteil einer flexibleren Lösung, da neue Entwicklungen weiter berücksichtigt werden können.

Art. 4 Nr. 1 Satz 1 und 2 DSGVO-E

Für den Fall, dass es an dem Vorhaben einer Änderung des Art. 4 Nr. 1 DSGVO bleibt, wird folgende Formulierung für Art. 4 Nr. 1 Satz 1 und 2 DSGVO-E angeregt:

> *Art. 4 Nr. 1 DSGVO*
>
> *„personenbezogene Daten“: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt von dem Verantwortlichen oder einer anderen Person, Behörde, Einrichtung oder anderen Stelle, die diese Daten verarbeitet, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, eindeutig bestimmt werden kann.*
>
> *Informationen werden für den Verantwortlichen oder die andere Person, Behörde, Einrichtung oder andere Stelle nicht allein deswegen personenbezogen, weil ein Dritter, der diese Informationen nicht verarbeitet, über Mittel verfügt, die mit hinreichender Wahrscheinlichkeit zur Identifizierung der natürlichen Person, auf die sich die Angaben beziehen, verwendet werden können.“*

Begründung:
Im Zuge des „Omnibus“ das bereits seit der Richtlinie 95/46/EG bestehende Problem beseitigt wird, dass die Definition von „identifizierbar“ zirkulär erscheint, wenn sich der zu definierende Begriff in der Umschreibung wiederfindet: „als identifizierbar wird eine natürliche Person angesehen, die … identifiziert werden kann“.

VII. Änderung der Regelungen zur Pseudonymisierung

Zu begrüßen ist der Ansatz, die Einhaltung der Vorschriften der DSGVO durch Unterstützung der (für die Datenverarbeitung) Verantwortlichen hinsichtlich der Kriterien und Mittel zur Feststellung, ob Daten, die sich aus der Pseudonymisierung ergeben, personenbezogene Daten sind oder nicht (I., 1. b.)) zu erleichtern und die Auslegung des EuGH zur Pseudonymisierung personenbezogener Daten in die Vorschriften aufzunehmen (II.,1.).

Die geplanten Regelungen sollten jedoch ebenfalls angepasst werden.

1. Problemstellung

Nach Art. 4 Nr. 5 DSGVO ist „Pseudonymisierung“ die Verarbeitung personenbezogener Daten in einer Weise, dass diese ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Der EuGH hat klargestellt, dass die Pseudonymisierung kein Element des Begriffs „personenbezogene Daten“ ist, sondern sich auf die Umsetzung technischer und organisatorischer Maßnahmen bezieht, die das Risiko verringern sollen, dass ein bestimmter Datensatz mit der Identität der betroffenen Person in Verbindung gebracht wird (EuGH, Urt. v. 4.9.2025 – C-413/23 P SRB, Rn. 72). Der Begriff „Pseudonymisierung“ setzt voraus, dass Informationen vorliegen, die eine Identifizierung der betroffenen Person ermöglichen. Die bloße Existenz solcher Informationen spricht dagegen, dass Daten, die pseudonymisiert wurden, in jedem Fall als anonymisierte Daten betrachtet werden können,

die vom Anwendungsbereich der DSGVO ausgenommen werden können (EuGH, Urt. v. 4.9.2025 – C-413/23 P SRB, Rn. 73).

Die Pseudonymisierung zielt darauf ab, zu verhindern, dass die betroffene Person allein anhand pseudonymisierter Daten identifiziert werden kann (EuGH, Urt. v. 4.9.2025 – C-413/23 P, SRB, Rn. 74). Werden technische und organisatorische Maßnahmen ergriffen, die eine Zuordnung der in Rede stehenden Daten zu der betroffenen Person verhindern, sodass diese nicht oder nicht mehr identifizierbar ist, kann die Pseudonymisierung dazu führen, dass der Personenbezug entfällt (EuGH, Urt. v. 4.9.2025 – C-413/23 P, SRB, Rn. 75).

Bei der Prüfung der Identifizierbarkeit sind alle Mittel zu berücksichtigen, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren. Bei der Prüfung, ob Mittel wahrscheinlich zur Identifizierung genutzt werden, sind alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand heranzuziehen. Dabei ist die zum Zeitpunkt der Verarbeitung verfügbare Technologie und sind die technologischen Entwicklungen zu berücksichtigen (EuGH, Urt. v. 4.9.2025 – C-413/23 P, SRB, Rn. 79).

Die zum Zeitpunkt der Verarbeitung zum Schutz vor Re-Identifizierung durch der Zusatzinformationen eingesetzten Mittel, insbesondere die eingesetzte Technologie und die Wirksamkeit der Verfahren zur Beseitigung der identifizierenden Merkmale, entscheiden darüber, ob aus den pseudonymisierten Daten eine Identifizierung möglich ist oder nicht. Soweit sich durch technisch-organisatorische Maßnahmen sicherstellen lässt, dass eine Identifizierung nicht möglich ist, sind pseudonymisierte Daten für Personen, die einen Personenbezug nicht herstellen können, anonyme Daten. Die Pseudonymisierung kann also eine anonymisierende Wirkung haben.

2. Vorschlag zu Art. 41a DSGVO-E

Bei den Pseudonymisierungstechnologien setzt die geplante Einführung des neuen Art. 41a DSGVO-E an. Nach Abs. 1 kann die EU-Kommission Durchführungsrechtsakte erlassen, um Mittel und Kriterien festzulegen, mit denen bestimmt wird, ob Daten, die sich aus der Pseudonymisierung ergeben, für bestimmte Einrichtungen keine personenbezogenen Daten mehr darstellen. Nach der aufgezeigten Konzeption des EuGH im Einklang mit

Erwägungsgrund (26) S. 4 DSGVO bestimmen diese Mittel und Kriterien darüber, ob aus pseudonymisierten Daten eine Identifizierung der betroffenen Person vorgenommen werden kann oder nicht.

Das Verhältnis und die Bedeutung dieser neuen Regelung des Art. 41a DSGVO-E zur Definition der Pseudonymisierung nach Art. 4 Nr. 5 DSGVO ist in dem Entwurf noch nicht klar geregelt:

- Zum einen sollte klar festgelegt werden, dass es sich bei den in Art. 41a DSGVO-E vorgesehenen Regelungen um Kriterien für die technischen und organisatorischen Maßnahmen iSd Art. 4 Nr. 5 DSGVO handelt. Zum anderen bleibt die an den Einsatz solcher Mittel geknüpfte Rechtsfolge unklar.

- Art. 41a Abs. 3 DSGVO-E sieht lediglich vor, dass die Umsetzung der in einem Durchführungsakt festgelegten Mittel und Kriterien als Kriterium verwendet werden kann, um nachzuweisen, dass Daten nicht zu einer Re-Identifizierung der betroffenen Personen führen können. Unklar bleibt jedoch, welche Bedeutung diesem Nachweis zukommt, und welchen Umfang er haben soll. Es kann sich um eine widerlegbare Vermutung iS eines prima facie Beweises handeln, zwingend ist dies aufgrund der Formulierung jedoch nicht, wenn die Mittel und Kriterien lediglich als ein Kriterium zum Nachweis des Ausschlusses einer Re-Identifizierung genutzt werden können. Wenn es sich hierbei lediglich um ein Kriterium unter anderen Kriterien zum Nachweis eines solchen Ausschlusses handelt, ist fraglich, welcher Vorteil sich in der Praxis zur Führung dieses Nachweises ergibt.

Eine widerlegbare Vermutung würde für Verantwortliche die von der EU-Kommission angestrebten Erleichterungen bei der Einhaltung der DSGVO bringen. Die derzeit in der Praxis sehr aufwendige Prüfung, ob und wenn welche Empfänger der Daten über welche Mittel zur Identifizierung der betroffenen Person verfügen, würde erst dann relevant, wenn die Vermutung widerlegt würde. So könnte für Sicherheit bei der Anwendung von Pseudonymisierungstechnologien gesorgt werden. Zugleich könnte die Definition der Anonymisierung im Definitionskatalog der DSGVO ergänzt und - wie in Erwägungsgrund 26 S. 6 aufgeführt - klargestellt werden, dass nur anonymisierte Daten aus dem Anwendungsbereich der DSGVO fallen. Pseudonymisierte Daten wären dann als anonym anzusehen, wenn die Identifizierung aufgrund des Einsatzes der in dem Durchführungsakt von der EU-Kommission festgelegten Mittel und Kriterien nicht wahrscheinlich ist.

Art. 41a DSGVO-E könnte, wie folgt, lauten:

Artikel 41a

(1) Die Kommission kann Durchführungsrechtsakte erlassen, um Mittel und Kriterien für die technischen und organisatorischen Maßnahmen iSv Art. 4 Nr. 5 DSGVO festzulegen, mit denen bestimmt wird, ob Daten, die sich aus der Pseudonymisierung ergeben, für bestimmte Einrichtungen keine personenbezogenen Daten mehr darstellen.

(2) Für die Zwecke des Absatzes 1 wird die Kommission wie folgt tätig:

a) sie bewertet den Stand der verfügbaren Techniken,

b) sie entwickelt Kriterien und/oder Kategorien für Verantwortliche und Empfänger, um das Risiko einer Re-Identifizierung im Hinblick auf typische Empfänger von Daten zu bewerten.

c) Sie bewertet die verfügbaren Techniken regelmäßig auf Aktualität und passt die Durchführungsrechtsakte entsprechend der technologischen Entwicklungen und Sicherheitsanforderungen an.

(3) Bei der Umsetzung der in einem Durchführungsrechtsakt festgelegten Mittel und Kriterien spricht eine widerlegbare Vermutung dafür, dass Daten nicht zu einer Re-Identifizierung führen und die Identifizierung der betroffenen Person ausgeschlossen ist.

(4) Die Kommission bezieht den EDSA eng in die Ausarbeitung der Durchführungsrechtsakte ein. Der EDSA gibt innerhalb von acht Wochen nach Eingang des Entwurfs des Durchführungsrechtsakts der Kommission eine Stellungnahme dazu ab.

(5) Der Durchführungsrechtsakt wird gemäß dem in Artikel 93 Absatz 3 genannten Prüfverfahren erlassen.

Hieran anknüpfend erscheint es erwägenswert, den Begriff der „Anonymisierung“ aus Erwägungsgrund (26) DSGVO heraus- und in den Definitionskatalog des Art. 4 DSGVO aufzunehmen. Die in Erwägungsgrund (26) angelegte Definition sollte unter Berücksichtigung der Ergänzungen zur Pseudonymisierung geändert werden, um Klarheit zu schaffen, welche Daten als pseudonym und welche als anonym geltem:

Art. 4 Nr. 5a DSGVO

„Anonymisierung“ ist die Verarbeitung personenbezogener Daten derart, dass sich diese Daten nicht mehr auf eine identifizierte oder identifizierbare natürliche Person oder personenbezogene Daten beziehen, und die betroffene Person nicht oder nicht mehr identifiziert werden kann. Um festzustellen, ob eine natürliche Person identifizierbar ist, weren alle Mittel berücksichtigt, die von dem Verantwortlichen oder einer anderen Person,

die diese Daten verarbeitet, nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.

Pseudonymisierte Daten (iSv Art. 4 Nr. 5 DSGVO) sind als anonymisierte Daten Sinn anzusehen, wenn ausgeschlossen ist, dass die dem Verantwortlichen oder einer anderen Person, die diese Daten verarbeitet, zur Identifizierung zur Verfügung stehenden Mittel die direkte oder indirekte Identifizierung der natürlichen Person ermöglichen.

VIII. Sonstige Änderungsvorschläge, insbesondere zum Data Act

Der DAV begrüßt grundsätzlich das Bestreben der Europäischen Kommission, den Data Act (Verordnung EU 2023/2854) im Rahmen des Vorschlags COM (2025) 837 final zu vereinfachen und zu einem umfassenden Datengesetzbuch auszuweiten. Der Kommissionsvorschlag enthält Ansätze zur Stärkung der Rechte von Dateninhabern, zum verbesserten Schutz von Geschäftsgeheimnissen und zur Vereinfachung internationalen Datentransfers, die indes die Praxisprobleme an diesen Stellen noch nicht hinreichend erfassen. Die detaillierte Analyse zeigt nach wie vor erhebliche Defizite in diesen wesentlichen Bereichen; der DAV bittet sehr zu überprüfen, ob in diesen Regelungsbereichen mit den nachfolgenden Vorschlägen eine weitergehende Rechtssicherheit und ein verbesserter Interessensausgleich zwischen den beteiligten Akteuren geschaffen werden kann. Dies betrifft auch grundlegend das Verhältnis von Data Act und DSGVO.

Im Folgenden weist der DAV auf konkreten Verbesserungsbedarf hin und unterbreitet präzise Vorschläge zur Optimierung des Regelungsvorschlags.

1. Verhältnis eines erweiterten Datengesetzbuches zu den Datenschutzvorschriften

Eine Zusammenfassung der Regelungen des Datenrechts in einer Verordnung erleichtert die Übersichtlichkeit über die relevanten Vorschriften und ist zu begrüßen. Die eigentlichen Herausforderungen bei der Rechtsanwendung werden aber nicht gelöst, wenn (1) das Verhältnis zu den Datenschutzvorschriften, insbesondere der DSGVO, nach wie vor nicht geregelt wird und (2) bestehende Regelungen, die in der Praxis – wie etwa der Data Governance Act – nicht zu den beabsichtigten Wirkungen führen, ohne hinreichende Überarbeitung übernommen werden.

Nach Art. 1 Abs. 5 gilt der Data Act „unbeschadet“ u.a. der DSGVO. Das Verhältnis von Data Act und DSGVO und den weiteren in Art. 1 Abs. 5 gelisteten Rechtsakten zum Schutz personenbezogener Daten, der Privatsphäre, der Vertraulichkeit der Kommunikation und der Integrität von Endgeräten, die für personenbezogene Daten gelten, ist danach in der Anwendung höchst komplex. Insbesondere wird das Bewertungsrisiko, ob eine datenschutzrechtliche Erlaubnisgrundlage für einen Datenzugang nach Data Act oder – künftig – eine Verarbeitung personenbezogener Daten durch Datenvermittlungsdienste oder datenaltruistische Organisation vollständig auf die Ebene der Rechtsanwender verlagert. Denn diese werden etwa unter Kapitel II Data Act zur Gewährung des Datenzugangs verpflichtet, besteht eine datenschutzrechtliche Erlaubnisgrundlage, während der Datenzugang nicht gewährt werden darf, besteht eine solche Erlaubnisgrundlage nicht. Ob eine datenschutzrechtliche Erlaubnis besteht, ist aber vielfach Gegenstand komplexer Prüfung und einer einzelfallabhängigen Interessenabwägung, die nur gelegentlich zu eindeutigen Ergebnissen führt.

Wie etwa auch im Rahmen der Verordnung (EU) 2025/327 zum EU-Gesundheitsdatenraum vorgesehen, sollte angesichts dessen das Bewertungsrisiko auf Ebene der zuständigen Behörden verlagert werden, jedenfalls sollte den zur Datenzugangsgewährung verpflichteten Akteuren ein Recht auf Anrufung einer Behörde eingeräumt werden, um – der Datengenehmigung nach der Verordnung zum EU-Gesundheitsdatenraum vergleichbar – eine verbindliche Behördenentscheidung über die Pflicht zur Gewährung des Datenzugangs oder aber die Pflicht, dies mangels datenschutzrechtlicher Erlaubnis nicht durchzuführen, zu erhalten.
Der vorliegende Verordnungsvorschlag COM (2025) 837 final sieht indes keine Änderungen am Art. 1 Abs. 5 Data Act vor. Der DAV regt an, dies im Sinne des Vorstehenden zu überdenken.

2. Änderungsvorschläge an den Begriffsbestimmungen des Art. 2 Data Act

a) Begriff des Dateninhabers

Die neue Begriffsdefinition – namentlich die Setzung des Kommas im letzten Satzteil – ist weder ausreichend klar noch löst sie die in der Praxis mit der Definition einhergehenden Probleme. Wir verstehen das Komma so, dass klargestellt wird, dass der Nebensatz nicht bestimmend ist und sich daher nicht auf die „product data“ bezieht. Damit wird für die Variante der verbundenen Dienstdaten klargestellt, dass der Dateninhaber faktisch in der

Lage sein muss, die Daten zugänglich zu machen, und nur eine Person ein Dateninhaber sein kann, die in dieser Position ist. Für die Produktdaten gibt es eine vergleichbare Aussage nicht. Im deutschen Schrifttum und letztlich auch in den FAQ der EU-Kommission wird aber davon ausgegangen, dass diese Anforderung besteht (dazu FAQ der Kommission zum Data Act, Version 1.4, Frage Nr. 34). Dieses sollte ebenfalls klargestellt werden. So ist beispielsweise der Hersteller, der das digitale Produkt, das Produktdaten abgibt, ohne verbundenen Dienst oder sonstige Zugriffsmöglichkeiten anbietet, regelmäßig schon gar nicht in der Position Daten gemäß Art. 4 Data Act zugänglich zu machen. Er unterfällt ggf. nur Art. 3 Data Act.

Die Definition des Dateninhabers ist nach allgemeiner Meinung im deutschen Schrifttum zirkulär (sie wird teils auch als „verwirrend“ oder „unbrauchbar“ bezeichnet). Dies rührt u.a. daher, dass die Verpflichtung Daten zugänglich zu machen zuvörderst aus Art. 4 Data Act resultiert, wenn nicht andere Normen greifen, Art. 4 Data Act aber wiederum den Dateninhaber adressiert. Der DAV regt an, dieses zirkuläre Element dringend zu beseitigen, es sei denn, dass es so gemeint ist, dass es einer vertraglichen (oder anderweitigen gesetzlichen) Berechtigung bedarf, wie dies im Schrifttum auch teils vertreten wird. Dann wäre alternativ auch das klarer zu fassen.

Schwierigkeiten bereitet auch, dass es Fälle geben kann, bei denen es aufgrund des von der EU-Kommission vertretenen Prinzips, dass ein Nutzer kein Dateninhaber sein kann (dazu FAQ der Kommission zum Data Act, Version 1.4, Frage Nr. 34), es keinen Dateninhaber, sehr wohl aber einen Nutzer mit und einen ohne Datenzugriff geben kann. Der zweite Nutzer hat dann aber keinen Anspruch auf Zugänglichmachung der Daten. Dies betrifft etwa die Situation bei der Vermietung oder dem Leasing in der Vertragskette. Will man die Datensilos aber öffnen, wäre eigentlich hier klarzustellen, dass entweder der erste Nutzer parallel auch Dateninhaber ist, wobei dann u.a. die Regelungen unter Art. 4 Abs. 12 und 13 Data Act anzupassen wären, um nicht Nutzern den Umgang mit den eigenen Daten zu verbieten, oder aber die Ansprüche nach Art. 4 und 5 müssten auch gegen Nutzer gerichtet werden, wenn es keinen Dateninhaber gibt.

Hinzuweisen ist noch, dass im deutschen Schrifttum teils auch ein relativer Begriff des Dateninhabers vertreten wird. Auch dieser Ansatz könnte das Problem lösen, müsste dann aber klargestellt werden. Mit Blick auf Erwägungsgrund 22 Data Act („Auftragsverarbeiter im Sinne von Artikel 4 Nummer 8 der Verordnung (EU) 2016/679 gelten nicht als Dateninhaber.“) ist überdies unklar, in welchen Situationen von einer die Dateninhaberschaft

des Auftragnehmers ausschließenden Auftragsdatenverarbeitung auszugehen ist, insbesondere ob das in Erwägungsgrund 22 Data Act niedergelegte nur für die Auftragsverarbeitung i.S.v. Art. 28 DSGVO gilt, also bei personenbezogenen Daten. Eine differenzierte Behandlung je nach Personenbezug der Daten dürfte schwer zu begründen und überdies in der Praxis auch schwer bzw. praktisch nicht zu handhaben sein.

b) Begriff der Weiterverwendung

Wir regen an, die Definition der „Weiterverwendung“, wie sie in Art. 2 Nr. 52 des neuen Data Act aufgenommen werden soll, klarer zu begrenzen: Der Begriff der Weiterverwendung wird dort für die Regelungen definiert, die aus dem Data Governance Act in den Data Act überführt werden. Für diesen Bereich ist die Definition auch stimmig. Wenn indes allgemein „Weiterverwendung“ für den gesamten Data Act derart begrenzend definiert wird, wie jetzt vorgeschlagen, geht dies an der allgemeinen Praxis vorbei, da etwa auch die über einen Datenzugang erhaltenen Daten „weiterverwendet“ werden, obwohl es sich dabei nicht um – wie in der Legaldefinition des neuen Art. 2 Nr. 52 Data Act vorgesehen – Dokumente im Besitz öffentlicher Stellen oder öffentlicher Unternehmen handelt. Die Definition sollte daher spezifisch bezogen werden auf die Regelungen der Verwendung von Daten öffentlicher Stellen, etwa indem sie wie folgt gefasst wird:

„52. ‚Weiterverwendung nach Kapitel VIIc‘ die Nutzung …“

Entsprechend wäre dann auch die Begriffsbestimmung in Art. 2 Nr. 57 anzupassen:

„57. ‚Weiterverwender nach Kapitel VIIc‘ eine natürliche oder juristische Person …“

Zudem sollten die Begriffe nicht auf die Weiterverwendung von Dokumenten beschränkt sein, da Art. 32i des Verordnungsvorschlags – zutreffend – auch die Weiterverwendung von Daten umfasst.

3. Verpflichtungen der Hersteller zur data accessibility by design und Verhältnis zum Dateninhaber

Art. 3 Abs. 1 Data Act verpflichtet Hersteller, vernetzte Produkte so zu konzipieren und herzustellen sowie verbundene Dienste so zu konzipieren und zu erbringen, dass die entsprechenden Produkt- und verbundenen Dienstdaten „direkt zugänglich sind“. Diese

Produktdesignpflicht, den Datenzugang qua Produktgestaltung zu ermöglichen, ist ein wesentlicher Anker der Datenzugangsvorschriften in Kapitel II Data Act. Indes fehlt es an einer klaren Normierung der Rechtsfolgen und Durchsetzbarkeit sowie Verzahnung mit den Pflichten des Dateninhabers, die Daten bereitzustellen, womöglich auch im Fall einer data accessibility by design noch an den Datenempfänger. Dies sollte im Zuge der Novellierung klargestellt werden.

Hinzu kommt, dass unklar ist, was mit dem Begriff des „direkten Zugangs“ gemeint ist und in welchem Verhältnis Dateninhaber und Hersteller zueinanderstehen. Wir verweisen insofern auf die DAV-Stellungnahme Nr. 40/2022, die in diesen Punkten nach wie vor relevant ist.

Überdies geht die Kommission für die derzeitige Fassung des Art. 3 Abs. 1 Data Act davon aus, dass der Hersteller ein gewisses Ermessen hat, die Daten zugänglich zu machen oder auch nicht; sie stützt sich dazu auf den Wortlaut „where relevant and technically feasible“ (dazu FAQ der Kommission zum Data Act, Version 1.4, Frage Nr. 22), übersieht aber, dass der gleiche Wortlaut in Art. 4 Abs. 1 Data Act eindeutig eine Pflicht begründen soll. Auch spricht die Gesetzeshistorie und der Zweck des Data Act, Datenzugänge zu schaffen, gegen diese Auslegung. Die Frage des Ermessens ist daher von Gesetzgeber zu klären und ggf. nachzubessern.

4. Entwicklung zum Schutz von Geschäftsgeheimnissen insb. nach Art. 4 Abs. 8, Art. 5 Abs. 11 Data Act-Entwurf

Sollte eine solche Nachbesserung nicht erfolgen, sollten auch den Herstellern ähnliche Rechte (Einreden) gewährt werden, wie sie nach Art. 4 Abs. 8, Art. 5 Abs. 11 Data Act-Entwurf vorgesehen sind bzw. in Fällen, die einen Geheimnisschutz erfordern, die Möglichkeit eröffnet werden, sich gegen den Datenzugang zu sichern und diesen nur unter den Bedingungen der Art. 4 Abs. 8, Art. 5 Abs. 11 Data Act-Entwurf zu gewähren.

Die klarstellende Ergänzung (“it is highly likely … or that the disclosure of trade secrets to the third party poses a high risk of unlawful acquisition, use, or disclosure to third country entities, or entities established in the Union under the direct or indirect control of such entities, which are subject to jurisdictions offering weaker or non-equivalent protection compared to that under Union law”) wird begrüßt. In der Tat ist das Risiko groß, dass Geschäftsgeheimnisse und Know-how der europäischen Unternehmen ungewollt abfließen und in konkurrierende Produkte eingehen. Insoweit ist sogar zu fragen, ob das Recht zur

Verweigerung nicht explizit auf die Fälle zu erstrecken ist, aus denen sich aus den Daten als abgeleitete Information dann leichter im Wege des Reverse Engineering auf besonders wertvolles technisches Know-how schließen lässt. Vorstellbar wäre etwa folgende Ergänzung:

> *"It is highly likely…, or where as a matter of the data to be made accessible underlying core know-how of a product or service apart from such data is indirectly disclosed or can be more easily accessed by reverse engineering."*

5. Regelungen zur Datenverwendung in Verträgen

Art. 13 Data Act reguliert missbräuchliche Vertragsklauseln in Bezug auf den Datenzugang und die Datennutzung zwischen Unternehmen. Die Absicherung fairer Vertragsklauseln ist ein berechtigtes und zu begrüßendes Anliegen. Der DAV regt aber an, die Regelungen im Detail zu überarbeiten, da sie derzeit punktuell zu übermäßigen, nicht mehr gerechtfertigten Einschränkungen führen.

Wir regen an, folgende Änderungen in Art. 13 Data Act vorzusehen:

Die Begriffe in Art. 13 Abs. 4 und 5 sollten durch eindeutige Legaldefinitionen geklärt und in ihrer Anwendung vereinheitlicht werden:

- „Nichterfüllung" umfasst alle Fälle der Nichterbringung der vertraglich geschuldeten Leistung
- „Verletzung von Vertragspflichten" bezeichnet die mangelhafte oder nicht vertragsgemäße Erbringung der Leistung
- „Haftung" bezieht sich auf Schadensersatzansprüche
- „Rechtsbehelfe" umfassen alle vertraglichen und gesetzlichen Rechtsmittel einschließlich Rücktritt, Minderung und Schadensersatz

Der Haftungsausschluss für die leicht fahrlässige Verletzung von Vertragspflichten sollte umfassend zulässig sein, was insbesondere unter Art. 13 Abs. 4 lit. b, Abs. 5 lit. a Data Act nicht klar ist. Auch dort sollte eine Begrenzung auf vorsätzliche oder grob fahrlässige Handlungen erfolgen, wie in Art. 13 Abs. 4 lit. a Data Act.

Ergänzung in den Erwägungsgründen, dass bei Online-Verträgen mit „Akzeptieren-Button“ das Verhandlungserfordernis als erfüllt gilt, wenn der Nutzer vor Vertragsschluss explizit auf die Möglichkeit zur Kontaktaufnahme für Verhandlungen hingewiesen wurde.

6. Änderungen an Kapitel V – Bereitstellung von Daten für öffentliche Stellen

Der Verordnungsvorschlag plant eine deutliche Einschränkung der Regelungen zur Herausgabepflicht von Daten an öffentliche Stellen durch Streichung der Art. 14, 15 Data Act in Kapitel V und Aufnahme eines neuen Art. 15a Data Act, der die Datenherausgabepflicht auf Situationen des öffentlichen Notstands begrenzt. Dies begrüßt der DAV.

7. Anpassungen im Kapitel VI zum Wechsel von Datenverarbeitungsdiensten

Die vorgeschlagenen Änderungen in Kapitel VI begrüßt der DAV ebenfalls, insbesondere die Ausnahmen vom Anwendungsbereich für an die spezifischen Kundenbedürfnisse angepasste Dienste und die Befugnis für Sanktionen bei vorzeitiger Kündigung. Die Anpassungen sollten allerdings noch weitergehen, um die Angemessenheit und Verhältnismäßigkeit des mit diesen Regelungen verbundenen Eingriffs in die Privatautonomie besser zu wahren.

Der Maßstab, ab dem an Kundenbedürfnisse angepasste Dienste vom Anwendungsbereich ausgenommen sind, müsste klar definiert werden. Derzeit wird dies über die Formulierung „die meisten Merkmale und Funktionen“ versucht zu erreichen. Hierbei wird es in der Praxis regelmäßig zu erheblichen Abgrenzungsproblemen und Umgehungsrisiken kommen, da etwa eine rein zahlenmäßige Bewertung über die Anpassung unzähliger unwesentlicher Funktionen erreicht werden kann, während maßgeblich die qualitative Wertung sein sollte, ob es ein standardisiertes Produkt oder ein tatsächlich individualisiertes ist. Dies kann beispielsweise an dem Anteil der Vergütung festgemacht werden, der auf die Anpassungen und Individualisierungen entfällt und nach sachgerechten Kriterien aufgeschlüsselt werden muss.

Die Befugnis nach Art. 31 Abs. 1b des Verordnungsvorschlags, verhältnismäßige Sanktionen bei vorzeitiger Kündigung aufzunehmen, entspricht dem Marktbedürfnis nach flexibleren Vertragslaufzeiten als dies unter den aktuell geltenden Regelungen möglich ist. Auch Kunden haben regelmäßig das Bedürfnis, längerfristige Verträge als über 30 Tage

plus 2 Monate zu schließen, wie dies aktuell vorgesehen ist bei Wechselkündigungen. Die Regelung reicht aber nicht aus, um ein ausgewogenes Verhältnis zwischen Vertragsfreiheit und Marktöffnung herzustellen. Es sollte eindeutig erlaubt werden, verschiedene Optionen mit unterschiedlicher Laufzeit anzubieten, solange die Konditionen zwischen den verschiedenen Optionen angemessen und diskriminierungsfrei gebildet werden. Unternehmenskunden ist es zuzumuten, vorab zwischen diesen zu wählen, wenn echte und faire Alternativen existieren. Wählen Kunden einen länger laufenden Vertrag, müssen sie sich daran auch festhalten lassen.

Leider bleibt auch ungeklärt, welche vertragsrechtlichen Folgen ein Verstoß des Anbieters gegen die Pflichten aus Art. 25 Data Act hat. Werden die nach dem Data Act gebotenen, aber im Vertrag nicht enthalten Vereinbarungen im Wege der ergänzenden Vertragsauslegung in den Vertrag hineininterpretiert? Hat der Kunde einen Anspruch auf Aufnahme ergänzender Vertragsregelungen? Oder bleibt der Verstoß gegen Art. 25 Data Act ohne vertragsrechtliche Folgen. Auch hier wäre eine Klarstellung nötig.

8. Klarere Regelungen zur Absicherung internationaler Datentransfers

Die vorgeschlagenen Änderungen im Bereich internationaler Datentransfers stellen eine Vereinfachung und Klarstellung dar. Art. 32 Abs. 1 sollte aber im Wortlaut stärker an Art. 32 DSGVO ausgerichtet werden, um Unklarheiten bei Auslegung und Anwendung zu vermeiden:

> *„… ergreifen unbeschadet der Absätze 2 und 3 unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, um den staatlichen Zugang zu in der Union gespeicherten oder in Drittländer übermittelte nicht-personenbezogenen Daten durch Einrichtungen aus Drittländern zu verhindern, wenn ein solcher Zugang im Widerspruch zum Unionsrecht oder zum nationalen Recht eines EU-Mitgliedstaats stünde.“*

Der DAV schlägt zudem vor, dass die EU-Kommission zur Gleichwertigkeit völkerrechtlicher Übereinkünfte oder entsprechender Vorgaben Durchführungsrechtsakte vergleichbar den Angemessenheitsbeschlüssen nach Art. 45 DSGVO erlassen und so die Bewertung für die einzelnen Einrichtungen erleichtern kann.

9. Konsolidierung datenrechtlicher Regelungen im Data Act

Der DAV begrüßt die Konsolidierung der datenrechtlichen Regelungen im Data Act ausdrücklich. Die Überarbeitung der Regelungen des Data Governance Act gehen indes nicht weit genug, um seine praktische Relevanz zu stärken und das Ziel erreichen zu können, dass Datenvermittlungsdienste vermehrt angeboten und datenaltruistische Organisationen registriert werden. Die Streichung der Regelungen zum Europäischen Einwilligungsformular sollte rückgängig gemacht und ein solches entwickelt werden, da dieses zu einer erheblich gesteigerten Rechtssicherheit für datenaltruistische Organisationen führen könnte, die aufgrund ihrer Organisation über nur begrenzte Ressourcen für eine Rechtsberatung und anderweitige Risikoreduktion verfügen.

Verteiler

Europa

Europäische Kommission
- Generaldirektion Kommunikationsnetze, Inhalte und Technologien (DG CNECT)
- Generaldirektion Justiz und Verbraucher (DG JUST)

Europäisches Parlament
- Rechtsausschuss (JURI)
- Ausschuss für Binnenmarkt und Verbraucherschutz (IMCO)
- Ausschuss für Bürgerliche Freiheiten, Justiz und Inneres (LIBE)

Rat der Europäischen Union
Ständige Vertretung der Bundesrepublik Deutschland bei der EU
Justizreferenten der Landesvertretungen bei der EU
Rat der Europäischen Anwaltschaften (CCBE)
Bundesverband der Freien Berufe (BFB) – Büro Brüssel
Deutsche Industrie- und Handelskammer (DIHK) – Büro Brüssel
Bundesverband der deutschen Industrie e.V. (BDI) – Büro Brüssel

Deutschland

Bundesministerium des Innern
Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium für Wirtschaft und Energie
Bundesministerium für Digitales und Staatsmodernisierung

Ausschuss für Inneres im Deutschen Bundestag
Ausschuss für Recht und Verbraucherschutz im Deutschen Bundestag
Ausschuss für Wirtschaft und Energie im Deutschen Bundestag
Ausschuss Digitale Agenda im Deutschen Bundestag
Fraktionen im Deutschen Bundestag

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Die Justizministerien der Länder
Die Datenschutzbeauftragten der Bundesländer

Europäische Kommission - Vertretung in Deutschland
Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe e.V.
Deutscher Richterbund, Bund der Richterinnen und Richter, Staatsanwältinnen und
Bund Deutscher Verwaltungsrichter und Verwaltungsrichterinnen
Staatsanwälte e.V. (DRB)
Deutscher Notarverein
Deutscher Steuerberaterverband e.V. Berlin
Bundesverband der Deutschen Industrie e.V.
Arbeitsgemeinschaft berufsständischer Versorgungseinrichtungen e.V.
Deutscher EDV-Gerichtstag e.V.
GRUR - Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht e.V.
Bitkom e. V.
Deutsche Gesellschaft für Recht und Informatik e.V. (DGRI)
ver.di - Vereinte Dienstleistungsgewerkschaft

Gewerkschaft der Polizei
Deutsche Polizeigewerkschaft im DBB (DPolG)

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Presse

Frankfurter Allgemeine Zeitung GmbH
Süddeutsche Zeitung GmbH
Redaktion NJW
JUVE Verlag für juristische Information GmbH
Redaktion Legal Tribune Online / LTO
Redaktion Anwaltsblatt
juris GmbH
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz ZD
Redaktion heise online
DER SPIEGEL GmbH & Co. KG
Computer und Recht