

Prof. Dr. Jürgen Kühling, LL.M., Prof. Dr. Mario Martini*

Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?

Die Datenschutz-Grundverordnung wird das Gesicht des Datenschutzrechts nachhaltig verändern. Es sind weniger die materiell-rechtlichen Neuerungen, mit denen sie Akzente setzt. Vor allem das Marktortprinzip und die institutionellen Modifikationen in der Struktur der europäischen Datenschutzaufsicht sorgen für eine datenschutzrechtliche Frischzellenkur, deren Ausstrahlungswirkung weit über die Grenzen der Union hinausreicht. Kombiniert mit dem Wechsel zur Handlungsform der Verordnung geht damit eine im Verhältnis zum bisherigen Richtlinienregime deutlich sichtbare Harmonisierung einher. In der Sache ist die DSGVO allerdings in Teilen eher eine Richtlinie im Verordnungsgewand: Mit rund vier Dutzend Öffnungsklauseln eröffnet sie den Mitgliedstaaten Spielraum für eigene normative Schattierungen. Der Beitrag wirft einen Blick darauf, welche Änderungen die DSGVO im deutschen Datenschutzrecht nach sich zieht und wie weit die nationalen Spielräume reichen.

The General Data Protection Regulation (GDPR) will significantly change privacy law in Germany and the EU. While the regulation is setting new standards, it is doing so through changes in applicable law and institutional modifications of the structure of European supervisory authorities rather than through the introduction of clauses in material law. In combination with the switch from a directive to a regulation, a new level of harmonization is made possible that goes beyond the current harmonization by the directive. However, the GDPR turns out to be a directive disguised as a regulation: In nearly 50 opening clauses, the regulation allows for national legislative action by the Member States. This article explores changes in German privacy law as a consequence of the GDPR and where the regulation gives legislative leeway.

I. Einführung

„Wer’s Recht hat und Geduld, für den kommt auch die Zeit“, heißt es in Goethes Faust.¹ Für die Datenschutz-Grundverordnung (im Folgenden: DSGVO) ist die Zeit nun gekommen: Nach langen Verhandlungen hat das Europäische Parlament sie am 14.4.2016 verabschiedet.² Am 4.5.2016 wurde sie im Amtsblatt veröffentlicht und ist 20 Tage später in Kraft getreten (Art. 99 I DSGVO). Geltung wird sie nach Art. 99 II DSGVO weitere zwei Jahre später entfalten, also

* Der Autor *Kühling* ist Inhaber des Lehrstuhls für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht u. Informationsrecht an der Universität Regensburg. Der Autor *Martini* ist Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht u. Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer sowie Leiter des Programmbereichs „Digitalisierung“ am Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer.

¹ So lässt *Goethe* den Erzbischof ausrufen, s. *Goethe*, Faust. Der Tragödie zweiter Teil, 1832, S. 296.

² Verordnung (EU) 2016/679 des Europ. Parlaments u. des Rates v. 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr u. zur Aufhebung der Richtlinie 95/46/EG, ABl.EU 2016, L 119/1.

ab dem 25.5.2018. Mit ihren 99 Artikeln bleibt sie numerisch zwar gerade noch im zweistelligen Bereich; die Anzahl der Normen hat sich gegenüber den 34 Artikeln der Datenschutz-Richtlinie (DSRL) aus dem Jahre 1995³ jedoch fast verdreifacht. Noch opulenter sind die 173 Erwägungsgründe ausgefallen, die fast zwei Fünftel des Veröffentlichungsumfangs einnehmen. Sie enthalten teils ergänzende Ausführungen zu dem eigentlichen Normtext, teilweise aber scheinen sie – insbesondere weil nicht gesondert in den Gremien beraten – nicht vollständig auf ihn abgestimmt (so etwa ErwG 121 S. 3 auf Art. 52 V DSGVO). Der textliche Umfang der einzelnen Erwägungsgründe korreliert dabei oftmals mit der politischen Brisanz, welche die Regelung in der Diskussion der europäischen Organe hatte: Je umstrittener sie im Gesetzgebungsprozess war, desto ausführlicher fällt auch der Erwägungsgrund tendenziell aus. Auf der Schlussgeraden wurde die Verordnung dann ganz offensichtlich „mit heißer Nadel gestrickt“: Manche ihrer Querverweise laufen ins Leere (zB der Verweis auf den nicht existenten „Art. 87 Absatz 2“ [gemeint ist Art. 93 II] in Art. 28 VII DSGVO). Sie enthält auch teils irritierende bzw. überraschende Regelungen, die gleichsam in letzter Minute Aufnahme in den Verordnungstext gefunden haben (siehe etwa die Öffnungsklauseln in Art. 6 II und IV sowie Art. 23 II DSGVO).

Anders als in anderen Rechtsbereichen trifft die DSGVO nicht auf ein weitgehend unbestelltes nationales Regulierungsfeld, sondern auf eine – gerade in Deutschland – hochgradig ausdifferenzierte Datenschutzlandschaft. Mit Rücksicht darauf gesteht die Verordnung, wiewohl sie mit ihrer unmittelbaren Geltung (Art. 288 II AEUV) das nationale Recht grundsätzlich vollständig verdrängt, den Mitgliedstaaten ausladende Regelungsspielräume zu, die Raum für nationale Sonderregelungen eröffnen – getreu der Demut des Kaisers vor dem Erzbischof in *Goethes Faust*: „Die Grenze sei von dir nach eigenem Maß gesteckt.“⁴ Das gilt etwa für die Datenverarbeitung im öffentlichen Interesse, insbesondere in den Kernbestimmungen des Artikels 6 II und III DSGVO. Gleichzeitig gibt die Verordnung dem nationalen Gesetzgeber teilweise explizite Regelungsaufträge mit auf den Weg – etwa bei der Ausgestaltung der Mitwirkung der nationalen Datenschutzbehörde(n) am Prozess der aufsichtsbehördlichen Zusammenarbeit (Art. 60 ff. DSGVO) oder der regulatorischen Auflösung der Konfliktlage zwischen Meinungs- und Informationsfreiheit (Art. 85 DSGVO).

Insgesamt entstehen so unterschiedliche Harmonisierungsgrade (dazu II). Diesen Aspekt der supranationalen Überformung und die Einpassung der Regelungsgehalte in das nationale Datenschutzrecht stellt der Beitrag in den Mittelpunkt seiner Betrachtung. Zugleich lädt er ein zu

³ Richtlinie 95/46/EG des Europ. Parlaments u. des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten u. zum freien Datenverkehr, ABl. 1009 L 281, 31.

⁴ *Goethe* (Fn. 1), S. 294

einer Tour d'Horizon über die wesentlichen Neuerungen der Verordnung mit einem Ausblick auf materiell-rechtliche (dazu III), prozedurale (dazu IV) und institutionelle (dazu V) Fragen.

II. Fragmentarischer Ordnungscharakter, Öffnungsklauseln und künftiges BDSG

1. Von der Grundverordnung zum „Handlungsformenhybrid“

Der Harmonisierungsansatz der Verordnung hat im Laufe des Gesetzgebungsprozesses einen nachhaltigen Wandel erfahren. Die Bezeichnung „Grundverordnung“ ist inzwischen irreführend. Die Kommission hatte diesen Begriff ursprünglich gewählt, da sie das Normenwerk als Magna Charta des europäischen Datenschutzes auf eine umfassende Harmonisierung ausrichten wollte, die in einem zweistufigen europäischen Gesetzgebungsprozess erfolgen sollte: Zentrale Bestimmungen sollten der „Grund“-Verordnung vorbehalten bleiben, während die Kommission die umfassende Konkretisierung und Ausdifferenzierung selbst vornehmen wollte. Die außerordentliche Vielzahl der Felder, in denen die Kommission sich in ihrem Entwurf die Befugnis zum Erlass delegierter Rechts- und Durchführungsrechtsakte einräumen lassen wollte,⁵ rief aus vertikaler Kompetenzverteilungsperspektive alsbald Bedenken mit Blick auf das Subsidiaritätsprinzip auf den Plan.⁵

Entscheidender für die Abkehr von dem zweistufigen Normierungskonzept dürfte jedoch die Sorge gewesen sein, dass sich die Kommission in wesentlichen Bereichen zum primären Gesetzgeber aufgeschwungen hätte, was unter horizontalen Gewaltenteilungsgesichtspunkten rechtspolitisch, aber mit Blick auf die Wesentlichkeitsvorgaben der Art. 291 und 292 AEUV auch primärrechtlich Bauchgrimmen verursacht hätte.

Die Konkretisierungsbefugnisse der Kommission sind inzwischen fast vollständig der Streichung zum Opfer gefallen. Sie beschränken sich im Wesentlichen auf die Ausgestaltung von Bildsymbolen für die Erfüllung der Informationspflicht (Art. 12 VIII DSGVO) und die (praktisch relevantere) Allgemeinverbindlicherklärung von Verhaltensregeln sowie die Festlegung technischer Standards und Verfahren für Zertifizierungsverfahren, Datenschutzsiegel und -prüfzeichen (s. Art. 40 IX, VIII, IX DSGVO).⁶

⁵ *Gola*, RDV 2013, 1 (2), weist insoweit darauf hin, dass bei nahezu jeder dritten Bestimmung des Entwurfs eine Konkretisierungsmöglichkeit vorgesehen war; eine exemplarische Aufzählung liefern *Schild/Tinnefeld*, DuD 2012, 312 (316).

⁵ BR-Drucks. 52/12 v. 30.3.2012; *Schild/Tinnefeld*, DuD 2012, 312 (314); ausführlich dazu *Nguyen*, ZeuS 2012, 277 ff.; vgl. auch *Koós*, ZD 2014, 9 (11 ff.).

⁶ Die Kommission kann auch Standardvertragsklauseln zur Konkretisierung der Zusammenarbeit zw. dem Auftragsgeber u. dem Verantwortlichen festlegen (Art. 28 VII DSGVO). Ferner sieht Art. 45 DSGVO Durchführungsrechtsakte im Rahmen der Datenübermittlung an Drittländer auf der Grundlage eines Angemessenheitsbeschlusses

Geblichen ist jedoch die begriffliche Offenheit (und Unbestimmtheit) zahlreicher Vorschriften. Im Gefolge dessen wächst den Datenschutzaufsichtsbehörden und der Rechtsprechung – also ultimativ dem *EuGH* – eine wichtige Rolle bei der inhaltlichen Konkretisierung der DSGVO zu.

Zugleich behalten die Mitgliedstaaten in vielen Rechtsbereichen das Heft der Regulierung in der Hand: Eine nähere Befassung mit dem Text und seinen zahlreichen Öffnungsklauseln offenbart, dass die Grundverordnung faktisch ein atypischer Hybrid aus Verordnung und Richtlinie ist.

2. Umfangreiche Öffnungsklauseln

Vor allem im Bereich der im öffentlichen Interesse (nicht notwendig aber durch öffentliche Stellen⁷) erfolgenden Datenverarbeitung greifen umfängliche Öffnungsklauseln.⁸ Sie sind zu einem erheblichen Teil das Produkt der Änderungen, welche die Trilog-Verhandlungen nach Art. 294 X ff. AEUV mit sich gebracht haben. In 45 Bestimmungen des verfügenden Teils der DSGVO, also fast der Hälfte der Vorschriften, finden sie sich – und dies teils mit Wirkung für eine Vielzahl weiterer Vorschriften (so etwa in Art. 23 DSGVO, der sich auf sämtliche Betroffenenrechte bezieht). Die Klauseln lassen sich in verschiedener Hinsicht klassifizieren:

- *Allgemeine* Öffnungsklauseln – wie Art. 23 DSGVO – eröffnen eine ganze Reihe von Abweichungsmöglichkeiten, ohne auf ein spezifisches Themengebiet beschränkt zu sein; *spezifische* Öffnungsklauseln ermöglichen demgegenüber sektorale Teilregelungen in einzelnen Regelungsfeldern – so etwa Art. 8 I DSGVO, der nur den sehr beschränkten Bereich der Einwilligung von Personen zwischen 13 und 16 Jahren bei der Nutzung von Diensten der Informationsgesellschaft betrifft. Einzelne Öffnungsklauseln beziehen sich zwar nur auf *eine Norm*, entfalten aber dennoch eine ganz erhebliche Breitenwirkung, wie insbesondere die Öffnungsklauseln im allgemeinen Zulässigkeitstatbestand des Art. 6 II, III bzw. IV DSGVO.
- In den meisten Fällen weisen die Öffnungsklauseln dem nationalen Normgeber *fakultative* Handlungsspielräume zu – vielfach, insbesondere im institutionellen Bereich, aber auch *obligatorische* Handlungsaufträge, denen die Mitgliedstaaten nachkommen müssen, um dem Inhalt der Verordnung Leben einzuhauchen. Die *fakultativ* eingeräumten Handlungsmöglichkeiten

vor – ebenso Art. 47 III DSGVO für verbindliche interne Datenschutzvorschriften. Im institutionellen Bereich gesellt sich die Konkretisierungskompetenz im Bereich der Amtshilfe beim Informationsaustausch zwischen den Behörden hinzu, Art. 61 IX und Art. 67 DSGVO.

⁷ Die das dt. Recht durchziehende Differenzierung zwischen öff. und nicht-öff. Stellen, die schon in der DSRL nicht angelegt war, findet sich in der DSGVO ebenso wenig wieder.

⁸ Dazu ausführlich *Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl/Wenzel*, Die DSGVO und das nat. DatenschutzR, 2016 (in Vorbereitung); dazu jetzt auch *Bennecke/Wagner*, DVBl. 2016, 600.

lassen sich in drei Kategorien einteilen: (i) die Konkretisierung, das heißt die nähere Bestimmung der jeweiligen DSGVO-Regelung durch nationales Recht, (ii) die Ergänzung, also eine Vervollständigung der DSGVO-Regelungen durch nationales Recht, und (iii) die Modifikation, das heißt die Möglichkeit, durch nationales Recht von dem Regelungsinhalt der DSGVO-Norm abzuweichen. Die Kategorien schließen sich dabei nicht gegenseitig aus: Öffnungsklauseln können den Mitgliedstaaten auch alle drei Handlungsmöglichkeiten gleichzeitig einräumen.

In zentralen Regelungsbereichen ist ein Handeln des nationalen Gesetzgebers letztlich unumgänglich. Denn in weiten Teilen ist die DSGVO für das komplexe und grundrechtssensible Datenschutzregime des digitalen Zeitalters als solche nicht hinreichend vollzugsfähig. Das gilt insbesondere für die Verarbeitung von Daten im öffentlichen Interesse bzw. in Ausübung öffentlicher Gewalt nach Art. 6 I UAbs. 1 Buchst. e und gegebenenfalls für Fälle des Buchst. c DSGVO. Für sie setzt Art. 6 III DSGVO ausdrücklich eine Rechtsgrundlage im mitgliedstaatlichen Recht (oder im Unionsrecht) voraus.⁹

3. Konsequenzen für ein BDSG-Nachfolgegesetz

Entgegen manch ursprünglicher Erwartung verbleibt dem nationalen Gesetzgeber ein erheblicher Handlungsspielraum; er sieht sich aber auch einem spürbaren Handlungsdruck ausgesetzt – insbesondere in zeitlicher Hinsicht. Bis zum Mai 2018 hat Deutschland Zeit, den Rahmen auszufüllen. Anders als bei Richtlinien kann es diesen Zeitpunkt nicht geflissentlich verstreichen lassen, ohne sich selbst substanziell zu schaden. Sonst hinterlässt es seinen Bürgern und Unternehmen einen vollzugsunfähigen Regelungstorso; so wäre etwa im institutionellen Bereich mit seinen obligatorischen Öffnungsklauseln keine Beteiligung Deutschlands an dem Abstimmungs- und Kohärenzverfahren der Aufsichtsbehörden, das die Art. 60 ff. DSGVO etablieren, möglich. Auch im Bereich fakultativer Ausgestaltungsmöglichkeiten entstünde eine nicht hinnehmbare Rechtsunsicherheit. Ob die allgemeinen Bestimmungen im BDSG und den Landesdatenschutzgesetzen bzw. in den bereichsspezifischen Vorschriften, etwa im TMG, überhaupt noch neben der DSGVO anwendbar wären, bliebe unklar.

Auf Bundesebene verschärft sich der Zeitdruck dadurch, dass die Legislaturperiode nur noch bis zum September 2017 währt und bis dato unfertige Entwürfe dem Diskontinuitätsgrundsatz zum Opfer fallen. Der zwingende Handlungsbedarf auf Bundesebene wird daher faktisch bis spätestens Mitte 2017 abgearbeitet und ein BDSG-Nachfolgegesetz beschlossen sein müssen.

⁹ Von diesen Regelungsmöglichkeiten umfänglich Gebrauch zu machen, ist für die Mitgliedstaaten auch insoweit bes. attraktiv, als dann die aufsichtsrechtlichen Abstimmungsbedürfnisse des Kohärenzverfahrens u. des Verfahrens der Zusammenarbeit entfallen (Art. 55 II 2 DSGVO); siehe hierzu unten V. 2.

Ein koordiniertes Zusammenwirken von Bund und Ländern ist dabei noch ratsamer als sonst. Andernfalls könnte der skurrile Effekt eintreten, dass der mit dem Ziel einer vertieften europaweiten Harmonisierung erfolgte Wechsel der Handlungsform von einer Richtlinie zu einer Verordnung die Regelungsheterogenität im deutschen Föderalstaat steigert, statt sie zu reduzieren. Dieses Risiko ist Teil eines allgemeinen regulatorischen Dilemmas, mit dem sich der nationale Gesetzgeber bei der Ausschöpfung seines Regelungsspielraums konfrontiert sieht: Je stärker er von der ihm eingeräumten Regelungskompetenz Gebrauch macht, umso eher kann er das bisherige nationale Datenschutzniveau aufrechterhalten. In gleichem Maße konterkariert er dann aber die eigene grundlegende politische Zielsetzung, ein unionsweit einheitliches Datenschutzregime hervorzubringen.

III. Zaghafte Evolution statt Revolution im materiellen Recht

Inhaltliche konzeptionelle Umwälzungen sucht man in der DSGVO weitgehend – auf allen Stufen ihres Entstehungsprozesses – vergebens. Noch auf der Zielgeraden wurden umstrittene Harmonisierungsvorgaben deutlich zurückgestutzt. Insbesondere die in Deutschland intensiv geführte Debatte, vom Verbotsprinzip abzurücken, hat in den Textentwürfen der EU-Organe keinen Widerhall gefunden.¹⁰ Auch die Erlaubnistatbestände des Art. 6 DSGVO entsprechen überwiegend denen der DSRL, legen diese jedoch für den wichtigen Bereich der nicht-öffentlichen Stellen grundsätzlich in die ausschließliche Regelungsbefugnis der Union. In besonders sensiblen Bereichen, wie dem Gesundheits- und vor allem dem Arbeitnehmerdatenschutz, hat die Verordnung ihren Harmonisierungsanspruch weitgehend aufgegeben: Die Vorschrift zur Datenverarbeitung im Beschäftigtenkontext in Art. 88 DSGVO etabliert kaum relevante Vorgaben für das nationale Recht¹¹ – die Norm zum Gesundheitsdatenschutz wurde gleich ganz gestrichen. Neuerungen wie die Figur eines gemeinsam Verantwortlichen in Art. 26 DSGVO fallen dagegen eher bescheiden aus.

1. Einführung des Marktortprinzips

Die wohl gewichtigste materielle Änderung zieht die Einführung des Marktortprinzips nach sich. In seinem Google-Urteil¹² hatte der *EuGH* – auf der Grundlage einer extensiven Interpretation der Richtlinie – die nun explizit in Art. 3 II Buchst. a DSGVO vorgesehene Regelung

¹⁰ Treffend die Zurückweisung entspr. Ansinnen bei *Buchner*, DuD 2016, 155 (157 f.), der zugleich die Fehlverständnisse der Befürworter eines Abrückens v. Verbotsprinzip aufzeigt.

¹¹ S. zu den gleichwohl bestehenden Auswirkungen der DSGVO *Sörup/Marquardt*, ArbRAktuell 2016, 103; *Wybitul/Pöppers*, RDV 2016, 10.

¹² *EuGH*, ECLI:EU:C:2014:317 = EuZW 2014, 541 (Rs. C-131/12); dazu etwa *Kühling*, EuZW 2014, 527.

allerdings bereits teilweise „vorweggenommen“. ¹³ Eine Niederlassung des Verantwortlichen in der EU ist nunmehr zwar der primäre, aber nicht mehr der ausschließliche Anknüpfungspunkt, um den Anwendungsbereich der Verordnung zu eröffnen. Vielmehr findet sie nach Art. 3 II DSGVO auch auf außerhalb der EU niedergelassene Verantwortliche Anwendung, wenn diese Daten verarbeiten, um entweder „Personen in der Union Waren oder Dienstleistungen anzubieten“ (Buchst. a) oder das Verhalten Betroffener zu beobachten, also insbesondere ein Profiling zu betreiben (Buchst. b).

Das gilt aus gutem Grund auch unabhängig davon, ob der Nutzer für die Dienstleistung ein Entgelt zahlt. ¹⁴ Denn ein (monetäres) Entgelt entrichten die Nutzer zahlreicher Internetdienste von Suchmaschinenbetreibern à la Google oder sozialen Netzwerken wie Facebook typischerweise nicht. Der Kunde „zahlt“ in derartigen sog. „Two-sided-markets“ ¹⁵ vielmehr mit seiner Aufmerksamkeit gegenüber Werbung und/oder mit seinen Daten. Um dem Marktortprinzip auch praktisch zur Geltung zu verhelfen, legt die DSGVO Verantwortlichen und Auftragsverarbeitern, die in der Union keine Niederlassung haben, auf, einen Vertreter zu benennen (Art. 27 DSGVO).

2. „Recht auf Vergessenwerden“ und „Recht auf Datenportabilität“

Eine zunächst völlig neue materiell-rechtliche Figur schien der jetzige Art. 17 DSGVO in die datenschutzrechtliche Normenfamilie einzubringen: das „Recht auf Vergessenwerden“. Bei diesem scheinbaren Titanen handelt es sich bei näherer Betrachtung aber um einen „Scheinriesen“. Er entpuppt sich im Wesentlichen als „normale“ Löschverpflichtung, wie sie (bekräftigt durch das Google-Urteil des *EuGH*) auch bereits in der DSRL angelegt war.

Disruptiver ist da schon das Recht auf Datenportabilität nach Art. 20 DSGVO. Bei ihm handelt es sich allerdings weniger um eine Datenschutzbestimmung im eigentlichen Sinne denn um eine Verbraucherschutz- bzw. Marktregulierungsvorschrift: Verantwortliche Stellen müssen den Betroffenen künftig das Recht einräumen, die ihnen anvertrauten personenbezogenen Daten auf Wunsch „in einem strukturierten, gängigen und maschinenlesbaren Format“ dem Antragsteller oder einem Dritten zu übermitteln. Die Regelung überträgt damit ein aus der Telekommunikations- und Infrastrukturregulierung bekanntes und dort bewährtes Konzept der

¹³ S. zum Vgl. des § 1 V BDSG mit der Regelung der DSGVO idF des Kommissionsentwurfs *Wieczorek*, DuD 2013, 644.

¹⁴ Dazu ausf. *Klar*, ZD 2013, 109 (113).

¹⁵ S. dazu etwa *Rochet/Tirole*, Two-Sided Markets: A Progress Report, abrufbar unter http://idei.fr/doc/wp/2005/2sided_markets.pdf (Datum des letzten Aufrufs: 18.5.2016), mwN.

Markttöffnung in das Datenschutzrecht. Das soll „Lock-in“-Effekte verringern, die durch umfangreiche personenbezogene Datenverknüpfungen bei einem Anbieter entstehen, und dadurch das Selbstbestimmungsrecht des Betroffenen über „seine Daten“ stärken sowie einen Wechsel zu anderen Diensteanbietern erleichtern. Der Normgeber verbindet damit die Hoffnung auf einen Wettbewerb um datenschutzfreundliche Grundeinstellungen: Er soll solche Big-Data-Kollektoren, welche die informationelle Selbstbestimmung ihrer Nutzer mit Füßen treten, einer Abstimmung mit den Füßen aussetzen. Ob dies allerdings einen Exodus aus datenschutzfeindlichen Netzwerken wie Facebook auslöst, ist mit Blick auf deren Marktmacht und das allenthalben zu beobachtende Auseinanderklaffen zwischen abstrakter Wertschätzung der Nutzer für Datenschutz und ihrem konkret an den Tag gelegten Verhalten („Privacy Paradox“¹⁶) alles andere als ausgemacht. In der Anwendungspraxis wird die Umsetzung des Rechts auf Datenportabilität auch noch eine Fülle spannender Fragen zur richtigen Zuordnung personenbezogener Daten aufwerfen. Denn Daten – zumal in sozialen Netzwerken – betreffen typischerweise mehr als eine Person. Lassen sich die Datenarkaden nicht ohne Reibungsverluste automatisiert in die Architektur eines anderen Anbieters eingliedern, entpuppt sich die Vorschrift („gängig und maschinenlesbar“) als normatives Luftschloss.

3. Einwilligung

Zahlreiche Regelungsvorschläge, welche die Kommission bzw. das Parlament als Anreicherung in das System der DSGVO implementieren wollten, haben keinen Eingang in die Endfassung gefunden. So schließt Art. 7 DSGVO nicht – wie von der Kommission vorgesehen – die Freiwilligkeit der Einwilligung in Situationen klaren Ungleichgewichts zwischen Verantwortlichem und Betroffenen weitgehend aus. Als Beispiel hatte Erwägungsgrund 34 des Kommissionsentwurfs insoweit explizit Arbeitsverhältnisse aufgeführt. Dies hätte die Möglichkeit, Einwilligungen zur Legitimation von Datenverarbeitungen im Beschäftigtenverhältnis zu erteilen, massiv eingeschränkt. Nachdem der Vorschlag jedoch keinen Niederschlag in die abschließende Fassung gefunden hat, ist weiterhin eine differenzierte Prüfung der Freiwilligkeit im Einzelfall geboten. Erwägungsgrund 43 DSGVO schließt eine Einwilligung aus, wenn „in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde“ und nennt als Beispiel, die Einwilligung gegenüber einer Behörde. Stattdessen integriert die DSGVO ein umfassendes Kopplungsverbot in ihren Normbestand (Art. 7 IV DSGVO). Es stellt die Freiwilligkeit einer Einwilligung infrage, wenn ein Anbieter

¹⁶ Dazu bspw. *Martini in Hill/Martini/Wagner, Die digitale Lebenswelt gestalten*, 2015, 9 (29 ff. mwN).

von ihr die Erbringung einer Leistung abhängig macht, ohne dass dies für die Erfüllung des Vertrages erforderlich ist (vgl. auch die noch etwas zaghaftere deutsche Regelung des § 28 III b 1 BDSG). Ausscheiden werden künftig auch so genannte Opt-out-Lösungen, bei denen die Einwilligung dadurch erfolgen soll, dass der Betroffene von einer vorkonfigurierten Abwahlmöglichkeit (etwa per Häkchen in einem Kästchen) keinen Gebrauch macht. Die expliziten Erfordernisse der Unmissverständlichkeit und Eindeutigkeit der Einwilligungserklärung (vgl. EG 32 S. 1, 2 DSGVO) verlangen grundsätzlich Opt-in-Lösungen.¹⁷

Neu sind auch ergänzende Regelungen zu den Bedingungen, unter denen Kinder in die Datenverarbeitung von Diensten der Informationsgesellschaft einwilligen können (Art. 8 DGSVO). Bis zur Vollendung des 16. Lebensjahres ist die Einwilligung der Erziehungsberechtigten erforderlich. Die Mitgliedstaaten können allerdings auch eine niedrigere Altersgrenze oberhalb des vollendeten 13. Lebensjahrs ansetzen (Art. 8 I UAbs. 2 DSGVO). Jene Vorschrift ist auch eine der wenigen, die sich materiell-rechtlich explizit mit neuartigen Phänomenen der Datenverarbeitung in der Informationsgesellschaft des 21. Jahrhunderts befasst.

4. Zweckbindung, Zweckänderung und zweckkompatible Weiterverarbeitung

Zahlreiche normative Impulse der DSGVO sind in ihren Auswirkungen gegenwärtig noch schwer abschätzbar. Das gilt insbesondere für den Zweckbindungsgrundsatz. Die Verordnung gestattet in ihrem Art. 6 IV DSGVO eine Weiterverarbeitung zu anderen Zwecken als denjenigen, zu denen die Datenerhebung erfolgte. Dafür setzt sie entweder eine Einwilligung des Betroffenen oder eine Rechtsvorschrift der Union bzw. der Mitgliedstaaten voraus, die sich als eine in einer demokratischen Gesellschaft „notwendige und verhältnismäßige Maßnahme“ zum Schutz der Gemeinschaftsgüter des Art. 23 I DSGVO darstellt.

Ob die Mitgliedstaaten von dieser Möglichkeit der Befreiung von der Zweckbindung in allen Regelungskontexten Gebrauch machen dürfen oder vielmehr nur in den Bereichen, in denen sie auch für eine Erstverarbeitung eine Regelungsbefugnis haben – also im Wesentlichen in den Fällen des Art. 6 I UAbs. 1 Buchst. c und e DSGVO – ist eine spannende, noch offene Frage. Dass sich die Mitgliedstaaten über das Instrument der zweckändernden Rechtfertigung einer Verarbeitung sonst weitergehende Regelungsbefugnisse zugestehen könnten, als ihnen Art. 6 I–III DSGVO grundsätzlich einräumen will, streitet für ein enges Verständnis der Öffnungsklausel.

¹⁷ So sieht ErwG 32 S. 2 DSGVO vor, dass die Einwilligung „etwa durch Anklicken eines Kästchens beim Besuch einer Internetseite“ vorgenommen werden könnte; s. dazu bereits *Buchner*, DuD 2016, 155 (158); *Caspar*, DuD 2013, 767 (770); ferner *Albrecht*, CR 2016, 88 (91); sehr kritisch zu den Änderungen mit dem sehr weit gehenden Fazit, die Einwilligung werde als Legitimationsgrundlage allzu sehr geschwächt *Härting*, ITRB 2016, 36 (40).

Besonders legitimierungsbedürftig sind nicht alle Weiterverarbeitungen, sondern nur solche, die mit dem ursprünglichen Zweck nicht vereinbar sind. Für die Unterscheidung zwischen kompatiblen und inkompatiblen Zweckänderungen führt die DSGVO eine Reihe von Gewichtungsparametern an (Verbindung zwischen dem ursprünglichen und dem neuen Zweck; Zusammenhang der Datenerhebung; Folgen für den Betroffenen etc., Art. 6 IV DSGVO aE), deren Ausfüllung künftig über die Reichweite der zweckkompatiblen Weiterverarbeitung entscheiden wird.¹⁸ Daraus kann sich möglicherweise eine weitere relevante materiell-rechtliche Verschiebung gegenüber dem Verständnis des bisherigen deutschen Datenschutzrechts ergeben. Dieses ist bislang tendenziell von einem engen Verständnis der Zweckbindung geprägt. Die DSGVO scheint hingegen – entsprechend dem niederländischen Modell – ein weiter gehendes Verständnis zugrunde zu legen: Erwägungsgrund 50 S. 2 macht deutlich, dass bei *zweckkompatiblen* Weiterverarbeitungen künftig „keine andere gesonderte Rechtsgrundlage erforderlich“ sein soll. Zur Rechtfertigung reicht also die ursprüngliche Rechtsgrundlage für die Datenerhebung. Am Beispiel des § 28 a BDSG wird deutlich, was das bedeutet: Die Mitteilung eines Forderungsausfalls an eine Auskunftfei kann sich – jedenfalls unter den engen Restriktionen des § 28 a BDSG – als eine zweckkompatible Weiterverarbeitung iSd Art. 6 IV DSGVO aE darstellen. Denn es besteht eine enge Verbindung zur Vertragserfüllung und damit zum ursprünglichen Verarbeitungszweck; schließlich hat der Schuldner den Vertrag ja gerade nicht erfüllt. Auch die weiteren Bewertungsparameter (Zusammenhang der Datenerhebung; Art der personenbezogenen Daten, die grundsätzlich keine besonderen Kategorien personenbezogener Daten iSd Art. 9 DSGVO darstellen; die zwar nicht unerheblichen, aber „selbst verschuldeten“ Konsequenzen etc.) können durchaus für eine Zweckkompatibilität sprechen. Die DSGVO macht dadurch sogar eine Weitergabe von Daten an Auskunftfeien in einem Umfang denkbar, der über das aktuell nach § 28 a BDSG Zulässige hinausgeht. Starre Grenzen, wie sie das BDSG normiert, lassen sich dem Art. 6 IV aE DSGVO jedenfalls schwerlich entnehmen.

IV. Nachhaltige Änderungen im flankierenden prozeduralen Bereich

Deutlich weiter als die materiellen Veränderungen reichen die konzeptionellen Innovationen im flankierenden prozeduralen Bereich, der die Durchsetzung der normativen Gebote sichern soll. So hat die DSGVO insbesondere die Bußgeldtatbestände in ihren Art. 82 ff. erheblich ausgebaut und verschärft. Dem unionalen Bußgeldrecht wachsen Zähne:¹⁹ Art. 83 V DSGVO sieht nicht nur Geldbußen von bis zu einer absoluten Höhe von 20 Mio. Euro vor, sondern auch

¹⁸ S. dazu auch *Buchner*, DuD 2016, 155 (157); sehr krit. zu diesem Regelungsansatz das Positionspapier der Datenschutzkonferenz zur DSGVO v. 26.8.2015, abgedruckt ua in DuD 2015, 722.

¹⁹ Dazu auch *Faust/Spittka/Wybitul*, ZD 2016, 120; s. auch *Gierschmann*, ZD 2016, 51 (52).

bis zu einer Höhe von 4 % des Jahresumsatzes des Unternehmens. Die Regelungsbefugnis für Geldbußen geht vollständig auf die Unionsebene über, so dass § 43 BDSG wegfällt. Eigene Gestaltungsspielräume verbleiben den Mitgliedstaaten – obgleich die Verordnung dies in der missglückten terminologischen Abgrenzung der Art. 83 und 84 DSGVO nur verklausuliert zum Ausdruck bringt – grundsätzlich lediglich für andere Sanktionsformen, insbesondere Straftatbestände und Verwaltungssanktionen (Art. 84 DSGVO) sowie Geldbußen gegen Behörden und öffentliche Stellen (Art. 83 VII DSGVO), womöglich auch für den Bereich von Verstößen gegen nationale Normen, die von Öffnungsklauseln Gebrauch machen.

Aufnahme in den prozeduralen Instrumentenkasten fand auch eine Regelung zu angemessenen technischen und organisatorischen Datenschutzmaßnahmen in Art. 25 DSGVO („*privacy by default/privacy by design*“). Ferner normiert die Verordnung eine umfassende Pflicht zur Datenschutz-Folgenabschätzung für datenintensive Dienste (Art. 35 DSGVO). Beide Nova sind Ausdruck eines (stärker als bisher) risikobasierten Regulierungsansatzes.²⁰

Kontroversen zwischen den Mitgliedstaaten hatte im Beratungsprozess die Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten in Art. 37 DSGVO ausgelöst. Das deutsche Konzept hat sich am Ende durchgesetzt und avanciert nun zu einem unionalen Exportschlager. Die DSRL hatte den Datenschutzbeauftragten bislang lediglich als freiwillige Option implementiert, die gegebenenfalls Privilegien bei den Meldepflichten von Datenverarbeitungsprozessen mit sich bringen sollte (s. Art. 18 II Spstr. 1 DSRL). In ihrem Verordnungsentwurf hatte die Kommission noch vorgeschlagen, zwar eine Bestellungsverpflichtung vorzusehen, diese aber auf Betriebe mit mehr als 250 Beschäftigten zu beschränken. Das hätte die Regelung faktisch weitgehend leerlaufen lassen, da der weit überwiegende Teil der Unternehmen – gerade in Deutschland – weniger als 250 Beschäftigte hat. Es war daher nicht weiter verwunderlich, dass sich der Vorschlag scharfer Kritik ausgesetzt sah.²¹ Die jetzige Regelung findet einen sachgerechten Kompromiss: Sie unterwirft neben Behörden und öffentlichen Stellen nur solche Verantwortliche einer Benennungspflicht, die in ihrer Kerntätigkeit Daten verarbeiten und daher einer besonderen Überwachung bedürfen. Den Mitgliedstaaten steht es gem. Art. 37 VI 1 Hs. 2 DSGVO jedoch frei, ihren Unternehmen weiter greifende Verpflichtungen aufzuerlegen; Deutschland darf (und wird im Zweifel) seine bisherige umfassende Regelung in § 4f BDSG mit einer Bestellungsverpflichtung im Falle der automatisierten Datenverarbeitung beibehalten.

²⁰ Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 14/EN WP 218.

²¹ S. etwa *Gola*, RDV 2013, 1 (5); *Hornung*, ZD 2012, 99 (104); *Jaspers*, DuD 2012, 571 (574); ausdr. gg. die Mitarbeiterzahl als einzigem Anknüpfungspunkt *Dehmel/Hullen*, ZD 2013, 147 (152).

Die DSGVO stärkt den bislang gerade im deutschen Datenschutzrecht schwach gelebten Gedanken „regulierter Selbstregulierung“. Die Art. 40 ff. DSGVO sollen dazu beitragen, dessen Gestaltungspotenziale besser zur Entfaltung zu bringen – von den Möglichkeiten europaweiter Zertifizierungsverfahren bis hin zu einem „Europäischen Datenschutzsiegel“.²²

Keine durchgreifenden Änderungen beschert die Verordnung dem System der Betroffenenrechte. Im politischen Verfahren konnte man sich hier offensichtlich nicht einigen, so dass der Harmonisierungseffekt disparat bleibt: Obwohl die Verordnung die Betroffenenrechte umfangreich selbst regelt, räumt sie den Mitgliedstaaten in Art. 23 DSGVO umfassende Abweichungsrechte ein. Eine konkretisierende Gestaltung auf nationaler Ebene macht das letztlich unausweichlich. Dem BDSG-Nachfolgegesetz und den Landesdatenschutzgesetzen wird es angelegen sein, von der Regulationsstruktur in der DSGVO auszugehen und inhaltliche Abweichungen auf das zwingend Gebotene zu beschränken. Nur so kann die wünschenswerte Harmonisierung der Betroffenenrechte auf europäischer Ebene mittelfristig Wirklichkeit werden. Gleichzeitig vermeidet dies Inländerdiskriminierungen insbesondere gegenüber in Deutschland ansässigen Unternehmen.

V. Kleine Revolution im institutionellen Design – EDA und Kohärenzverfahren

1. Unionales Koordinierungssystem

Um ihrem Anspruch gerecht zu werden, ein einheitliches Datenschutzniveau in der Union herzustellen, verzahnt die Verordnung die Datenschutzaufsicht zu einem konsistenten System unionaler Koordinierung. Davon geht ein ebenso nachhaltiger wie heilsamer Veränderungsdruck auf das bisherige fragmentierte System der Datenschutzaufsicht aus.

Der Vollzug der Verordnung liegt zwar weiterhin grundsätzlich in den Händen der „völlig unabhängigen“²³ mitgliedstaatlichen Aufsichtsbehörden.²⁴ Doch ergeben sich deren Aufgaben (Art. 57 DSGVO) und Befugnisse (Art. 58 DSGVO) nunmehr grundsätzlich unmittelbar und damit frei von mitgliedstaatlichen Spielräumen ausschließlich aus der DSGVO selbst.²⁵ Die Zeiten nationaler Datenschutz-Fürstentümer sollen auch verfahrensrechtlich der Vergangenheit

²² Dazu etwa *Martini*, NVwZ-Extra 3/2016, 1 (10 ff.).

²³ Art. 52 I DSGVO. Das Merkmal entspricht den vormaligen Vorgaben des Art. 28 I UAbs. 1 RL 95/46/EG; dazu *EuGH*, ECLI:EU:C:2010:125 = EuZW 2010, 296 (Rs. C-518/07); *EuGH*, ECLI:EU:C:2012:631 = BeckRS 2012, 82023 (Rs. C-614/10).

²⁴ Art. 4 Nr. 21, Art. 55 I DSGVO. Wie bereits in der DSRL (dort: „Kontrollstelle“) umfasst der Terminus sowohl diejenigen Behörden, die den öff. Bereich überwachen, als auch solche, die selbige Aufgabe für den privaten Bereich wahrnehmen.

²⁵ Ausnahmen stellen einzig die Art. 57 I Buchst. c DSGVO u. Art. 58 I Buchst. f, III Buchst. b, IV–VI DSGVO dar.

angehören: Die DSGVO verpflichtet die Aufsichtsbehörden zum einen zur engen Kooperation untereinander im Rahmen eines Zusammenarbeits- (Art. 60 DSGVO) und Kohärenzverfahrens (Art. 63 DSGVO). Ihrer bedarf es insbesondere dann, wenn der Verantwortliche mehrere Niederlassungen in der Union unterhält. Die Aufsichtsbehörde der Hauptniederlassung übernimmt dann die Federführung im aufsichtsbehördlichen Verfahren (Art. 56 I DSGVO) und arbeitet mit den anderen betroffenen Aufsichtsbehörden konsensorientiert zusammen (Art. 60 I DSGVO).

Um eine einheitliche Anwendung der Verordnung in der ganzen Union zu erzielen, richtet die Verordnung zum anderen ein neues Koordinierungsgremium ein, das die unter der DSRL bestehende Art. 29-Datenschutzgruppe ablöst:²⁶ den Europäischen Datenschutzausschuss (EDA). Wie schon seine Vorgängerin nimmt er nicht nur Beratungsaufgaben wahr (Art. 70 I Buchst. b und c DSGVO), stellt Leitlinien, Empfehlungen und bewährte Verfahren zusammen (Art. 70 I Buchst. f–j DSGVO) und gibt Empfehlungen ab; er erlässt vielmehr auch – ein Novum – in Streitfällen die nationalen Aufsichtsbehörden *bindende* Beschlüsse (Art. I DSGVO). Für das System der zerklüfteten europäischen Aufsichtsstrukturen ist das ein regulatorischer Durchbruch. Der Ausschuss avanciert damit zur zentralen Koordinierungsinstanz einer unionalen Datenschutzaufsicht, welche die unternehmerische Strategie regulatorischen Rosinenpickens in Gestalt geschickter Standortwahl (sog. Forum Shopping) im Idealfall unattraktiv macht.

Der EDA rekrutiert sich zwar grundsätzlich aus den nationalen Aufsichtsbehörden. Er ist aber keine mitgliedstaatliche, sondern eine unionale Einrichtung mit eigener Rechtspersönlichkeit (vgl. Art. 68 I DSGVO). Als solche nimmt er keinen mitgliedstaatlichen Vollzug des Unionsrechts wahr, sondern einen Vollzug des EU-Rechts durch eine EU-Einrichtung.

In den EDA dürfen die Mitgliedstaaten nur jeweils einen Vertreter, nämlich den Leiter einer Aufsichtsbehörde, entsenden (Art. 68 III DSGVO). Föderal strukturierten Staaten wie der Bundesrepublik Deutschland verwehrt das zwar nicht per se, an ihrem feingliedrigen System mehrerer Aufsichtsbehörden festzuhalten. Das stellen Art. 51 I („eine oder mehrere“) und III DSGVO sowie Art. 68 IV DSGVO klar. Deutschland sieht sich dann aber der brisanten Frage ausgesetzt, wer Ansprechpartner für die Kommunikation zum EDA sowie zu den Aufsichtsbehörden der anderen Mitgliedstaaten ist (dazu 2) und welche der Aufsichtsbehörden die übrigen als *primus inter pares* im EDA vertritt (Art. 51 III DSGVO und Art. 68 IV DSGVO; dazu 3).²⁷

²⁶ Vgl. auch ErwG 139 DSGVO.

²⁷ Hierbei handelt es sich um eine obligatorische Öffnungsklausel (vgl. nur Art. 51 III DSGVO). Dem nat. Gesetzgeber steht es zwar frei, mehrere unabhängige Aufsichtsbehörden zu installieren, jedoch muss er die Vertretung der mitgliedstaatlichen Aufsichtsbehörden dann regeln, wenn er von der durch Art. 51 I DSGVO eröffneten Möglichkeit Gebrauch macht.

2. Zentrale Kontaktstelle

Wenn die Akteure im unionsrechtlichen Koordinierungsmechanismus, insbesondere die nationalen Aufsichtsbehörden anderer Mitgliedstaaten, viel Zeit darauf verwenden müssten, sich durch das Dickicht innerstaatlicher Zuständigkeitsregelungen zu schlagen, litte darunter der wirksame Vollzug. Daher legt die Verordnung denjenigen Mitgliedstaaten, die mehrere Aufsichtsbehörden einrichten, auf, eine zentrale Anlaufstelle für die Kommunikation der nationalen Aufsichtsbehörden mit dem EDA sowie mit den Aufsichtsbehörden der anderen Mitgliedstaaten zu benennen (ErwG 119 DSGVO). Eine solche an die Konstruktion des „Einheitlichen Ansprechpartners“ angelehnte Kommunikationsschnittstelle soll eine reibungsfreie und zügige Kommunikation innerhalb der Union gewährleisten.

3. Vertretung der Aufsichtsbehörden im EDA

Während sich die zentrale Anlaufstelle als gleichsam gemeinsamer Briefkasten noch vergleichsweise unkompliziert in das deutsche System implementieren lässt, erschwert der föderale Staatsaufbau der Bundesrepublik die Ausgestaltung der aufsichtsbehördlichen Vertretung im EDA – sowohl im Hinblick auf die Regelungskompetenz (a) als auch hinsichtlich ihrer organisatorischen Ausgestaltung (b).

a) Verbandskompetenz für die Bestimmung des Vertreters

Wem im föderalen Bundesstaat die Verbandskompetenz für die Bestimmung eines Vertreters der deutschen Aufsichtsbehörden zukommt, ist keineswegs klar. Denkbar ist sowohl eine alleinige Kompetenz des Bundes oder der Länder als auch die Notwendigkeit eines Zusammenwirkens beider Verbände. Die DSGVO regelt die Frage der Bestimmung eines nationalen Vertreters nicht selbst, sondern überlässt ihre Beantwortung dem Recht der Mitgliedstaaten („im Einklang mit den Rechtsvorschriften dieses Mitgliedstaats“, Art. 68 IV DSGVO).

Die Vorschriften des Grundgesetzes zu den Verwaltungskompetenzen (Art. 83 ff. GG) eignen sich insoweit nur bedingt als Anknüpfungspunkt. Zwar sind die in den EDA entsandten Vertreter der Aufsichtsbehörden Teil der mitgliedstaatlichen Exekutive; sie handeln dort jedoch (auch) für eine Unionseinrichtung. Die Aufsichtsbehörden vollziehen im EDA kein nationalstaatliches Recht, sondern Unionsrecht.

Misst man eine Regelung zum aufsichtsbehördlichen Vertreter im EDA an den Art. 70 ff. GG, erschließt sich ein geteiltes Kompetenzfeld: Die materielle Kompetenz für das Datenschutzrecht fällt als Teil des Rechts der Wirtschaft (Art. 74 I Nr. 11 GG) dem Bund zu; die Aufsicht

über die eigenen öffentlichen Stellen fällt jedoch in die Regelungskompetenz der Länder. Diese ist originärer Ausdruck ihrer Staatlichkeit. Teilen sich die föderalen Ebenen die Verbandskompetenz, ist grundsätzlich ein koordiniertes Tätigwerden durch Staatsvertrag erforderlich.

Eine Gesetzgebungskompetenz des Bundes lässt sich unter Umständen aus Art. 73 I Nr. 1 Alt. 1 GG ableiten. Er gesteht dem Bund eine ausschließliche Kompetenz für die „auswärtigen Angelegenheiten“ zu. Doch repräsentiert der Vertreter im EDA grundsätzlich nicht die Bundesrepublik als solche,²⁸ sondern primär die (unabhängigen) Aufsichtsbehörden des Bundes und der Länder als Mitglieder eines EU-Gremiums. Rekurierte man auf Art. 73 I Nr. 1 Alt. 1 GG, bestünde die Gefahr, die verfassungsrechtliche Kompetenzverteilung unter Rückgriff auf einen Auslandsbezug zu überspielen.²⁹ Denkbar ist alternativ, die Regelungskompetenz aus der Zuständigkeit für die Außenvertretung herzuleiten. Diese weist die Verfassung dem Bund zu (vgl. Art. 32 I und Art. 23 I 2 GG). Ob sich auf diesem Weg entweder in direkter Anwendung oder als Annexkompetenz³⁰ eine alleinige Bundeskompetenz für die Regelung der Vertretung der deutschen Aufsichtsbehörden beim EDA begründen lässt, harrt einer Klärung.

b) Denkbare Ausgestaltungsmodelle

Als Modus der Vertretungsregelung ist ein Rotationsverfahren der Aufsichtsbehörden vorstellbar, kompetenziell schonend und auch unionsrechtlich zulässig. Will Deutschland in der Union mit wahrnehmbarer Stimme sprechen, ist ein solcher Weg jedoch nicht ratsam: Wer einmal in drei Jahren die nationalen Aufsichtsbehörden im EDA vertritt, ist in die Gruppendynamischen Prozesse sowie die Professionalisierung der Gremienstrukturen nicht ausreichend eingebunden. Empfehlenswert ist ein „Ständiger Vertreter“ nach dem Vorbild beispielsweise des Art. 23 VI 1 GG, der an das Mandat gebunden ist, das ihm die betroffenen Aufsichtsbehörden mit auf den Weg geben. Sich in dem vielstimmigen Chor der nationalen Aufsichtsbehörden auf einen Stimmführer zu einigen, wird im Zweifel nicht ohne Konflikte zwischen den – an ihren eigenen Taktstock gewöhnten – Aufsichtsbehörden vonstattengehen. In der Diskussion dominiert dem Vernehmen nach gegenwärtig die Idee einer Sprachrohrfunktion der BfDI. Die Rolle ihres Stellvertreters soll zwischen den Aufsichtsbehörden der Länder rotieren. Liegt die europäische Hauptniederlassung eines Unternehmens in einem Bundesland, wie etwa der Allianz in Bayern,

²⁸ S. Art. 51 III DSGVO („diese Behörden im Ausschuss vertritt“); die Bundesrepublik als solche wird allenfalls mittelbar vertreten.

²⁹ S. in diesem Kontext *BVerfGE* 100, 313 (368) = *NJW* 2000, 55.

³⁰ Hierfür etwa *Wolff*, Rechtsvorgaben für die Besetzung der Art. 29-Gruppe, Kurzgutachten im Auftrag der BfDI, 2015, S. 19 f.

soll ausnahmsweise die Aufsichtsbehörde des Sitzlandes im Kohärenzverfahren die EDA-Vertretung übernehmen. Das ermöglicht eine ebenso sachgerechte wie effiziente Arbeitsteilung.

VI. Fazit

Die DSGVO unterwirft das europäische und deutsche Datenschutzrecht keinem revolutionären, sondern einem evolutionären Wandel. Den einer Verordnung an sich immanenten Anspruch auf Vollharmonisierung löst sie indes nicht ein. Das gilt nicht nur für die Datenverarbeitung im öffentlichen Interesse: Ihr legt die Verordnung eher richtlinienähnliche Vorgaben mit weitreichenden Öffnungsklauseln auf, so dass Deutschland für den öffentlichen Bereich an seinen Regelungen der §§ 12 ff. BDSG in leicht modifizierter Form wird festhalten können. Auch bei zentralen prozeduralen Bestimmungen – etwa den Betroffenenrechten oder Vorschriften zu betrieblichen Datenschutzbeauftragten – wird es künftig bei einem bunten Strauß unterschiedlicher nationaler Regelungen bleiben.

Umso wichtiger wird es sein, dass der *EuGH* und die Koordinierung der Aufsichtsbehörden eine deutliche Verbesserung eines harmonisierten Normvollzugs in der Union erzielen. Davon könnte durchaus ein erheblicher Harmonisierungsschub ausgehen. Insbesondere von dem Rollenfindungsprozess des EDA wird es entscheidend abhängen, inwieweit es gelingt, diese Zielsetzung mit Leben zu füllen. Das gilt vor allem für die Vereinheitlichung der Aufsicht über die materiell-rechtlichen Standards im nicht-öffentlichen Bereich. Das Regelungsregime, dem die Datenverarbeiter insoweit unterworfen sind, liegt nunmehr fast ausschließlich in den Händen der Union. In diesem Regelungsbereich greift im Vergleich zum bisherigen Rechtsrahmen inhaltlich eine Vielzahl kleinerer Änderungen, die in der Summe durchaus zu Verschiebungen führen, auch wenn sie keine substanziellen Neuansätze beinhalten. Insoweit hat in der Tat keine grundlegende Anpassung des konzeptionellen Regimes der Richtlinie stattgefunden.³¹ Gerade die Rechtsprechung des *EuGH* im Fall Google hat jedoch zugleich gezeigt, dass auch ein 20 Jahre alter Rechtsrahmen, bei dessen Entstehen es das Internet in seiner jetzigen Form noch nicht und erst recht keine von Algorithmen gesteuerten Suchmaschinen gab, sehr wohl auf neuartige Datenverarbeitungsprozesse angewandt werden kann.

Bis zur Geltung der Verordnung am 25.5. 2018 wird der deutsche Gesetzgeber alle Hände voll damit zu tun haben, die zwingend erforderliche Begleitgesetzgebung auf den Weg zu bringen. Gleichwohl sollte er das Ziel einer Vereinfachung und Entschlackung des sektorspezifisch hoch

³¹ Krit. dazu *Härtig/Schneider*, CR 2015, 819.

ausdifferenzierten deutschen Datenschutzrechts (am sinnfälligsten im Gesundheitsdatenschutzrecht³²) nicht aus den Augen verlieren – auch wenn die Verordnung mit ihrer unmittelbaren Anwendbarkeit den Handlungsdruck insoweit reduziert hat. Das deutsche Datenschutzrecht steht im Jahre 2016 jedenfalls vor dem größten Facelifting seit seinen Anfängen in den 1970er Jahren, das – *lege artis* vorgenommen – dem Persönlichkeitsschutz auch in Zukunft gut zu Gesicht stehen kann. Wenn der Gesetzgeber seine Handlungsspielräume (insbesondere mit Blick auf das Ziel der Harmonisierung) behutsam nutzt, kann er auch anschließend noch guten Gewissens in den Spiegel schauen.

³² Dazu grdl. *Kingreen/Kühling*, JZ 2015, S. 213; *dies.*, GesundheitsdatenschutzR, 2015.