DIE DATENSCHUTZ-GRUNDVERORDNUNG UND DAS NATIONALE RECHT

ERSTE ÜBERLEGUNGEN ZUM INNERSTAATLICHEN REGELUNGSBEDARF

von

PROF. DR. IUR. JÜRGEN KÜHLING, LL.M. (BRÜSSEL)
Universität Regensburg, Lehrstuhl für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht

PROF. DR. IUR. MARIO MARTINI
Deutsche Universität für Verwaltungswissenschaften Speyer, Lehrstuhl für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht

JOHANNA HEBERLEIN, LL.M. (CHICAGO-KENT)
Mitarbeiterin am Lehrstuhl für Öffentliches Recht, Immobilienrecht, Infrastrukturrecht und Informationsrecht, Regensburg

BENJAMIN KÜHL
Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer und Rechtsreferendar am Landgericht Karlsruhe

DAVID NINK
Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer

QUIRIN WEINZIERL
Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer

MICHAEL WENZEL
Mitarbeiter am Lehrstuhl für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht, Speyer

MV WISSENSCHAFT

Zitierempfehlung:
Kühling/Martini et al., Die DSGVO und das nationale Recht, 2016

Satz: Johanna Heberlein
Abbildungen: Mario Martini, Quirin Weinzierl
Umschlag: MV-Verlag
Druck und Bindung: MV-Verlag

ISBN:

Vorwort

Die Datenschutz-Grundverordnung wälzt das europäische Datenschutzregime nachhaltig um. Sie verfolgt – gestützt auf Art. 16 Abs. 2 AEUV – das Ziel einer Vollharmonisierung. Zugleich belässt sie den Mitgliedstaaten substanzielle Regelungsspielräume. Diese auszufüllen, ist für den nationalen Gesetzgeber eine Herkulesaufgabe. Denn ihm bleibt bis zum 25. Mai 2018 nur noch ein Zeitraum von zwei Jahren, bis die Datenschutz-Grundverordnung anwendbar sein wird und damit das ausdifferenzierte nationale Datenschutzregime angepasst sein muss.[1] Auf Bundesebene müssen die zwingenden Anpassungsschritte wegen des Diskontinuitätsgrundsatzes bis zum Abschluss der Legislaturperiode bewältigt sein. Diese läuft aber schon im Herbst 2017 aus, faktisch – wahlkampfbedingt – noch früher.

Eben dieser Handlungsdruck und der in der Sache komplexe Rahmen von Regelungs- und Öffnungsklauseln in der DSGVO veranlasste das auf Bundesebene mit dem Datenschutzrecht federführend betraute Bundesministerium des Innern im Januar 2016, ein Rechtsgutachten in Auftrag zu geben. Seine Aufgabe war es, die den Mitgliedstaaten eingeräumten Regelungsspielräume und Fortgeltungsmöglichkeiten des bestehenden bundesrechtlichen Datenschutzrechts (im Kern binnen des Zeitraums von Mitte Januar bis Ende März) zu analysieren. Die Untersuchung stellt sich dieser Aufgabe in vier Schritten: Nach einer Analyse der Steuerungsvorgaben, welche das unionsrechtliche Primärrecht und die Datenschutz-Grundverordnung für die Mitgliedstaaten vorhalten, entwickelt sie eine Typologie der (disparaten) Öffnungsklauseln. Mit diesem Handwerkszeug dekliniert sie sämtliche (echten und unechten)[2] Öffnungsklauseln der Datenschutz-Grundverordnung auf den Regelungsspielraum durch, den sie eröffnen, ordnet sie dabei jeweils in das System der Öffnungsklauseln ein, nimmt einen Vergleich zu den bisherigen Regelungen der Datenschutzrichtlinie vor, erläutert den Inhalt und die Reichweite der Öffnungsklausel, um sie dann mit dem nationalen Recht abzugleichen. In einem zweiten Teil bricht die Analyse dieser Ergebnisse systematisch auf allen Normen des BDSG herunter und fragt diese danach ab, welche

[1] Dazu auch *Kühling/Martini*, EuZW 2016, 448 (449 f.).
[2] Zu dieser Terminologie siehe S. 11.

Regelungen (ggf. modifiziert) bestehen bleiben können bzw. gestrichen werden müssen.
Die Ergebnisse des Gutachtens möchten die Autoren der Öffentlichkeit zugänglich machen und zur Diskussion stellen. Die Autoren sind sich dabei – nicht zuletzt mit Blick auf den erheblichen Zeitdruck, unter dem sich die Begutachtung (anfangs noch auf der Grundlage der englischsprachigen Trilog-Fassung) vollzog – bewusst, dass die Bearbeitung weder alle Fragen mit dem Anspruch auf angemessene, umfassende Durchdringung beantworten kann, die sich mit Öffnungsklauseln der DSGVO verbinden, noch von Unzulänglichkeiten frei sein kann. Vielmehr wollen sie einen ersten, wissenschaftlichen Blick auf die sich stellenden Herausforderungen richten und damit auch eine Diskussion anregen, die sich in vielen Bereichen noch erheblich ausdifferenzieren wird. Vor diesem Hintergrund freuen sie sich über hilfreiche Anregungen auf einem noch lange währenden Weg spannenden wissenschaftlichen Austausches. Denn der Gegenstand der DSGVO ist immerhin nichts anderes als der Grundstein des europäischen Datenschutzrechts für das 21. Jahrhundert.
Die Autoren sind dem Datenschutzreferat im BMI für das Vertrauen dankbar, das es ihnen entgegengebracht hat. Sie danken allen Mitarbeitern des zuständigen Referats, allen voran Herrn Regierungsdirektor *Jörg Eickelpasch*, sowie darüber hinaus Herrn Ministerialrat *Ulrich Weinbrenner* für die äußerst angenehme Zusammenarbeit sowie den intensiven und bereichernden Gedankenaustausch.

Regensburg und Speyer im Juni 2016

Jürgen Kühling, Mario Martini, Johanna Heberlein, Benjamin Kühl,
David Nink, Quirin Weinzierl und Michael Wenzel

Inhaltsübersicht

Inhaltsverzeichnis

I. Die Datenschutz-Grundverordnung als Hybrid zwischen Richtlinie und Verordnung

Die Datenschutz-Grundverordnung markiert den bislang wichtigsten Meilenstein des unionsrechtlichen Datenschutzrechts. Ein über fünf Jahre währender Gesetzgebungsprozess hat mit ihrer Verkündung am 27. April 2016 sein vorläufiges Ende gefunden. Sie stellt sich der Herausforderung, ein (zumindest weitgehend) harmonisiertes und effektives europäisches Datenschutzniveau auf den Weg zu bringen, das den digitalen Rahmenbedingungen des 21. Jahrhunderts gewachsen ist.

Dem Ende des unionalen Gesetzgebungsprozesses wohnt ein nicht weniger bedeutender Anfang eines Anpassungsprozesses auf nationaler Ebene inne. Die Verordnung setzt das nationale Datenschutzrecht nachhaltigen Umwälzungen aus. Die wohl wichtigste Erkenntnis für den nationalen Gesetzgeber ist dabei: Die Datenschutz-Grundverordnung gilt zwar unmittelbar. Der Wechsel zur Handlungsform der Verordnung täuscht aber leicht darüber hinweg, dass die DSGVO in der Sache in Teilen eher eine Richtlinie im Verordnungsgewand darstellt. Mit rund vier Dutzend Öffnungsklauseln belässt sie den Mitgliedstaaten reichlich normativen Gestaltungsspielraum für eigene Regelungen (S. 2 ff.). Das gilt für Regelungen im allgemeinen und bereichsspezifischen Datenschutzrecht (z. B. Art. 6 Abs. 2, 3 und 4 [ex Art. 6 Abs. 2a, 3 und 3a], Art. 23 [ex Art. 21], Art. 32 Abs. 4 [ex Art. 30 Abs. 2b], Art. 37 Abs. 4 [ex Art. 35 Abs. 4] oder Art. 91 [ex Art. 85] DSGVO), aber auch für weiterführende Rechtsgebiete mit datenschutzrechtlichen Bezügen (z. B. Art. 85 Abs. 1 und 2 [ex Art. 80 Abs. 1 und 2] DSGVO). Die Öffnungsklauseln lassen sich in (fakultative) Gestaltungsspielräume und obligatorische Ausfüllungspflichten der Mitgliedstaaten unterscheiden (S. 9 ff.). Insbesondere die Erfüllung Letzterer ist erforderlich, um die Durchführung der Datenschutz-Grundverordnung zu gewährleisten (z. B. Art. 84 Abs. 1 S. 1 [ex Art. 79b Abs. 1 S. 1] DSGVO). Ziel der Öffnungsklauseln ist es, den unterschiedlichen Ausgangspositionen der Mitgliedstaaten in dem Prozess der Konvergenz unterschiedlicher Rechtsordnungen angemessen Rechnung zu tragen und alle auf dem Weg der Harmonisierung mitzunehmen. Zugleich lässt die Europäische Union den Mitgliedstaaten zur Anpassung der nationalen Rechtsordnung aber nur wenig Zeit. Zwei Jahre nach ihrem Inkrafttreten, mithin ab dem 25. Mai 2018, wird die Verordnung anwendbar sein (siehe

Art. 99 Abs. 2 DSGVO). Welche Vorschriften des allgemeinen und bereichsspezifischen deutschen Datenschutzrechts bestehen bleiben können, welche zu modifizieren sind und welcher zusätzlichen Vorschriften es bedarf, um den Anforderungen der Datenschutz-Grundverordnung gerecht zu werden, ist gegenwärtig noch offen. Es ist daher von besonderer Bedeutung, dass sich die Gesetzgeber des Bundes und der Länder schnell Klarheit darüber verschaffen, über welchen nationalstaatlichen Regelungsspielraum sie verfügen. Wo es an gesetzgeberischem Spielraum fehlt, erübrigt sich eine nationale Diskussion über das nationale Datenschutzrecht der Zukunft. Wo er besteht, ist die Kenntnis seiner Grenzen zwingende Grundlage einer sachgerechten Auseinandersetzung.

Auf Bundesebene müssen die zwingenden Anpassungsschritte im allgemeinen, aber auch im bereichsspezifischen Recht bis zum Abschluss der Legislaturperiode bewältigt sein, die aber schon im Herbst 2017 ausläuft. Bereits bis zur Sommerpause 2016 sind daher entsprechende Regelungen zur Wahrnehmung des mitgliedstaatlichen Regelungsspielraums zu entwickeln.

II. Unionsrechtliche Steuerungsvorgaben für Öffnungsklauseln

Die Datenschutz-Grundverordnung regelt kein vollkommen neues Rechtsgebiet, sondern löst die Richtlinie 95/46/EG[3] ab, die mehr als zwanzig Jahre das unionsrechtliche Datenschutzregime bestimmt hat. Der neue, unmittelbar geltende Rechtsakt trifft dabei auf ein ausdifferenziertes nationales Rechtsregime, das durch allgemeine Datenschutzgesetze auf Bundes-, aber auch auf Länderebene eine intensive normative Durchdringung erfahren hat. Vor allem die Prägung durch eine Vielzahl bereichsspezifischer Regelungen ist dabei die Folge eines streng verstandenen Gesetzesvorbehalts.[4] In welchem Umfang dieses bereits bestehende ausdifferenzierte Rechtssystem im Zuge der Anwendung der Datenschutz-Grundverordnung überformt und verdrängt wird, harrt einer Klärung. Zur Beantwortung dieser Frage gilt es, die Reichweite

[3] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG 1995, L 281/31 (im Folgenden DSRL).

[4] Dazu zuletzt kritisch *Kingreen/Kühling*, JZ 2015, 213 ff.

des Anpassungszwangs (dazu 1.) sowie damit verknüpft des Anwendungsbereichs der Verordnung (dazu 2.) und des Wiederholungsverbots des Unionsrechts in mitgliedstaatlichen Rechtsvorschriften (dazu 3.) auszuloten.

1. Reichweite des Anpassungszwangs und Öffnungsklauseln

Nach der Rechtsprechung des EuGH genießt das Unionsrecht Vorrang gegenüber dem nationalen Recht.[5] Dieser Vorrang stellt sich als sogenannter Anwendungsvorrang ein, d. h. die nationalen Stellen müssen dem Unionsrecht entgegenstehende nationale Regelungen unangewendet lassen.[6] Diese sind jedoch nicht eo ipso nichtig, denn die Entscheidung über die Gültigkeit von nationalem Recht fällt nicht in den Kompetenzbereich der Union.[7]
Dennoch müssen die Mitgliedstaaten das nationale Recht anpassen, um Rechtsunsicherheiten bei den Normadressaten zu verhindern.[8] Tun sie dies nicht und behalten nationale Regelungen bei, die dem Unionsrecht widersprechen, verstoßen sie damit gegen ihre Verpflichtung aus dem europäischen Primärrecht zur loyalen Zusammenarbeit (Art. 4 Abs. 3 EUV).[9] Der Anpassungszwang endet allerdings dort, wo der zwingende Anwendungsbefehl des Unionsrechts seine Grenzen erreicht.
Das gilt bei der Datenschutz-Grundverordnung insbesondere für die Öffnungsklauseln, die den Mitgliedstaaten explizit die Möglichkeit zum Erlass nationaler Regelungen eröffnen. Die Öffnungsklauseln der Verordnung sind Ausfluss des Respekts der Union vor den mitgliedstaatlichen, durch den Grundsatz der begrenzten Einzelermächtigung (Art. 5 Abs. 2 AEUV) gesicherten Kompetenzen und dem mit einer Verordnung als Regelungsinstrument einhergehenden intensiven Einwirken der Union in diesen Kompetenzbereich. Mit ihnen erfüllt die Union ihrerseits ihre Pflicht zur loyalen Zu-

[5] *EuGH*, Rs. 6/64, Slg. 1964, 1141, 1269 f. – Costa/E.N.E.L; Rs. 106/77, Slg. 1978, 629, Rn. 17 f. – Simmenthal II.
[6] *EuGH*, Rs. 106/77, Slg. 1978, 629, Rn. 17 f., 21, 23 – Simmenthal II; Rs. C-10/97 u. C-22/97, Slg. 1998, I-6307, Rn. 20 f. – IN.CO.GE.
[7] *Nettesheim*, in: Grabitz/Hilf (Hrsg.), EU-Recht, 41. EL, Art. 1 AEUV, Rn. 80; *Funke*, DÖV 2007, 733 (736).
[8] *EuGH*, Rs. 168/85, Slg. Slg. 1986, 2945, Rn. 13 f. – Kommission/Italien; Rs. C-74/86, Slg. 1988, 2139, Rn. 10 f. – Kommission/Deutschland.
[9] *EuGH*, Rs. C-74/86, Slg. 1988, 2139, Rn. 11 – Kommission/Deutschland.

sammenarbeit und wahrt das Subsidiaritäts- und Verhältnismäßigkeitsprinzip (Art. 4 Abs. 3, Art. 5 Abs. 3 und 4 EUV).[10] Insoweit ist auch die unmittelbare Wirkung der Datenschutz-Grundverordnung letztlich beschränkt. Insbesondere mit Blick auf die weitreichenden allgemeinen Öffnungsklauseln Art. 6 Abs. 2, 3 und 4 (ex Art. 6 Abs. 2a, 3 und 3a) DSGVO verbleiben erhebliche mitgliedstaatliche Handlungsspielräume. Das gilt insbesondere für die Regelung des Datenschutzes bei der Verarbeitung durch öffentliche Stellen und für weite Teile des bereichsspezifischen Datenschutzrechts in Deutschland.

2. Grundsätzlich abschließender Charakter der Verordnung im Übrigen; Anwendungsbereich

Entsprechend ihrer im Titel anklingenden Grundlagenorientierung und ihrer Vielzahl von Öffnungsklauseln regelt die Datenschutz-Grundverordnung den unionalen Datenschutz nur im Grundsatz abschließend. Soweit der Anwendungsbereich der Verordnung reicht, dürfen die Mitgliedstaaten eine Modifikation der Vorgaben aber umgekehrt nur vornehmen, soweit die Verordnung selbst dies eröffnet.

Der sachliche Anwendungsbereich der Verordnung markiert daher eine wichtige Weichenstellung. Art. 2 DSGVO formt ihn im Einzelnen aus; er entspricht im Wesentlichen den Vorgaben der DSRL. Diese war schon immer breit auf jede Form der Verarbeitung personenbezogener Daten ausgerichtet, ohne dass es des spezifischen Nachweises eines Binnenmarktbezugs bedurft hätte. Auch die Datenschutz-Grundverordnung nimmt keine entsprechende Beschränkung vor. Vielmehr geht sie angesichts der vielfältigen und regelmäßig zumindest potenziell grenzüberschreitenden Relevanz jeder Datenverarbeitung ganz allgemein im Falle einer entsprechenden Verarbeitung nach Art. 2 Abs. 1 DSGVO von der Öffnung des Anwendungsbereichs ratione materiae aus. Das entspricht ihrer weiten kompetenzrechtlichen Grundlage: Sie stützt sich auf Art. 16 Abs. 2 AEUV. Daran ändert auch Art. 2 Abs. 2 lit. a DSGVO nichts. Er bestimmt, dass die Verordnung auf Tätigkeiten, die

[10] Dazu *Obwexer*, in: von der Groeben/Schwarze/Hatje (Hrsg.), EU-Recht, 7. Aufl., 2015, Art. 4 EUV, Rn. 142 ff; sowie *Kadelbach*, in: von der Groeben/Schwarze/Hatje (Hrsg.), EU-Recht, 7. Aufl., 2015, Art. 5 EUV, Rn. 25 ff.

nicht in den Anwendungsbereich des Unionsrechts fallen, keine Anwendung findet. Dies ist lediglich als Hinweis auf die Grenzen der Kompetenzen für die Gesetzgebung zu verstehen. Denn der Regelungsgehalt der Verordnung kann nicht weiter reichen als die Ermächtigungsgrundlage in Art. 16 Abs. 2 AEUV.[11] Eine weitere Beschränkung verbindet sich mit dieser Norm nicht.
Die Verordnung regelt auch nicht die Datenverarbeitung im Kontext der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten sowie der Vollstreckung strafrechtlicher Urteile (Art. 2 Abs. 2 lit. d [ex Abs. 2 lit. e] DSGVO). Insoweit greift die parallel verabschiedete Richtlinie für den Datenschutz bei Polizei und Strafjustiz.[12] Diese zielt auf einen Kompromiss zwischen den neuen technischen Möglichkeiten der (insbesondere grenzüberschreitenden) Datenerhebung und des Datenaustauschs im Bereich der Strafverfolgung und öffentlichen Sicherheit auf der einen Seite und den Bedürfnissen eines angemessenen Schutzes des informationellen Selbstbestimmungsrechts Betroffener auf der anderen Seite. Die Richtlinie wird den Rahmenbeschluss 2008/977JI ersetzen. Erstmals wird die Union damit die innerstaatliche Datenverarbeitung in den Bereichen der Gefahrenabwehr- und Strafverfolgungsbehörden regeln. Sie wagt sich dadurch in ihrem Regelungsgehalt weit in Kernkompetenzbereiche der Mitgliedstaaten vor. Entsprechend ist sie in ihrer inhaltlichen Regelungstiefe zur Zurückhaltung genötigt. Sie trifft deshalb kaum Regelungen, die das deutsche Recht nicht bereits enthält: Die inhaltlichen Auswirkungen der Richtlinie für den Bereich der Gefahrenabwehr- und Strafverfolgungsbehörden auf das nationale einfachgesetzliche Recht werden entsprechend sehr begrenzt sein.
Inhaltlich enthalten Verordnung und Richtlinie ähnliche Regelungen, etwa sub specie der Aufsichtsbehörden (Kapitel VI) sowie der Zusammenarbeit der Aufsichtsbehörden oder der Verantwortlichkeit (Kapitel IV). Umso bedeut-

[11] Zur Subsidiaritätsrüge des Deutsches Bundesrates BR-Drucks. 51/12 und 52; dazu auch ausführlich *Nguyen*, ZeuS 2012, 277 ff. Zur Subsidiaritätsrüge des Deutsches Bundesrates BR-Drucks. 51/12 und 52; dazu auch ausführlich *Nguyen* (Fn. 11) ff.
[12] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl. (EU), L 119 v. 4.5.2016, S. 89 ff.

samer ist für den Handlungsspielraum auf nationaler Ebene die klare Abgrenzung beider Regelungswerke: Wenn Justizbehörden, die Polizei oder andere Strafverfolgungsbehörden bzw. andere Stellen öffentliche Aufgaben oder hoheitliche Befugnisse zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung wahrnehmen, ist die Richtlinie einschlägig. Wenn solche Stellen personenbezogene Daten zu anderen Zwecken als der Ausübung öffentlicher Aufgaben und/oder hoheitlicher Befugnisse zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung verarbeiten, ist demgegenüber die Datenschutz-Grundverordnung anwendbar (EG 11 S. 2 und 3 Datenschutzrichtlinie; EG 19 S. 2 ff. [ex EG 16 S. 2 ff.] DSGVO). Wiewohl die Datenschutzrichtlinie für das nationale Recht wenig unmittelbaren Regelungsbedarf auslöst, strahlt sie in einer anderen Hinsicht nachhaltig auf die nationale Rechtsordnung aus: Mit ihr verbindet sich eine Verschiebung der grundrechtlichen Kontrollgewalt zwischen der Union und den Mitgliedstaaten. Sobald die Richtlinie Vorgaben für das nationale Recht statuiert, ist deren Anwendung eine Ausführung und damit Durchführung der Richtlinie i. S. d. Art. 51 GrCh. Dadurch geraten mitgliedstaatliche Eingriffsbefugnisse in den Prüfungsradius des EuGH. Es kommt zu einer Unitarisierung des Grundrechtsschutzes in Europa auch für den Bereich der Polizei und der Justiz. Die Besonderheit der Richtlinie besteht damit vor allem in einer Verschiebung der Kompetenzen, insbesondere der grundrechtlichen Rechtsschutzhoheit vom BVerfG zum EuGH.[13]

3. Reichweite des Wiederholungsverbots

Jenseits der Möglichkeiten, auf der Grundlage von Öffnungsklauseln von den Regelungen der Datenschutz-Grundverordnung abzuweichen, stellt sich die Frage, ob gegebenenfalls eine nationale Gesetzgebung auch bloß wiederholende Regelungen – also ohne eine inhaltliche Modifikation – enthalten darf. Dem setzt das europarechtliche Wiederholungsverbot Grenzen. Dieses untersagt den Mitgliedstaaten, mit einer Verordnung im Wortlaut übereinstimmen-

[13] Dazu bereits *Bäcker/Hornung*, ZD 2012, 147 (152).

de Regelungen im nationalen Recht zu erlassen. Denn die Datenschutz-Grundverordnung beansprucht gem. Art. 288 Abs. 2 AEUV unmittelbare Geltung und bedarf demnach – anders als eine Richtlinie (Art. 288 Abs. 3 AEUV) – keines Umsetzungsaktes in nationales Recht.

Das Wiederholungsverbot soll verhindern, dass die gem. Art. 267 AEUV alleinige Kompetenz des EuGH zur Auslegung des Unionsrechts oder zur Feststellung der Gültigkeit von Unionsrechtsakten[14] durch den Erlass gleichlautender nationaler Bestimmungen begrenzt wird.[15] Dies ist insbesondere der Fall, wenn mitgliedstaatliche Regelungen den Anwendungsbefehl des Unionsrechts verdecken können.[16] So kann ein Mitgliedstaat nicht die Bestimmungen einer unmittelbar geltenden Verordnung in nationales Recht übernehmen, da er damit die Zuständigkeit des EuGH in Frage stellen würde und eine einheitliche Anwendung der Verordnung innerhalb der EU nicht mehr gewährleistet wäre.[17]

Im Gegensatz zu einer weitflächigen Übernahme des Verordnungswortlauts in nationale Bestimmungen eröffnen die Öffnungsklauseln der Datenschutz-Grundverordnung den Mitgliedstaaten jedoch gerade Freiräume für den Erlass nationaler Regelungen. Damit bestimmen die Öffnungsklauseln die Normsetzungskompetenz der Mitgliedstaaten in den adressierten Bereichen. Ihre Auslegung der jeweiligen Öffnungsklauseln entscheidet darüber, in welchem Maße und Umfang den Mitgliedstaaten der Erlass nationalstaatlicher Regelungen gestattet ist. Der Telos des Wiederholungsverbots, eine Beschneidung der Auslegungskompetenz des EuGH zu verhindern, bedeutet im Umkehrschluss, dass der nationale Gesetzgeber innerhalb seiner durch die Öffnungsklauseln zugewiesenen Normsetzungskompetenz Teile des Verordnungswortlautes übernehmen darf,[18] um die nationale Norm klarer zu gestalten. Entsprechend hat der EuGH entschieden, dass die punktuelle Wiederholung des Wortlauts einer Verordnung keinen Verstoß gegen Unionsrecht darstellt, wenn unionsrechtliche, einzelstaatliche und regionale Vorschriften für eine

[14] *EuGH*, Rs. 314/85, Slg. 1987, 4199, Rn. 15 – Foto Frost.
[15] *EuGH*, Rs. 34/73, Slg. 1973, 981, Rn. 9 ff. –Variola.
[16] *EuGH*, Rs. 94/77, Slg. 1978, 99, Rn. 22/27 – Zerbone.
[17] *EuGH*, Rs. 34/73, Slg. 1973, 981, Rn. 10 – Variola; Rs. 39/72, Slg. 1973, 101, Rn. 16 ff. – Kommission/Italien.
[18] Vgl. *Schweitzer*, Staatsrecht III, 10. Aufl., 2010, Rn. 343b.

umfassende Regelung zusammentreffen und die Wortlautwiederholung im Interesse des inneren Zusammenhangs und der Verständlichkeit für die Normadressaten liegt.[19] Entscheidend ist also stets, dass die Wiederholung die unmittelbare Wirkung der Verordnung nicht behindert.[20]
Dann muss die punktuelle Wiederholung aber erst recht möglich sein, wenn die Verordnung gerade Freiräume für die Normsetzungskompetenz der Mitgliedstaaten schafft. Eine Stütze findet dieses Ergebnis in EG 8 (ex EG 6a) DSGVO, der die Rechtsprechung des EuGH zum Wiederholungsverbot normativ auflädt. Er bringt die Leitvorstellung des Verordnungsgebers aus, den Mitgliedstaaten zu gestatten, Teile der Datenschutz-Grundverordnung in nationales Recht zu inkorporieren, sofern dies erforderlich ist, um die Normen für die Normadressaten verständlicher zu machen oder die Kohärenz zu wahren. EG 8 (ex EG 6a) DSGVO knüpft dafür kumulativ an drei Voraussetzungen an: Die Wiederholung muss erforderlich sein für die bessere Verständlichkeit beim Normadressaten (1) und die Kohärenz (2). Die Übernahme des Textes der Datenschutz-Grundverordnung muss im sachlichen Zusammenhang mit einer Öffnungsklausel stehen, die dem Mitgliedstaat „Präzisierungen oder Einschränkungen“ von Vorschriften der Datenschutz-Grundverordnung einräumt (3). Gerade die dritte Voraussetzung schränkt den normativen Handlungsspielraum des nationalen Gesetzgebers nachhaltig ein und lässt für implizite Öffnungsklauseln grundsätzlich keinen Raum.

4. Regelung „durch Rechtsvorschrift“

Erteilt die Datenschutz-Grundverordnung den Mitgliedstaaten einen Regelungsauftrag oder gesteht ihnen einen Regelungsspielraum zu, ergänzt sie ihn im Kontext der unionsrechtlichen Aufsichtsstrukturen häufig um den Passus, dass die Mitgliedstaaten durch „Rechtsvorschrift“ tätig werden müssen (z. B. Art. 23 Abs. 1, Art. 54 Abs. 1, Art. 58 Abs. 5). Unter einer „Rechtsvorschrift“ versteht sie nicht allein ein Parlamentsgesetz, also ein Gesetz im formellen

[19] *EuGH*, Rs. 272/83, Slg. 1985, 1057, Rn. 26 f. – Kommission/Italien.
[20] Vgl. *EuGH*, Rs. 272/83, Slg. 1985, 1057 Rn. 25 – Kommission/Italien; Rs. 94/77, Slg. 1978, 99, Rn. 22/27 – Zerbone; Rs. 34/73, Slg. 1973, 981, Rn. 10 f. – Variola; Rs. 39/72, Slg. 1973, 101, Rn. 17 – Kommission/Italien.

Sinne. Sie lässt vielmehr auch ein Gesetz im materiellen Sinne genügen. Zur nationalstaatlichen Ausgestaltung eines durch die Datenschutz-Grundverordnung eröffneten Regelungsspielraums kommen somit auch Rechtsverordnungen in Betracht. Dies macht EG 41 (ex EG 31a) DSGVO deutlich, der eine entsprechende Klarstellung des Begriffs der Rechtsgrundlage für die Datenschutz-Grundverordnung vornimmt.
Dessen ungeachtet kann sich das Erfordernis einer formell-gesetzlichen Regelung aber – wie auch EG 41 (ex EG 31a) DSGVO betont – aus dem Recht des jeweiligen Mitgliedstaats, genauer gesagt aus dessen „Verfassungsordnung", ergeben. Übertragen auf die Bundesrepublik Deutschland bedeutet dies, dass bei einem durch die Datenschutz-Grundverordnung eröffneten Regelungsspielraum stets zu eruieren ist, inwieweit das Grundgesetz eine parlamentsgesetzliche Ausgestaltung erfordert. Das BVerfG beantwortet diese Frage auf Grundlage des Rechtsstaats- und Demokratieprinzips mit der sog. „Wesentlichkeitstheorie": „Der Gesetzgeber ist verpflichtet, alle wesentlichen Entscheidungen selbst zu treffen, und darf sie nicht anderen Normgebern überlassen. Wann es danach einer Regelung durch den parlamentarischen Gesetzgeber bedarf, lässt sich nur im Blick auf den jeweiligen Sachbereich und auf die Eigenart des betroffenen Regelungsgegenstandes beurteilen."[21]

III. Typologie der Öffnungsklauseln

Die verschiedenen Öffnungsklauseln lassen sich Kategorisierungen zuordnen, die angesichts der horizontalen Relevanz, an dieser Stelle „vor die Klammer gezogen" erläutert werden.

1. Reichweite der Öffnungsklauseln: allgemeine und spezifische Öffnungsklauseln

Die Öffnungsklauseln lassen sich in allgemeine und spezifische scheiden. Erstere eröffnen eine Vielzahl von Abweichungsmöglichkeiten, ohne auf ein

[21] BVerfGE 98, 218 (251). Siehe auch BVerfGE 40, 237 (248 ff.); 49, 89 (126 f.); 95, 267 (307 f.).

spezifisches Themengebiet beschränkt zu sein. Ein Beispiel für diese Kategorie ist Art. 23 (ex Art. 21) DSGVO, der Abweichungen von allen Betroffenenrechten eröffnet – ebenso (bei einem weiten Verständnis) Art. 85 Abs. 1 DSGVO, der den Mitgliedstaaten den sektorübergreifenden Regelungsauftrag erteilt, den Konflikt zwischen dem informationellen Selbstbestimmungsrecht und der Informations- sowie Meinungsfreiheit durch Rechtsvorschriften normativ zu entschärfen. Art. 8 Abs. 1 DSGVO ist hingegen als spezifische Öffnungsklausel zu qualifizieren, da er nur den sehr beschränkten Bereich der Einwilligung von Personen zwischen 13 und 16 Jahren bzgl. der Nutzung von Diensten der Informationsgesellschaft betrifft.

2. Anpassungstypus

a. Handlungsoptionen: Konkretisierung, Ergänzung, Modifikation

Die Handlungsmöglichkeiten, welche die Öffnungsklauseln zuweisen, lassen sich in drei Kategorien einteilen: erstens die *Konkretisierung*, d. h. die nähere Bestimmung der jeweiligen DSGVO-Regelung durch nationales Recht, zweitens die *Ergänzung*, d. h. eine Vervollständigung der DSGVO-Regelungen durch nationales Recht, und drittens die *Modifikation*, also die Möglichkeit der Abweichung von dem Regelungsinhalt der DSGVO-Norm durch nationales Recht. Es ist auch möglich, dass Öffnungsklauseln den Mitgliedstaaten alle drei Handlungsmöglichkeiten einräumen.[22]

b. Regelungsgebote/Ausgestaltungsnotwendigkeiten – obligatorische und fakultative Öffnungsklauseln

Anders als Fälle der Regelungsoptionen sind die Fälle notwendiger mitgliedstaatlicher Ausgestaltung einzuordnen. Hier verlangt die Datenschutz-Grundverordnung explizit, dass die Mitgliedstaaten Regelungen treffen, um – insbesondere im institutionellen Bereich – der Verordnung Wirkung zu verleihen. Das gilt vor allem im Bereich der Zusammenarbeit und Kohärenz nach Kapitel VII der Verordnung.

[22] Siehe auch *Kühling/Martini* (Fn. 1), 449.

3. Echte und unechte Öffnungsklauseln

Dass es sich bei Vorschriften der Datenschutz-Grundverordnung um Öffnungsklauseln handelt, ergibt sich vielfach zweifelsfrei aus der Handlungsoptionen eröffnenden oder Handlungspflichten auferlegenden Formulierung, so etwa „nach dem Ermessen der Mitgliedstaaten“ (Art. 35 Abs. 10 DSGVO), „die Mitgliedstaaten können vorsehen...“ (Art. 80 Abs. 2 DSGVO), „die Mitgliedstaaten können näher bestimmen…“ (Art. 87 DSGVO), „die Mitgliedstaaten bringen durch Rechtsvorschriften…“ (Art. 85 Abs. 1).
An verschiedenen Stellen verweist die Datenschutz-Grundverordnung aber schlicht auf das „Recht der Union oder der Mitgliedstaaten“ und dort enthaltene Regelungen. Dieser Verweis auf das mitgliedstaatliche Recht *kann*, muss indes nicht zwingend eine Öffnungsklausel darstellen. Es kann sich dabei einerseits um die Ermächtigung zu selbständigem mitgliedstaatlichem Tätigwerden handeln (*echte Öffnungsklausel*) – ebenso aber um den Verweis auf eine anderweitig in der Verordnung angelegte mitgliedstaatliche Handlungsbefugnis, die sich nicht unmittelbar aus der Wendung selbst, sondern aus einer anderen Öffnungsklausel, etwa den allgemeinen Verarbeitungsgrundlagen in Art. 6 Abs. 1 UAbs. 1 lit. c oder e DSGVO, ergibt (*unechte Öffnungsklausel*).
Ob es sich um eine echte oder unechte Öffnungsklausel handelt, lässt sich nur durch eine Auslegung der jeweiligen Vorschrift ermitteln. Ein Beispiel für eine echte Öffnungsklausel ist Art. 37 Abs. 4 Hs. 2 DSGVO. Danach ist ein Datenschutzbeauftragter zu benennen, wenn dies nach dem Recht der Mitgliedstaaten vorgeschrieben ist. Die Datenschutz-Grundverordnung adressiert mit ihrer Formulierung hier zwar nicht unmittelbar den Mitgliedstaat und gesteht ihm ausdrücklich eine Regelungsbefugnis zu. Jedoch ergibt sich aus der Offenheit für eine aus dem Recht der Mitgliedstaaten folgende Pflicht zur Bestellung eines Datenschutzbeauftragen, dass die Mitgliedstaaten eben auch berechtigt sein müssen, diese Verpflichtung zu erlassen.
Anders ist zum Beispiel Art. 28 Abs. 3 S. 2 lit. a DSGVO einzuordnen. Nach dieser Bestimmung darf eine Auftragsverarbeitung grundsätzlich nur auf dokumentierte Weisung des Verantwortlichen hin erfolgen, sofern der Auftragsverarbeiter nicht durch das Recht der Union oder der Mitgliedstaaten, dem er unterliegt, hierzu verpflichtet ist. Hier räumt die Vorschrift den Mit-

gliedstaaten nicht das Recht ein, generell Verarbeitungspflichten zu begründen. Vielmehr nimmt die Vorschrift bestehende Verarbeitungspflichten in Bezug, die selbst insbesondere aufgrund des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO erlassen werden können. Verstünde man die Norm selbst als (umfassende) Öffnungsklausel zum Erlass von Verarbeitungspflichten, drohte das nämlich das ausdifferenzierte System der Erlaubnistatbestände der Datenschutz-Grundverordnung, insbesondere nach Art. 6 und 9 DSGVO, zu unterlaufen. Ähnlich liegt es bei Art. 17 Abs. 1 lit. e und Abs. 3 lit. b DSGVO, die im Rahmen des „Rechts auf Vergessenwerden" auf das mitgliedstaatliche Recht verweisen. Sie eröffnen keinen zusätzlichen Spielraum, um innerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung[23] Rechtsgrundlagen zu erlassen, die das Recht auf Löschung begründen (Art. 17 Abs. 1 lit. e DSGVO) oder beschränken (Abs. 3 lit. b DSGVO). Vielmehr verweist die Norm auf die Voraussetzungen anderer Öffnungsklauseln der Datenschutz-Grundverordnung und mitgliedstaatliches Recht, das außerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung besteht bzw. künftig erlassen wird.

Eine etwas andere Regelungskonstellation eines Verweises auf mitgliedstaatliche Handlungsbefugnisse beschreibt Art. 80 Abs. 1 DSGVO. Er regelt die Vertretung betroffener Personen durch Einrichtungen, Organisationen oder Vereinigungen, die ohne Gewinnerzielungsabsicht handeln und „ordnungsgemäß nach dem Recht eines Mitgliedstaates gegründet" sind. Die Befugnis zur Gründung solcher Einrichtungen fußt selbstredend nicht auf einer in der Verordnung begründeten Handlungsermächtigung, sondern setzt auf einer selbstständigen, den Mitgliedstaaten originär zugewiesenen gesellschaftsrechtlichen Regelungsbefugnis auf und verweist auf diese.

4. Kategorien der Datenverarbeiter und Reichweite der Öffnungsklauseln

Das deutsche Datenschutzrecht differenziert bislang kategorial zwischen öffentlichen und nicht-öffentlichen Stellen. Diese schon in der Richtlinie nicht

[23] Vgl. S. 4.

angelegte Unterscheidung findet sich in der Datenschutz-Grundverordnung in dieser Klarheit nicht wieder (siehe aber immerhin den Rekurs in EG 80 S. 1 a. E., EG 92, 93, 108 S. 4, 154 S. 4, Art. 27 Abs. 2 lit. b, Art. 37 Abs. 3, Art. 41 Abs. 6, Art. 83 Abs. 7 DSGVO). Daher stellt sich jeweils im Einzelfall die Frage, inwiefern die Öffnungsklauseln für die Erfüllung öffentlicher Aufgaben relevant sind und daher primär öffentliche Stellen im Sinne der überkommenen deutschen Trennung adressiert werden oder primär nicht-öffentliche Stellen oder beide Verarbeiter gleichermaßen. Für die anschließende Anpassungsnotwendigkeit des deutschen Datenschutzrechts ist diese Unterscheidung von besonderer Relevanz.

Die Öffnungsklauseln des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO nehmen faktisch auf die Unterscheidung zwischen öffentlichen und nicht-öffentlichen Stellen Bezug. Sie bringen jedenfalls zum Ausdruck, dass die Verordnung das Ziel der Vollharmonisierung im öffentlichen Bereich nicht in gleichem Umfang wie im nicht-öffentlichen Bereich verfolgt. Das folgt auch aus EG 10 DSGVO, in dem es heißt: „Hinsichtlich der Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, sollten die Mitgliedstaaten die Möglichkeit haben, nationale Bestimmungen, mit denen die Anwendung der Vorschriften dieser Verordnung genauer festgelegt wird, beizubehalten oder einzuführen.“ Im nicht-öffentlichen Bereich zielt die Datenschutz-Grundverordnung dagegen grundsätzlich auf eine Vollharmonisierung und will durch ein einheitlich hohes Schutzniveau einen freien Datenverkehr im (digitalen) Binnenmarkt herstellen. EG 9 DSGVO erläutert, dass unterschiedliche Datenschutzstandards den unionsweit freien Datenverkehr behindern können und sich durch den bisherigen Richtlinienansatz nicht hinreichend verhindern ließen. Das Harmonisierungsziel lässt sich insoweit besser durch die Handlungsform einer Verordnung erreichen, die eine einheitliche Auslegung, insbesondere im Kohärenzverfahren bzw. durch den EuGH, erfährt.

Das Argument des freien Datenflusses trägt hingegen nicht im öffentlichen Bereich. Hier kommt es weniger auf Einheitlichkeit an, was insbesondere die Konstruktion in Art. 6 Abs. 1 UAbs. 1 lit. c und e i. V. m. Art. 6 Abs. 2, 3 DSGVO belegt. Die Regelungen vermitteln dem nationalen Gesetzgeber

weitgehenden Spielraum zum Erlass der Rechtsgrundlagen und der Einzelheiten der Verarbeitung.

IV. Mitgliedstaatliche Regelungsgebote und -spielräume der DSGVO

1. Übersichtstabelle

Öffnungsklausel	**Korrespondierende Erwägungsgründe**	**Durch die Öffnungsklausel ausgelöster nationalstaatlicher Regelungsbedarf?**	**Vorgängerregelung in der DSRL**	**Im nationalen Recht betroffene Vorschriften (exemplarisch)**
EG 20 (ex EG 16a)	-	Fakultativ	-	
EG 27 S. 2 (ex EG 23aa S. 2)	-	Fakultativ	-	§ 35a BDSG als Regelungsoption, ggf. klarstellender Hinweis in § 3 Abs. 1 BDSG
Art. 4 Nr. 7 (ex Art. 4 Nr. 5)	-	Fakultativ	Art. 2 lit. d	§ 3 Abs. 7 BDSG
Art. 4 Nr. 9 (ex Art. 4 Nr. 7)		Fakultativ	-	
Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e[24], Abs. 2 (ex Abs. 2a) Abs. 3	Nr. 10 (ex 8); 45 (ex 36); 50 (ex 40)	Fakultativ	Art. 7 lit. c bzw. e EG 22	§ 13 Abs. 1 BDSG
Art. 6 Abs. 4 (ex Art. 6 Abs. 3a)	Nr. 50 (ex 40)	Fakultativ	-	Teilweise § 14 Abs. 2 BDSG

[24] Art. 6 Abs. 1 DSGVO wurde erst nach der Bereinigung in zwei Unterabsätze aufgeteilt, so dass aus Art. 6 Abs. 1 lit. f S. 1 in der Fassung des Trilog Art. 6 Abs. 1 UAbs. 1 lit. f in der endgültigen Fassung wurde und Art. 6 Abs. 1 lit. f S. 1 zu Art. 6 Abs. 1 UAbs. 2. Insgesamt wurden damit auch die Art. 6 Abs. 1 lit. a bis e zu den Art. 6 Abs. 1 UAbs. 1 lit. a bis e. Dies heben die Klammerverweise auf die Trilog-Fassung der DSGVO im Folgenden nicht eigens hervor, um Missverständnisse zu vermeiden.

Art. 8 Abs. 1	Nr. 38 (ex 29)	Fakultativ	-	§ 4a Abs. 1 BDSG
Art. 9 Abs. 2 lit. a, b, g, h, i, j; Abs. 3, 4 (ex Art. 9 Abs. 2 lit. a, b, g, h, hb, i; Abs. 4, 5)	Nr. 51 - 55 (ex 51 - 43); 58 (ex 46)	Fakultativ	Art. 8 Abs. 2	§ 13 Abs. 2 BDSG
Art. 10 (ex Art. 9a)	-	Fakultativ	Art. 8 Abs. 5	§ 4 BZRG
Art. 14 (ex Art. 14a)		Fakultativ	Art. 11	§ 19a Abs. 1 BDSG
Art. 17 Abs. 1 lit. e; Abs. 3 lit. b	Nr. 65, 66	Fakultativ; unecht	Art. 12 lit. b	§ 35 Abs. 2 BDSG
Art. 22 Abs. 2 lit. b (ex Art. 20 Abs. 1a lit. b)	Nr. 71 (ex 58)	Fakultativ	Art. 15 Abs. 2 lit. b	§ 6a BDSG
Art. 23 (ex Art. 21)	Nr. 73 (ex 59)	Fakultativ	Art. 13	§ 20 Abs. 5 S. 2 BDSG
Art. 26 (ex Art. 24)	Nr. 79 (ex 62)	Fakultativ	-	§ 6 Abs. 2 BDSG
Art. 28 Abs. 3 UAbs. 1 S. 1 (ex Art. 26 Abs. 2 S. 1)	Nr. 81 (ex 63a)	Fakultativ	Art. 17 Abs. 3	§ 11 Abs. 2 S. 3 BDSG
Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a Hs. 1 (ex Art. 26 Abs. 2 lit. a)	Nr. 81 (ex 63a)	Fakultativ, unecht	Art. 17 Abs. 3	§ 11 Abs. 3
Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a Hs. 2 (ex Art. 26 Abs. 2 lit. a)		Fakultativ; wohl unecht	Art. 17 Abs. 3	§ 11 Abs. 3
Art. 28 Abs. 3 UAbs. 1 S. 2 lit. g (ex Art. 26 Abs. 2 lit. g)	Nr. 81 (ex 63a)	Fakultativ; unecht	-	§ 20 Abs. 2 Nr. 2, Abs. 3 BDSG; § 4 Abs. 1 BDSG
Art. 28 Abs. 4 (ex Art. 26 Abs. 2a)	-	Fakultativ	-	§ 11 Abs. 1-4 BDSG

Art. 29 (ex Art. 27)	-	Fakultativ; unecht	Art. 16	§ 11 Abs. 3 BDSG
Art. 32 Abs. 4 (ex Art. 30 Abs. 2b)	-	Fakultativ; unecht	Art. 16	-
Art. 35 Abs. 10 (ex Art. 33 Abs. 5)	Nr. 92 f. (ex 72 f.)	Fakultativ	-	§ 4d Abs. 5 BDSG
Art. 36 Abs. 4 (ex Art. 34 Abs. 7)	Nr. 96 (ex 74b)	Obligatorisch (ohne nationalen Regelungsbedarf auszulösen)		
Art. 36 Abs. 5 (ex Art. 34 Abs. 7a)		Fakultativ	Art. 18, 20	§§ 4d, 4e BDSG
Art. 37 Abs. 4 S. 1 Hs. 2 (ex Art. 35 Abs. 4)	Nr. 97 (ex 75)	Fakultativ	EG 49; Art. 18 Abs. 2 Spstr. 1, Art. 20 Abs. 2	§ 4f Abs. 1, 2 BDSG
Art. 43 Abs. 1 (ex Art. 39a Abs. 1)	-	Obligatorisch bzgl. des „Ob“; Wahlfreiheit bzgl. des „Wie“	-	-
Art. 49 Abs. 1 lit. d bzw. g, Abs. 5 (ex Art. 44 Abs. 1 lit. d bzw. g, Abs. 5a)	Nr. 111, 112 (ex 86, 87)	Fakultativ	Art. 26 lit. d bzw. f	§ 4c Abs. 1 S. 1 Nr. 4 Alt. 1 bzw. Nr. 6 BDSG
Art. 51 Abs. 1 i. V. m. Art. 54 Abs. 1 lit. a (ex Art. 46 Abs. 1 i. V. m. Art. 49 Abs. 1 lit. a)	Nr. 117 (ex 92 [ff.])	Obligatorisch	Art. 28 Abs. 1 S. 1	§ 22 BDSG; § 38 Abs. 6 BDSG
Art. 51 Abs. 3 sowie Art. 68 Abs. 4 (ex Art. 46 Abs. 2 sowie Art. 64 Abs. 3)	Nr. 119 (ex 93)	Obligatorisch	Art. 29 Abs. 2 UAbs. 2	Berührungspunkte mit § 26 Abs. 4 BDSG

Art. 52 Abs. 4 (ex Art. 47 Abs. 5)	Nr. 120 (ex 94)	Obligatorisch	-	-
Art. 52 Abs. 5 (ex Art. 47 Abs. 6)	Nr. 121 (ex 95)	Obligatorisch	-	-
Art. 52 Abs. 6 (ex Art. 47 Abs. 7)	Nr. 118, 120 (ex 92a, 94)	Obligatorisch	-	-
Art. 53 Abs. 1 i. V. m. Art. 54 Abs. 1 lit. c (ex Art. 48 Abs. 1 i. V. m. Art. 49 Abs. 1 lit. c)	Nr. 121 (ex 95)	Obligatorisch	-	§ 22 Abs. 1 S. 1 und 3 BDSG
Art. 54 Abs. 1 lit. a i. V. m. Art. 51 Abs. 1 (ex Art. 49 Abs. 1 lit. a i. V. m. Art. 46 Abs. 1)	Nr. 117 ff. (ex 92 ff.)	Obligatorisch	Art. 28 Abs. 1 S. 1	§ 22 BDSG; § 38 Abs. 6 BDSG
Art. 54 Abs. 1 lit. b i. V. m. Art. 53 Abs. 2 (ex Art. 49 Abs. 1 lit. b i. V. m. Art. 48 Abs. 2)	Nr. 121 (ex 95)	Obligatorisch	-	- (§ 22 Abs. 1 S. 2 BDSG)
Art. 54 Abs. 1 lit. c i. V. m. Art. 53 Abs. 1 (ex Art. 49 Abs. 1 lit. c i. V. m. Art. 48 Abs. 1)	Nr. 121 (ex 95)	Obligatorisch	-	§ 22 Abs. 1 S. 1 und 3 BDSG
Art. 54 Abs. 1 lit. d i. V. m. Art. 53 Abs. 3 (ex Art. 49 Abs. 1 lit. d i. V. m. Art. 48	-	Obligatorisch	-	Hinsichtlich des normeigenen Inhalts: § 22 Abs. 3 S. 1 BDSG Hinsichtlich des Inhalts von Art. 48

Abs. 3)				Abs. 3: § 22 Abs. 3 BDSG; § 23 Abs. 1 S. 2 und 3 BDSG
Art. 54 Abs. 1 lit. e (ex Art. 49 Abs. 1 lit. e)	-	Obligatorisch	-	§ 22 Abs. 3 S. 2 BDSG
Art. 54 Abs. 1 lit. f i. V. m. Art. 52 Abs. 3 sowie Art. 53 Abs. 3 und 4 (ex Art. 49 Abs. 1 lit. f i. V. m. Art. 47 Abs. 3 sowie Art. 48 Abs. 3 und 4)	Hinsichtlich des Inhalts von Art. 47 Abs. 3: Nr. 121 (ex 95)	Obligatorisch	-	Hinsichtlich des normeigenen Inhalts: § 22 Abs. 5 S. 3 BDSG i. V. m. §§ 30 ff. BBG Hinsichtlich des Inhalts von Art. 47 Abs. 3: § 23 Abs. 2 BDSG Hinsichtlich des Inhalts von Art. 48 Abs. 3: § 22 Abs. 3 BDSG; § 23 Abs. 1 S. 2 und 3 BDSG Hinsichtlich des Inhalts von Art. 48 Abs. 4: § 23 Abs. 1 S. 3 BDSG i. V. m. § 21 DRiG
Art. 54 Abs. 2 (ex Art. 49 Abs. 2)	-	Obligatorisch, sofern das Unionsrecht keine entsprechende Regelung enthält	Art. 28 Abs. 7	§ 23 Abs. 4-6 BDSG; § 22 Abs. 5 S. 3 BDSG i. V. m. § 67 BBG
Art. 55 Abs. 3 (ex Art. 51 Abs. 3)	Nr. 20 (ex 16a)	Fakultativ/ Bereichsausnahme		§ 24 Abs. 3 BDSG
Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab)		Obligatorisch	Art. 28 Abs. 2	§ 22 Abs. 2 S. 1, 3; § 38 Abs. 1 S. 1, 2
Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db)	Nr. 129 S. 3 - 5 (ex 100 S. 3 - 5)	Fakultativ	Art. 28 Abs. 3 Spstr. 1	§ 24 Abs. 1 und Abs. 4 S. 2 Nr. 1, 2; § 38 Abs. 4
Art. 58 Abs. 3 lit. b (ex Art. 53		Fakultativ	Art. 28 Abs. 3 UAbs. 1 Spstr.	§ 26 Abs. 1 S. 1, Abs. 3

Abs. 1c lit. aa)			2	
Art. 58 Abs. 4 (ex Art. 53 Abs. 2)	Nr. 129 S. 4 - 9 (ex 100 S. 4 - 9)	Obligatorisch	Art. 28 Abs. 3 UAbs. 2	VwVfG, §§ 42 f. VwGO
Art. 58 Abs. 5 (ex Art. 53 Abs. 3)	Nr. 129 S. 1 (ex 100 S. 1)	Obligatorisch	Art. 28 Abs. 3 Spstr. 3	§ 38 Abs. 1 S. 6; § 44 Abs. 2; § 12a UKlaG
Art. 58 Abs. 6 (ex Art. 53 Abs. 4)		Fakultativ	Art. 28 Abs. 3 UAbs. 1	§§ 23-26; § 38
Art. 59 S. 2 (ex Art. 54 S. 2)		Tw. obligatorisch, tw. fakultativ	Art. 28 Abs. 5	§ 26 Abs. 1 S. 1; § 38 Abs. 1 S. 7
Art. 62 Abs. 3 S. 1 Hs. 1 (ex Art. 56 Abs. 3 S. 1 Hs. 1)		Obligatorisch		
Art. 62 Abs. 3 S. 1 Hs. 2 (ex Art. 56 Abs. 3 S. 1 Hs. 2)		Fakultativ		
Art. 80 Abs. 2 (ex Art. 76 Abs. 2)	Nr. 141 (ex 112 S. 2 u. 3)	Fakultativ	Art. 28 Abs. 4 S. 1	Verbraucherschutzrecht
Art. 83 Abs. 7 (ex Art. 79 Abs. 3b)	Nr. 150 (ex 120)	Fakultativ	Art. 24; EG 55	§ 43 BDSG
Art. 83 Abs. 8 (ex Art. 79 Abs. 4)	Nr. 148 S. 4 (ex 118b)	Obligatorisch		Verfahrensgarantien nach OWiG
Art. 83 Abs. 9 (ex Art. 79 Abs. 5)	Nr. 151 (ex 120a)	Fakultativ		Thematisch § 43 BDSG; für Deutschland hat Abs. 9 aber keine Bedeutung
Art. 84 (ex Art. 79b)	Nr. 148, 149 (ex 118b, 119)	Obligatorisch	Art. 24	§ 44 BDSG
Art. 85 Abs. 1 (ex Art. 80 Abs. 1)	Nr. 153, 154 (ex 121, 121a)	Obligatorisch, unecht	Art. 9	§ 41 BDSG
Art. 85 Abs. 2	Nr. 153 (ex	Obligatorisch	Art. 9, EG 37	§ 47 RStV; Länder-

(ex Art. 80 Abs. 2)	121)			recht, z. B. § 12 RhPfLMG
Art. 86 (ex Art. 80a)	Nr. 154 (ex 121a)	Fakultativ	(EG 72)	§ 5 IFG
Art. 87 (ex Art. 80b)	-	Fakultativ	Art. 8 Abs. 7	-
Art. 88 (ex Art. 82)	Nr. 155 (ex 124)	Fakultativ	-	§ 32 BDSG
Art. 89 Abs. 2, 3 (ex Art. 83 Abs. 2, 3)	Nr. 156, 157 (ex 125, 126)	Fakultativ	11 Abs. 2; 13 Abs. 2; 32 Abs. 3	§ 20 Abs. 9 BDSG
Art. 90 (ex Art. 84)	Nr. 164 (ex 127)			
Art. 91 Abs. 2 i. V. m. Abs. 1 (ex Art. 85 Abs. 2 i. V. m. Abs. 1)	Nr. 165 (ex 128)	Fakultativ	-	Art. 137 Abs. 3 WRV i. V. m. Art. 140 GG; z.B. § 18 ff. DSG-EKD

2. EG 20 S. 1 (ex EG 16a S. 1)

Schon in den Erwägungsgründen der Datenschutz-Grundverordnung finden sich Öffnungsklauseln, insbesondere in EG 20 S. 1 (ex EG 16a S. 1). Dort nimmt die Datenschutz-Grundverordnung ihren Geltungsanspruch für den Bereich der Justiz zurück. Der Erwägungsgrund gestattet es den Mitgliedstaaten, „festzulegen, wie die Verarbeitungsvorgänge und Verarbeitungsverfahren bei der Verarbeitung personenbezogener Daten durch Gerichte und Justizbehörden im Einzelnen auszusehen haben“. Die Datenverarbeitung der Justiz unterliegt folglich nicht den materiellen Regelungen der Datenschutz-Grundverordnung, wenn die Mitgliedstaaten von dieser Regelungsfreiheit Gebrauch machen. Das gilt auch für die Datenschutzaufsicht. Entsprechend können die Mitgliedstaaten für die justizielle Tätigkeit besondere Stellen im Justizsystem mit der Datenschutzaufsicht betrauen (EG 20 S. 3 [ex EG 16a S. 3], Art. 55 Abs. 3 [ex Art. 51 Abs. 3] DSGVO).[25]

[25] Ausführlicher zu dieser Thematik auf S. 174 ff.

3. EG 27 S. 2 (ex EG 23aa S. 2): Datenschutz Verstorbener

a. Inhalt und Voraussetzungen der Öffnungsklausel bzw. Bereichsausnahme

EG 27 S. 2 (ex EG 23aa S. 2) DSGVO ermächtigt die Mitgliedstaaten, datenschutzrechtliche Bestimmungen für Daten Verstorbener vorzusehen. Für diesen Bereich reklamiert die Datenschutz-Grundverordnung also keinen eigenen Normierungsanspruch (EG 27 S. 1, 160 S. 2 Hs. 2), sondern nimmt ihn aus ihrem Regelungsbereich bewusst und ausdrücklich aus.
Auch wenn S. 2 nur von Vorschriften für die Verarbeitung der Daten Verstorbener spricht, sind davon auch Vorschriften zur Geltendmachung etwaiger Rechte Lebender erfasst, die sich auf diese Daten beziehen. Anderenfalls wäre die Datenschutz-Grundverordnung doch entgegen ihrer Ratio teilweise auf die Daten Verstorbener anwendbar. Soweit sich die Daten auch auf lebende Personen beziehen, greift die Bereichsausnahme demgegenüber nicht.[26] Vielmehr finden dann die allgemeinen Bestimmungen Anwendung.

b. Gestaltungsoptionen für das mitgliedstaatliche Recht

Von dem Regelungsspielraum für den Datenschutz Verstorbener sollte der nationale Gesetzgeber jedenfalls mittelfristig Gebrauch machen. Bislang ist dieses Regelungsfeld in besonderer Weise durch Rechtsunsicherheit gekennzeichnet.

aa) Verfassungsrechtliche und einfachrechtliche Rahmenbedingungen

Obgleich mit dem Tod die Fähigkeit zur Entfaltung der Persönlichkeit erlischt, die das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG als Keimzelle des Datenschutzrechts voraussetzt, bleibt das Persönlichkeitsrecht Verstorbener verletzbar.[27]

---

[26] Dies gilt etwa für Angaben über (schwere) erbliche Krankheiten, dazu *Dammann*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 3, Rn. 17.
[27] *Martini*, JZ 2012, 1145 (1148, 1150).

(1) Gatekeeper-Funktion der Diensteanbieter

Telemedienrechtliche Diensteanbieter haben zwar keine strafbewehrte, über den Tod hinauswirkende Stellung eines Berufsgeheimnisträgers wie des Arztes inne (§ 203 Abs. 2 StGB), die ihn auch über Tod des Vertragspartners hinaus zum Stillschweigen anhält. Gleichwohl befinden sich telemedienrechtliche Diensteanbieter in einer strukturell ähnlichen Rolle: Als „Gatekeeper" haben nur sie die Möglichkeiten, den in dem Account des verstorbenen Nutzers verborgenen Datenschatz zu heben. § 13 Abs. 4 Nr. 3 TMG verpflichtet sie, die Nutzung der Telemedien gegen die Kenntnisnahme Dritter zu schützen, Letzteren also keinen Zugang zu eröffnen.[28] Diese vertragliche Pflicht kann bei einem weiten Verständnis auch über den Tod hinaus wirken. Das gilt jedenfalls dann, wenn das Datenschutzrecht auch Daten Verstorbener als personenbezogene Daten in seinen Schutz einbezieht.

(2) Zum Personenbezug von Daten Verstorbener und ihrem verfassungsrechtlichen Schutz

Wie offen der Begriff „personenbezogene Daten" des § 3 Abs. 1 BDSG ist, ist umstritten. Richtigerweise genügt schon, dass das jeweilige Datum *zum Entstehungszeitpunkt* einen Personenbezug zu einem lebenden Menschen aufweist, um von einem personenbezogenen Datum zu sprechen.[29] Denn mit dem Tod endet der Bezug eines Datums zu einer Person nicht.
Das Verfassungsrecht stützt diese einfachgesetzliche Schutzwertung. Verstorbene können zwar den ihnen aus der Menschenwürde gemäß Art. 1 Abs. 1 GG zukommenden Achtungsanspruch nicht mehr selbst wahrnehmen. Sie gehen dadurch des verfassungsrechtlichen Schutzes der lebenslangen Persönlichkeitsentfaltung vor postmortalen Verfälschungen oder Ausspähungen als wesensgleiches Minus zum Persönlichkeitsschutz Lebender aber nicht verlus-

[28] Der vor dem LG Berlin verhandelte Fall betraf die besondere Konstellation, in der die Eltern als Erben ihres Kindes Auskunft verlangten und zugleich Sachwalter des Persönlichkeitsrechts ihres Kindes waren, LG Berlin, Urt. v. 17.12.2015 – 20 O 172/15, juris, Rn. 32.
[29] *Martini* (Fn. 27), 1148; a. A. etwa *Dammann* (Fn. 26), § 3, Rn. 17.

tig.[30] Denn der Umgang mit den Daten Verstorbener wirkt auf die Persönlichkeitsentfaltung Lebender zurück: Wer in der Erwartung leben muss, dass höchstpersönliche Sachverhalte nach seinem Tod nicht mehr geschützt sind, z. B. einem Arzt anvertraute Erkrankungen, der wird sein Verhalten zu Lebzeiten anpassen und seine Persönlichkeitsentfaltung insoweit einschränken.[31] Nur wenn der Schutz vor Ausspähungen über den eigenen Tod hinausreicht, kann der Einzelne darauf vertrauen, dass seine zu Lebzeiten geschützten persönlichen Daten, sei es die heimliche Liebschaft, seien es Erwägungen zu Vererbungsstrategien, auch nach dem Ableben geheim bleiben und nicht einem Angehörigen oder sonstigem Dritten offenbar werden.[32] Der Persönlichkeitsschutz Verstorbener ist integraler Bestandteil des Persönlichkeitsschutzes Lebender. Die Würde des Einzelnen wirkt insoweit post mortem nach. Im Verfassungsrecht ist daher ein postmortales Persönlichkeitsrecht anerkannt.[33]

bb) Rechtspolitische Handlungsempfehlungen

Rechtspolitisch ist es sinnvoll, Diensteanbieter zu verpflichten, ihre Nutzer schon zu Lebzeiten, beispielsweise bei der Eröffnung eines Accounts und bei fehlender Erklärung in gewissen Zeitabständen, zu einer Verfügung darüber zu animieren, wie der Diensteanbieter im Todesfall mit den Daten verfahren soll:[34] So kann der Nutzer dann etwa zwischen der Herausgabe seiner Account-Daten an bestimmte Personen, der unverzüglichen Löschung seiner Daten oder der Umwandlung in ein digitales Kondolenzbuch wählen. Bislang kann der Nutzer das bei den meisten seiner Accounts nicht regeln. § 13 Abs. 4 TMG könnte beispielsweise um eine Nr. 3a ergänzt werden, die den Diensteanbietern abringt, dass „die Nutzer die Möglichkeit haben, Regelun-

[30] *Martini*, Wenn ich einmal soll scheiden…Der digitale Nachlass und seine unbewältigte rechtliche Abwicklung, in: Hill/Martini/Wagner (Hrsg.), Facebook, Google & Co, 2013, S. 77 (100 ff.).
[31] *Martini* (Fn. 30), S. 108; so auch *Herzog*, NJW 2013, 3745 (3749).
[32] *Martini* (Fn. 27), 1151 f.
[33] A. A. *Klas/Möhrke-Sobolewski*, NJW 2015, 3473 (3477).
[34] *Martini* (Fn. 30), S. 122 f.

gen für die Verwendung ihrer personenbezogenen Daten nach dem Tod zu treffen."

Um die Nutzer dazu zu animieren, von der Möglichkeit tatsächlich Gebrauch zu machen, sollte die Regelung um einen § 13 Abs. 4 Nr. 3a S. 2 TMG-E ergänzt werden: „Sofern die Nutzer keine Vorgaben für den Todesfall getroffen haben, fordern die Diensteanbieter die Nutzer in regelmäßigen Abständen zu einer entsprechenden Erklärung auf, soweit der jeweilige Nutzer dem nicht widerspricht." Für den Fall, dass die Nutzer von dieser Regelung zu Lebzeiten keinen Gebrauch machen, ist eine gesetzgeberische Privacy-by-default-Regelung (vgl. auch Art. 25 Abs. 2 DSGVO) sachgerecht, welche die Verfügungslücke durch eine normative, dem Persönlichkeitsschutz hinreichend gerecht werdende Wertungsentscheidung ausfüllt.

Dem postmortalen Persönlichkeitsrecht adäquat erscheint die Wertung, dass Account-Daten – soweit sie nicht zumindest auch vermögensrechtliche Positionen betreffen – im Zweifel nicht an die Angehörigen herauszugeben sind. Hierfür böte sich eine Novellierung des § 13 Abs. 4 TMG an: „Hat der verstorbene Nutzer keine oder eine ablehnende Verfügung über den Zugang zu seinen Daten getroffen, können Angehörige nur die datenschutzrechtlichen Rechte in Bezug auf im Internet öffentlich verfügbare personenbezogene Informationen wahrnehmen. Im Übrigen darf der Dienstanbieter keinen Zugang gewähren."[35] Alternativ wäre auch folgender Wortlaut denkbar: „(…) Zugang nur gewähren, soweit dies zur Wahrnehmung vermögensrechtlicher Rechte der Erben erforderlich ist."

Führt man sich vor Augen, dass die gesetzliche Hinweispflicht gegenüber Diensteanbietern zu Lebzeiten des Nutzers eintritt, lässt sich zwar grundsätzlich hinterfragen, ob die mitgliedstaatliche Norm dann noch als Ausfüllung der Öffnungsklausel bzw. Bereichsausnahme des EG 27 (ex EG 23aa) DSGVO anzusehen ist. Diese Zweifel überzeugen aber nicht: Die Hinweispflicht ist allein auf die Verarbeitung der Daten Betroffener gerichtet, wenn sie tot sind. Sinn und Zweck einer solchen Norm wären also auf den Zeitraum nach Ableben des Nutzers gerichtet und füllen somit die Öffnungsklausel aus.

[35] *Martini* (Fn. 30), S. 113 ff.

4. Art. 4 Nr. 7 (ex Nr. 5): Definition „Verantwortlicher“

a. Struktur und Entstehungshintergrund

Art. 4 Nr. 7 (ex Nr. 5) DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, den Verantwortlichen oder spezifische Kriterien für seine Benennung zu bestimmen, wenn sich die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten aus mitgliedstaatlichem Recht ergeben. Eine fast wortlautgetreue Bestimmung findet sich bereits in Art. 2 lit. d DSRL. Die Möglichkeit der Benennung eines Verantwortlichen soll der Komplexität vieler Verarbeitungsvorgänge und deren Umsetzung in der Praxis Rechnung tragen.[36]

b. Qualifikation der Öffnungsklausel

Die Norm markiert einen fakultativen Regelungsbedarf. Sie gibt Mitgliedstaaten die Möglichkeit, unter bestimmten Voraussetzungen den Verantwortlichen näher zu benennen, also zu konkretisieren. Dies gilt gerade für öffentliche und nicht-öffentliche Stellen in der überkommenen deutschen Unterscheidung und für die Frage der Aufrechterhaltung der Differenzierung zwischen diesen Kategorien.

c. Voraussetzungen der Öffnungsklausel

aa) Verantwortlicher

Verantwortlicher ist derjenige, der über die Zwecke und Mittel der Verarbeitung entscheidet (Art. 4 Nr. 7 DSGVO). Dieses Merkmal grenzt den Verantwortlichen vom Auftragsdatenverarbeiter ab.[37]

bb) Benennung des Verantwortlichen

Wo die Mitgliedstaaten Zweck und Mittel der Verarbeitung bestimmen können, eröffnet Art. 4 Nr. 7 (ex Art. 4 Nr. 5) DSGVO ihnen auch die Möglichkeit, den Verantwortlichen zu benennen. Die englische Formulierung des Art. 4 Nr. 7 Hs. 2 (ex Art. 4 Nr. 5 Hs. 2) DSGVO „(…) *where* the purposes and means of such processing are determined by (…) Member State law (…)“

---

[36] *Dammann/Simitis*, EG-Datenschutzrichtlinie, 1997, Art. 2, Rn. 14.
[37] *Ehmann/Helfrich*, EG-Datenschutzrichtlinie, 1999, Art. 2, Rn. 44.

zeigt auf, dass die Benennung nur dort möglich ist, wo die Datenschutz-Grundverordnung überhaupt Öffnungsklauseln für die Bestimmung von Zwecken und Mitteln der Verarbeitung vorhält. Ansonsten stünde eine Bestimmung der Zwecke und Mittel durch mitgliedstaatliches Recht aufgrund des abschließenden Charakters der Verordnung nämlich gar nicht offen.[38] Diese Möglichkeit eröffnet unter bestimmten Voraussetzungen etwa Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO[39] i. V. m. Art. 6 Abs. 3 DSGVO.

Die Öffnungsklausel des Art. 4 Nr. 7 (ex Art. 4 Abs. 5) DSGVO erstreckt sich nur auf den *Verantwortlichen*, nicht auf die Verarbeitung insgesamt, wie bereits aus dem englischen Begriff „controller" deutlich wird. Hinsichtlich des Verantwortlichen können die Mitgliedstaaten sowohl konkret Verantwortliche bestimmen als auch spezifische Kriterien festlegen, mittels derer der Verantwortliche bestimmt werden soll. Damit ist auch eine Kategorisierung der Verantwortlichen eröffnet. Diese könnte etwa in der Aufrechterhaltung der im deutschen Datenschutzrecht bestehenden Unterscheidung zwischen öffentlichen und nicht-öffentlichen Stellen liegen, soweit Öffnungsklauseln Spielräume für die Mitgliedstaaten markieren. Beispielhaft lässt sich hier etwa § 3 BMG i. V. m. §§ 1 f. BMG nennen, dessen Normadressaten explizit Meldebehörden als durch Landesrecht bestimmte Behörden sind.[40]

Hinsichtlich der bisher abweichenden Terminologie der Verarbeitung im deutschen Datenschutzrecht[41] sagt Art. 4 Nr. 7 (ex Art. 4 Nr. 5) DSGVO nichts aus. Die Definition der Verarbeitung findet sich in Art. 4 Nr. 2 (ex Art. 4 Nr. 3) DSGVO und enthält keine Öffnungsklausel. Allerdings kann sich aus anderen Öffnungsklauseln, wie etwa aus Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO, ergeben, dass die Beibehaltung der deutschen Differenzierung in die Schritte des Erhebens, Verarbeitens und Nutzens zulässig ist.[42]

---

[38] Vgl. hierzu S. 4.
[39] Vgl. S. 27.
[40] Zur Möglichkeit der Aufrechterhaltung von § 3 BMG vgl. S. 36.
[41] So unterscheidet etwa § 3 Abs. 3, 4 BDSG die Erhebung von der Verarbeitung, während Art. 4 Nr. 2 (ex Art. 4 Nr. 3) DSGVO die Erhebung unter den Verarbeitungsbegriff stellt.
[42] Siehe S. 372.

5. Art. 4 Nr. 9 (ex Art. 4 Nr. 7): Definition „Empfänger“

Art. 4 Nr. 9 DSGVO nimmt eine Definition des Begriffs „Empfänger“ in die Datenschutz-Grundverordnung auf. Das deutsche Recht regelte den Inhalt dieses datenschutzrechtlichen Topos bisher in § 3 Abs. 8 BDSG. Im Gefolge der unmittelbaren Anwendbarkeit der Datenschutz-Grundverordnung wird diese Regelung obsolet. Die Union lässt den Mitgliedstaaten jedoch in geringem Umfang Regelungsspielraum: Soweit die Mitgliedstaaten Behörden durch ihr eigenes Recht einen Untersuchungsauftrag zuweisen, der ihnen den Zugang zu personenbezogenen Daten verschafft, gelten sie nicht als Empfänger. Die Mitgliedstaaten können durch die Zuweisung eines Untersuchungsauftrages also – in beschränktem Umfang – über die Reichweite des Begriffs „Empfänger“ entscheiden.

6. Art. 6 Abs. 1 UAbs. 1 lit. c, e i. V. m. Abs. 2 (ex Abs. 2a), 3: allgemeine Zulässigkeit – allgemeine Öffnungsklauseln für Verarbeitungsgrundlagen

a. Struktur und Entstehungshintergrund

Art. 6 Abs. 1 DSGVO regelt allgemein die Rechtmäßigkeit der Datenverarbeitung: Die Verarbeitung ist nur in den in Art. 6 Abs. 1 DSGVO abschließend genannten Fällen[43] rechtmäßig. Die Datenschutz-Grundverordnung greift somit das Prinzip des Verbots mit Erlaubnisvorbehalt[44] auf, das schon Art. 7 DSRL bzw. § 4 Abs. 1 BDSG enthalten. Art. 6 Abs. 2 (ex Abs. 2a) und Abs. 3 S. 3 DSGVO geben den Mitgliedstaaten allgemeine Öffnungsklauseln an die Hand, um die in Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO geregelten Fälle näher zu konturieren. Demnach können Mitgliedstaaten sowohl bereits bestehende Regelungen erhalten als auch neue, spezifischere Regelungen erlassen, um die Anwendung der Vorschriften der Verordnung hinsichtlich der Verarbeitung von personenbezogenen Daten in Übereinstimmung mit Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO anzupassen, also eine Datenverar-

[43] So der *EuGH* bereits für Art. 7 RL 95/46/EG, Rs. C-468/10 und C-469/10, Slg. 2011, I-12181, Rn. 30 – ASNEF und FECMD.
[44] *Kühling/Seidel/Sivridis*, Datenschutzrecht, 3. Aufl., 2015, Rn. 204.

beitung zur Erfüllung einer rechtlichen Verpflichtung bzw. im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt zu ermöglichen. Damit sind die allgemeinen Öffnungsklauseln in Art. 6 Abs. 1 UAbs. 1 lit. c, e i. V. m. Abs. 2 (ex Abs. 2a), 3 DSGVO von zentraler Bedeutung, um die breite Palette der Datenverarbeitung im öffentlichen Interesse im bereichsspezifischen Datenschutzrecht in Deutschland aufrechterhalten zu können.

Die Vorgaben des Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO entsprechen denjenigen der Vorgängerregelung des Art. 7 lit. c bzw. e DSRL. Anders als die Datenschutz-Richtlinie bestimmt die Datenschutz-Grundverordnung in Art. 6 Abs. 3 S. 1 DSGVO nun explizit, dass die Verarbeitung personenbezogener Daten i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. c, e DSGVO einer *rechtlichen* Grundlage bedarf.[45] EG 41 (ex EG 31a) DSGVO präzisiert, dass es sich insoweit *nicht* um ein Parlamentsgesetz handeln muss. Das Erfordernis einer *gesetzlichen* Grundlage ergibt sich aber schon bisher aus Art. 8 Abs. 2 GrCh bzw. Art. 2 GG i. V. m. Art. 1 GG.[46] Die Voraussetzungen an die nationalen Regelungen zur Konkretisierung der Bestimmungen aus Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO fächern Art. 6 Abs. 2 (ex Abs. 2a) DSGVO sowie Art. 6 Abs. 3 S. 2 ff. DSGVO weiter auf.

b. Qualifikation der Öffnungsklausel

Art. 6 Abs. 2 (ex Abs. 2a) und Abs. 3 S. 2 f. DSGVO sind allgemeine Öffnungsklauseln. Sie gestatten Mitgliedstaaten, die Regelungen der Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO unter den Voraussetzungen des Abs. 2 (ex Abs. 2a) und Abs. 3 S. 3 zu konkretisieren, d. h. anzupassen und auszufüllen. Art. 6 Abs. 2 (ex Abs. 2a) und Abs. 3 S. 3 DSGVO eröffnen eine fakultative Regelungsmöglichkeit.

Macht der nationale Gesetzgeber von diesen Spielräumen Gebrauch, öffnet sich ihm ein weiteres Fenster zu einem nationalstaatlichen Regelungsspielraum: Die grundsätzlich nach Art. 35 (ex Art. 33) DSGVO bestehende Pflicht zur Datenschutz-Folgenabschätzung ist gemäß Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO aufgehoben, es sei denn, der nationale Gesetzgeber hält es

[45] Vgl. *Schneider*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, Syst. B Europäische Datenschutzrichtlinie, Rn. 93 f.

[46] *Schneider* (Fn. 45), Syst. B Europäische Datenschutzrichtlinie, Rn. 93 f.

für erforderlich, mittels einer Rückausnahme eine Folgenabschätzung vorzusehen[47]. Die Aufsicht über diese Tätigkeit ist von den Vorschriften über die federführende Behörde sowie das Prinzip der zentralen Anlaufstelle befreit (Art. 55 Abs. 2 [ex Art. 51 Abs. 2], EG 128 S. 1 [ex EG 98 S. 1] DSGVO).[48] Adressat der mitgliedstaatlichen Erlaubnis des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO können sowohl öffentliche als auch nicht-öffentliche Stellen sein. Während Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO sich gleichermaßen an öffentliche wie nicht-öffentliche Stellen richtet, sind Adressaten des Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1 DSGVO überwiegend öffentliche Stellen, da es hier um die Wahrnehmung von Aufgaben geht, die im öffentlichen Interesse liegen. Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 2 DSGVO richtet sich an solche öffentliche wie nicht-öffentliche Stellen, die in Ausübung der ihnen übertragenen hoheitlichen Gewalt handeln.

c. Voraussetzungen der Öffnungsklauseln

aa) Gesetzliche Verpflichtung zur Datenverarbeitung, Abs. 1 UAbs. 1 lit. c

Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO bestimmt die Rechtmäßigkeit der Verarbeitung in den Fällen, in denen die Verarbeitung für die Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Als zusätzliche Voraussetzung muss die Rechtsgrundlage, auf die sich die Verarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO stützt (also die rechtliche Verpflichtung zur Verarbeitung) ein im öffentlichen Interesse liegendes Ziel verfolgen. Dies leitet sich aus Art. 6 Abs. 3 S. 4 DSGVO ab. Er fordert – nach seinem systematischen Zusammenhang zu Art. 6 Abs. 3 S. 1 DSGVO – sowohl bei Art. 6 Abs. 1 UAbs. 1 lit. c als auch lit. e DSGVO ein entsprechendes öffentliches Interesse. Dass Art. 6 Abs. 1 UAbs. lit. e DSGVO – anders als Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO – auch noch selbst auf das öffentliche Interesse Bezug nimmt, ist insoweit eine Dopplung, die aber nicht das Erfordernis eines öffentlichen Interesses auch für Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO in Frage stellt.

[47] Dazu S. 89.
[48] Dazu S. 242.

i. Rechtliche Verpflichtung

Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO entspricht Art. 7 lit. c DSRL. Beide Vorschriften eröffnen Mitgliedstaaten die Möglichkeit, eine rechtliche Verpflichtung zu begründen bzw. bereits bestehende rechtliche Verpflichtungen aufrechtzuerhalten. Denn aus Art. 6 Abs. 3 S. 1 DSGVO ist herauszulesen, dass Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO alleine, ohne gesonderte Rechtsgrundlage, nicht ausreicht, um eine Verarbeitung zu rechtfertigen. Solche rechtlichen Verpflichtungen können in allen Formen des objektiven Rechts bestehen und folglich sowohl dem formellen wie materiellen Recht erwachsen, d. h. die rechtliche Verpflichtung kann sich nicht nur aus Bundes- und Landesgesetzen sondern etwa auch aus Rechtsverordnungen ergeben.[49]

ii. Begriff der Erforderlichkeit in Art. 6 Abs. 1 UAbs. 1 lit. c

Der Begriff der Erforderlichkeit i. S. d. DSRL ist nach der EuGH-Rechtsprechung ein autonomer Begriff des Unionsrechts, der nicht der Interpretationsmacht der Mitgliedstaaten unterliegt. Das ergibt sich aus der bereits durch die DSRL verfolgten Harmonisierung des Datenschutzrechts und dem Bestreben, ein gleichwertiges Schutzniveau in allen Mitgliedstaaten herzustel-

[49] *Brühann*, in: Grabitz/Hilf (Hrsg.), EU-Recht, 57. Erg.-Lfg., 2015, Art. 7 Datenschutzrichtlinie, Rn. 16; *Scholz/Sokol*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 4, Rn. 9 ff. Fraglich ist, ob dies auch für den normativen Teil von Tarifverträgen gilt. Die wohl überwiegende Meinung in Deutschland geht bisher davon aus, dass auch diese als Rechtsvorschrift, aus denen eine rechtliche Verpflichtung erwachsen kann, gelten; vgl. *BAG*, Az. 7 ABR 8/95; *Scholz/Sokol* (Fn. 49), § 4, Rn. 10; *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 4, Rn. 7; *Bäcker*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 4 BDSG, Rn. 13. Dieser Ansatz ist kritisch zu bewerten, da dadurch auch eine Unterschreitung des Datenschutzstandards des BDSG möglich wäre; vgl. *Scholz/Sokol* (Fn. 49), § 4, Rn. 17. Im Übrigen bleiben vor dem Hintergrund der Anforderungen des Art. 8 Abs. 2 GrCh durchaus nicht unerhebliche Restzweifel, da die danach erforderliche Rechtsgrundlage eine demokratisch legitimierte Rechtsnorm erfordert. Das Europäische Parlament hatte einen Zusatz über die insoweit erfolgende Erfassung von Tarifverträgen in EG 36 ergänzt. Dieser Zusatz wurde jedoch nicht in die endgültige Fassung der DSGVO übernommen, was dafür spricht, dass Tarifverträge nicht als rechtliche Verpflichtung i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO gelten sollen. Allerdings eröffnet gerade Art. 88 Abs. 1 (ex Art. 82 Abs. 1) DSGVO den Mitgliedstaaten Spielraum, eine Datenverarbeitung auch auf der Grundlage von Kollektivvereinbarungen zu eröffnen, was dafür spricht, dass die Verordnung insoweit auch Tarifverträge als ausreichende rechtliche Grundlage ansieht.

len. Der Erforderlichkeitsgrundsatz i. S. d. DSRL ist dergestalt auszulegen, dass er dem Ziel der DSRL aus Art. 1 Abs. 1, dem Schutz der Grundrechte und Grundfreiheiten und insbesondere dem Schutz der Privatsphäre, bei der Verarbeitung personenbezogener Daten entspricht.[50] Wenn mit dieser Argumentation der Erforderlichkeitsbegriff bereits in der DSRL der Interpretation der Mitgliedstaaten entzogen war, gilt dies erst recht für die unmittelbar geltende Datenschutz-Grundverordnung. Der Begriff der Erforderlichkeit ist daher anhand des Ziels der Datenschutz-Grundverordnung i. S. d. Art. 1 Abs. 2 DSGVO, der Art. 1 Abs. 1 DSRL entspricht, auszulegen.

iii. Öffentliches Interesse

Der Begriff des öffentlichen Interesses räumt den Mitgliedstaaten einen Wertungsspielraum ein. Das ergibt sich zunächst aus dem Wortlaut des Art. 6 Abs. 2 (ex Art. 6 Abs. 2a) DSGVO. Er gesteht den Mitgliedstaaten für die Fälle des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO zu, spezifischere Regelungen für die Anpassung anzuwendender Verordnungsregelungen aufrechtzuerhalten oder zu erlassen, und zwar gerade, indem präzisere spezifische Voraussetzungen für die Verarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO festgelegt werden. Solche Voraussetzungen können auch Voraussetzungen an das öffentliche Interesse sein. Dieses Ergebnis unterstützt EG 10 S. 4 (ex EG 8 S. 4) DSGVO, der den Mitgliedstaaten explizit einen Spielraum zur Spezifizierung ihrer nationalen Vorschriften zugesteht. Nach EG 10 S. 5 (ex EG 8 S. 5) DSGVO schließt die Verordnung die Mitgliedstaaten nicht davon aus, die Umstände der spezifischen Verarbeitungssituationen einschließlich der Bedingungen zu definieren, unter denen die Verarbeitung personenbezogener Daten rechtmäßig sein soll. Schließlich oblag auch die Interpretation des öffentlichen Interesses in Art. 7 lit. e DSRL ausschließlich den Mitgliedstaaten.[51] Daran ändert auch nichts, dass die Datenschutz-Grundverordnung im Unterschied zur DSRL unmittelbar anwendbar ist.
Im Sinne einer einheitlichen Anwendung des Unionsrechts könnte man zwar davon ausgehen, dass das öffentliche Interesse nicht der Auslegung durch die

[50] *EuGH*, Rs. C-524/06, Slg. 2008, I-9705 Rn. 52 – Huber.
[51] *Brühann* (Fn. 49), Art. 7 Datenschutzrichtlinie, Rn. 18.

Mitgliedstaaten zugänglich, sondern unionsrechtautonom zu definieren ist. Allerdings entfaltete auch die DSRL bereits weitgehend vollharmonisierende Wirkung: Von dem Inhalt der Zulässigkeitsvoraussetzungen einer Datenverarbeitung durften nationale Regelungen weder negativ noch positiv abweichen.[52] Schließlich wird die Konkretisierung des öffentlichen Interesses durch die Mitgliedstaaten auch der Tatsache gerecht, dass die öffentlichen Interessen von Staat zu Staat unterschiedlich sein können. Demnach ermöglicht die Öffnungsklausel des Art. 6 Abs. 2 (ex Art. 6 Abs. 2a) DSGVO i. V. m. Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO nicht nur, durch nationales Recht Rechtsgrundlagen für die Verarbeitung von personenbezogenen Daten aus Gründen des öffentlichen Interesses zu schaffen, sondern dieses öffentliche Interesse auch näher zu konkretisieren. Das bedeutet, dass sich hinsichtlich dieses Begriffs keine Veränderungen gegenüber der DSRL ergeben. Als öffentliches Interesse gilt im deutschen Recht etwa der gesamte Bereich der Ordnungsverwaltung (wie die Regelung des Straßenverkehrs), der Leistungsverwaltung (wie die Daseinsvorsorge) sowie der Lenkungsverwaltung, wie die Förderung kultureller Angebote (z. B. Theater).[53]

bb) Öffentliches Interesse und hoheitliche Gewalt, Abs. 1 lit. e.

Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO, der Art. 7 lit. e DSRL entspricht, gestattet die Verarbeitung von personenbezogenen Daten, wenn sie für die Wahrnehmung einer Aufgabe (i) erforderlich ist (ii.), die im öffentlichen Interesse liegt, oder in Ausübung hoheitlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde (iii).

i. Wahrnehmung von Aufgaben im öffentlichen Interesse

Für das öffentliche Interesse gilt das zu Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO Gesagte.[54] Daraus ergibt sich, dass die Mitgliedstaaten die Aufgaben, die im öffentlichen Interesse liegen, ebenfalls selbst festlegen können.[55]

---

[52] *EuGH*, Rs. C-468/10 und C-469/10, Slg. 2011, I-12181 Rn. 30 – ASNEF und FECMD; hierzu *Kühling*, EuZW 2012, 281 (282).
[53] *Maurer*, Allgemeines Verwaltungsrecht, 18. Aufl., 2011, § 1, Rn. 12 ff.
[54] Vgl. S. 31.
[55] *Brühann* (Fn. 49), Art. 7 Datenschutzrichtlinie, Rn. 18.

ii. Erforderlichkeit

Für die Erforderlichkeit gilt das zu Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO Gesagte.[56]

iii. Übertragung hoheitlicher Gewalt

EG 45 S. 6 (ex EG 36 S. 6) DSGVO stellt den Mitgliedstaaten frei, wer Beliehener der hoheitlichen Gewalt sein kann, d. h. ob es sich hier um eine öffentliche Stelle oder eine private Stelle handeln soll. Für die Übertragung hoheitlicher Gewalt i. S. d. Art. 7 lit. e DSRL ist ein förmlicher Rechtsakt notwendig.[57] Aus dem Text der Datenschutz-Grundverordnung ergibt sich keine Abweichung von diesem Erfordernis; Art. 7 lit. e DSRL und Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO weisen in dieser Hinsicht denselben Wortlaut auf.[58] In Deutschland ist die Übertragung hoheitlicher Befugnisse an Privatpersonen, die sog. Beleihung, ebenso an einen förmlichen, auf gesetzlicher Grundlage erfolgenden Rechtsakt gebunden.[59] In dieser Hinsicht ergeben sich für Deutschland also keine Veränderungen im Prozess der Verleihung von hoheitlichen Befugnissen.

cc) Allgemeine Öffnungsklausel, Art. 6 Abs. 2 (ex Art. 6 Abs. 2a)

Art. 6 Abs. 2 (ex Art. 6 Abs. 2a) DSGVO erlaubt es Mitgliedstaaten, bereits bestehende spezifischere Vorschriften aufrechtzuerhalten oder solche Vorschriften zu erlassen, um die Anwendung von Verordnungsbestimmungen, welche die Verarbeitung personenbezogener Daten regeln, in Übereinstimmung mit Art. 6 Abs. 1 UAbs. 1 lit c und e DSGVO anzupassen. Die Vorschriften müssen dazu präzise spezifische Voraussetzungen für die Verarbeitung und andere Maßnahmen zur Sicherstellung einer Verarbeitung nach Recht und Gesetz, einschließlich anderer spezieller Verarbeitungssituationen in Kapitel IX der DSGVO, bestimmen. Die *spezifische* Regelung muss *spezifische* Voraussetzungen und andere Maßnahmen zur Sicherung einer Verar-

[56] Vgl. S. 30.
[57] *Brühann* (Fn. 49), Art. 7 Datenschutzrichtlinie, Rn. 18.
[58] „(…) in excercise of official authority vested in the controller (…)".
[59] Vgl. *Kiefer*, LKRZ 2009, 441 (443).

beitung nach Recht und Gesetz hinsichtlich der Datenverarbeitung in Übereinstimmung mit Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO *präziser* regeln. Als Maßnahmen zur Sicherstellung einer Verarbeitung nach Recht und Gesetz führt EG 45 S. 6 (ex EG 36 S. 5) DSGVO beispielhaft Zweckbegrenzungen und Speicherfristen an. Die Norm eröffnet den Mitgliedstaaten einen weiten Spielraum hinsichtlich der Ausgestaltung der zu konkretisierenden Vorschriften. Die Bedingungen, wann eine Verarbeitung nach Recht und Gesetz stattfindet, können die Mitgliedstaaten namentlich innerhalb des durch die Öffnungsklauseln zugewiesenen Spielraums präzisieren, vgl. EG 10 S. 5 (ex EG 8 S. 5) DSGVO. Als ein Anforderungsmerkmal für eine Verarbeitung nach Recht und Gesetz nennt EG 39 (ex EG 30) DSGVO etwa den Transparenzgrundsatz, welcher auch dem deutschen Datenschutzrecht zugrunde liegt.[60]

dd) Voraussetzungen des Art. 6 Abs. 3

Art. 6 Abs. 3 S. 1 DSGVO fordert eine Rechtsgrundlage für Datenverarbeitungen nach Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO. Das Erfordernis einer gesetzlichen Grundlage ergibt sich allerdings bereits aus Art. 8 Abs. 2 GrCh bzw. Art. 2 GG i. V. m. Art. 1 GG,[61] so dass hier keine Änderungen zu beachten sind. Die Rechtsgrundlage für die Verarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO *muss* (im Englischen „shall“) den Verarbeitungszweck festsetzen, Art. 6 Abs. 3 S. 2 DSGVO. Art. 6 Abs. 3 S. 3 DSGVO führt eine nicht abschließende Reihe von spezifischen Bestimmungen zur Anpassung der Anwendbarkeit der Bestimmungen der Datenschutz-Grundverordnung an, die die Rechtsgrundlage nach Art. 6 Abs. 3 S. 1 DSGVO fakultativ enthalten kann, u. a. generelle Bedingungen hinsichtlich der Rechtmäßigkeit der Datenverarbeitung durch den Verantwortlichen, die Art der Daten, die verarbeitet werden sollen, und Bestimmungen zur Zweckbegrenzung. Diese Bestimmungen sind allerdings nicht zwingend in die nationalen Regelungen aufzunehmen. Zwar hat der Zweckbindungsgrundsatz keine explizite Normierung im deutschen Recht erfahren, taucht allerdings als Leitbild in einer Vielzahl von

[60] *Kühling/Seidel/Sivridis* (Fn. 44), Rn. 292.
[61] *Schneider* (Fn. 45), Syst. B Europäische Datenschutzrichtlinie, Rn. 93 f.

Vorschriften innerhalb und außerhalb des BDSG auf und ist damit fester Bestandteil des deutschen Datenschutzrechts.[62] Die Anforderungen an eine Erlaubnisnorm gem. § 4 Abs. 1 BDSG setzen bereits jetzt voraus, dass die Zwecksetzung in der Norm enthalten ist.[63] Ferner ist der Zweckbindungsgrundsatz primärrechtlich in Art. 8 Abs. 2 GrCh sowie sekundärrechtlich u. a. in Art. 6 lit. b DSRL verankert. Hier besteht also kein spezifischer Anpassungsbedarf in den allgemeinen und jeweiligen sektorspezifischen Vorgaben.
Entscheidend ist jedoch, dass die Rechtsgrundlage, aus der sich eine rechtliche Verpflichtung nach Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO ergibt, gemäß Art. 6 Abs. 3 S. 4 DSGVO einem öffentlichen Interesse dienen *muss*. Auch an eine Datenverarbeitung auf Grundlage von Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO ist daher die Anforderung zu stellen, dass diese aus Gründen eines öffentlichen Interesses vorgenommen wird. Ein solches explizites Gebot hinsichtlich der rechtlichen Verpflichtung zum Umgang mit Daten findet sich im deutschen Datenschutzrecht bisher nicht. Gem. § 4 Abs. 2 S. 2 Nr. 1 Alt. 2 BDSG etwa reicht für die Zulässigkeit der Erhebung von personenbezogenen Daten ohne Mitwirkung des Betroffenen aus, dass eine rechtliche Vorschrift dies zwingend voraussetzt. Das Vorliegen eines öffentlichen Interesses ist keine explizite Voraussetzung hierfür. Es können demnach nur solche rechtlichen Vorschriften aufrechterhalten oder neu geschaffen werden, die einem öffentlichen Interesse dienen. Das aber wird regelmäßig der Fall sein, da andernfalls der Grundrechtseingriff einer Verarbeitungspflicht ohnehin nicht gerechtfertigt wäre.
Im Übrigen verlangt Art. 6 Abs. 3 S. 4 DSGVO, dass die von der rechtlichen Grundlage erlaubte Verarbeitung verhältnismäßig zum verfolgten legitimen Ziel ist. Dabei handelt es sich um eine allgemeine Verhältnismäßigkeitsanforderung, die bereits jetzt grundrechtlich vorgegeben ist.

[62] *Kühling/Seidel/Sivridis* (Fn. 44), Rn. 286.
[63] *Gola/Klug/Körffer* (Fn. 49), § 4, Rn. 8.

d. Abgleich mit dem bestehenden nationalen Recht am Beispiel des § 13 Abs. 1 BDSG

§ 13 Abs. 1 BDSG erlaubt eine Erhebung von personenbezogenen Daten durch öffentliche Stellen dann, wenn die Kenntnis der Daten zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Damit entspricht die Norm in großen Teilen der Vorgabe des Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1 DSGVO – mit dem Unterschied, dass § 13 Abs. 1 BDSG explizit nur auf öffentliche Stellen anwendbar ist. Daneben bestehen zahlreiche bereichsspezifische Normen, die die Datenerhebung und Verarbeitung zur Wahrnehmung öffentlicher Aufgaben regeln, wie etwa die Bestimmungen des § 3 BMG i. V. m. § 2 Abs. 1, 2 BMG.

e. Handlungsmöglichkeiten am Beispiel des § 13 Abs. 1 BDSG

Bei einer Betrachtung des § 13 Abs. 1 BDSG stellt sich die Frage, ob die Norm die Voraussetzungen des Art. 6 DSGVO erfüllt. Insbesondere könnte es an einer nötigen Spezifikation bzw. Präzisierung mangeln. Die Formulierungen in Art. 6 Abs. 2 (ex Art. 6 Abs. 2a) DSGVO („spezifischere Bestimmungen [...] beibehalten oder einführen“ / „maintain or introduce *more specific* provisions“ sowie „spezifische Anforderungen [...] präziser bestimmen“ / „determining *more precisely specific* requirements“) deuten jedenfalls daraufhin, dass die Normen ein „Mehr“ an Regelungsgehalt als die Normen der Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO beinhalten müssen. Nicht ausreichend kann demnach eine Regelung sein, die lediglich die Vorgaben aus Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO wiederholt. Gleichzeitig ist der Wortlaut der Öffnungsklausel relativierend gehalten, spricht er doch lediglich von „spezifischeren Bestimmungen“[64] und davon, „spezifische Anforderungen (…) präziser [zu] bestimmen“[65]. Daraus lässt sich noch keine Aussage über die nötige Reichweite der Spezifizierung und Präzisierung ableiten. EG 45 S. 2 (ex EG 36 S. 2) DSGVO stellt hierzu klar, dass kein spezifisches Gesetz für jeden individuellen Verarbeitungsvorgang nötig ist. Es soll demnach auch ausreichen, wenn ein Gesetz Basis für mehrere Verarbeitungsvor-

[64] „(…) more specific provisions (…)“.
[65] „(…) determining more precisely specific requirements (…)“.

gänge i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO ist. Das spricht dafür, dass die Normen um eine Anwendung für eine Mehrzahl von Fällen zu ermöglichen, abstrakt gehalten werden können.
Hinzu kommt, dass der Wortlaut des Art. 6 Abs. 3 DSGVO, demzufolge die rechtliche Grundlage für solche Verarbeitungen spezifischere Regelungen enthalten *kann*, wie etwa *generelle* Bedingungen über die Rechtmäßigkeit der Datenverarbeitung durch den Verantwortlichen oder die Art der Daten, die verarbeitet werden dürfen, den Mitgliedstaaten Handlungsbefugnisse bloß eröffnet, sie aber nicht dazu zwingt, diese auch auszuüben.
Daraus ist zu schließen, dass die Mitgliedstaaten nach Art. 6 Abs. 2 (ex Art. 6 Abs. 2a) DSGVO zwar keine Regelungen erlassen können, die rein den Wortlaut der Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO wiedergeben. Sollten diese Regelungen die genaueren Umstände aber präzisieren, sind die Anforderungen aus Art. 6 Abs. 2 (ex Art. 6 Abs. 2a) DSGVO erfüllt. Das „Mehr“ an Präzision in den nationalen Normen muss demnach nicht sehr groß sein. Aus dem Zusammenspiel von Art. 6 Abs. 2 (ex Art. 6 Abs. 2a) und Abs. 3 DSGVO könnte man sogar schließen, dass eine allgemeine, letztlich wiederholende Bestimmung zu Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO in einem allgemeinen datenschutzrechtlichen Teil zulässig wäre und nur im Falle einer bereichsspezifischen Regelung aus der Konkretisierungsoption des Art. 6 Abs. 3 DSGVO eine (sehr moderate) Konkretisierungspflicht des Art. 6 Abs. 2 (ex Art. 6 Abs. 2a) DSGVO erwächst.
Danach erfüllt § 13 Abs. 1 BDSG die Voraussetzungen der Art. 6 Abs. 3 DSGVO womöglich sogar, obwohl die Norm keinen signifikanten Regelungsgehalt enthält, der über Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO hinausgeht. § 13 Abs. 1 BDSG könnte daher zulässigerweise aufrechterhalten werden. Allerdings bleiben gewisse Restzweifel, so dass eine geringfügige Konditionierung des § 13 Abs. 1 BDSG denkbar wäre, etwa in Form der exemplarischen Anführung öffentlicher Interessen, die jene Restzweifel beseitigt.
Unabhängig davon können jedenfalls sämtliche bereichsspezifische Regelungen des deutschen Datenschutzrechts im öffentlichen Bereich, welche die Vorgaben des Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO erfüllen, aufrechterhalten werden, da sie einen über diese Normen hinausgehenden Regelungsgehalt aufweisen. Der Spielraum für die Mitgliedstaaten, die Vorgaben des Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO zu konkretisieren, ist demnach

äußerst groß. Damit besteht insoweit ein Gegensatz zu den von Art. 23 (ex Art. 21) DSGVO eröffneten Handlungsmöglichkeiten, die an hohe Anforderungen geknüpft sind.[66]

7. Art. 6 Abs. 4 (ex Art. 6 Abs. 3a): Weiterverarbeitung von Daten zu anderen Zwecken

a. Struktur und Hintergrund

Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO gestattet eine Weiterverarbeitung zu anderen als den Zwecken, zu denen die Daten erhoben wurden. Diese ist einerseits dann erlaubt, wenn der Betroffene einwilligt oder sich die Weiterverarbeitung auf unionales oder mitgliedstaatliches Recht stützen kann. Andererseits ist sie erlaubt, wenn die Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar ist (zweckkompatible Weiterverarbeitung). Im Fall der zweckkompatiblen Zweckänderung bedarf die Weiterverarbeitung keiner gesonderten Rechtsgrundlage, wie EG 50 S. 2 (ex EG 40 S. 2) DSGVO klarstellt. Die Frage der Vereinbarkeit stellt sich nach diesem Verständnis aber nur, wenn die Weiterverarbeitung sich nicht ohnehin auf eine Einwilligung oder eine gesetzliche Rechtsgrundlage im Recht der Union oder eines Mitgliedstaates stützen kann. Der „Chapeau“ des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO eröffnet den Mitgliedstaaten damit die Möglichkeit, nationale rechtliche Grundlagen zur zweckändernden Weiterverarbeitung selbst dann zu erlassen, wenn die Zwecke inkompatibel sind. Damit eröffnet sich die Möglichkeit eines Datenumgangs aus anderen als den ursprünglichen Datenerhebungszwecken.

Auch die Entwürfe der Datenschutz-Grundverordnung der Kommission und des Rats sahen die Zweckänderung in Art. 6 Abs. 4 DSGVO vor. Zweckänderungen sollten demnach immer dann möglich sein, wenn sich die Zweckänderung auf einen der *Gründe* nach Art. 6 Abs. 1 UAbs. 1 lit. a - e DSGVO stützen konnte.[67] Gegen diese Bestimmung haben die Art. 29-Gruppe sowie der

[66] Vgl. hierzu S. 68.

[67] Dies ist zu unterscheiden von Fällen, in denen sich die Weiterverarbeitung auf eine Rechtsgrundlage aus Art. 6 Abs. 1 UAbs. 1 lit. a - e stützen kann. Nach der Formulierung des Art. 6 Abs. 4 DSGVO hätte eine Weiterverarbeitung beispielsweise aus *Gründen* der Wahrnehmung

Europäische Datenschutzbeauftragte große Bedenken geäußert,[68] was zur Streichung des Art. 6 Abs. 4 DSGVO in dieser Fassung führte.

Voraussetzung für einen Erlaubnistatbestand im nationalen Recht, Daten (auch) zu inkompatiblen Zwecken weiterzuverarbeiten, ist nach Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO, dass das nationale Gesetz eine erforderliche und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft zum Schutz der in Art. 23 Abs. 1 lit. a - j (ex Art. 21 Abs. 1 lit. aa - g) DSGVO aufgelisteten Ziele darstellt. Zu beachten ist, dass die Öffnungsklausel gerade für solche Fälle gilt, in denen der Zweck der Weiterverarbeitung nicht mit dem ursprünglichen Zweck vereinbar ist. Dies stellt EG 50 S. 7 (ex EG 40 S. 7) DSGVO klar. Es ergibt sich ferner aus der Systematik des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO: Unionsrechtliche oder mitgliedstaatsrechtliche Grundlagen, auf die eine zweckändernde Verarbeitung gestützt werden kann, sollen vorrangig herangezogen werden. Nur ohne eine solche Grundlage soll der Verantwortliche die Vereinbarkeit der weiteren Verarbeitung mit dem Zweck, aus dem die Daten ursprünglich erhoben wurden, prüfen.[69] Auch eine nationale Bestimmung für Verarbeitungen nach Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO[70] kann eine Grundlage für eine Zweckänderung darstellen, vgl. EG 50 S. 5 (ex EG 40 S. 5) DSGVO. Folgerichtig kann dies für Zweckveränderungen, die inkompatibel mit dem Zweck der ursprünglichen Datenerhebung sind, allerdings nur gelten, soweit diese Grundlage dem Erfordernis

---

einer öffentlichen Aufgabe ausgereicht, auch wenn diese Weiterverarbeitung keine Rechtsgrundlage im nationalen Recht hätte und mit dem ursprünglichen Zweck unvereinbar wäre.

[68] Vgl. *Art. 29-Datenschutzgruppe*, WP 191, S. 11 f.; *EDSB*, Stellungnahme v. 7.3.2012, Rn. 120 ff.

[69] Vgl. Wortlaut des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO: „Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche — um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist — unter anderem (…)".

[70] EG 50 S. 5 (ex 40 S. 5) spricht lediglich von der „im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehene[n] Rechtsgrundlage". Hier kann es sich bei mitgliedstaatlichem Recht aber nur um eine Rechtsgrundlage für Verarbeitungen nach Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO handeln, da nur diese eine Normsetzungskompetenz der Mitgliedstaaten eröffnen.

des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO genügt, also eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO genannten Ziele darstellt. Dabei muss nicht das vollständige Programm des Art. 23 (ex Art. 21) DSGVO „abgearbeitet" werden, sondern es genügt, dass einer der dort genannten Ziele verfolgt und die Verhältnismäßigkeit gewahrt wird.

b. Voraussetzungen der Öffnungsklausel

aa) Weiterverarbeitung von Daten zu anderen Zwecken i. S. d. Art. 6 Abs. 4 (ex Art. 6 Abs. 3a)

Für die Beurteilung der Handlungsoptionen stellt sich zunächst die Frage, auf welchen Zweck die Datenschutz-Grundverordnung bei der Beurteilung der Kompatibilität abstellt. Entscheidend ist dies etwa für solche Fälle, in denen ein personenbezogenes Datum erstmalig beim Betroffenen erhoben wurde und dann zweckverändernd an Dritte übermittelt wird, die dieses personenbezogene Datum verarbeiten. Denkbar ist dabei sowohl, auf den Zweck der Ersterhebung des personenbezogenen Datums als auch auf den Zweck der ersten Erhebung durch die verantwortliche Stelle abzustellen, etwa wenn ein Dritter dieser verantwortlichen Stelle das Datum übermittelt hat. Art. 6 Abs. 4 des Rats-Entwurfs sah noch vor, dass ausschließlich auf den Verantwortlichen abzustellen ist. Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO trifft diese Aussage jedoch gerade nicht. Für das Abstellen auf den Zweck, zu dem die Daten erstmalig beim Betroffenen erhoben wurden, streitet EG 50 S. 1 (ex EG 40 S. 1) DSGVO, der von einer *ursprünglichen* Erhebung der Daten spricht. Diese Bewertung entspricht auch dem Zweckbindungsgrundsatz, der in Art. 5 Abs. 1 lit. b DSGVO niedergelegt ist. Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO stellt insofern eine Durchbrechung des Zweckbindungsgrundsatzes dar, die im Sinne eines möglichst hohen Niveaus des Schutzes von personenbezogenen Daten wohl restriktiv auszulegen ist, wobei sich dies erst im Rahmen der Anwendung der Verordnung in der Praxis zeigen wird. So können sich möglicherweise im Rahmen der Anwendung dieser Norm auch datenschutzrechtliche Vorverständnisse oder mitgliedstaatliche Rechtsanwendungstraditionen durchsetzen, die einen größeren Spielraum im Rahmen der zweckkompatiblen Weiterverarbeitung vorsehen und insoweit auf

den Schutz des freien Verkehrs personenbezogener Daten in Art. 1 DSGVO verweisen. Das Ziel der Datenschutz-Grundverordnung des Schutzes der personenbezogenen Daten nach Art. 1 Abs. 2 DSGVO spricht gegebenenfalls aber eher für ein restriktives Verständnis. Für die Weiterverarbeitung kommt es demnach nicht darauf an, ob diese durch denselben oder einen anderen Verantwortlichen vorgenommen wird. Entscheidend ist der ursprüngliche Zweck.

bb) Vereinbarkeit der Verarbeitungszwecke an praktischen Beispielen

Die Öffnungsklausel des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO gestattet den Mitgliedstaaten den Erhalt oder Erlass von Normen, die eine Weiterverarbeitung zu Zwecken ermöglicht, die mit den bisherigen Zwecken unvereinbar sind. Dabei zeigt der Katalog des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO Merkmale zur Beurteilung der Vereinbarkeit auf. Die Vorgaben des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO sind nicht abschließend, wie die Formulierung „unter anderem" zeigt. Ferner sind sie nicht obligatorisch, da sie nach dem Wortlaut des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO von dem Verantwortlichen lediglich berücksichtigt werden sollen.[71] Dabei obliegt die Beurteilung der Vereinbarkeit dem Verantwortlichen. Die Beurteilung muss umso umfangreicher ausfallen, je weiter der geänderte, neue Zweck vom ursprünglichen Zweck entfernt ist.[72] Maßgeblich ist dabei die Erwartungshaltung des Betroffenen hinsichtlich des Datenverwendungszwecks.[73]
Die (Un-)Vereinbarkeit mit dem ursprünglichen Zweck lässt sich an praktischen Beispielen darstellen: Wenn etwa ein Autohaus dem Bundeskriminalamt einen Hinweis auf einen „verdächtigen" Barkauf eines Neuwagens gibt, liegt der Zweck der Übermittlung der Daten an das Bundeskriminalamt durch den Autohändler in der Unterstützung der Strafprävention und -verfolgung.[74]

---

[71] „take into account", Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) a. E. DSGVO
[72] Vgl. Darstellung unterschiedlicher Szenarien für die Vereinbarkeit durch die *Art. 29-Datenschutzgruppe*, WP 203, S. 22 ff.
[73] Vgl. praktische Beispiele der *Art. 29-Datenschutzgruppe*, WP 203, S. 56 ff.
[74] Die Weitergabe der personenbezogenen Daten durch das Autohaus könnte sich auf die Rechtsgrundlage des Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO stützen. Das Beispiel bedingt allerdings zusätzlich die Besonderheit, dass rechtsaktübergreifend Daten aus dem Bereich der Da-

Der ursprüngliche Zweck der Datenerhebung lag aber in der Vertragsbegründung und -durchführung. Der Autoerwerber wird grundsätzlich nicht davon ausgehen, dass seine personenbezogenen Daten zu Strafpräventions- oder Strafverfolgungszwecken weiterverarbeitet werden. Die beiden Verarbeitungszwecke haben auch keinerlei Berührungspunkte i. S. d. Art. 6 Abs. 4 lit. a (ex Art. 6 Abs. 3a lit. a) DSGVO. Die Auswirkungen auf den Betroffenen dürften gleichzeitig sehr hoch sein, Art. 6 Abs. 4 lit. d (ex Art. 6 Abs. 3a lit. d) DSGVO. Damit ist keine Vereinbarkeit der Zwecke gegeben und es bedürfte für die Weiterverarbeitung (also der Übermittlung durch das Autohaus an das Bundeskriminalamt) einer allgemeinen Rechtsgrundlage, die einem der in Art. 23 Abs. 1 (ex 21 Abs. 1) DSGVO festgelegten Ziele dient; im vorliegenden Fall namentlich der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten (Art. 23 Abs. 1 lit. d [ex Art. 21 Abs. 1 lit. b] DSGVO). Für solche inkompatiblen Zwecke kann der nationale Gesetzgeber also Rechtsgrundlagen erlassen.

Anders können womöglich Übermittlungen bewertet werden, die an Auskunfteien in Deutschland bislang auf der Basis des § 28a BDSG erfolgen. So kann durchaus argumentiert werden, dass die Mitteilung eines Forderungsausfalls – jedenfalls unter den engen in § 28a BDSG angeführten Restriktionen – durchaus eine zweckkompatible Weiterverarbeitung darstellt, da eine enge Verbindung zum ursprünglichen Verarbeitungszweck – Vertragserfüllung – besteht, da der Vertrag seitens des Schuldners gerade nicht erfüllt wird. Auch die weiteren Bewertungsparameter (Zusammenhang der Datenerhebung; Art der personenbezogenen Daten, die grundsätzlich keine besonderen Kategorien personenbezogener Daten im Sinne des Art. 9 DGSVO darstellen; die zwar nicht unerheblichen, aber „selbst verschuldeten“ Konsequenzen etc.) können durchaus für eine Zweckkompatibilität sprechen. Damit wird exemplarisch deutlich, dass die künftige Anwendung des Unionsrechts mit der Figur der zweckkompatiblen Weiterverarbeitung hier eine wichtige Auslegungsfrage aufwirft.

---

tenschutz-Grundverordnung in den der Richtlinie für den Datenschutz bei Polizei und Strafjustiz übermittelt werden. Diese Besonderheiten sollen vorliegend nicht näher problematisiert werden.

cc) Reichweite der eine Weiterverarbeitung zu anderen Zwecken legitimierenden Tatbestände

Von besonderer Bedeutung ist auch die Frage, ob eine zweckändernde Weiterverarbeitung nur in Fällen, in denen zuvor eine Datenverarbeitung im Rahmen des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO erfolgt ist, legitimiert werden darf, oder ob dies für sämtliche Fälle des Art. 6 Abs. 1 DSGVO möglich ist. Nur im Falle der zweiten, weiten Interpretation wäre etwa eine – für § 28a BDSG gegebenenfalls gar nicht erforderliche (dazu soeben bb)) – Eröffnung einer zweckändernden Weiterverarbeitung zulässig. Für die zweite Auslegungsvariante spricht der Wortlaut des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO, der keine Beschränkung auf Abs. 1 UAbs. 1 lit. c und lit. e enthält. Auch ein Vergleich in systematischer Perspektive mit den Abs. 2 und 3, die eine entsprechende beschränkende Bezugnahme auf Abs. 1 UAbs. 1 lit. c und lit. e enthalten, spricht gegen eine restriktive Interpretation des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO. Dasselbe gilt in systematischer Perspektive angesichts der in Bezug genommenen Ziele des Art. 23 Abs. 1 DSGVO in Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO, die ebenfalls deutlich über die Ziele des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO hinausweisen – insbesondere in Art. 23 Abs. 1 lit. i DSGVO mit dem weit gefassten Ziel des Schutzes der betroffenen Person oder der Rechte und Freiheiten anderer Personen. Diese starken Anhaltspunkte in Wortlaut und Systematik dürften kaum durch teleologische Gründe überspielt werden können, die vor dem Hintergrund eines effektiven Schutzes personenbezogener Daten für eine Restriktion von Weiterverarbeitungstatbeständen per se auf die Fälle des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO sprechen könnten. Insoweit ist es vielmehr überzeugender, angesichts der nach Art. 6 Abs. 4 DSGVO indizierten Verhältnismäßigkeitsprüfung, Weiterverarbeitungstatbestände insgesamt auf das erforderliche Maß zu beschränken. Zugleich birgt aber ein Verständnis des Art. 6 Abs. 4 DSGVO, das nicht auf der Trennung zwischen unionalen und mitgliedstaatlichen Regelungsbefugnissen aufsetzt, das Risiko, dass Art. 6 Abs. 4 DSGVO den Mitgliedstaaten Regelungsbefugnisse in einem Bereich zuweist, in dem die Union ihnen diese nicht hat zugestehen wollen. Insbesondere könnten Mitgliedstaaten diese geöffnete Tür als Einladung nutzen, um sich Regelungsbefugnisse anzumaßen, die ihnen Art. 6 Abs. 1 – 3 DSGVO nicht

zugestehen wollen. Die Regelungsbefugnisse im Bereich der Erstverarbeitung und der Zweckänderung wären dann asynchron. Insofern streiten auch gute Gründe für ein Verständnis, bei dem Art. 6 Abs. 4 DSGVO den Mitgliedstaaten eine Zweckänderung kraft eigener Regelungsbefugnis nur dort eröffnet, wo diese selbst nach Art. 6 Abs. 1 - 3 DSGVO eine nationalstaatliche Regelungsbefugnis haben.

dd) Konkretisierung der Vereinbarkeit

Den Mitgliedstaaten kommt ein Gestaltungsspielraum bei der Frage der Vereinbarkeit der weiteren Datenverarbeitung mit dem ursprünglichen Zweck zu. So können sie in den nationalen Regelungen, die als Grundlage für eine Datenverarbeitung nach Maßgabe der Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO dienen, die Vereinbarkeit einer weiteren Datenverarbeitung von zu diesen Zwecken verarbeiteten Daten konkretisieren, wie EG 50 S. 3 (ex EG 40 S. 3) DSGVO klarstellt. Im Sinne eines umfassenden Schutzes personenbezogener Daten muss sich die Konkretisierung der Fälle, in denen eine Zweckänderung noch als vereinbar mit dem ursprünglichen Zweck gilt, an den Beispielen aus Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO für eine Vereinbarkeit orientieren. D. h. es sollte etwa der Kontext der Datenerhebung sowie die Folgen einer Weiterverarbeitung für den Betroffenen in Betracht gezogen werden. EG 50 S. 4 (ex EG 40 S. 4) DSGVO sieht eine Fiktion der Vereinbarkeit für die Weiterverarbeitung zu Archivierungszwecken, die im öffentlichen Interesse liegen, sowie zu wissenschaftlichen, historischen oder statistischen Zwecke vor. Diese Fiktion greift also nur für einen ganz beschränkten Bereich.

c. Abgleich mit bestehendem nationalen Recht am Beispiel von § 14 Abs. 2 Nr. 6 Var. 2 BDSG

Auch nach aktueller Rechtslage erlauben bestimmte Normen wie etwa § 14 Abs. 2 BDSG eine Weiterverarbeitung unter Zweckänderung, allerdings stets unter den strengen Bedingungen der Norm. Dazu gehört beispielsweise die Einwilligung des Betroffenen, § 14 Abs. 2 Nr. 1 BDSG. Diese Normen können unproblematisch aufrechterhalten werden, soweit sie den Anforderungen aus Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) i. V. m den Zielen des Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO genügen. Dies gilt beispielsweise für § 14 Abs. 2 Nr.

6 Var. 2 BDSG, nach dem eine erforderliche Zweckänderung zur Abwehr einer Gefahr für die öffentliche Sicherheit zulässig ist, Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. c (ex Art. 21 Abs. 1 lit. a) DSGVO.

d. Handlungsoptionen am Beispiel des „Once Only"-Prinzips für deutsche Behörden

Das „Once Only"-Prinzip sieht vor, dass öffentliche Stellen dasselbe personenbezogene Datum eines Bürgers nur einmal erheben und untereinander austauschen. Damit soll ein Abbau an Bürokratie erreicht und die Effizienz der Verwaltung gesteigert werden.[75] Die Datenschutz-Grundverordnung eröffnet, wie gezeigt, verschiedene Möglichkeiten für eine solche Zweckänderung. Für Behörden, die in Wahrnehmung öffentlicher Aufgaben i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO handeln, gibt die Öffnungsklausel des Art. 6 Abs. 2 (ex Art. 6 Abs. 2a) DSGVO den Mitgliedstaaten die Möglichkeit zum Erhalt oder Erlass von Normen zur Anpassung der Anwendbarkeit der Verordnung hinsichtlich solcher Verarbeitungen. Nach EG 50 S. 3 (ex EG 40 S. 3) DSGVO können Mitgliedstaaten in diesen Fällen näher konkretisieren, wann eine zweckändernde Verarbeitung als vereinbar mit dem Zweck der ursprünglichen Erhebung gelten soll. Für diese Weiterverarbeitungen bedürfte es dann keiner erneuten rechtlichen Grundlage.[76] Angesichts der ausgeprägten Bereichsspezifik im deutschen Datenschutzrecht, die weitgehend aufrechterhalten bleiben kann,[77] ist ein Rückgriff auf diese Möglichkeit allerdings kaum nötig. Denkbar wäre mit Blick auf den sehr großen von Art. 6 Abs. 2 (ex Art. 6 Abs. 2a) DSGVO eröffneten Spielraum auch die Schaffung einer allgemeinen Norm, etwa durch eine Erweiterung des § 14 Abs. 2 BDSG mit Bestimmungen dahin gehend, wann auch ein innerbehördlicher Austausch der personenbezogenen Daten möglich ist. Die Norm könnte die Voraussetzungen konkretisieren, etwa indem sie eine Einschränkung der Art der Behörden vornimmt, oder um das Kriterium der hypothetischen Zu-

[75] Vgl. Erläuterungen und Pläne für eine Anwendung des „Once Only"-Prinzips auf EU-Ebene *Kommission*, Co-creation between public administrations: once-only principle, abrufbar unter http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/h2020/topics/3074-co-creation-05-2016.html#fn1, abgerufen am 29.07.2016.
[76] Vgl. S. 38.
[77] Vgl. S. 36.

lässigkeit einer Erhebung des personenbezogenen Datums durch die empfangende Behörde ergänzt, Art. 6 Abs. 4 lit. d (ex Art. 6 Abs. 3a lit. d) DSGVO. Darüber hinaus wäre die Schaffung einer Grundlage für einen innerbehördlichen Austausch der Daten auch bei Unvereinbarkeit der Zwecke nach Maßgabe des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO i. V. m. Art. 23 Abs. 1 lit. e (ex Art. 21 Abs. 1 lit. c) denkbar. Damit eröffnet die Datenschutz-Grundverordnung grundsätzlich die Möglichkeit der Umsetzung des „Once Only"-Prinzips. Die Grenzen dieses Prinzips ergeben sich daher eher aus dem nationalen Verfassungsrecht. Angesichts des streng verstandenen Gesetzesvorbehalts im Datenschutzrecht wirft das „Once Only"-Prinzip zahlreiche verfassungsrechtliche Fragen auf.[78]

8. Art. 8: Einwilligungsalter des Kindes

Mitgliedstaaten können die Altersgrenze für die Einwilligung eines Kindes national innerhalb des Korridors von 13 bis 16 Jahren regeln und damit von der auf 16 Jahre festgesetzten Altersgrenze der Datenschutz-Grundverordnung abweichen.[79] Das gilt allerdings nur in Fällen, in denen dem Kind direkt Dienste der Informationsgesellschaft angeboten werden.

a. Struktur und Hintergrund; Qualifikation der Öffnungsklausel

Art. 8 Abs. 1 DSGVO stellt eine fakultative Öffnungsklausel dar, die in dieser Form erst im Rahmen des Trilogs in die Datenschutz-Grundverordnung aufgenommen wurde. Adressat sind vor allem nicht öffentliche Stellen in der überkommenen Differenzierung des deutschen Datenschutzrechts. Es handelt sich um eine eng gefasste, bereichsspezifische Klausel für Angebote von Diensten der Informationsgesellschaft.

[78] Kritisch zum Parlamentsvorbehalt im Datenschutzrecht *Kingreen/Kühling* (Fn. 4), 213 ff.
[79] Probleme können sich dann stellen, wenn grenzüberschreitend Dienste angeboten werden und die Mitgliedstaaten unterschiedliche Altersgrenzen festlegen.

b. Möglichkeiten zur Modifikation; kein Handlungsbedarf im deutschen Recht

Eine vergleichbare explizite Altersregelung wie die des Art. 8 Abs. 1 DSGVO findet sich im deutschen Datenschutzrecht nicht. Nach ständiger Rechtsprechung des BVerfG handelt es sich bei der Einwilligung um die Wahrnehmung von Grundrechten, weswegen es entscheidend auf die Einsichts- und Urteilsfähigkeit des Kindes ankommt.[80] Damit ist die Wirksamkeit der Einwilligung eines Minderjährigen bisher nur einzelfallbezogen bestimmbar. Eine ausdifferenzierte Rechtsprechung zu der Frage, wann die Einsichtsfähigkeit normalerweise gegeben ist, gibt es nicht. Nach einem Urteil des BGH jedoch ist die Einsichtsfähigkeit bei Jugendlichen im Alter von 15 bis 17 Jahren noch nicht gegeben.[81] Nach deutscher Rechtsprechung ist tendenziell also vor einem Alter von 16 Jahren auch keine Einsichtsfähigkeit gegeben.
Daraus ergibt sich, dass keine spezialrechtliche Regelung notwendig ist, um den geltenden Rechtsstand zu erhalten. Ein Gebrauchmachen von der Öffnungsklausel und damit ein Absenken des Alters, ab dem eine Einwilligung zulässig ist, stößt womöglich an verfassungsrechtliche Grenzen.

9. Art. 9: Verarbeitung besonderer Daten

a. Struktur und Entstehungshintergrund

Art. 9 DSGVO normiert entsprechend Art. 8 DSRL einen strengeren Rechtfertigungs-Standard für die Verarbeitung einzelner Datenkategorien, die als besonders sensibel eingestuft werden. Dies sind – insoweit in Übereinstimmung mit der DSRL – solche Daten, die sich auf die rassische oder ethnische Herkunft, die politischen, religiösen und philosophischen Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit sowie das Sexualleben und die sexuelle Orientierung beziehen. In Ergänzung zu den bisherigen Kategorien

[80] Ständige Rspr. BVerfGE 10, 302 ff.; vgl. auch *Kühling*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 4a BDSG, Rn. 33; *Simitis*, in: ders. (Hrsg.), BDSG, 8. Aufl., 2014, § 4a, Rn. 21; *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 4a, Rn. 25.
[81] *BGH*, Urt. v. 22.1.2014 – I ZR 218/12.

der DSRL sind zusätzlich die Fälle der genetischen Daten und biometrischer Daten, die eine spezifische Person identifizieren können, aufgenommen worden. Die letztgenannte Kategorie ist erst im Rahmen des Trilogs in den Text eingefügt worden. Für all jene Daten gilt im Grundsatz, dass jegliche Datenverarbeitung verboten ist, Art. 9 Abs. 1 DSGVO. Dieses Verbot gilt nach Art. 9 Abs. 2 DSGVO nicht, sofern verschiedene Voraussetzungen vorliegen[82]. Diese sind vollharmonisiert, eröffnen aber Abweichungsmöglichkeiten im Fall der Einwilligung der betroffenen Person (lit. a), bei Datenverarbeitungen zur Erfüllung bestimmter Pflichten im Bereich der sozialen Sicherheit und des Sozialschutzes (lit. b), aus Gründen eines gewichtigen öffentlichen Interesses (lit. g), im Bereich des Gesundheitsschutzes im weitesten Sinne (lit. h, i [ex lit. h, hb]) sowie schließlich im Forschungs- und Statistikbereich in Verbindung mit Art. 89 (ex Art. 83) (lit. j [ex lit. i]). Die wesentliche Änderung dieser Norm ist im Vergleich zum Kommissionsentwurf erfolgt, der noch in Art. 81 DSGVO-E eine strenge Überformung des nationalen Gesundheitsdatenschutzrechtssystems vorgesehen hatte.

b. Qualifikation der Öffnungsklausel

Art. 9 DSGVO stellt grundsätzlich eine gemischte Öffnungsklausel dar, die einerseits in bestimmen Sektoren (Sozialdatenschutz; Gesundheitsdatenschutz) ausstrahlt. Andererseits ist sie, angesichts der Breite und Relevanz besonderer Datenkategorien, jedoch letztlich von erheblicher und tendenziell horizontaler Bedeutung.

Da die Norm keine Konkretisierung erfordert, sondern lediglich Abweichungsmöglichkeiten vorsieht, handelt es sich um eine fakultative Öffnungsklausel. Ein Handlungsbedürfnis auf nationaler Ebene ist daher nur indiziert, wenn der nationale Gesetzgeber die Anforderungen an die Verarbeitung besonderer Datenkategorien verschärfen, erleichtern oder modifizieren möchte.

---

[82] Ergänzend könnte auch noch die Frage gestellt werden, inwiefern Art. 9 Abs. 2 DSGVO eigenständig als Öffnungsklausel greift oder nicht zusätzlich noch ein Rückgriff auf die Öffnungsklausel in Art. 6 Abs. 1 UAbs. 1 lit. e i. V. m. Art. 6 Abs. 3 DSGVO notwendig ist. Dagegen spricht allerdings, dass Art. 9 Abs. 2 DSGVO spezifische und teils strengere Anforderungen vorsieht (etwa Gründe eines qualifizierten öffentlichen Interesses nach Art. 9 Abs. 2 lit. g DSGVO im Vergleich zu einem nicht näher qualifizierten öffentlichen Interesse in Abs. 1 lit. e i. V. m. Art. 6 Abs. 3 DSGVO).

Dabei sind sowohl horizontale Regelungen für alle Kategorien besonderer Daten möglich (wie etwa mit Blick auf die Einwilligung), als auch Bestimmungen in einzelnen Sektoren wie dem Gesundheitsdatenschutz. Adressat der Regelung sind sowohl öffentliche als auch nicht-öffentliche Stellen in der überkommenen deutschen datenschutzrechtlichen Differenzierung, da besondere Datenkategorien durch sämtliche Verantwortliche verarbeitet werden.

c. Voraussetzungen der Öffnungsklausel

aa) Ausschluss der Einwilligung, Abs. 2 lit. a

Art. 9 Abs. 2 lit. a DSGVO formuliert eine Rückausnahme von der Möglichkeit, das Verarbeitungsverbot durch Einwilligung einzuschränken. Sie räumt den Mitgliedstaaten die Befugnis ein, die Verarbeitung trotz Vorliegens einer ausdrücklichen Einwilligung durch Gesetz zu untersagen. Eine weitere Konditionierung der Voraussetzungen, um diese Rückausnahme zu aktivieren, nimmt die Verordnung nicht vor. Die Mitgliedstaaten sind daher grundsätzlich vollkommen frei, von dieser Regelungsoption Gebrauch zu machen. Beachten müssen sie jedoch grundrechtliche Grenzen – insbesondere mit Blick auf die informationelle Selbstbestimmung, die ja in einer Einwilligung Ausdruck findet. Bereichsspezifische Regelungen lassen sich damit im deutschen Recht ebenso aufrechterhalten wie allgemeine, horizontale Einschränkungen der Einwilligung.

Ob statt eines schlichten Ausschlusses der Einwilligung auch zusätzliche Anforderungen an die Einwilligung gestellt werden können, ist unklar. Dies ist mit Blick auf das gegenwärtige deutsche Datenschutzrecht durchaus relevant. Zwar sieht § 4a Abs. 3 BDSG dem Wortlaut nach alleine das Erfordernis einer ausdrücklichen Einwilligung in Fällen sensibler Daten vor. Dieses Erfordernis wird nicht vollständig von der Definition der Einwilligung in Art. 4 Nr. 11 (ex Art. 4 Abs. 8) DSGVO aufgefangen, die zwar eine „eindeutige“ Handlung, aber gerade keine „explizite“ Erklärung verlangt, wie es etwa noch im Kommissionsentwurf der Datenschutz-Grundverordnung vorgesehen war. Jedoch verlangt Art. 9 Abs. 2 lit. a DSGVO für die Ausnahme bei sensiblen Daten eine „ausdrückliche“ Einwilligung. Insoweit verschärft also § 4a Abs. 3 BDSG dem Wortlaut nach die Vorgaben der DSGVO nicht. Allerdings wird aus der Vorgabe des § 4a Abs. 3 BDSG teilweise darüber hinaus abge-

leitet, dass unter Berücksichtigung der Begründung des geänderten Vorschlags der Europäischen Kommission zur DSRL[83] grundsätzlich eine *schriftliche* Einwilligung des Betroffenen zu fordern ist.[84] Auch werden als weitere Konsequenz hieraus erhöhte Anforderungen an die Bestimmtheit und Genauigkeit der Einwilligung verlangt, insbesondere, was deren genaue Bezeichnung und den spezifischen Verwendungszusammenhang anbelangt.[85] Weitere Konkretisierungen im nationalen Recht sind denkbar. Würden diese im BDSG-Nachfolgegesetz erfolgen („schriftliche Einwilligung"), stellte sich die Frage, inwiefern eine derartige partielle Verschärfung zulässig ist. Schon jetzt stellt sich diese Frage in Bezug auf bereichsspezifische Regelungen etwa in § 8 Abs. 1 Gendiagnostikgesetz, der nicht nur eine ausdrückliche, sondern auch eine „schriftliche" Einwilligung vor Durchführung einer genetischen Untersuchung oder Analyse verlangt.
Insoweit spricht die den Mitgliedstaaten eingeräumte weitreichende und unkonditionierte Konkretisierungs- und Ausschlussbefugnis der Einwilligung in Bezug auf sensible Daten dafür, dass auch eine Verschärfung der Anforderungen an die Einwilligung in spezifischen Verwendungssituationen der Daten abgedeckt ist. Das ist zwar im Wortlaut der Öffnungsklausel nicht zwingend angelegt, ergibt sich aber als Minus angesichts der weitgehenden mitgliedstaatlichen Gestaltungsbefugnis.

bb) Lockerung im Bereich der Arbeitssicherheit/sozialen Sicherheit, Abs. 2 lit. b

Nach Art. 9 Abs. 2 lit. b DSGVO können Mitgliedstaaten durch Gesetz oder in Tarifvereinbarungen die Verarbeitung im Bereich der sozialen Sicherheit und auch der Beschäftigung zulassen. Diese Öffnungsklausel sieht also nicht nur eine reduzierende Konkretisierung eines Zulässigkeitstatbestands vor,

[83] Begründung des geänderten Vorschlags der Kommission für eine RL des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr v. 15.10.1992, KOM(92) 422 endg. – SYN 287 – ABl. EG 1992, C 311, 30, deutsche Fassung bei *Klug*, BDSG-Interpretation, 3. Aufl., 2007, S. 156.
[84] Vgl. *Gola/Klug*, Grundzüge des Datenschutzrechts, 2003, S. 59; ferner *Holznagel/Sonntag*, 4.8 Einwilligung des Betroffenen, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Rn. 56; dem folgend *Kühling/Seidel/Sivridis* (Fn. 44), Rn. 325.
[85] Dazu wiederum *Kühling/Seidel/Sivridis* (Fn. 44), Rn. 325.

sondern eröffnet letztlich eine weit gefasste und unkonditionierte Ausgestaltungsbefugnis für die Mitgliedstaaten im Bereich des Arbeitsrechts und der sozialen Sicherheit sowie des Sozialschutzes. Einzige Leitplanken der Ausübung dieser Gestaltungsbefugnis der Mitgliedstaaten ist die Erforderlichkeit der Datenverarbeitung zur Erfüllung der Rechte und Pflichten der Betroffenen und der Verantwortlichen in den genannten Gebieten. Der Hinweis auf die Notwendigkeit einer angemessenen Wahrung der Grundrechte und Interessen der Betroffenen ist als ergänzende Einschränkung kaum von eigenständiger Relevanz, da sich dies ohnehin aus der Grundrechtecharta bzw. dem nationalen Verfassungsrecht ergibt.

cc) Ausnahmen im Bereich der Gesundheit und Sozialfürsorge, Abs. 2 lit. h, i, Abs. 4, 5 (ex Abs. 2 lit. h, hb, Abs. 3, 4)

Ähnlich in der Struktur wie Art. 9 Abs. 2 lit. b DSGVO ist die Öffnungsklausel des Art. 9 Abs. 2 lit. h DSGVO und den korrespondierenden EG 52 und 53 (ex EG 42 und 42a) DSGVO. Danach können Mitgliedstaaten die Verarbeitung zu Zwecken u. a. der medizinischen Diagnose, zur Feststellung der Arbeitsfähigkeit von Beschäftigten oder zum Zwecke des Managements von Gesundheits- oder Sozialfürsorgesystemen im Gesetzeswege näher in ihrer Zulässigkeit ausgestalten. Art. 9 Abs. 3 (ex Art. 9 Abs. 4) DSGVO lässt die Verarbeitung besonderer Daten insoweit allerdings zu Zwecken des Art. 9 Abs. 2 lit. h DSGVO nur zu, sofern der Verarbeiter ein Berufsgeheimnisträger ist. Letzteres kann sich auch nach dem mitgliedstaatlichen Recht richten. Damit wird die Ausgestaltungsbefugnis ratione personae erheblich eingeschränkt und auf entsprechendes Fachpersonal beschränkt.
Ähnliches gilt für Art. 9 Abs. 2 lit. i (ex Art. 9 Abs. 2 lit. hb) sowie EG 54 (ex EG 42b) DSGVO, der eine strukturell vergleichbare Öffnungsklausel für die Verarbeitung im Bereich der öffentlichen Gesundheit insgesamt vorsieht, ohne allerdings eine derartige Einschränkung ratione personae vorzunehmen. Der Begriff der öffentlichen Gesundheit ist dabei weit zu verstehen, wie EG 54 S. 3 (ex EG 42b S. 2) DSGVO deutlich macht: „In diesem Zusammenhang sollte der Begriff ‚öffentliche Gesundheit' im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates vom 16. Dezember 2008 zu Gemeinschaftsstatistiken über öffentliche

Gesundheit und über Gesundheitsschutz und Sicherheit am Arbeitsplatz ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen.“ Lediglich geringfügig einschränkend ergänzt EG 54 S. 4 (ex EG 42b S. 3) DSGVO: „Eine solche Verarbeitung personenbezogener Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber, Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten.“

Art. 9 Abs. 4 (ex Art. 9 Abs. 5) DSGVO (ergänzt durch die letzten beiden Sätze des EG 54 [ex EG 42a] DSGVO) eröffnet den Mitgliedstaaten schließlich die Möglichkeit, weitere Voraussetzungen einschließlich weiterer Beschränkungen – aber eben auch Zulässigkeitstatbeständen, Modifikationen etc. – für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten national zu regeln.

Damit erlangen die Mitgliedstaaten letztlich insbesondere im Rahmen des Art. 9 Abs. 2 lit. i (ex Art. 9 Abs. 2 lit. hb) DSGVO eine faktisch weitreichende Freiheit, die Datenverarbeitung im Bereich der Gesundheit und Sozialfürsorge eigenständig zu gestalten und die Vorgaben der Datenschutz-Grundverordnung insoweit zu konkretisieren, aber auch zu modifizieren im Sinne einer Verschärfung oder Erleichterung. Dabei sieht die Datenschutz-Grundverordnung auch – anders als noch der ursprünglich vorgesehene Art. 81 im Kommissionsentwurf, bestätigt im Parlamentsentwurf – keine Konditionierung dieser Gestaltungsbefugnis vor. Der Verweis auf die angemessenen Grundrechtsgarantien in Art. 9 Abs. 2 lit. i (ex Art. 9 Abs. 2 lit. hb) DSGVO einschließlich der Wahrung des Berufsgeheimnisses und des Erforderlichkeitsgrundsatzes ist insoweit wenig limitierend. Denn diese Gehalte sind ohnehin in Deutschland durch die verfassungsrechtlichen Vorgaben indiziert, die durch das Datenschutzgrundrecht der Grundrechtecharta in Art. 8 GrCh ergänzt werden.

dd) Archivierungsfälle, Abs. 2 lit. j (ex Abs. 2 lit. i)

Ähnlich wie Art. 9 Abs. 2 lit. i (ex Art. 9 Abs. 2 lit. hb) DSGVO ist auch die Öffnungsklausel gemäß Art. 9 Abs. 2 lit. j (ex Art. 9 Abs. 2 lit. i) DSGVO einzuordnen. Ihr zufolge dürfen demnach Mitgliedstaaten im nationalen Recht die Verarbeitung besonderer Daten für privilegierte Verarbeitungszwecke – der Archivierung zu öffentlichen Zwecken oder wissenschaftliche oder historische Forschungszwecke sowie statistische Zwecke – erlauben. Die weitere Konditionierung des Gestaltungsspielraums der Mitgliedstaaten entspricht weitgehend dem zu Art. 9 Abs. 2 lit. h und i (ex hb) DSGVO Gesagten. Zunächst erfolgt zwar eine zusätzliche Verpflichtung auf den Verhältnismäßigkeitsgrundsatz und die Wesensgehaltsgarantie. Aber auch insoweit handelt es sich lediglich um Vorgaben, die den grundrechtlichen Direktiven des Grundgesetzes und der Grundrechtecharta entsprechen.
Relevanter ist hingegen die Anforderung, dass eine entsprechende gesetzliche Regelung „angemessene und spezifische Maßnahmen“ vorsehen muss, um jene Rechte zu schützen. Hier ist fraglich, ob diese Maßnahmen über die allgemeinen Verpflichtungen der Datenschutz-Grundverordnung hinausgehen müssen oder ob insoweit etwa die Betroffenenrechte genügen. Der Hinweis auf den spezifischen Charakter der Maßnahme spricht dabei eher für eine eigenständige Absicherung. Hier haben die Mitgliedstaaten aber einen weiten Spielraum und können etwa besondere Kontrollgremien beispielsweise im Bereich der medizinischen Forschung vorsehen.

ee) Wichtiges öffentliches Interesse, Abs. 2 lit. g

Schließlich enthält Art. 9 Abs. 2 lit. g DSGVO die Möglichkeit, dass Mitgliedstaaten die Verarbeitung im wichtigen öffentlichen Interesse im Gesetzeswege zulassen. Zwar wird man den Mitgliedstaaten auch hier einen Spielraum bei der Festlegung entsprechender Interessen zubilligen können. EG 46 (ex EG 37) DSGVO macht jedoch allgemein – zur Erläuterung des Art. 6 Abs. 1 UAbs. 1 lit. d DSGVO – in Bezug auf den Begriff des wichtigen öffentlichen Interesses deutlich, dass nicht jedes Interesse, sondern nur solche mit besonderer Bedeutung erfasst sind. Dies zeigt ein Blick auf die exemplarisch aufgeführten entsprechenden Interessen: „So kann beispielsweise die Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von

Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen erforderlich sein.“ Etwas schwächer ist der Verweis auf wichtige öffentliche Interessen in EG 112 (ex EG 87) DSGVO. Dort heißt es: „Diese Ausnahmen sollten insbesondere für Datenübermittlungen gelten, die aus wichtigen Gründen des öffentlichen Interesses erforderlich sind, beispielsweise für den internationalen Datenaustausch zwischen Wettbewerbs-, Steuer- oder Zollbehörden, zwischen Finanzaufsichtsbehörden oder zwischen für Angelegenheiten der sozialen Sicherheit oder für die öffentliche Gesundheit zuständigen Diensten, beispielsweise im Falle der Umgebungsuntersuchung bei ansteckenden Krankheiten oder zur Verringerung und/oder Beseitigung des Dopings im Sport.“
Letztlich ist damit jedoch ein weiterer Gestaltungsspielraum horizontaler Art geschaffen, sofern sich darlegen lässt, dass eine gesetzliche Regelung zur Datenverarbeitung ein derartiges, gehoben bedeutsames öffentliches Interesse verfolgt. Der Anforderungskatalog an die Ausgestaltung entspricht sodann den zu Art. 9 Abs. 2 lit. j (ex Art. 9 Abs. 2 lit. i) DSGVO angeführten Anforderungen, so dass die allgemeinen Anforderungen des Verhältnismäßigkeitsgrundsatzes und des Wesensgehalts zu wahren sind. Darüber hinaus sind auch spezifische grundrechtsschützende Sicherungsmaßnahmen zu ergreifen, deren Konkretisierung wiederum weitgehend dem Mitgliedstaat überlassen bleibt.

d. Verhältnis des Art. 9 zu Art. 6

Das Verhältnis des Art. 9 DSGVO zu Art. 6 DSGVO ist weitgehend unklar. Das gilt insbesondere für die Frage, ob die Weiterverarbeitungsvorschrift des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO auch im Rahmen des Art. 9 DSGVO anzuwenden ist. Prima facie lässt sich Art. 9 DSGVO als „geschlossene“ Norm und abschließende lex specialis zu Art. 6 DGSVO verstehen. Dann wäre eine mitgliedstaatliche Abweichungsbefugnis nur im Rahmen der Anwendung des Art. 9 DSGVO gegeben. Der Wortlaut lässt sich durchaus so verstehen, zumal Art. 9 DSGVO nicht auf Art. 6 DSGVO verweist. Andererseits verfügten die Mitgliedstaaten schon nach dem Richtlinienrecht über eine weiter gefasste Konkretisierungsbefugnis. Es ist nicht ersichtlich, dass die DSGVO das einschränken wollte. Eine teleologische Bewertung bringt ein offenes Ergebnis hervor: Zwar spricht ein hoher Schutz personenbezogener

Daten durchaus für einen Ausschluss der Weiterverarbeitung von besonderen Kategorien personenbezogener Daten; allerdings lassen sich umgekehrt durchaus gewichtige gegenläufige Interessen für Verarbeitungen in diesem Bereich anführen. Auch dies wird für die Anwendungspraxis der DGSVO eine wichtige Frage sein.

e. Abgleich mit dem bestehenden nationalen Recht

Angesichts der Breite der Öffnungsklausel des Art. 9 DSGVO ist ein Abgleich mit dem bestehenden Recht nur in einer Tendenzaussage zusammenfassend möglich: Die Öffnungsklausel ermöglicht weitgehend unkonditionierte, weitreichende mitgliedstaatliche Gestaltungsspielräume im Bereich des Arbeitsrechts, des Gesundheitswesens und der Sozialfürsorge sowie bei der Verfolgung – eher eng zu verstehender – besonderer öffentlicher Interessen. Diese können zur Ermöglichung oder Einschränkung von Datenverarbeitungen genutzt werden. Die Öffnungsklauseln erlauben damit in den genannten Sektoren in erheblichem Umfang die Wahrung sektorspezifischer Regeln im nationalen Recht. Die Anforderungen an entsprechende Ausgestaltungen entsprechen eher den allgemeinen verfassungsrechtlichen Direktiven und verlangen nur im Fall der Art. 9 Abs. 2 lit. g (besonderes öffentliches Interesse) und lit. j (ex lit. i) (statistische Zwecke, Forschungszwecke, historische Zwecke) gesonderte Maßnahmen zur Sicherung der Grundrechte des Betroffenen. Zudem kann die Einwilligung im Bereich der besonderen Datenkategorien ausgeschlossen oder auch verschärfend modifiziert werden.

10. Art. 10 (ex Art. 9a): Verarbeitung von Daten über Strafurteile/Straftaten

Art. 10 (ex Art. 9a) DSVO sieht die Zulässigkeit der Verarbeitung von Daten über Strafurteile/Straftaten oder damit zusammenhängende Sicherungsmaßregeln auf der Basis mitgliedstaatlichen Rechts vor, das ebenfalls angemessene Garantien zum Schutz der Grundrechte der Betroffenen vorsehen muss. Damit wird für diese besondere Datenkategorie ebenfalls eine weitreichende mitgliedstaatliche Ausgestaltungsbefugnis geschaffen.

11. Art. 14 (ex Art. 14a): Informationspflicht, wenn Daten nicht bei Betroffenen erhoben

Art. 14 (ex Art. 14a) DSGVO regelt eine Informationspflicht für den Fall, dass die Daten nicht bei den Betroffenen erhoben werden. Die Regelung bestand in ähnlicher Form bereits in Art. 11 RL 95/46/EG. Von dieser Informationspflicht sieht Art. 14 Abs. 5 (ex Art. 14a Abs. 4) DSGVO Ausschlussgründe vor, die teilweise mitgliedstaatliche Regelungen voraussetzen. Das gilt nach Art. 14 Abs. 5 lit. c (ex Art. 14a Abs. 4 lit. c) DSGVO zunächst in der Konstellation, dass mitgliedstaatliche Normen die Erlangung oder Weitergabe der Daten regeln. Dies ist insbesondere der Fall, wenn die Voraussetzungen nach Art. 6 Abs. 2, Abs. 3 i. V. m. Art. 6 Abs. 1 UAbs. 1 lit. c (ex Art. 6 Abs. 2a, Abs. 3 i. V. m. Art. 6 Abs. 1 UAbs. 1 lit. c) DSGVO vorliegen und der Verantwortliche einer rechtlichen Verpflichtung unterliegt (insoweit kann auf das unter 2.c.aa. Ausgeführte verwiesen werden). Jedenfalls ergibt sich eine entsprechende Regelung aber aus bereits vorhandenen Gesetzen im nationalen Recht, so dass insoweit kein neuer Regelungsbedarf entsteht.[86] Art. 14 Abs. 3 (ex Art. 14a Abs. 3) DSGVO tritt hier an die Stelle des § 19a Abs. 2 Nr. 3 BDSG. Voraussetzung ist insoweit im Übrigen lediglich, dass jene spezifische Regelung geeignete Maßnahmen zum Schutz der berechtigten Interessen der betroffenen Person vorsieht.

Ferner ist eine Information ausgeschlossen, wenn die relevanten Daten einem Berufsgeheimnis bzw. einer satzungsmäßigen Geheimhaltungspflicht unterliegen. Insoweit ist ebenfalls grundsätzlich kein spezifisches Gesetzgebungsbedürfnis ersichtlich, da sich jene Pflichten aus spezifischen Normen außerhalb datenschutzrechtlicher Regelungen ergeben. Der Ausschluss der Informationspflicht knüpft hieran ipso iure an; das nationale Recht muss ihn nicht gesondert anordnen.

Schließlich tritt der allgemeine Ausschlussgrund der Unmöglichkeit bzw. Unverhältnismäßigkeit der Information nach Art. 14 Abs. 5 lit. b (ex Art. 14a Abs. 4 lit. b) DSGVO an die Stelle des § 19a Abs. 2 Nr. 2 BDSG.

---

[86] Siehe als Beispiel etwa den in der Literatur genannten Fall der Kontrollmitteilung einer Finanzbehörde, *Eßer*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, Art. 19a BDSG, Rn. 24.

Die Regelung steht im Übrigen im Zusammenhang mit der Datenverarbeitung zu Archivierungszwecken im öffentlichen Interesse bzw. zu wissenschaftlichen und historischen Forschungszwecken und zu statistischen Zwecken in Verbindung mit Art. 89 (ex Art. 83) DSGVO (siehe dazu unten S. 298).
Art. 14 (ex Art. 14a) DSGVO löst für sich betrachtet daher keinen spezifischen Regelungsbedarf aus bzw. verlangt gegebenenfalls Streichungen paralleler Vorschriften im nationalen Recht.

12. Art. 17 Abs. 1 lit. e und Abs. 3 lit. b: Löschpflichten („Recht auf Vergessenwerden“)

a. Struktur und Entstehungshintergrund

Art. 17 DSGVO gibt Betroffenen das Recht auf Löschung ihrer personenbezogenen Daten unter den Voraussetzungen des Art. 17 Abs. 1 DSGVO. Art. 17 Abs. 3 DSGVO schränkt dieses Recht wiederum ein, wenn die Verarbeitung für einen der in Abs. 3 genannten Zwecke, etwa zur Ausübung des Rechts auf freie Meinungsäußerung, erforderlich ist.
An zwei Stellen öffnet sich Art. 17 DSGVO für das mitgliedstaatliche Recht: Eine mitgliedstaatliche rechtliche Verpflichtung kann sowohl das Recht auf Löschung begründen (Art. 17 Abs. 1 lit. e DSGVO) als auch einschränken (Art. 17 Abs. 3 lit. b DSGVO).
Art. 17 Abs. 1 lit. e DSGVO erhielt auf Wunsch des Parlaments Eingang in die DSGVO. Zuvor fand sich dieses Merkmal zur Begründung einer Löschpflicht nicht in Art. 17 Abs. 1 DSGVO.
Der Anwendungsbereich des Art. 17 Abs. 3 lit. b DSGVO erfuhr im Entwurf des Rats erhebliche Ausweitung: Sah die Norm in den Entwürfen von Kommission und Parlament noch eine Beschränkung der Löschpflicht nur aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit vor, bestimmt Art. 17 Abs. 3 lit. b DSGVO nunmehr auch eine Beschränkung jener Pflicht aus Gründen einer rechtlichen Verpflichtung, die sich aus nationalem oder unionalem Recht ergibt, sowie bei Erforderlichkeit für die Wahrnehmung öffentlicher Aufgaben oder übertragener hoheitlicher Gewalt.

b. Qualifikation der Öffnungsklausel

Die Öffnungsklauseln des Art. 17 DSGVO stellen lediglich unechte Öffnungsklauseln dar. Sie erlauben nicht selbst die Etablierung von Lösch- und Verarbeitungspflichten, sondern beziehen sich alleine auf andernorts bereits bestehende entsprechende Verpflichtungen des Verarbeiters. Art. 17 Abs. 1 lit. e DSGVO, und für die Beschränkung des Löschanspruchs entsprechend Art. 17 Abs. 3 lit. b DSGVO, geben den Mitgliedstaaten daher keinen zusätzlichen Spielraum, um innerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung[87] Rechtsgrundlagen zu erlassen, die das Recht auf Löschung begründen (Abs. 1 lit. e) oder beschränken (Abs. 3 lit. b).

aa) Rechtliche Verpflichtung, Abs. 1 lit. e bzw. Abs. 3 lit. b Var. 1

Rechtliche Verpflichtungen des mitgliedstaatlichen Rechts i. S. d. Art. 17 Abs. 1 lit. e DSGVO können sich insbes. auf Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO[88] stützen. Dies folgt aus dem insoweit gleichen Wortlaut. Da es Art. 6 Abs. 1 UAbs. 1 lit. c i. V. m. Art. 6 Abs. 2, 3 (ex Art. 6 Abs. 2a, 3) DSGVO den Mitgliedstaaten ermöglicht, rechtliche Verpflichtungen zu etablieren, aus denen auch das Erfordernis einer Löschung von Daten folgen kann, können auf diesem Weg Löschpflichten erwachsen.
Weniger klar ist hingegen, ob Art. 17 Abs. 1 lit. e DSGVO auch Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO in Bezug nimmt. Dies ist nach dem klaren Wortlaut – und anders als bei Art. 17 Abs. 3 lit. b DSGVO – nicht der Fall. Ob dies ein Redaktionsversehen ist, scheint zweifelhaft. Vielmehr liegt die Vermutung nahe, dass der Normgeber davon ausgegangen ist, dass die Verarbeitung zur Wahrnehmung einer Aufgabe zwar ein zwingendes Speicher-, aber kein zwingendes Löschbedürfnis begründen kann. Dies ist nachvollziehbar, da eine Aufgabenwahrnehmung zumeist mit der Verarbeitung i. S. e. Nutzung von Daten verbunden sein wird. Gleichwohl kann dies in Ausnahmefällen anders liegen. In diesem Fall kann allenfalls eine analoge Anwendung des Art. 17 Abs. 3 lit. b DSGVO oder eine grundrechtskonforme Auslegung da-

[87] Vgl. S. 4.
[88] Vgl. S. 30.

hin angezeigt sein, dass auch Aufgabenwahrnehmungen nach Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO eine Löschpflicht hervorrufen können.

bb) Wahrnehmung von Aufgaben im öffentlichen Interesse und hoheitliche Gewalt, Abs. 3 lit. b Var. 2

Art. 17 Abs. 3 lit. b DSGVO gestattet es den Mitgliedstaaten, die Löschpflicht zu beschränken, wenn die Verarbeitung erforderlich ist zur Wahrnehmung von Aufgaben im öffentlichen Interesse oder zur Ausführung von hoheitlicher Gewalt, die dem Verantwortlichen übertragen wurde. Art. 17 Abs. 3 lit. b Var. 2 DSGVO nimmt damit auf Verarbeitungen Bezug, die nach Art. 6 Abs. 1 UAbs. 1 lit. c oder e DSGVO zulässig sind.

c. Abgleich mit dem bestehenden nationalen Recht am Beispiel des § 35 Abs. 2 BDSG; Handlungsmöglichkeiten

Löschpflichten ergeben sich im nationalen Recht etwa aus § 35 Abs. 2 S. 2 BDSG, der allgemeine Löschpflichten begründet. Die dortigen Löschpflichten decken sich teilweise mit den Vorgaben des Art. 17 Abs. 1 DSGVO[89], begründen aber teilweise auch diesem gegenüber abweichende Löschpflichten. So sieht § 35 Abs. 2 S. 2 Nr. 2 BDSG eine Löschpflicht von personenbezogenen Daten für sensible Daten vor, deren Richtigkeit von der verantwortlichen Stelle nicht bewiesen werden kann, während Art. 17 Abs. 1 DSGVO eine solche für sensible Daten nach Art. 9 DSGVO und den Grund der Nicht-Beweisbarkeit nicht explizit regelt. Es stellt sich insofern die Frage, ob die Reichweite der unechten Öffnungsklausel des Art. 17 Abs. 1 lit. e DSGVO die Aufrechterhaltung bzw. den Erlass von einer derartigen allgemeinen Norm umfasst. Da diese grundsätzlich nur auf rechtliche Verpflichtungen nach Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO mit Art. 6 Abs. 2, 3 (ex Art. 6 Abs. 2a, 3) DSGVO verweist, fehlt es in Art. 17 DGSVO an einer generellen Klausel, die den Mitgliedstaaten explizit die Möglichkeit gibt, allgemeine Löschpflichten vorzusehen. Die rechtliche Verpflichtung kann also nur aus

[89] Vgl. § 35 Abs. 2 S. 2 Nr. 1 BDSG, der eine Löschpflicht für unzulässigerweise *gespeicherte* personenbezogene Daten regelt. Art. 17 Abs. 1 lit. a DSGVO regelt die Löschpflicht für unzulässigerweise *verarbeitete* personenbezogene Daten und geht damit über § 35 Abs. 2 S. 2 Nr. 1 BDSG hinaus.

mitgliedstaatlichem Recht erwachsen, das außerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung besteht bzw. künftig erlassen wird, oder in mitgliedstaatlichem Recht liegen, das durch eine echte Öffnungsklausel der Datenschutz-Grundverordnung aufrechterhalten oder erlassen werden konnte.[90]

Ob die Vorschrift des § 35 Abs. 2 S. 2 Nr. 2 BDSG damit noch nach Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO i. V. m. Art. 6 Abs. 2, 3 (ex Art. 6 Abs. 2a, 3) DSGVO aufrechterhalten werden kann, ist zweifelhaft. Denn sie begründet keinen Löschungsbedarf zur Erfüllung einer besonderen Verbindlichkeit, sondern macht die Löschung selbst zu einer Verbindlichkeit. Dies ist wohl eher eine unzulässige Konkretisierung des Art. 17 Abs. 1 DSGVO (oder gar Abweichung von Art. 16 DSGVO, der in Fällen der Unrichtigkeit keine Löschung, sondern eine Berichtigung vorsieht), als eine nach Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO zulässige Öffnung. Dies kann alleine mit Blick auf die Öffnungsklausel des Art. 23 Abs. 1 (insbes. lit. i) DSGVO anders gesehen werden. Denn eine von der DSGVO nicht vorgesehene Pflicht zur Löschung bei nicht beweisbarer Richtigkeit von besonderen personenbezogenen Daten ist in jedem Fall geeignet, die betroffene Person zu schützen.

13. Art. 22 Abs. 2 lit. b (ex Art. 20 Abs. 1a lit. b) und Abs. 4 i. V. m. Art. 9 Abs. 2 lit. g: automatisierte Generierung von Einzelentscheidungen

Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO etabliert ein Verbot automatisierter Einzelfallentscheidungen: Er will den Einzelnen davor schützen, zum Objekt von Einzelfallentscheidungen zu werden, die nicht ein Mensch (nach individueller Einschätzung und Bewertung) getroffen hat. Ihren normativen

[90] Indes ist es wichtig zu erwähnen, dass der Verarbeitungsbegriff aus Art. 4 Nr. 2 (ex Art. 4 Nr. 3) DSGVO auch die Löschung umfasst. Am Beispiel des Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO, Abs. 2 (ex Abs. 2a) DSGVO bedeutet das etwa, dass nicht nur, wie die Ausführungen aus S. 36 zeigen, eine Vielzahl von bereichsspezifischen Normen aufrechterhalten werden können, sondern auch die Aufrechterhaltung der korrespondierenden Löschungspflichten von *dieser* Öffnungsklausel umfasst sind. Es sind hier also keine Widersprüche dahin gehend zu befürchten, dass Mitgliedstaaten die Zulässigkeitstatbestände der Verarbeitung erweitern, korrespondierende Löschpflichten jedoch nicht regeln könnten.

Anspruch erstreckt die Vorschrift auf alle Entscheidungen, die auf der Grundlage rein maschinell-automatischer Verfahren entstanden sind, sofern die jeweilige Entscheidung dem Betroffenen gegenüber rechtliche Wirkung entfaltet oder ihn erheblich beeinträchtigt.[91] Das Verbot spricht die DSGVO jedoch nicht vorbehaltlos aus. Die Mitgliedstaaten (und die Union) dürfen durch Rechtsvorschrift Ausnahmen erlassen. Diese Rechtsvorschrift muss aber angemessene Maßnahmen („suitable safeguards") enthalten, um die Interessen der Betroffenen zu schützen, Art. 22 Abs. 2 lit. b (ex Art. 20 Abs. 1a lit. b) DSGVO.

a. Einordnung der Öffnungsklausel in das System mitgliedstaatlicher Regelungsspielräume

Die Öffnungsklausel des Art. 22 Abs. 2 lit. b (ex Art. 20 Abs. 1a lit. b) DSGVO erlaubt eine Absenkung des Schutzniveaus für das allgemeine Persönlichkeitsrecht. Es handelt sich nicht um eine obligatorische, sondern um eine fakultative Öffnungsklausel.

b. Vergleich zur Datenschutzrichtlinie

Art. 22 (ex Art. 20) DSGVO führt den Grundgedanken des Art. 15 DSRL fort. Auch er ließ es bereits zu, dass die Mitgliedstaaten automatisierte Einzelentscheidungen gestatten dürfen (Art. 15 Abs. 2 lit. b DSRL). Die Richtlinie stellte dies aber (wie auch jetzt Art. 22 Abs. 2 lit. b DSGVO) unter den Vorbehalt, dass das die Rechtsvorschrift Garantien zur Wahrung der berechtigten Interessen der betroffenen Person festlegt.

c. Anwendungsbereich der Öffnungsklausel – Entscheidung, die auf einer automatisierten Datenverarbeitung beruht

Wann eine Entscheidung vorliegt, die allein auf einer automatisierten Datenverarbeitung beruht, spezifizieren weder die Datenschutz-Grundverordnung noch die DSRL. Orientiert man sich am *Wortlaut der Vorschrift („based*

[91] Ob die rechtlichen Folgen positiver oder negativer Natur sind, ist unerheblich, so zur DSRL *Brühann*, in: Grabitz/Hilf (Hrsg.), EU-Recht, 51. EL, 2013, Art. 15 Datenschutzrichtlinie, II. 2., Rn. 6.

solely on automated processing"), so sind damit solche Entscheidungen gemeint, bei denen *kein menschlicher Entscheidungsschritt* zwischentritt.[92]
Einen Grenzfall bilden solche Konstellationen, in denen eine natürliche Person einen *rein formalen letzten Schlussakt der Bestätigung* setzt. In diesem Fall hat die automatisierte Verarbeitung die wesentliche Vorentscheidung bereits herbeigeführt. Für die Differenzierung kommt es darauf an, ob ein Mensch auf die Entscheidung substanziellen Einfluss nimmt.
Fehlt einem Sachbearbeiter eine eigene menschliche Entscheidungsbefugnis, trifft er jedenfalls keine Entscheidung. Verbleibt ihm dagegen eine eigene inhaltliche Entscheidungsbefugnis, heißt das zugleich noch nicht zwingend, dass ein Mensch eine Entscheidung trifft. Erst dann, wenn er seine Entscheidungsmacht ausübt und nicht vollständig einem Algorithmus überlässt, wirkt er auf den Entscheidungsablauf ein. Die Entscheidung, *nicht* auf den automatisierten Prozess einzuwirken, genügt insoweit noch nicht, um von einem menschlichen Eingreifen zu sprechen. Auch eine Stichprobenkontrolle reicht nicht aus. Erforderlich ist vielmehr ein Eingreifen in den Entscheidungsprozess, der über eine rein formelhafte Bestätigung des computertechnisch ermittelten Ergebnisses hinausgeht.
Für eine solche (auch dem bisherigen deutschen Recht entsprechende) Auslegung streitet sowohl der enge Wortlaut („*ausschließlich*[93] auf einer automatisierten Verarbeitung")[94] als auch das Telos des Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO: Die Vorschrift zielt ebenso wie § 6a Abs. 1 S. 2 BDSG nicht darauf, die Entscheidungs*unterstützung* und -*vorbereitung* durch automatisierte Verfahren zu verhindern. Vielmehr will er die Gefahren begrenzen, die von nicht überprüften automatisierten *Entscheidungen*, insbesondere durch Bildung von Persönlichkeitsprofilen, ausgehen. Der Einzelne soll nicht bloßes Objekt eines Entscheidungsautomatismus werden, weil das schwerwiegende Folgen für den Persönlichkeitsschutz zeitigen könnte.[95]

---

[92] So wohl zur DSRL *Brühann* (Fn. 91), Art. 15 Datenschutzrichtlinie, II. 2., Rn. 7.
[93] Hervorhebung d. Verf.
[94] Ähnlich EG 71 UAbs. 1 S. 1 (ex 58 S. 1) DSGVO, der klarstellt, dass das grundsätzliche Verbot der Datenschutz-Grundverordnung sich auf „ausschließlich auf einer automatisierten Verarbeitung" beruhende Vorgänge erstreckt.
[95] *Scheja/Haag*, in: Leupold/Glossner (Hrsg.), HdBuch IT-Recht, 3. Aufl., 2013, Teil 5 - Datenschutzrecht, Rn. 225.

EG 71 UAbs. 1 S. 4 a. E. (ex EG 58 S. 4) und Art. 22 Abs. 3 (ex Art. 20 Abs. 1b) DSGVO scheinen auf den ersten Blick eine andere Deutung nahe zu legen. Sie lassen sich bei weiter Interpretation so lesen, dass Art. 22 (ex Art. 20) Abs. 1 DSGVO solche Fälle meint, in denen ein automatisierter Vorgang eine menschliche Entscheidung vorbereitet. Sie sprechen nämlich von einem „Eingreifen einer Person" in den Entscheidungsprozess.
Diese Deutung greift allerdings zu kurz. Denn die Vorschrift geht vielmehr umgekehrt davon aus, dass in diesen Fällen eine ausnahmsweise zulässige *automatisierte* Entscheidung vorliegt, stellt ihre Zulässigkeit aber unter den Vorbehalt, dass der Betroffene im Einzelfall einen Anspruch auf direktes Eingreifen in den vollständig automatisierten Entscheidungsprozess geltend machen kann. Die Vorschrift bestätigt daher das Gegenteil: Art. 22 (ex Art. 20) DSGVO knüpft ausschließlich an eine *ohne jegliche* menschliche Entscheidungsgewalt stattfindende Entscheidung an.[96] Ausnahmen von diesem Verbot dürfen die Mitgliedstaaten nur in dem Bereich eröffnen, in dem der Grundtatbestand des Art. 22 Abs. 1 (ex Art. 20 Abs. 1 DSGVO) überhaupt tatbestandlich berührt ist.

d. Voraussetzungen der Öffnungsklausel

Die Datenschutz-Grundverordnung benennt in ihren Erwägungsgründen exemplarisch Anwendungsfälle, in denen eine automatisierte Verarbeitung zu Zwecken der Profilbildung zulässig sein kann: um Betrug sowie Steuerhinterziehung zu überwachen und verhindern oder die Zuverlässigkeit und Sicherheit eines Dienstes zu gewährleisten, den der Verantwortliche bereitgestellt hat (EG 71 UAbs. 1 S. 3 [ex EG 58 S. 3] DSGVO). Diese Anwendungsfälle schließen andere nicht aus. Vielmehr knüpft der Unionsgesetzgeber die Öffnungsklausel an drei Voraussetzungen.

aa) Gesetzliche Erlaubnis des Mitgliedstaats

Vom Verbot automatisierter Einzelfallentscheidung darf der Mitgliedstaat nur durch Rechtsvorschrift („law") dispensieren. Was die Datenschutz-Grundverordnung darunter versteht, erhellt ein Blick auf die Ratio der Vor-

[96] Dazu auch *Martini*, in: Paal/Pauly (Hrsg.), DSGVO, 2016, Art. 22, Rn. 16 ff.

schrift sowie den EG 41 (ex EG 31a) DSGVO: Nach dem Sinnzusammenhang einer Öffnung der Regelungsbefugnis für nationales Recht reicht grundsätzlich jede normative Rechtsregel des nationalen Rechts aus. Es muss sich also nicht unbedingt um ein formelles Gesetz handeln.[97]. Es kann auch materielles Gesetzesrecht wie z. B. Satzungsrecht genügen (vgl. auch S. 8). Nicht ausreichend sind aber Selbstregulierungsregeln im Sinne des Art. 40 (ex Art. 38) DSGVO. Bei ihnen handelt es sich nicht um *staatliches* Recht.

bb) Anwendbarkeit des nationalen Rechts auf den Verantwortlichen

Von dem Verbot des Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO kann das nationale Recht nur befreien, wenn der Verantwortliche dem deutschen Recht unterliegt. Das ergibt sich außer aus dem Wortlaut der Norm auch aus den Grenzen des Anwendungsbereichs der Datenschutz-Grundverordnung. Den Rahmen dafür zieht Art. 4 Nr. 16 lit. a und b (ex Art. 4 Abs. 13 lit. a, b) DSGVO. Hat der Verantwortliche seine Niederlassung in der Bundesrepublik, unterfällt er deutschem Datenschutzrecht. Bei mehreren Niederlassungen entscheidet gem. Art. 4 Nr. 16 lit. a (ex Art. 4 Abs. 13 lit. a) DSGVO der Sitz der Hauptverwaltung oder der einer anderen Niederlassung – aber nur, wenn Letztere die Ziele und Mittel der Verarbeitung festlegt und befugt ist, diese Entscheidungen umsetzen zu lassen. Für die Auftragsdatenverarbeitung bestimmt Art. 4 Nr. 16 lit. b (ex Art. 4 Abs. 13 lit. b) DSGVO, dass primär der Sitz der Hauptverwaltung entscheidet – und nur, wenn diese sich nicht in der Union befindet, diejenige Niederlassung in der Union, in der die Auftragsdatenverarbeitung hauptsächlich stattfindet, soweit der Auftragsverarbeiter spezifischen Pflichten der Datenschutz-Grundverordnung unterliegt.

cc) Geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person

Den Schutzstandard des Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO dürfen die Mitgliedstaaten nicht beliebig aushöhlen und damit die Wertungen des Unionsrechts konterkarieren. Sie müssen – auch wenn sie von der Öffnungs-

[97] Aus der Perspektive des nationalen Rechts, insbesondere aus dem Wesentlichkeitsvorbehalt der Verfassung, kann sich Anderes ergeben.

klausel Gebrauch machen – Maßnahmen treffen, die dem Recht auf informationelle Selbstbestimmung des Betroffenen, welches die Vorschrift schützen will, einen geeigneten Schutz verleihen.

Die Zielrichtung und den gewollten Inhalt solcher Schutzmaßnahmen deuten die EG 71 UAbs. 1 S. 4, 67 S. 2 und 3 (ex EG 58 S. 4, 54a S. 2)[98] und 68 S. 1 (ex 55 S. 1)[99] sowie Art. 22 Abs. 3 (ex Art. 20 Abs. 1b) a. E. DSGVO an.[100] Zu den Schutzmaßnahmen können danach insbesondere eine spezifische Unterrichtung des Betroffenen, ein Anspruch auf direktes Eingreifen einer Person, Ansprüche auf Darlegung des eigenen Standpunkts sowie auf Erläuterung und die Möglichkeit zur Überprüfung der getroffenen Entscheidung zählen. Automatisierte Entscheidungen sollten zudem kein Kind betreffen (EG 71 UAbs. 1 S. 5 [ex EG 58 S. 4 enthielt noch ein dahin gehendes *Verbot*] DSGVO). Die Analyse muss auch auf geeigneten mathematischen bzw. statistischen Verfahren beruhen, die das Risiko von Fehlern minimieren und zur Korrektur unzutreffender Daten führen, insbesondere diskriminierende Wirkungen nach Möglichkeit ausschließen (EG 71 UAbs. 2 S. 1 [ex EG 58 S. 5] DSGVO). Den Anforderungen der Verordnung genügt es grundsätzlich, wenn die Maßnahmen geeignet sind, dem Betroffenen Einsicht in die Bewertungsmaßstäbe zu gewähren[101] und die Möglichkeit zu eröffnen, seinen Standpunkt

---

[98] „In automatisierten Dateisystemen sollte die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel so erfolgen, dass die personenbezogenen Daten in keiner Weise weiterverarbeitet werden und nicht verändert werden können. Auf die Tatsache, dass die Verarbeitung der personenbezogenen Daten beschränkt wurde, sollte in dem System unmissverständlich hingewiesen werden."

[99] Dieser Erwägungsgrund gibt der Verordnung sowie den Mitgliedstaaten mit auf den Weg, dass im Rahmen automatisierter Datenverarbeitung Betroffene grundsätzlich berechtigt sein sollen, die sie betreffenden Daten in strukturierter, gängiger und maschinenlesbarer Form zu erhalten. Dieses Recht soll aber nach EG 68 S. 4 (ex 55 S. 4) gerade nicht bei derjenigen Verarbeitung Anwendung finden, die sich auf eine gesetzliche Erlaubnis außerhalb der Einwilligung bezieht. Dem folgend soll gemäß EG 68 S. 5 (ex 55 S. 5) jenes Recht nicht gegen solche Verantwortliche ausgeübt werden, deren Datenverarbeitung sich als Erfüllung öffentlicher Aufgaben darstellt. Dies eröffnet für die Datenverarbeitung öffentlicher Stellen eine bei gleicher Einschränkbarkeit weniger weitgehende Verpflichtung, hinreichende Sicherungsmaßnahmen in die Erlaubnisnorm einzuziehen. Demgegenüber haben private Verantwortliche dieser Auskunftsverpflichtung grundsätzlich nachzukommen.

[100] Dazu und zum Folgenden *Martini* (Fn. 96), Art. 22, Rn. 35 f.

[101] So auch schon EG 41 DSRL: „Jede Person muß ein Auskunftsrecht hinsichtlich der sie betreffenden Daten, die Gegenstand einer Verarbeitung sind, haben, damit sie sich insbesondere

deutlich hervorzuheben. Eine Offenlegung des die Entscheidung herbeiführenden Algorithmus gegenüber dem Betroffenen ist regelmäßig nicht erforderlich.[102] Denn dadurch würden schutzwürdige Geheimhaltungsinteressen der Verarbeiter, namentlich Betriebs- und Geschäftsgeheimnisse, verletzt. Diesen darf der Mitgliedstaat bei seiner Regelung Rechnung tragen.
Da Art. 22 Abs. 1 Alt. 1 (ex Art. 20 Abs. 1 Alt. 1) DSGVO nur auf mit Persönlichkeitsbeeinträchtigungen verbundene Rechtsfolgen abhebt, ist eine für den Betroffenen *positive* Entscheidung in der Regel vom Erfordernis geeigneter Schutzmaßnahmen dispensiert.

dd) Rückausnahme nach Art. 22 Abs. 4 (ex Art. 20 Abs. 3)

Automatisierte Einzelentscheidungen darf das mitgliedstaatliche Recht ausnahmsweise dann nicht erlauben, wenn sie auf besonderen Kategorien personenbezogener Daten nach Art. 9 Abs. 1 DSGVO beruhen. Den Begriff der „besonderen Kategorien personenbezogener Daten“ definiert Art. 9 Abs. 1 DSGVO. Das grundsätzliche Verbot ihrer automatisierten Verarbeitung gilt aber seinerseits vorbehaltlos. Die Verordnung lässt ihre Einbeziehung in eine automatisierte Verarbeitung in zwei Fällen zu: zum einen, sofern der Betroffene in die Verarbeitung für einen oder mehrere festgelegte Zwecke ausdrücklich *einwilligt* (es sei denn die Union oder der Mitgliedstaat schränkt das durch Sonderregeln ausdrücklich ein – Art. 22 Abs. 4 i. V. m. Art. 9 Abs. 2 lit. a DSGVO), zum anderen grundsätzlich, sofern die Verarbeitung wegen eines *erheblichen öffentlichen Interesses* erforderlich und auch insgesamt verhältnismäßig ist (Art. 22 Abs. 4 i. V. m. Art. 9 Abs. 2 lit. g DSGVO).[103] Im letztgenannten Fall darf nicht nur die Union, sondern auch jeder Mitgliedstaat eine eigene Verarbeitungserlaubnis schaffen. Einer solchen bedarf es

---

von der Richtigkeit dieser Daten und der Zulässigkeit ihrer Verarbeitung überzeugen kann. Aus denselben Gründen muß jede Person außerdem das Recht auf Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten, zumindest im Fall automatisierter Entscheidungen im Sinne des Artikels 15 Absatz 1, besitzen. Dieses Recht darf weder das Geschäftsgeheimnis noch das Recht an geistigem Eigentum, insbesondere das Urheberrecht zum Schutz von Software, berühren. Dies darf allerdings nicht dazu führen, daß der betroffenen Person jegliche Auskunft verweigert wird.“

[102] Dazu etwa BGHZ 200, 38 – Scorewerte.

[103] Siehe dazu S. 53.

dann aber auch, um die Verarbeitung solcher Daten aus Gründen öffentlichen Interesses zuzulassen. Im Hinblick auf das besondere Gefährdungspotenzial legt die Union die Maßstäbe für eine solche Öffnungsklausel inhaltlich hoch: Die Erlaubnis (des Mitgliedstaates bzw. der Union) muss den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene sowie spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen Betroffener vorsehen.

e. Abgleich mit dem bestehenden nationalen Recht

Eine Regelung über automatisierte Einzelentscheidungen enthält das nationale Recht bislang in § 6a BDSG. Es macht damit von dem bisher – auf der Grundlage der DSRL bestehenden – Regelungsspielraum des Unionsrechts bereits Gebrauch. § 6a Abs. 2 Nr. 2 BDSG befreit von dem Verbot automatisierter Einzelentscheidungen, wenn die berechtigten Individualinteressen durch geeignete Maßnahmen gewahrt sind und der Verantwortliche dem Betroffenen „die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert."[104] Insbesondere der zweite Halbsatz des § 6a Abs. 2 Nr. 2 BDSG bewegt sich in dem Spielraum, den die Öffnungsklausel des Art. 22 Abs. 2 lit. b DSGVO (bzw. bislang die DSRL) belässt; der erste Halbsatz transferiert lediglich die angemessenen Maßnahmen („suitable safeguards") der Öffnungsklausel in nationales Recht.

Für den Bereich der öffentlichen Verwaltung erlangt die Öffnungsklausel des Art. 22 (ex Art. 20) DSGVO insbesondere dann Bedeutung, wenn der Bundesgesetzgeber seinen Plan zur Zulassung automatisierter Verwaltungsverfahren im Steuerverfahren umsetzt. Einen entsprechenden Beschluss hat das Kabinett Ende 2015 getroffen (vgl. § 155 Abs. 4 AO-E – Regierungsentwurf für ein Gesetz zur Modernisierung des Besteuerungsverfahrens).[105]

---

[104] Vgl. zum darin zu sehenden dreistufigen Verfahren aus Information über die automatisierte Einzelentscheidung, Mitteilung und Erläuterung der wesentlichen Entscheidungsgründe auf Anfrage des Betroffenen und schließlich die Möglichkeit, den eigenen Standpunkt deutlich zu machen, um ggf. eine Revision der Entscheidung zu erreichen, *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 6a, Rn. 14, 14a.

[105] Dazu *Braun Binder*, NVwZ 2016, 342 ff.

Aber auch hinsichtlich der bestehenden Regelungen zum Scoring verdient die Öffnungsklausel des Art. 22 (ex Art. 20) DSGVO detaillierte Betrachtung. Nicht ganz klar ist, inwieweit § 28b BDSG (ähnlich auch § 28a BDSG) sich auf sie stützen lässt und daher im neuen nationalen Datenschutzrecht aufrechterhalten bleiben kann. EG 71 UAbs. 1 S. 1 und 2 (ex EG 58 S. 1 und 2) DSGVO indizieren, dass das Verbot aus Art. 22 (ex Art. 20) DSGVO grundsätzlich auch das Scoring adressiert („Online-Kreditantrags", „unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person […], insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage"). Allerdings bezieht sich das dann nur auf die ausschließlich automatisierte Entscheidung, der *keine menschliche Entscheidung* vorausgeht. In diesem Fall eröffnet die Öffnungsklausel die Möglichkeit einer mitgliedstaatlichen Regelung des Scorings. Das Scoring selbst ist aber noch keine Entscheidung, sondern bereitet diese lediglich vor. Eine mitgliedstaatliche Regelung des Scorings, die der Rechtssicherheit dient und den Zielen der DSGVO nicht zuwiderläuft, sondern diese nur für einen praktisch relevanten Bereich näher präzisiert, ist allenfalls implizit von der Öffnungsklausel des Art. 22 Abs. 2 lit. b (ex Art. 20 Abs. 1a lit. b) DSGVO[106] oder Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO umfasst.[107]

14. Art. 23 (ex Art. 21): Betroffenenrechte

a. Struktur und Entstehungshintergrund

Art. 23 (ex Art. 21) DSGVO sieht die Möglichkeit zur Abweichung von den Art. 12 bis 22 (ex Art. 12 bis 20) DSGVO, also den Betroffenenrechten, sowie dem „besonderen Betroffenenrecht" des Art. 34 (ex Art. 32) DSGVO, der Benachrichtigung der betroffenen Person im Fall einer Verletzung des Schutzes ihrer personenbezogenen Daten, und den in Art. 5 DSGVO normierten Grundprinzipien vor, soweit sie mit den Betroffenenrechten der Art. 12 - 22 (ex Art. 12 – 20) DSGVO zusammenhängen (dazu aa)). Dazu muss die Ab-

[106] Für einen Rückgriff auf diese Öffnungsklausel plädierend *Taeger*, ZRP 2016, 72 (74 f.) m. w. N.
[107] Dazu im Einzelnen unten S. 440.

weichung die in Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO näher angeführten, vielfältigen öffentlichen Interessen sicherstellen (dazu bb)). Zudem müssen die Betroffenenrechte soweit wie möglich durch die Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO aufgeführten spezifischen Regelungen geschützt werden sowie insgesamt „in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme“ darstellen (Art. 23 Abs. 1 [ex Art. 21 Abs. 1 DSGVO]) (dazu cc)).

Die Möglichkeit zur Abweichung samt entsprechender Gründe hatte bereits der Kommissionsentwurf vorgesehen. Der Entwurf des Europäischen Parlaments sah erstmals die ausdifferenzierte Einschränkung dieser Abweichungsmöglichkeit in Form des Anforderungskatalogs vor. Diese Grundstruktur wurde in der Ratsfassung dem Grunde nach gebilligt und war – mit jeweils kleineren Modifikationen – Ergebnis des Trilogs.

Erwägungsgründe, die näheren Aufschluss über die Reichweite und Stoßrichtung der Öffnungsklausel geben, finden sich in der Datenschutz-Grundverordnung nicht.

Auch die DSRL sah bereits Abweichungsmöglichkeiten von den Betroffenenrechten vor – und zwar sowohl bei den einzelnen Betroffenenrechten als auch eine generelle Beschränkungsmöglichkeit in Art. 13 DSRL. So schränkt Art. 14 lit. a DSRL das Widerspruchsrecht für den Fall „einer im einzelstaatlichen Recht vorgesehenen entgegenstehenden Bestimmung“ ein. EG 69 S. 1 DSGVO und Art. 21 Abs. 1 DSGVO bestätigen insoweit, dass ein Widerspruchsrecht der Betroffenen aus „sich aus ihrer besonderen Situation ergebenden Daten“ eigentlich gerade auch in Bezug auf eine rechtmäßige Datenverarbeitung im öffentlichen Interesse bestehen sollte.

b. Qualifikation der Öffnungsklausel

Art. 23 (ex Art. 21) DSGVO stellt angesichts der Breite seines Anwendungsbereichs eine allgemeine Öffnungsklausel dar, die in zahlreichen Sektoren bereichsspezifisch oder auch horizontal die Beschränkung der Betroffenenrechte und korrespondierender Regelungen eröffnet. Da sie eine Abweichung jedoch nicht vorgibt, handelt es sich um eine fakultative Öffnungsklausel, die in der Sache Modifikationen des Regelungsgehalts der Verordnung ermöglicht. Ein Handlungsbedürfnis auf nationaler Ebene besteht demnach nur, sofern der nationale Gesetzgeber die Betroffenenrechte im Bereich der Da-

tenverarbeitung zu besonderen öffentlichen Zwecken einschränken möchte. Dann greifen anspruchsvolle Anforderungen an derartige Einschränkungen. Da Einschränkungen grundsätzlich zur Verfolgung öffentlicher Zwecke erfolgen können, sind Adressat der Regelung vor allem öffentliche Stellen in der überkommenen deutschen datenschutzrechtlichen Differenzierung.

c. Voraussetzungen der Öffnungsklausel

aa) Abweichungsmöglichkeiten von Art. 12 bis 22 (ex Art. 12 bis 20), 5 und 34 (ex 32)

Die Art. 12 bis 22 (ex Art. 12 bis 20) DSGVO definieren umfassend die Betroffenenrechte, von denen gemäß Art. 23 (ex Art. 21) DSGVO Abweichungsmöglichkeiten bestehen.[108]
Ergänzend verweist die Datenschutz-Grundverordnung auf das spezifische Betroffenenrecht in Art. 34 (ex Art. 32) DSGVO zur Benachrichtigung der

[108] Es handelt sich dabei namentlich um:
Art. 12: prozedural begleitend für alle Betroffenenrechte „das Verfahren und Vorkehrungen, damit die betroffene Person ihre Rechte ausüben kann“;
Art. 13 (ex Art. 14): Informationspflichten des Verantwortlichen gegenüber der betroffenen Person einschließlich entsprechender Ausnahmen;
Art. 14 (ex Art. 14a): entsprechende Informationspflichten, „wenn die Daten nicht bei der betroffenen Person erhoben wurden“, einschließlich korrespondierender Ausnahmen;
Art. 15: Auskunftsrecht der betroffenen Person gegenüber der Verantwortlichen;
Art. 16: „Recht auf Berichtigung“;
Art. 17: „Recht auf Vergessenwerden und auf Löschung“ einschließlich entsprechender Einschränkungen;
Art. 18 (ex Art. 17a): „Recht auf Einschränkung der Verarbeitung“, das eingeschränkte Verarbeitungsmöglichkeiten in Fällen der umstrittenen Richtigkeit von Daten, der Verwendung von Daten zur Sicherung von Rechtsansprüchen und eines noch nicht geklärten Widerspruchs vorsieht;
Art. 19 (ex Art. 17b): „Mitteilungspflicht im Zusammenhang mit der Berichtigung, Löschung oder Einschränkung“, also der Art. 16, 17 und 18 (ex 17a);
Art. 20 (ex Art. 18): „Recht auf Datenübertragbarkeit“;
Art. 21 (ex Art. 19): „Widerspruchsrecht“,
Art. 22 (ex Art. 20): Recht, nicht Adressat einer allein auf einer automatisierten Verarbeitung beruhenden Entscheidung zu sein, wobei insoweit kein klassisches prozedurales Betroffenenrecht, sondern eher ein materiell-rechtlich geprägtes Recht vorliegt.
Das korrespondierende Recht wird daher systematisch überzeugender im BDSG auch nicht bei den Betroffenenrechten der §§ 19 ff. BDSG normiert, sondern im Allgemeinen Teil in § 10 BDSG.

betroffenen Person von einer Verletzung des Schutzes ihrer personenbezogenen Daten sowie auf die allgemeinen Verarbeitungsregeln in Art. 5 DSGVO – damit korrespondierend die Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten.
Damit ist eine Abweichungsmöglichkeit ratione materiae im umfassenden Sinne für sämtliche Betroffenenrechte geschaffen worden.

bb) Gründe für Abweichungen

Vielfältig sind auch die öffentlichen Interessen, die eine Abweichung rechtfertigen. Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO führt sie auf. Dies sind namentlich nationale Sicherheit; Verteidigung; öffentliche Sicherheit; Strafprävention, -verfolgung und -vollstreckung; wichtige Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaates; Schutz der Gerichtsverfahren und der Unabhängigkeit der Justiz; Prävention, Verfolgung etc. von berufsständischen Verstößen; Kontrollfunktionen im Rahmen der Ausübung öffentlicher Gewalt; Schutz der betroffenen Person und der Freiheiten anderer Personen und die Durchsetzung zivilrechtlicher Ansprüche.

cc) Voraussetzungen für Abweichungen

Umfangreich sind auch die Anforderungen, die entsprechende nationale Gesetze gemäß Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO spezifisch regeln müssen, soweit dies mit dem verfolgten Zweck vereinbar ist („gegebenenfalls“). Gleichzeitig ist die Liste der Regelungen nicht abschließend („zumindest“). Insofern führt die Datenschutz-Grundverordnung als grundsätzlich notwendige Regelungsgegenstände auf: Verarbeitungszweck, Datenkategorien, Umfang der Einschränkung, Datensicherungsmaßnahmen, Kategorien der Verarbeiter, Speicherdauer, Risiken für die Rechte und Freiheiten der Betroffenen und dem Recht des Betroffenen, über die Einschränkungen informiert zu werden.
Außerdem muss die Maßnahme in einer demokratischen Gesellschaft notwendig und verhältnismäßig sein (Art. 23 Abs. 1 [ex Art. 21 Abs. 1] DSGVO). Art. 23 Abs. 1 deutet mit der Wendung „durch Rechtsvorschriften der Mitgliedstaaten […] im Wege von Gesetzgebungsmaßnahmen“ prima facie auch an, dass die Mitgliedstaaten die entsprechenden Regelungen im Wege

eines Parlamentsgesetzes treffen müssen. Darauf deutet jedenfalls die Dopplung der normativen Vorgabe (insbesondere wäre der zweite Passus grammatikalisch nicht zwingend erforderlich gewesen) und das insgesamt bewusst hoch gesteckte Anforderungsniveau hin. Gesetzgebungsmaßnahmen können aber in den Mitgliedstaaten eine sehr unterschiedliche Gestalt aufweisen. Auch das Verfahren des Erlasses von Rechtsverordnungen lässt sich beispielsweise als (materielle) Gesetzgebungsmaßnahme verstehen. Daher handelt es sich bei der Wendung „im Wege von Gesetzgebungsmaßnahmen" wohl eher um eine im Wesentlichen tautologische Betonung besonderer mitgliedstaatlicher Regelungsbedürfnisse, die in einer demokratischen Gesellschaft ein Parlamentsgesetz voraussetzen kann, nicht aber per definitionem notwendig muss.
Während demnach in der DSRL pauschale Einschränkungsmöglichkeiten bei der Einräumung von Betroffenenrechten vorgesehen waren, konditioniert die Datenschutz-Grundverordnung entsprechende Abweichungsmöglichkeiten mit einem umfassenden Forderungskatalog.

d. Abgleich mit dem bestehenden nationalen Recht am Beispiel des Widerspruchsrechts aus Art. 21 (ex Art. 19) und der Frage der Beibehaltung des Regelungsgehalts des § 20 Abs. 5 S. 2 BDSG

aa) Der Ausschluss des Widerspruchsrechts in § 20 Abs. 5 S. 2 BDSG

Im deutschen Datenschutzrecht finden sich sowohl im allgemeinen als auch im bereichsspezifischen Datenschutzrecht Abweichungen von den Betroffenenrechten. Im BDSG ist vor allem § 20 Abs. 5 S. 2 BDSG von Bedeutung. Dieser schließt das Widerspruchsrecht pauschal aus, sofern eine gesetzliche Verpflichtung zum Datenumgang besteht. Die Bestimmung definiert weder die Konstellationen näher, in denen eine entsprechende Verpflichtung erfolgt, noch nennt sie die sachlichen bzw. materiellen Rechtfertigungsgründe für die Abweichung. Vielmehr geht der Gesetzgeber des BDSG davon aus, dass sich diese aus entsprechenden Speicherpflichten in den Spezialgesetzen ergeben. Ein Beispiel für derartige Speicherpflichten ist etwa § 3 Bundesmeldegesetz (BMG), der zur Erfüllung der Aufgaben der Meldebehörden das Speichern eines näher spezifizierten Satzes von Meldedaten verlangt.

bb) Ausnahme des § 20 Abs. 5 S. 2 BDSG nicht vom allgemeinen Regelwerk der Datenschutz-Grundverordnung gedeckt

Ob das allgemeine Regelwerk der Datenschutz-Grundverordnung die Ausnahme des § 20 Abs. 5 S. 2 BDSG abdeckt, ist nicht zweifelsfrei. Das Widerspruchsrecht in der Datenschutz-Grundverordnung nach Art. 21 Abs. 1 (ex Art. 19 Abs. 1) greift bei einer Verarbeitung aufgrund von Art. 6 lit. e oder lit. f DSGVO, also insbesondere der Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung hoheitlicher Gewalt, die dem Verantwortlichen übertragen wurde. Auch in diesen Fällen soll der Betroffene grundsätzlich sein Widerspruchsrecht ausüben können, wie EG 69 (ex EG 56) DSGVO deutlich macht. Die Geltendmachung des Widerspruchsrechts verlangt allerdings stets, dass der Betroffene seinen Widerspruch mit seiner besonderen Situation begründet. Erfolgt dies, muss der Verantwortliche zwingende legitime Gründe darlegen, warum ein Widerspruch trotzdem ausgeschlossen ist. Sowohl die besondere Situation, die ein Widerspruchsrecht zu begründen vermag, als auch die zwingenden schutzwürdigen Gründe werden dabei in der Datenschutz-Grundverordnung nicht näher definiert. Anschließend hat eine Abwägung zwischen den kollidierenden Interessen zu erfolgen.

Sofern die gesetzliche Verpflichtung zwingende schutzwürdige Gründe darstellten, die sich sodann in der Abwägung, zwingend durchsetzen, wären damit im Fall des § 20 Abs. 5 S. 2 BDSG die Anforderungen des Art. 21 Abs. 1 (ex Art. 19 Abs. 1) DSGVO inhaltlich erfüllt. Es bedürfte dann keines Rückgriffs auf die Abweichungsklausel. Eine solche Pauschalisierung trägt die einzelfallorientierte Regelung der DSGVO zum Widerspruchsrecht jedoch nicht. Denn es ist keinesfalls zwingend, dass bei jeder gesetzlichen Verpflichtung stets überwiegende schutzwürdige Gründe vorliegen. Für die Vielfalt denkbarer gesetzlicher Speicherpflichten kann dies nicht generell vorausgesetzt werden. Auch hier können im Einzelfall besonders schutzwürdige Interessen des Einzelnen höher zu gewichten sein.

Daher ist eine Aktivierung der Öffnungsklausel notwendig, soll das Widerspruchsrecht im Fall gesetzlicher Speicherpflichten automatisch ausgeschlossen werden.

cc) Handlungsoptionen im Fall der Aktivierung der Öffnungsklausel

Wenn die Öffnungsklausel genutzt werden soll, knüpft sich daran die Frage, welche Umsetzungsoptionen bestehen. Ist dann ein allgemeiner Ausschluss im BDSG-neu möglich? Lässt es die DSGVO zu, dass die Anforderungen des Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO in eine einzelne, allgemeine Norm übernommen werden, die im Falle einer gesetzlichen Speicherverpflichtung das Widerspruchsrecht allgemein ausschließt? Der nationale Gesetzgeber verfügt grundsätzlich über eine weite Freiheit, wie er die Öffnungsklausel technisch umsetzt, sofern die Grenzen der Öffnungsklauseln nicht überschritten werden. Der deutsche Gesetzgeber kann also regelungstechnisch versuchen, weiterhin möglichst viele allgemeine Anforderungen an das Datenschutzrecht im Rahmen der Ausschöpfung der Öffnungsklauseln in einem allgemeinen Datenschutzgesetz zu normieren und nur das Minimum an bereichsspezifischen Regeln tatsächlich in spezifische Gesetze auszulagern. Er kann jedoch auch umgekehrt vorgehen und eine Vielzahl bereichsspezifischer Abweichungen schaffen.

Der Wortlaut des Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO, der „spezifische Vorschriften“ verlangt, lässt sich einerseits streng so verstehen, dass diese Normen für die jeweils angeführten besonderen Anforderungen bezogen auf den konkreten Ausschluss formuliert sein müssen. Dann schiede eine allgemeine Regelung aus. Vom Wortlaut her umfasst ist allerdings auch eine weitere Interpretation des Adjektivs „spezifisch“ dahin gehend, dass unabhängig vom jeweiligen Verarbeitungskontext jedenfalls eigenständige Regelungen erforderlich sind, die dann eher die spezifische Reichweite und die Voraussetzungen für die Einschränkung des Betroffenenrechts definieren, aber durchaus für eine Mehrzahl von Spezialbereichen allgemeine Vorgaben für die Abweichung formulieren. Da ohnehin eine gesetzliche Regelung verlangt wird, würde die Anforderung der Spezifizität dann aber keine relevante zusätzliche Steuerungswirkung entfalten, was aus systematischer Sicht eher für die strenge Auslegung spricht. Andererseits ist in teleologischer Hinsicht darauf hinzuweisen, dass die Mitgliedstaaten durch die Öffnungsklausel einen materiell-rechtlichen Gestaltungsspielraum erlangen. Dass spricht dafür, dass sie erst recht einen gestaltungstechnischen Spielraum erlangen, wie sie von diesem inhaltlichen Abweichungsspielraum Gebrauch machen.

Mag die DSGVO den regelungstechnischen Spielraum für eine allgemeine Ausschlussregelung gewähren, heißt dies noch nicht, dass eine solche auch mit den materiellen Anforderungen an den Ausschluss des Widerspruchsrechts in Einklang gebracht werden kann. Denn die Analyse der einzelnen Anforderungsvoraussetzungen an die Beschränkung der Betroffenenrechte macht deutlich, dass diese nicht alle pauschal für eine Vielzahl von gesetzlichen Speicherpflichten formuliert werden können. Das gilt namentlich für die Verarbeitungszwecke, die Datenkategorien, die Kategorien der Verarbeiter und die Speicherdauer. Hingegen lassen sich Datensicherungsmaßnahmen in diesem Zusammenhang durchaus in einem allgemeinen Gesetz formulieren. Dies gilt auch für den Umfang der Einschränkung und das Recht des Betroffenen, über die Einschränkungen informiert zu werden. Bei den Risiken für die Rechte und Freiheiten der Betroffenen ist unklar, welchen Regelungsgehalt eine entsprechende Norm haben soll, vollkommen unabhängig davon, ob dieser in eine allgemeine oder bereichsspezifische Norm gefasst wird. Tendenziell ist eine Klärung der Risiken für die Rechte und Freiheiten der Betroffenen allerdings wohl nur spezifisch im jeweiligen Verarbeitungskontext möglich. Dabei müsste auf die jeweils spezifischen gesetzlichen Vorgaben verwiesen werden. Am sinnvollsten lässt sich die Vorgabe dabei insoweit verstehen, dass sie eher im Rahmen der Konkretisierung der Einschränkung der Betroffenenrechte verlangt, dass die Risiken bzw. negativen Auswirkungen, die das für die Datenschutzrechte der Betroffenen mit sich bringt, angemessen gewürdigt und bei der Prüfung und gegebenenfalls Ausgestaltung kompensierender Maßnahmen berücksichtigt wird. Da Speicherpflichten einen Eingriff in die Datenschutzgrundrechte der Betroffenen darstellen, werden derartige Überlegungen im Rahmen der Konkretisierung des Gesetzes regelmäßig erfolgen.

Folglich könnte eine Einschränkung des Widerrufsrechts für den Fall der Speicherpflicht aufgrund einer gesetzlichen Regelung entsprechend dem bisherigen § 20 Abs. 5 S. 2 BDSG beibehalten werden – ergänzt um den Hinweis, dass der Betroffene über die Einschränkung zu informieren ist. In der allgemeinen Norm könnte auch darauf hingewiesen werden, dass ein entsprechender Ausschluss nur dann zulässig ist, wenn die Speicherpflicht einen der in Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO angeführten Einschränkungsgründe verfolgt.

Soll dieser Ansatz einer Aufteilung verfolgt werden, bleibt die Frage zu beantworten, ob die Anforderungen des Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO überhaupt in ein allgemeines und ein spezifisches Gesetz aufgespalten werden dürfen. Dagegen spricht, dass der Wortlaut der Verordnung auf eine spezifische Legislativmaßnahme abstellt. Allerdings müssen die jeweiligen Speicherzwecke etc. ohnehin in einem eigenständigen Gesetz formuliert werden. Da die Datenschutz-Grundverordnung auch nicht explizit verlangt, dass alle Regelungsgehalte in ein- und demselben Gesetz erfolgen, ist ein Auseinanderfallen nicht von vornherein ausgeschlossen und mit dem bereits angeführten teleologischen Argument eines regelungstechnischen Gestaltungsspielraums der Mitgliedstaaten rechtfertigbar. Insbesondere muss den Mitgliedstaaten die regelungstechnische Flexibilität belassen werden, Formulierungen, die letztlich in allen bereichsspezifischen Regelungen identisch wären, gleichsam vor die Klammer in einen Allgemeinen Teil des Datenschutzrechts zu ziehen. Dies geht auch nicht mit einer Gefährdung des gewünschten Datenschutzes einher, da entsprechende Überlegungen der Rechtfertigbarkeit einer Speicherung im Rahmen der Auferlegung der Speicherpflicht erfolgen. Zwar verbleiben gewisse Restrisiken, da möglicherweise die Datenschutz-Grundverordnung auf eine geschlossene und individualisierte, bereichsspezifische Ausgestaltung der Einschränkungen ausgerichtet ist. Eine gemischte Regelung mit allgemeinen und bereichsspezifischen Vorschriften erscheint jedoch vertretbar.

Weniger problematisch ist im Übrigen die Erfüllung der Anforderungen an die Verhältnismäßigkeitsprüfung. Dabei handelt es sich letztlich um allgemeine, auch durch das Datenschutzgrundrecht vorgegebene Verhältnismäßigkeitsanforderungen. Auch bislang bestanden insoweit keine Bedenken gegen den Pauschalausschluss im BDSG. Prophylaktisch könnte bei der Formulierung der Ausschlussnorm im allgemeinen Datenschutzgesetz darauf hingewiesen werden, dass ein Ausschluss nur aufgrund der in Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO verfolgten Zwecke unter Wahrung des Verhältnismäßigkeitsgrundsatzes zulässig ist.

Für das Melderegister wäre das angesichts der öffentlichen Sicherheitsinteressen und der Berechtigung entsprechender Speicherpflichten unproblematisch der Fall.

15. Art. 26 (ex Art. 24): Gemeinsam für die Verarbeitung Verantwortliche

Mitgliedstaaten dürfen gesetzlich Verantwortlichkeiten „gemeinsamer Verarbeiter“ („joint controller“) regeln. Die Vorschrift will insbesondere den Kooperationsformen der digitalen Welt Rechnung tragen, die neue, kollaborative Verantwortlichkeitsstrukturen generieren. Zu diesem Zweck räumt sie gemeinsam tätig werdenden Akteuren das Recht ein, die Verantwortlichkeiten, welche sie auf der Grundlage der Verordnung treffen, arbeitsteilig wahrzunehmen und über das Arbeitsteilungsmuster zu disponieren. Dieser Dispositionsfreiheit können die Mitgliedstaaten aber Grenzen ziehen. Sie können (ebenso wie die Union) Aufgaben der Verantwortlichen *einer bestimmten Person* zuweisen und damit deren Dispositionsbefugnis ausschließen.

a. Einordnung in das System der Öffnungsklauseln

Die Öffnungsklausel des Art. 26 (ex Art. 24) DSGVO ist fakultativer Natur: Ihr Regelungsspielraum erstreckt sich auf alle Aufgaben, die Verantwortliche nach der Datenschutz-Grundverordnung treffen, nicht nur die Informationspflicht nach Art. 13 und 14 (ex Art. 14 und 14a) DSGVO.

b. Voraussetzungen der Öffnungsklausel

Wenn die Mitgliedstaaten von der Öffnungsklausel Gebrauch machen, genießen sie erhebliche Freiheit: Art. 26 (ex Art. 24) DSGVO bindet die Öffnungsklausel nicht an einschränkende Voraussetzungen. Ihr Anwendungsbereich ist jedoch eng. Sie setzt inhaltlich voraus, dass mehrere Personen für die Verarbeitung verantwortlich sind und die Zwecke sowie Mittel der Verarbeitung gemeinsam festlegen, indem sie einem der gemeinsam Verantwortlichen die Pflichten auferlegen.

Fälle, in denen eine Disposition der gemeinsam Verantwortlichen über ihre Aufgaben den regulatorischen Zielvorstellungen der Mitgliedstaaten zuwiderläuft, werden selten sein. Dies liegt insbesondere daran, dass Art. 26 Abs. 3 (ex Abs. 2) DSGVO vorsieht, dass die betroffene Person ihre Rechte gegenüber *jedem* einzelnen der Verantwortlichen geltend machen kann. Insoweit muss der nationale Gesetzgeber also nicht zum Schutz des Einzelnen tätig werden, um zum Beispiel zu verhindern, dass in grenzüberschreitenden Zu-

sammenarbeitsfällen Zuständigkeiten auf den im Ausland sitzenden Verarbeiter übertragen werden.
Gleichwohl kann der Gesetzgeber bestrebt sein, in grenzüberschreitenden Fällen Zuständigkeiten bei dem im Inland niedergelassenen Verarbeiter zu halten, um die örtliche Zuständigkeit seinen eigenen Aufsichtsbehörden zu sichern (vgl. Art. 55 Abs. 1 [ex Art. 51 Abs. 1] DSGVO). In diesem Fall stellen sich intrikate Fragen zur Regelungszuständigkeit der Mitgliedstaaten, die hier jedoch zu weit führen.
Da sich der Anspruch der bis zum Inkrafttreten der Datenschutz-Grundverordnung einzuleitenden gesetzgeberischen Maßnahmen aus Zeitgründen auf den *zwingenden* Regelungsbedarf beschränkt, ist ein Gebrauchmachen von der Öffnungsklausel für den deutschen Gesetzgeber nicht zwingend geboten.

16. Art. 28 (ex Art. 26): Auftragsverarbeiter

Die Datenschutz-Grundverordnung räumt den Mitgliedstaaten einzelne Befugnisse ein, die Art und Weise, in der die Auftragsverarbeitung zu erfolgen hat, gesetzlich zu regeln (Art. 28 Abs. 3 [ex Art. 26 Abs. 2] DSGVO). In begrenztem Umfang dürfen sie dabei von den grundsätzlichen Vorgaben der Datenschutz-Grundverordnung abweichen.

a. Art. 28 Abs. 3 UAbs. 1 S. 1 (ex Art. 26 Abs. 2)

aa) Inhalt der Öffnungsklausel

Art. 28 Abs. 3 UAbs. 1 S. 1 (ex Art. 26 Abs. 2) DSGVO gibt die konkrete Handlungsform einer Zusammenarbeit zwischen dem Verantwortlichen sowie dem Auftragsverarbeiter vor. Sie kann auf einem Vertrag basieren. Alternativ dürfen die Mitgliedstaaten ein „anderes Rechtsinstrument“ vorsehen, das die Auftragsdatenverarbeitung näher ausgestaltet. Sie müssen dabei aber den Anforderungen genügen, welche Art. 28 Abs. 3 UAbs. 1 S. 1 (ex Art. 26 Abs. 2) DSGVO formuliert. Das Rechtsinstrument muss den Auftragsverarbeiter an den Verantwortlichen binden. Darüber hinaus muss es den Gegenstand und die Dauer der Verarbeitung, ihre Art und ihren Zweck, die Art der

personenbezogenen Daten, die Kategorien von betroffenen Personen sowie die Verpflichtungen und Rechte des Auftragsverarbeiters festlegen.
Die Datenschutz-Grundverordnung überlässt es grundsätzlich dem Verantwortlichen sowie dem Auftragsverarbeiter, ob sie einen Individualvertrag schließen wollen oder sich für die Verwendung von Standardklauseln entscheiden (EG 81 S. 3 [ex EG 63a S. 3] DSGVO). Letztere hat die Kommission zu erlassen – entweder direkt oder nach Abschluss eines Kohärenzverfahrens mit abschließender Annahme durch eine Aufsichtsbehörde. Alternativ können die Standardklauseln auch Bestandteil einer Zertifizierung sein, die im Rahmen eines Zertifizierungsverfahrens erteilt wurde (EG 81 S. 4 [ex EG 63a S. 4] DSGVO). Welcher Rechtsnatur hingegen der Vertrag ist, gibt die Rechtsordnung nicht vor; auch ein öffentlich-rechtlicher Vertrag ist prinzipiell denkbar.[109]

bb) Einordnung in das System der Öffnungsklauseln

Ob Art. 28 Abs. 3 UAbs. 1 S. 1 (ex Art. 26 Abs. 2) DSGVO eine (fakultative oder obligatorische) Öffnungsklausel etabliert, ist dem Wortlaut nicht mit letzter Eindeutigkeit zu entnehmen. Vordergründig scheint Art. 28 Abs. 3 UAbs. 1 S. 1 (ex Art. 26 Abs. 2) DSGVO den Fall zu regeln, dass der Verantwortliche und der Auftragsverarbeiter keine vertragliche Regelung treffen *wollen*. Ein solches Wahlrecht räumt die Verordnung ihnen aber nicht ein – und will es auch nicht einräumen. Denn die Parteien *müssen* ihre rechtliche Beziehung regeln, um den Datenschutzerfordernis Rechnung zu tragen. Die Datenschutz-Grundverordnung eröffnet vielmehr den Mitgliedstaaten die Möglichkeit, anstelle der Vertragsform (ggf. zwingend) eine andere instrumentelle Gestaltung der Rechtsbeziehungen zwischen dem Verantwortlichen und dem Auftragsverarbeiter, namentlich andere schon bestehende mitgliedstaatliche oder noch zu schaffende Handlungsformen, vorzusehen. Die Datenschutz-Grundverordnung verweist hier auf die Befugnis der Mitgliedstaaten zur Regelung ihrer rechtlichen Handlungsinstrumente. Diese ist Teil der mitgliedstaatlichen Verfahrensautonomie. Eine inhaltliche Regelungsbefugnis

[109] Vgl. hierzu für das deutsche Recht *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl., 2015, § 11 BDSG, Rn. 7.

verbindet sich mit der instrumentellen Handlungsformenwahlfreiheit demgegenüber nicht. Den Inhalt der rechtlichen Beziehung zwischen Auftragsverarbeiter und Verantwortlichem gibt die Verordnung vielmehr selbst vor. Die Datenschutz-Grundverordnung eröffnet also keinen Spielraum hinsichtlich des inhaltlichen „Ob", sondern hinsichtlich des instrumentellen „Wie".

cc) Vergleich mit der Vorgängerregelung in der Datenschutzrichtlinie 95/46/EG

Art. 28 Abs. 3 UAbs. 1 S. 1 (ex Art. 26 Abs. 2) DSGVO folgt einem ähnlichen regulatorischen Strickmuster wie Art. 17 Abs. 3 DSRL: Auch sie sah vor, dass die Auftragsverarbeitung auf der Grundlage eines Vertrages oder eines Rechtsaktes erfolgt, die den Auftragsverarbeiter an den Verantwortlichen bindet. Zwar trifft die Richtlinie hinsichtlich der konkreten Ausgestaltung auch Vorgaben. Anders als die Datenschutz-Grundverordnung, die insbesondere den Umfang der Verarbeitung konkretisieren will, verlangt die Richtlinie weit weniger: Entscheidend ist, dass auch die Auftragsverarbeitung den Datenschutz durch Technik und Organisation umsetzt (vgl. Art. 17 Abs. 3 Spstr. 2 DSRL).

dd) Abgleich mit dem bestehenden nationalen Recht

Die Anforderungen an die rechtliche Beziehung zwischen dem Verantwortlichen und dem Auftragsverarbeiter formuliert im nationalen Recht bisher die Vorschrift des § 11 Abs. 2 S. 2 BDSG. Er enthält die Bestimmungen zur Vertragsgestaltung, die nunmehr unmittelbar die DSGVO vorsieht. Die inhaltlichen Regelungen trifft Art. 28 Abs. 3 DSGVO grundsätzlich abschließend. Eine die Handlungsformwahlfreiheit ausschöpfende Vorschrift und damit eine Abweichung von der vertraglichen Regelung der Beziehung zwischen Verantwortlichem und Auftragsverarbeiter sieht das BDSG nicht vor. Der Vorschrift bedarf es nicht mehr.

b. Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a (ex Art. 26 Abs. 2 lit. a)

aa) Hs. 1

Grundsätzlich darf der Auftragsverarbeiter personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeiten. Das Recht der

Mitgliedstaaten kann den Auftragsverarbeiter aber auch unmittelbar zur Verarbeitung verpflichten. So bestimmt es Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a Hs. 1 (ex Art. 26 Abs. 2 lit. a Hs. 1) DSGVO. Eine Weisung ist dann nicht mehr erforderlich –weder als Legitimierungs- noch als Zurechnungsgrund.
Hieraus ergibt sich zugleich, dass die Vorschrift wohl keine echte Öffnungsklausel für Regelungen zur Verarbeitung selbst enthält. Vielmehr verweist sie alleine auf nach nationalem Recht bestehende Verarbeitungspflichten: Soweit diese im Anwendungsbereich der Datenschutz-Grundverordnung liegen, ist für diese eine Öffnungsklausel nach einer anderen Vorschrift, insbes. Art. 6 Abs. 1 UAbs. 1 lit c DSGVO, erforderlich. Wäre es anders, dürfte der Mitgliedstaat nach Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a Hs. 1 (ex Art. 26 Abs. 2 lit. a Hs. 1) DSGVO, gleichsam durch die Hintertür, Verarbeitungspflichten begründen, die nicht an die besonderen und speziellen Anforderungen des Art. 6 Abs. 1 UAbs. 1 lit c, Abs. 2 und 3 DSGVO gebunden wären. Die Grenzen für mitgliedstaatliche Verarbeitungsbefugnisse, die das differenzierte Ausgestaltungssystem des Art. 6 Abs. 1 i. V. m. Abs. 2 und 3 DSGVO setzt, ließen sich dann unterlaufen.[110] Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a Hs. 1 DSGVO bringt nach seinem Kerngehalt zum Ausdruck, dass eine mitgliedstaatlich auf der Grundlage anderer Öffnungsklauseln der Datenschutz-Grundverordnung bestehende Verarbeitungspflicht des Auftragsverarbeiters auch auf Art. 28 Abs. 3 und Abs. 1 S. 2 DSGVO durchschlägt und damit eine dokumentierte Weisung des Verantwortlichen nicht mehr erforderlich ist.

bb) Hs. 2

i. Inhalt der Öffnungsklausel

Verarbeitet der Auftragsverarbeiter personenbezogene Daten aufgrund einer gesetzlichen Verarbeitungspflicht und damit nicht auf Weisung des Verantwortlichen, teilt er dies dem Verantwortlichen grundsätzlich mit (Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a Hs. 2 [ex Art. 26 Abs. 2 lit. a Hs. 2] DSGVO). Der

[110] Die Vorschrift ist aber interpretationsoffen. In ihrer offenen Formulierung lässt sie sich (auch wenn die wohl besseren Gründe für eine andere Sichtweise sprechen) durchaus auch so deuten, dass sie den Mitgliedstaaten eine selbstständige Regelungsbefugnis der Mitgliedstaaten für eine Verarbeitungserlaubnis vermittelt.

Mitgliedstaat kann eine solche Mitteilung aber wegen eines wichtigen öffentlichen Interesses untersagen (Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a Hs. 2 a. E. [ex Art. 26 Abs. 2 lit. a Hs. 2 a. E.] DSGVO).

ii. Einordnung in das System der Öffnungsklauseln

Auch Art. 28 Abs. 3 S. 2 lit. a Abs. 2 DSGVO lässt offen, ob es sich um eine echte Öffnungsklausel handelt oder diese lediglich auf eine anderweitig in der Verordnung begründete oder außerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung liegende Regelungsbefugnis verweist. Die unmittelbare Kohärenz mit der Regelung des Hs. 1 streitet für eine äquivalente Deutung beider Normen. Die Datenschutz-Grundverordnung lässt dem Mitgliedstaat in beiden die Freiheit zu entscheiden, in welchen Situationen er es für geboten erachtet, dass der Auftragsverarbeiter den Verantwortlichen nicht über die Verarbeitung informiert, dispensiert aber nicht vom Erfordernis einer Verarbeitungsgrundlage in Art. 6 DSGVO, schafft eine solche insbesondere nicht. Insoweit handelt es sich um eine fakultative, unechte[111] Öffnungsklausel.

iii. Vergleich zur Vorgängerregelung in der Datenschutzrichtlinie 95/46/EG

Die Datenschutzrichtlinie hatte keine der Datenschutz-Grundverordnung vergleichbaren Vorgaben getroffen.

iv. Abgleich mit dem bestehenden nationalen Recht

Auch das BDSG enthält (mit Ausnahme Verpflichtung auf die Weisungsbindung in § 12 Abs. 3 S. 1 BDSG) bislang keine mit dem Regelungsgehalt des Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a vergleichbaren Regelungen. Ob ihrer Spezialität sind diese ggf. vorrangig in bereichsspezifischen Gesetzen zu suchen.

[111] Zu dieser Terminologie siehe S. 11.

c. Art. 28 Abs. 3 UAbs. 1 S. 2 lit. g (ex Art. 26 Abs. 2 lit g)

aa) Inhalt der Norm

Art. 28 Abs. 3 UAbs. 1 S. 2 lit. g (ex Art. 26 Abs. 2 lit. g) DSGVO verlangt grundsätzlich, dass der Auftragsverarbeiter, nachdem er die Datenverarbeitungsdienstleistungen erbracht hat, die personenbezogenen Daten „löscht oder zurückgibt". Das Wahlrecht steht insoweit dem Verantwortlichen zu. Diese Pflicht besteht dann nicht, wenn das Unionsrecht oder das Recht des Mitgliedstaates, dem der Auftragsverarbeiter unterliegt, eine Pflicht zur Speicherung der gewonnenen Daten vorsieht.

bb) Einordnung in das System der Öffnungsklauseln

Auch Art. 28 Abs. 3 UAbs. 1 S. 2 lit. g (ex Art. 26 Abs. 2 lit. g) DSGVO begründet keine Öffnungsklausel im eigentlichen Sinne: Die Mitgliedstaaten können dem Auftragsverarbeiter allein auf der Grundlage dieser Vorschrift nicht die Pflicht auferlegen, die gesammelten personenbezogenen Daten zu speichern. Vielmehr setzt sie eine anderweitig begründete Speicherpflicht voraus. Soweit diese im Anwendungsbereich der Datenschutz-Grundverordnung liegen, ist für diese eine Öffnungsklausel nach einer anderen Vorschrift, insbes. Art. 6 Abs. 1 UAbs. 1 lit c DSGVO erforderlich. Art. 6 Abs. 3 S. 3 DSGVO zeigt, dass das mitgliedstaatliche Recht auch Regelungen zur Speicherung treffen darf.

cc) Vergleich zur Vorgängerregelung in der Datenschutzrichtlinie 95/46/EG

Die Datenschutzrichtlinie hatte keine der Datenschutz-Grundverordnung vergleichbaren Vorgaben getroffen.

dd) Abgleich mit dem bestehenden nationalen Recht

Das BDSG enthält neben der allgemeinen Pflicht, Daten zu löschen, wenn sie zur Erfüllung der Verarbeitungsaufgaben nicht mehr erforderlich sind (§ 20 Abs. 2 Nr. 2 BDSG), in § 11 Abs. 2 S. 2 Nr. 4 BDSG speziell für das Auftragsverhältnis auch vertragliche Festlegungspflichten im Hinblick auf die Löschung und Sperrung von Daten.

d. Art. 28 Abs. 4 (ex Art. 26 Abs. 2a)

aa) Inhalt der Öffnungsklausel

Art. 28 Abs. 4 (ex Art. 26 Abs. 2a) DSGVO regelt den Fall, dass der Auftragsverarbeiter auf einen weiteren Auftragsverarbeiter zurückgreift und damit eine Verarbeitungskette aufmacht. Auch hier muss am Ende der Verarbeitungskette der Verantwortliche stehen. Ebenso wie für den Fall der Verbindung zwischen dem Verantwortlichen und dem Auftragsverarbeiter gilt auch hier: Zwischen dem ersten und dem weiteren Auftragsverarbeiter muss entweder eine vertragliche Regelung bestehen oder ein anderes Rechtsinstrument nach dem Unionsrecht bzw. dem nationalen Recht vorhanden sein. Diese Bindeglieder sollen gewährleisten, dass auch für den weiteren Auftragsverarbeiter die gleichen datenschutzrechtlichen Standards (Art. 28 Abs. 3 [ex Art. 26 Abs. 2] DSGVO) gelten wie gegenüber dem primären Auftragsverarbeiter. Insbesondere gilt es, eine Umgehung der Datenschutzpflichten durch Einschaltung eines Dritten zu verhindern. Art. 28 Abs. 4 S. 1 (ex Art. 26 Abs. 2a S. 1) DSGVO legt dabei besonderen Wert auf die Einhaltung des Datenschutzes durch Technik und Organisation (dazu auch Art. 24 Abs. 1 und 25 Abs. 1 u. 2 DSGVO). Hält sich der weitere Auftragsverarbeiter nicht an seine Verpflichtungen, so muss der erste Auftragsverarbeiter im Innenverhältnis gegenüber dem Verantwortlichen für die Einhaltung dieser Pflichten einstehen (Art. 28 Abs. 4 S. 2 [ex Art. 26 Abs. 2a S. 2] DSGVO). Im Außenverhältnis trifft alle Mitglieder der Verarbeitungskette grundsätzlich eine gesamtschuldnerische gemeinsame Haftung nach Art. 82 Abs. 4 DSGVO.

bb) Einordnung in das System der Öffnungsklauseln

Ebenso wie im Falle des Art. 28 Abs. 3 (ex Art. 26 Abs. 2) DSGVO ergibt sich auch im Fall des Art. 28 Abs. 4 (ex Art. 26 Abs. 2a) DSGVO aus der Norm selbst nicht eindeutig, ob sich die Öffnungsklausel als für Normadressaten obligatorisch darstellt oder ob sie fakultativer Natur ist. Entsprechend der Funktion der Öffnungsklausel handelt es sich um eine Regelungsbefugnis der Mitgliedstaaten: Die Mitgliedstaaten haben die Möglichkeit, anstelle der Vertragsform eine andere Gestaltung der Rechtsbeziehungen zwischen dem Auftragsverarbeiter und dem Sub-Auftragsverarbeiter vorzusehen. Sie müs-

sen dies aber zum einen nicht; zum anderen erschöpft sich ihre Regelungsbefugnis darin: Art. 28 Abs. 4 S. 1 eröffnet den Mitgliedstaaten (ebenso wie Art. 28 Abs. 3 UAbs. 1 S. 1) keine inhaltliche Ausgestaltungsbefugnis für die Auftragsverarbeitung, sondern verweist lediglich auf die Freiheit der Mitgliedstaaten, bei der Umsetzung der inhaltlichen Anforderungen alternative Handlungsformen zu wählen.
Bei Art. 28 Abs. 4 S. 1 (ex Art. 26 Abs. 2a S. 1) DSGVO handelt es sich daher um eine *enge*, *fakultative Öffnungsklausel*.

cc) Vergleich zur Vorgängerregelung in der Datenschutzrichtlinie 95/46/EG

Die Regelung des Art. 28 Abs. 4 (ex Art. 26 Abs. 2a) DSGVO ist ohne Vorbild in der Datenschutzrichtlinie 95/46/EG.

dd) Abgleich mit dem bestehenden nationalen Recht

Das BDSG regelt die Unterauftragserteilung bisher nur rudimentär. Wenn der Auftragnehmer zur Begründung von Unterauftragsverhältnissen berechtigt ist, bedarf das einer schriftlichen Fixierung im Auftragsverhältnis (§ 11 Abs. 2 S. 2 Nr. 6 BDSG). Anderenfalls sind Unterbeauftragungen ausgeschlossen. Eine ausdrückliche Einstandspflicht zur Einhaltung der Vorschriften durch den weiteren Auftragsverarbeiter kennt das BDSG hingegen nicht. Sie ergibt sich aber auch bisher schon aus der Rationalität einer Unterbeauftragung. Ein Unterauftrag kann der Sache nach nur soweit reichen wie der Hauptauftrag und muss dem Unterauftragnehmer die gleichen Pflichten auferlegen wie dem Hauptauftragnehmer, um eine Unterwanderung datenschutzrechtlicher Pflichten zu verhindern. Die Regelungsbefugnis wandert insoweit nunmehr aber vom deutschen Gesetzgeber zum Unionsgesetzgeber, der die *inhaltliche* Ausformung der betroffenen Rechtsverhältnisse abschließend ohne inhaltliche Ausformungsbefugnis der Mitgliedstaaten regelt.

17. Art. 29 (ex Art. 27): Aufsicht des Verantwortlichen

Personen, die dem Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind – ebenso der Auftragsverarbeiter selbst, dürfen nach dem Willen des

unionsrechtlichen Datenschutzregimes Daten grundsätzlich ausschließlich auf Weisung des Verantwortlichen verarbeiten. Die Verordnung will damit sicherstellen, dass die Auftragsverarbeitung ihrem Wesen gerecht wird, nämlich die Verarbeitung den Vorgaben des Verantwortlichen folgt, und die Befugnis zur Verarbeitung personenbezogener Daten auf eine enge Personengruppe, namentlich die Verantwortlichen bzw. den Auftragsverarbeiter beschränkt bleibt. Nach dem Grundgedanken der Datenschutz-Grundverordnung soll es der Verantwortliche daher in der Hand haben, ob sich die Verarbeitungskette entsprechend seinen Anweisungen verlängert oder nicht. Dabei kann er nicht nur über das „Ob" der Verarbeitung entscheiden; ihm obliegt es zugleich, den *Umfang* der konkreten Tätigkeit festzulegen. Dementsprechend darf der in die Verarbeitung Einbezogene nur solche Verarbeitungen vornehmen, die den Weisungen entsprechen.[112] Diese sonstigen Personen haben die Verarbeitung personenbezogener Daten zu unterlassen, es sei denn, der Verantwortliche hat eine entsprechende Anweisung erteilt.

Das Recht der Mitgliedstaaten kann den Auftragsverarbeiter oder die unterstellten Personen aber auch unmittelbar zur Verarbeitung verpflichten. Denkbar können insoweit beispielsweise strafrechtliche Ermittlungszwecke sein.[113] In diesem Fall sieht Art. 29 Hs. 2 (ex Art. 27 Hs. 2) DSGVO (wie auch oben bereits Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a Hs. 1 (ex Art. 26 Abs. 2 lit. a Hs. 1) DSGVO für den Auftragsverarbeiter) vor, dass eine Weisung nicht mehr erforderlich ist. Der Verarbeitungsgrund ergibt sich unmittelbar aus der rechtlichen Verpflichtung. Daraus folgt zugleich nicht zwingend, dass Art. 29 *selbst* den Mitgliedstaaten eine solche umfassende Regelungsbefugnis zuerkennt. Die Vorschrift kann auch ebenso auf sich aus anderen Vorschriften der DSGVO, insbesondere Art. 6 Abs. 1, 2 und 3 ergebende Regelungsbefugnisse der Mitgliedstaaten verweisen (vgl. auch bereits oben die Darstellung zu Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a Hs. 1 (ex Art. 26 Abs. 2 lit. a Hs. 1) DSGVO, S. 80). Dafür streitet zumindest das ausdifferenzierte Regelungskonzept der Verarbeitungsgrundlagen des Art. 6 DSGVO. Dürfte der Mitgliedstaat auf

[112] Vgl. *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 11, Rn. 24.

[113] *Brühann*, in: Grabitz/Hilf (Hrsg.), EU-Recht, 57. Erg.-Lfg., 2015, Art. 16 Datenschutzrichtlinie, Rn. 11, Fn. 1.

der Grundlage des Art. 29 DSVO ohne Rückbindung an die besonderen Voraussetzungen des Art. 6 Abs. 1 UAbs. 1 lit c, Abs. 2 und 3 DSGVO mitgliedstaatliche Verarbeitungsbefugnisse begründen, könnte er die speziellen Anforderungen des Art. 6 DSGVO vergleichsweise leicht unterlaufen und sich auf diese Weise einen weitgehend ungebundenen mitgliedstaatlichen Regelungsspielraum verschaffen.[114]

a. Einordnung in das System der Öffnungsklauseln

Art. 29 (ex Art. 27) DSGVO etabliert eine unechte,[115] fakultative Öffnungsklausel. Ob die Mitgliedstaaten von ihr Gebrauch machen und in welchem Umfang sie Personen, die in den Verarbeitungsvorgang einbezogen sind, Pflichten auferlegen, steht ihnen frei.

b. Vergleich zur Vorgängerregelung in der Datenschutzrichtlinie 95/46/EG

Art. 16 DSRL normierte eine dem Art. 29 (ex Art. 27) DSGVO im Wesentlichen vergleichbare Vorschrift. Auch dort sah die Union eine Einbeziehung Dritter in den Verarbeitungsvorgang vor, wenn „gesetzliche Verpflichtungen" bestanden.

c. Abgleich mit dem bestehenden nationalen Recht

Das deutsche Datenschutzrecht regelt bislang in § 11 Abs. 3 S. 1 BDSG, dass der Auftragnehmer die Daten *nur* im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen darf; eine Bußgeldbewehrung verband das deutsche BDSG – anders als § 85 Abs. 1 Nr. 2 SGB X – damit nicht (§ 43 Abs. 1 Nr. 2b BDSG e contrario). Eine Verpflichtung zur Verarbeitung *aufgrund gesetzlicher Pflicht* begründet § 11 Abs. 3 BDSG nicht. Der Gesetzgeber kann eine solche etablieren, soweit er – jedenfalls wenn man Art. 29 DSGVO als unechte Öffnungsklausel versteht – die Anforderungen des Art. 6 Abs. 1-3 DSGVO einhält. Akuter Regelungsbedarf besteht insoweit aller-

[114] Siehe auch S. 80
[115] Zu diesem Begriffstypus siehe S. 11.

dings nicht. Im Übrigen regelt die DSGVO die rechtlichen Pflichten des Auftragsverarbeiters grundsätzlich unmittelbar und inhaltlich abschließend.[116]

18. Art. 32 Abs. 4 (ex Art. 30 Abs. 2b): Anweisung des Verantwortlichen

Der Verantwortliche und der Auftragsverarbeiter müssen grundsätzlich sicherstellen, dass ihnen unterstellte Personen mit Zugang zu personenbezogenen Daten diese nur auf Anweisung verarbeiten. Wenn die Mitgliedstaaten die Personen zur Verarbeitung verpflichten, dürfen diese aber auch ohne Anweisung des Verantwortlichen bzw. Auftragsverarbeiters datenverarbeitend tätig werden. Die Regelung korreliert mit Art. 29 Hs. 2 (ex Art. 27 Hs. 2) DSGVO sowie Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a Hs. 1 (ex Art. 26 Abs. 2 lit. a Hs. 1) DSGVO, nach denen eine Verarbeitung in solchen Konstellationen grundsätzlich nur aufgrund einer Weisung zulässig ist. Beide Vorschriften nehmen dabei eine andere Blickrichtung ein: Anders als Art. 29 (ex Art. 27) DSGVO richtet Art. 32 Abs. 4 (ex Art. 30 Abs. 2b) DSGVO seinen Regelungsfokus nicht auf die in die Verarbeitung einbezogenen Personen, sondern auf die Verantwortlichen und den Auftragsverarbeiter. *Diese* müssen grundsätzlich ihrer Pflicht zur Sicherstellung hinreichenden Datenschutzes bei der Einbindung anderer Personen genügen.

Ebenso wie Art. 29 Hs. 2 (ex Art. 27 Hs. 2) DSGVO sowie Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a Hs. 1 (ex Art. 26 Abs. 2 lit. a Hs. 1) DSGVO eröffnet auch Art. 32 Abs. 4 (ex Art. 30 Abs. 2b) DSGVO den Mitgliedstaaten wohl keine eigenständige Regelungsbefugnis, um vom Erfordernis einer Weisung eine Ausnahme vorzusehen. Gute Gründe sprechen dafür, dass sie vielmehr lediglich auf der Grundlage anderer Verarbeitungsgrundlagen, insbesondere Art. 6 Abs. 1-3 DSGVO bestehende Verarbeitungspflichten in Bezug nimmt.[117]

[116] Zu den Auswirkungen auf die Vorschrift des § 11 BDSG siehe S. 365.
[117] Dazu im Einzelnen oben S. 78 ff.

19. Art. 35 Abs. 10 (ex Art. 33 Abs. 5): Datenschutz-Folgenabschätzung

Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO etabliert eine Ausnahme von der Pflicht zur Vornahme einer Datenschutz-Folgenabschätzung (Art. 35 Abs. 1 – 7 [ex Art. 33 Abs. 1 – 3] DSGVO). Diese setzt auf der Öffnungsklausel des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO auf, welche den Mitgliedstaaten besonderen Handlungsspielraum im Hinblick auf die Verarbeitungsgrundlagen eröffnet. Falls diese Vorschrift konkrete Verarbeitungsvorgänge regelt und bereits bei dem Erlass der Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, hält die Verordnung eine weitere Folgenabschätzung nach Art. 35 Abs. 1 - 7 der DSGVO grundsätzlich für entbehrlich. Ratio legis ist die Vermeidung einer doppelten Folgenabschätzung für solche Fälle, in denen bereits im Zusammenhang mit dem Erlass der Rechtsgrundlage eine allgemeine Datenschutz-Folgenabschätzung erfolgte.
Die Mitgliedstaaten können aber von diesem Grundsatz eine Rückausnahme vorsehen, also eine zusätzliche Datenschutz-Folgenabschätzung anordnen, wenn sie dies nach ihrem Ermessen für erforderlich halten.

a. Einordnung in das System der Öffnungsklauseln

Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO sieht eine Rückausnahme von dem Ausschluss der grundsätzlich aus Art. 35 (ex Art. 33) DSGVO resultierenden Pflicht zur Folgenabschätzung einer Datenverarbeitung vor. Wenn ihre Voraussetzungen vorliegen, steht es im Ermessen des Mitgliedstaates, den Verantwortlichen den Pflichten des Art. 35 Abs. 1 – 7 (ex Art. 33 Abs. 1 – 3) DSGVO zu unterwerfen.

b. Inhalt der Öffnungsklausel

Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO legt die Entscheidung darüber, ob unter seinen tatbestandlichen Voraussetzungen eine (weitere) Datenschutz-Folgenabschätzung stattfinden muss, in die Entscheidungsfreiheit der Mitgliedstaaten. Dem liegt die Überlegung zugrunde, dass nur die Mitgliedstaaten selbst einschätzen können, ob neben der Datenschutz-Folgenabschätzung, die im Kontext des Erlasses der Rechtsnormen ergangen ist, eine weitere Folgenabschätzung bei der Anwendung auf den konkreten Fall noch sinnvoll

ist. Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO trifft für diese Konstellation zugleich eine (erst auf den zweiten Blick deutlich werdende) Grundentscheidung: Bleibt der Mitgliedstaat untätig, findet keine Datenschutz-Folgenabschätzung statt. Erst wenn der Mitgliedstaat sein Ermessen durch Erlass einer gesetzlichen Vorschrift dahin betätigt, muss eine solche Folgenabschätzung stattfinden. Bei Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO handelt es sich um eine mehrfach bedingte Öffnungsklausel. Um ihren Spielraum auszulösen, müssen kumulativ folgende Voraussetzungen erfüllt sein:
1. Eine Verarbeitung muss auf einer auf der Grundlage des Art. 6 Abs. 1 UAbs. 1 lit. c, e DSGVO geschaffenen Rechtsgrundlage beruhen. Dabei kann es sich sowohl um eine unionsrechtliche als auch um eine mitgliedstaatliche Norm handeln. Art. 35 Abs. 10 (ex Art. 33 Abs. 5) nimmt damit auf die wohl wichtigsten Öffnungsklauseln für nationales Recht Bezug, die den Mitgliedstaaten weite Regelungsspielräume – insbesondere für ihre öffentlichen Stellen – eröffnen und daran zusätzlich die mögliche Befreiung von einer Datenschutz-Folgenabschätzung knüpfen.
2. Diese Rechtsgrundlagen müssen den konkreten Verarbeitungsvorgang regeln. Sie dürfen also nicht nur allgemein in dem mitgliedstaatlichen Recht bestehen, sondern müssen den konkreten Verarbeitungsvorgang *tatbestandlich* erfassen. Dies lässt den Rechtsanwender mit der Frage zurück, auf welche Verarbeitung sich diese Rechtsgrundlage sonst beziehen soll, welche eigenständige Bedeutung das zweite Tatbestandsmerkmal also haben soll. Die Vorschrift muss als in das Allgemeine Persönlichkeitsrecht eingreifende Befugnisnorm nicht nur den Normverpflichteten, sondern auch das ihm abverlangte Verhalten regeln. Insofern erscheint Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO in seiner Formulierung missglückt. Das vermeintlich zweite Tatbestandsmerkmal geht daher weitgehend im ersten Tatbestandsmerkmal auf, dient wohl insbesondere der Klarstellung und besonderen Hervorhebung des Aspekts, dass nicht nur überhaupt eine nationale Verarbeitungsgrundlage bestehen, sondern diese auch auf den konkreten Fall anwendbar sein muss.
3. Schließlich muss eine Folgenabschätzung schon auf Grundlage jener Rechtsnormen „als Teil einer allgemeinen Folgenabschätzung“ erfolgt sein. Welche konkreten Anforderungen sich damit verbinden, lässt die Verordnung offen. Insbesondere sind die Vollzugsformen der Gesetzesfolgenabschätzung in den Mitgliedstaaten sehr unterschiedlich ausgeformt; zwischen der Geset-

zesfolgenabschätzung und der Abschätzung der Folgen auf den konkreten Fall besteht überdies ein methodischer Unterschied. Die Verordnung legt die Anforderungen mit der Wendung „eine Datenschutz-Folgenabschätzung erfolgte“ nicht sehr hoch. Es genügt, dass eine allgemeine, systematische Erfassung und Analyse der intendierten und unbeabsichtigten Folgen der Rechtsnorm stattgefunden hat. Die Auswirkungen auf den konkreten Fall braucht sie nicht unbedingt zu erfassen.

Verlangt Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO von den Mitgliedstaaten auf der Grundlage seiner Tatbestandsvoraussetzungen keine zusätzliche Folgenabschätzung, liegt die Frage, ob der Mitgliedstaat gleichwohl eine Datenschutz-Folgenabschätzung anordnet, in seiner pflichtgemäßen Prüfungs- und Entscheidungsfreiheit. Diese findet ihre Grenze in den europäischen Grundrechten der GrCh sowie nationalem Verfassungsrecht, insbesondere entsprechenden Schutzpflichten. Bleibt der Mitgliedstaat untätig, findet keine zweite Datenschutz-Folgenabschätzung statt. Betroffene können eine solche grundsätzlich nicht im Wege einer Klage erzwingen – oder verhindern, wenn der Mitgliedstaat von der Öffnungsklausel des Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO Gebrauch macht.

c. Abgleich mit dem bestehenden nationalen Recht

Weder in der DSRL noch im BDSG findet sich eine Pflicht zur Durchführung einer Folgenabschätzung vor Beginn der Datenverarbeitung. Am ehesten ist Art. 35 (ex Art. 33) DSGVO mit dem Datenschutzaudit gemäß § 9a BDSG vergleichbar: Mangels näherer Bestimmung durch ein entsprechendes Gesetz im Sinne des § 9a S. 2 BDSG handelt es sich dabei aber bislang im deutschen Recht nur um eine Programmnorm.[118] Da sich aus der Bewertung im Rahmen des Audits ein Wettbewerbsvorteil ergeben kann, ist die Bestimmung des § 9a BDSG eher mit der Zertifizierung gemäß Art. 42 (ex Art. 39) DSGVO vergleichbar.[119]

Substanzielle inhaltliche Parallelen zu Art. 35 (ex Art. 33) DSGVO weist aber § 4d Abs. 5 BDSG auf. Die Norm legt der datenverarbeitenden Stelle für

[118] *Scholz*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 9a, Rn. 1.
[119] *Scholz* (Fn. 118), § 9a, Rn. 12a.

gewisse Arten der Verarbeitung die Pflicht einer Vorabkontrolle auf, die inhaltlich mit der in Art. 35 (ex Art. 33) normierten Datenschutz-Folgenabschätzung vergleichbar ist.

20. Art. 36 Abs. 4 (ex Art. 34 Abs. 7): Mitgliedstaatliche Konsultationspflicht im Gesetzgebungsverfahren

Art. 36 Abs. 4 (ex Art. 34 Abs. 7) DSGVO legt den Mitgliedstaaten eine besondere Verfahrenspflicht auf: Sie ziehen die Aufsichtsbehörde bei der Ausarbeitung eines Vorschlags für (von einem nationalen Parlament) zu erlassende Gesetzgebungsmaßnahmen oder von auf solchen Gesetzgebungsmaßnahmen basierenden Regulierungsmaßnahmen, welche die Verarbeitung personenbezogener Daten betreffen, zu Rate.
Zwar berührt die Hinzuziehung auch das verfassungsrechtlich in den Art. 76 ff. GG detailliert geregelte Verfahren der Gesetzgebung. Das macht deren Änderung aber noch nicht erforderlich. Die Hinzuziehung berührt nicht generell das Verfahren, in dem Parlamentsgesetze in dem Zusammenspiel der Institutionen entsprechend der Verfassung zustande, sondern nur bestimmte Konstellationen datenschutzrechtlich relevanter Vorschriften. Es gilt kraft der unmittelbaren Wirkung der Verordnung überdies unabhängig von einer Verankerung im nationalen Recht. Die Pflicht des Art. 36 Abs. 4 (ex Art. 34 Abs. 7) DSGVO zur Hinzuziehung kann durch nationales Recht näher ausgestaltet und an das nationale Gesetzgebungsverfahren angepasst werden, bedarf dessen aber nicht zwingend.

21. Art. 36 Abs. 5 (ex Art. 34 Abs. 7a): Vorabkonsultation

Art. 36 Abs. 1 (ex Art. 34 Abs. 2) DSGVO regelt die Verpflichtung des Verantwortlichen, die Aufsichtsbehörde in besonderen Risikofällen bereits vor der Verarbeitung zu konsultieren (Vorabkonsultation). Eine solche Verpflichtung besteht, wenn eine Datenschutz-Folgenabschätzung gemäß Art. 35 (ex Art. 33) DSGVO ergibt, dass die Verarbeitung ein hohes Risiko zur Folge hätte und der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft. Die Mitgliedstaaten können weitere Verpflichtungen zur Vorabkonsultation vorsehen, wenn die Verarbeitung zur Erfüllung einer im öffentlichen

Interesse liegenden Aufgabe erfolgt – Art. 36 Abs. 5 (ex Art. 34 Abs. 7a) DSGVO.

a. Einordnung in das System der Öffnungsklauseln

Die Öffnungsklausel des Art. 36 Abs. 5 (ex Art. 34 Abs. 7a) DSGVO ist fakultativer Natur.

b. Vergleich zur Datenschutzrichtlinie 95/46/EG

Die Datenschutzrichtlinie sah für voll- oder teilautomatisierte Datenverarbeitungen ein Meldeverfahren vor (Art. 18 DSRL; §§ 4d Abs. 1 bis 4; 4e BDSG), von dem die Mitgliedstaaten Ausnahmen vorsehen konnten (Art. 18 Abs. 2 bis 4 DSRL; § 4d Abs. 2 bis 4 BDSG). Darüber hinaus gebot Art. 20 DSRL eine Vorabkontrolle, deren genauen Anwendungsbereich die Mitgliedstaaten selbst festlegen konnten (Art. 20 Abs. 1 DSRL; § 4d Abs. 4, 5 BDSG). Die Datenschutz-Grundverordnung übernahm die Meldepflicht nicht. Die Vorabkontrolle findet sich vielmehr in abgewandelter Form in der Vorabkonsultation wieder und ist an das Ergebnis der Datenschutz-Folgenabschätzung (Art. 35 [ex Art. 33] DSGVO) gekoppelt. Die Mitgliedstaaten können alleine weitere Fälle der Anwendung der Vorabkonsultation festlegen.

c. Anwendungsbereich der Öffnungsklausel

Die Vorschrift räumt den Mitgliedstaaten grundsätzlich einen weitgehenden Umsetzungsspielraum ein: Sie können *allen* Verarbeitern, also nach der Legaldefinition des Art. 4 Nr. 7 (ex Art. 4 Abs. 5) DSGVO öffentlichen und nicht-öffentlichen Verarbeitern, eine Pflicht zur Vorabkonsultation auferlegen. Der Regelungsspielraum erstreckt sich auf alle Bereiche der Verarbeitung personenbezogener Daten. Eine Beschränkung erfährt dieser Bereich jedoch insoweit, als nur Verarbeitungen erfasst sind, die ihre Rechtfertigung in einem öffentlichen Interesse finden (mithin für Datenverarbeitungen gemäß Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO, vgl. Art. 6 Abs. 3 S. 4 DSGVO). Der Begriff des *öffentlichen Interesses* ist in der Datenschutz-Grundverordnung nicht legaldefiniert (in Art. 36 Abs. 5 DSGVO lediglich mit dem Hinweis auf „Zwecke der sozialen Sicherheit und der öffentlichen Gesundheit“ beispielhaft konkretisiert), findet sich aber an zahlreichen ande-

ren Stellen des Verordnungstextes, etwa in Art. 5 Abs. 1 lit. b und e, Art. 6 Abs. 1 UAbs. 1 lit. e, Art. 6 Abs. 3 lit. b S. 2 und 5 (siehe dazu I. 6. C. aa) iii., S. 31), Art. 9 Abs. 2 lit. g DSGVO und ist grundsätzlich wie dort zu verstehen. Der Regelungsspielraum des Art. 36 Abs. 5 erstreckt sich damit jedenfalls auf alle Bereiche der Verarbeitung personenbezogener Daten, in denen die Mitgliedstaaten selbst die Verarbeitung vorsehen können (Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO). Der Begriff des öffentlichen Interesses nimmt Rekurs auf den Interessenwiderstreit zwischen Gemeinwohl und Individualbedürfnissen. Beide Interessen können gleichlaufen, einander aber auch widersprechen. „Öffentliche Interessen“ beschreiben allgemein diejenigen Ziele, Werte und Bedürfnisse, welche das Gemeinwesen konstituieren und für seinen gedeihlichen Zusammenhalt von besonderer Bedeutung sind. Es handelt sich zwar um einen originären unionsrechtlichen Begriff, dessen Ausfüllung den Mitgliedstaaten nicht vollkommen frei steht. Die Mitgliedstaaten genießen aber grundsätzlich ein Recht zur Bestimmung dessen, was für ihr demokratisches Gemeinwesen als staatlicher Einheit zur Befriedigung öffentlicher Interessen von besonderer Bedeutung ist.

d. Vereinbarkeit der bisherigen Regelung des BDSG mit der Datenschutz-Grundverordnung

Regelungen zur vorherigen Melde- und Kontrollpflicht bei den Aufsichtsstellen existieren durchaus bereits im bestehenden Bundes- und Landesrecht.
Im Bundesrecht finden sich Regelungen hinsichtlich nicht-öffentlicher Stellen und öffentliche Stellen des Bundes in den §§ 4d und 4e BDSG. Insbesondere § 4d Abs. 5 BDSG sieht eine Vorabkontrolle bei risikobehafteter, automatisierter Datenverarbeitung vor.
Auch das Landesrecht kennt Fälle einer präventiven Einbeziehung der Aufsichtsbehörde. Im Landesrecht legt zum Beispiel § 27 Abs. 1 S. 1 RhPfDSG den öffentlichen Stellen (des Landes) auf, dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit Verfahren anzumelden, in denen personenbezogene Daten automatisiert verarbeitet werden.
Die DSGVO ersetzt das System der Meldepflicht und Vorabkontrolle aber grundsätzlich durch die Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und eine daraus erwachsende vorherige Konsultationspflicht. Deren Voraussetzungen regelt die DSGVO grundsätzlich unmittelbar. Die Regelung des

§ 4d DSGVO ist entsprechend nunmehr grundsätzlich obsolet. Art. 36 Abs. 5 DSGVO räumt den Mitgliedstaaten aber das Recht ein, solche Konsultations- und Genehmigungspflichten für die Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe zu etablieren.

22. Art. 37 Abs. 4 S. 1 Hs. 2 (ex Art. 35 Abs. 4 Hs. 2); Art. 38 Abs. 5 (ex Art. 36 Abs. 4): Datenschutzbeauftragter

a. Inhalt

Art. 37 Abs. 4 S. 1 Hs. 2 (ex Art. 35 Abs. 4 S. 1 Hs. 2) DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, die Pflicht, einen Datenschutzbeauftragten zu benennen, auf weitere – von Abs. 1 nicht erfasste – Stellen auszudehnen.

b. Einordnung in das System der Öffnungsklauseln

Die Öffnungsklausel des Art. 37 Abs. 4 S. 1 Hs. 2 (ex Art. 35 Abs. 4 S. 1 Hs. 2) DSGVO ist fakultativer Natur: Die Mitgliedstaaten können von ihr Gebrauch machen, müssen es aber nicht. Sie richtet sich sowohl an öffentliche wie auch an nicht-öffentliche Stellen.

c. Einordnung in den Regelungskontext der Vorschrift

Art. 37 (ex Art. 35) DSGVO regelt, welche Stellen einen Datenschutzbeauftragten benennen müssen und legt in Grundzügen fest, wer als Datenschutzbeauftragter in Betracht kommt und wie dieser in der öffentlichen oder nicht-öffentlichen Stelle verortet sein muss.[120]
Grundsätzlich[121] müssen alle öffentlichen Stellen, die Daten i. S. v. Art. 2 Abs. 1 DSGVO verarbeiten, einen Datenschutzbeauftragten benennen (Abs. 1 lit. a). Ebenso müssen Stellen, deren „Kerntätigkeit“ die Verarbeitung von Daten ist, einen Datenschutzbeauftragten benennen, soweit entweder eine regelmäßige und systematische Beobachtung von Betroffenen erfolgt (Abs. 1

[120] Namentlich Abs. 5 – 7 (ex Art. 35 Abs. 8 und 9) regeln Qualifikationserfordernisse für Datenschutzbeauftragte und die Verpflichtung, die Kontaktdaten des Datenschutzbeauftragten und der Aufsichtsbehörde zu veröffentlichen.
[121] Ausnahmen gelten für die Gerichte für ihre rechtsprechende Tätigkeit, Art. 37 (ex Art. 35) Abs. 1 lit. a DSGVO (vgl. auch Art. 55 (ex Art. 51) Abs. 3 DSGVO).

lit. b) oder besonders sensible Daten nach Art. 9 DSGVO oder Art. 10 (ex Art. 9a) DSGVO verarbeitet werden (Abs. 1 lit. c). Unter bestimmten Voraussetzungen genügt es, für eine Gruppe von Unternehmen oder für mehrere öffentliche Stellen nur *einen* Datenschutzbeauftragen zu installieren (Abs. 2 und 3). Abs. 4 S. 1 Hs. 1 gestattet es sonstigen Stellen, freiwillig Datenschutzbeauftragte mit den damit verbundenen rechtlichen Konsequenzen zu bestellen. Außerdem erlaubt Abs. 4 S. 1 Hs. 2 den Mitgliedstaaten, weiteren als den in Abs. 1 lit. a bis c aufgeführten Stellen die Pflicht aufzuerlegen, einen Datenschutzbeauftragten vorzusehen.

d. Vergleich zur Datenschutzrichtlinie

Bisher waren der Datenschutzbeauftragte und seine Aufgaben nur rudimentär in EG 49 DSRL geregelt. Sie verpflichtete die Mitgliedstaaten nicht, Datenschutzbeauftragte vorzusehen. Vielmehr eröffnete der Datenschutzbeauftragte im Sinne der Richtlinie einen Weg, eine Befreiung von der Meldepflicht bei Datenverarbeitungen zu erreichen – sofern er sicherstellt, dass eine Beeinträchtigung der Rechte und Freiheiten Betroffener nicht zu erwarten ist (Art. 18 Abs. 2 Spstr. 1 RL 95/46/EG). Der Datenschutzbeauftragte musste „völlige Unabhängigkeit“ genießen, auch wenn er Angestellter des Verantwortlichen war (EG 49 S. 3 RL 95/46/EG).
Von der Möglichkeit, die Benennung eines Datenschutzbeauftragten vorzusehen, macht im deutschen Recht bisher § 4f BDSG für öffentliche Stellen des Bundes und nicht-öffentliche Stellen sowie ein Großteil der Landesdatenschutzgesetze für den öffentlichen Bereich der Länder (vgl. § 11 Abs. 1 S. 1 RhPfDSG) Gebrauch.
Art. 37 (ex Art. 35) Abs. 1 DSGVO exportiert dieses „deutsche Modell“ als zwingende Verpflichtung in die anderen Mitgliedstaaten der Union: Sowohl für den öffentlichen als auch für den nicht-öffentlichen Bereich ist die Benennung eines Datenschutzbeauftragten in weiten Bereichen nunmehr zwingend.[122] Dabei erstreckt sich die Aufgabe des Datenschutzbeauftragten sowohl auf die Einhaltung der Datenschutz-Grundverordnung als auch des nationalen Datenschutzrechts (Art. 39 [ex Art. 37] Abs. 1 lit. b DSGVO).

[122] Dazu auch *Kühling/Martini* (Fn. 1), 452.

e. Anwendungsbereich der Öffnungsklausel

Umsetzungsspielraum- und bedarf kann Art. 37 Abs. 4 (ex Art. 35 Abs. 4) DSGVO sowohl im Hinblick auf die Festschreibung weiterer Stellen auslösen, die einen Datenschutzbeauftragten benennen müssen, als auch im Hinblick auf die Festschreibung der Qualifikationserfordernisse für den Datenschutzbeauftragten.

aa) Festschreibung weiterer Stellen, die einen Datenschutzbeauftragten benennen müssen

i. Bedarf nach einer Regelung

Von der Öffnungsklausel des Art. 37 Abs. 4 S. 1 Hs. 2 (ex Art. 35 Abs. 4 S. 1 Hs. 2) DSGVO Gebrauch zu machen, kann dann angezeigt sein, wenn die Stellen, welche nunmehr die Datenschutz-Grundverordnung dazu verpflichtet, einen Datenschutzbeauftragten zu bestellen, nicht mehr mit den Stellen übereinstimmen, die der deutsche Gesetzgeber nach § 4f Abs. 1 BDSG hierzu verpflichten wollte und die nationalen Regelungen in ihrem aktuellen Stand wegen der Datenschutz-Grundverordnung nicht fortgelten. Soweit das nicht der Fall ist, fragt sich, ob die Anordnung der grundsätzlichen Verpflichtung zur Bestellung von Datenschutzbeauftragten neben Art. 37 (ex Art. 35) Abs. 1 DSGVO weiter bestehen kann.

– Überschneidungen und Abweichungen zwischen Art. 37 (ex Art. 35) Abs. 1 DSGVO und § 4f Abs. 1 S. 1, 3 BDSG

Jedenfalls die grundsätzliche Anordnung des *§ 4f Abs. 1 S. 1 BDSG* überschneidet sich weitgehend mit Art. 37 (ex Art. 35) Abs. 1 DSGVO. Allerdings ist die Beschränkung auf eine automatisierte Datenverarbeitung nur bedingt mit Art. 2 Abs. 1 DSGVO vereinbar: Er erstreckt den sachlichen Anwendungsbereich der Datenschutz-Grundverordnung nicht nur auf die *automatisierte* Verarbeitung personenbezogener Daten, sondern auch auf die *nicht-automatisierte* Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. Insoweit greift § 4f Abs. 1 S. 1 BDSG – gemessen am künftigen Unionsrecht – zu kurz. *§ 4f Abs. 1 S. 3 BDSG* erstreckt die Bestellungspflicht zwar auch auf sonstige

Formen der Datenverarbeitung. Er setzt aber voraus, dass in der Betriebseinheit mindestens 20 Personen mit der Verarbeitung beschäftigt sind.

– § 4f Abs. 1 S. 4 BDSG

Auch die Ausnahme des *§ 4f Abs. 1 S. 4* BDSG für nicht-öffentliche Stellen, die in der Regel höchstens neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, ist in ihrer jetzigen Form nicht mit der Datenschutz-Grundverordnung vereinbar. Denn diese etabliert eine Pflicht zur Bestellung eines Datenschutzbeauftragten unabhängig von der Zahl der mit der Verarbeitung beschäftigten Personen. Sie deckt keinen pauschalen Ausschluss bestimmter Behörden. Folglich bedürfen die Regelungen des § 4f Abs. 1 BDSG einer Anpassung.

– § 4f Abs. 1 S. 5 BDSG

§ 4f Abs. 1 S. 5 BDSG gestattet es öffentlichen Stellen, einen Beauftragten für den Datenschutz für mehrere Bereiche vorzusehen, soweit dies aufgrund der Struktur der Stelle erforderlich ist. Art. 37 (ex Art. 35) Abs. 1 lit. a DSGVO übernimmt diesen Grundgedanken und weitet ihn aus. Im Vergleich zum neuen Unionsrecht ist die deutsche Regelung zu eng gefasst. Sie sollte aufgehoben werden.

ii. Grundzüge einer nationalen Regelung

Die nationale Regelung muss festhalten, welche öffentlichen und nicht-öffentlichen Stellen zusätzlich zum Mindestanforderungsniveau der Verordnung einen Datenschutzbeauftragten zu bestellen haben, falls dies dem Willen des nationalen Gesetzgebers entspricht.

Die Regelungen in Bezug auf *öffentliche und nicht-öffentliche Stellen*, also § 4f Abs. 1 S. 3 BDSG, können insoweit aufrechterhalten bleiben, als sie solche Datenverarbeitungen erfassen, die über den Kreis der von Art. 2 Abs. 1 DSGVO erfassten Verarbeitungen hinausgehen (in diesem Fall ist auch das Kriterium von 20 Personen mit der Datenschutz-Grundverordnung vereinbar).

Die Regelungen des § 4f Abs. 1 S. 4, 6 BDSG, die sich *ausschließlich* auf *nicht-öffentliche Stellen* beziehen, können insoweit aufrechterhalten bleiben, als sie Datenverarbeiter betreffen, die nicht bereits aufgrund der Datenschutz-Grundverordnung zwingend zur Bestellung eines Datenschutzbeauftragten verpflichtet sind. Gleichzeitig ist im Interesse des Gleichlaufs hier eine Aus-

dehnung auch auf die weiteren Art. 2 Abs. 1 DSGVO unterfallenden Verarbeitungsvorgänge anzuraten, also die nicht-automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen.

bb) Festsetzung der Qualifikationsanforderungen an den Datenschutzbeauftragten, Art. 37 Abs. 5, Art. 38 Abs. 5

Ob und ggf. in welchem Umfang die Mitgliedstaaten auch die nötige Qualifikation des Datenschutzbeauftragten spezifizieren dürfen, ist nicht eindeutig. Farbe bekennt alleine Art. 38 Abs. 5 DSGVO: Die Mitgliedstaaten dürfen und müssen Regelungen erlassen, welche sicherstellen, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung bzw. Vertraulichkeit gebunden ist. Die Vorschrift verweist auf das nationale Verfahrensrecht und Arbeits- und Dienstrecht, welches die näheren prozeduralen Verpflichtungselemente bereithält, um die Geheimhaltung und Vertraulichkeit bei der Wahrnehmung des Amtes zu wahren. Den Mitgliedstaaten kommt insoweit eine Konkretisierungsbefugnis zu.
Dass die anderen Vorschriften des Art. 38 DSGVO keinen Verweis auf das mitgliedstaatliche Recht enthalten, legt einen Umkehrschluss nahe. Auch ein systematischer Vergleich mit den Regelungen der Datenschutz-Grundverordnung zu Aufsichtsbehörden widerstreitet einer nationalen Regelungsbefugnis. Art. 54 (ex Art. 49) Abs. 1 lit. b DSGVO sieht explizit eine Öffnungsklausel vor, nach der die Mitgliedstaaten für die Ernennung zum Mitglied einer Aufsichtsbehörde selbst ein gewisses Qualifikationsniveau festschreiben können und müssen. In Bezug auf den Datenschutzbeauftragten fehlt eine solche explizite Öffnungsklausel.
Andererseits darf es den Mitgliedstaaten nicht verwehrt sein, Regelungslücken, welche die Datenschutz-Grundverordnung lässt, durch Konkretisierung des Regelungsgehalts zu schließen, wenn sie von dem Regelungsspielraum einer Öffnungsklausel Gebrauch machen. Die vage Umschreibung der nötigen Qualifikation gerade für den Datenschutzbeauftragten, der eine wichtige Position im Datenschutzregime einnimmt, lässt sowohl die öffentlichen als auch die nicht-öffentlichen Stellen bei der Ernennung mit einem hohen substanziellen Grad an Rechtsunsicherheit zurück. EG 97 (ex EG 75) S. 3 DSG-

VO gleicht dies nur scheinbar durch weitere Präzisierung aus: Er bestimmt, dass sich der Grad des erforderlichen Fachwissens nach der Art der durchgeführten Datenverarbeitung und des erforderlichen Schutzes richtet. Damit spricht Einiges dafür, dass den Mitgliedstaaten ein Restregelungsspielraum bei der Ausfüllung der Qualitätsanforderungen an den Datenschutzbeauftragten verbleibt, die sie im Rahmen ihrer Öffnungsklauseln fordern. Handlungsbedarf ergibt sich im deutschen Recht im Übrigen aber insoweit, als bestehende Regelungen des BDSG bzw. der LDSG wegen eines mangelnden Umsetzungsspielraums oder jedenfalls wegen des Normwiederholungsverbotes gegen die Datenschutz-Grundverordnung verstoßen und anzupassen sind. Dem liegt die Prämisse zugrunde, dass aus einer Öffnungsklausel, welche das „Ob" (hier: die Verpflichtung zur Ernennung eines Datenschutzbeauftragten) erfasst, auch ein Mindestmaß an Freiheit hinsichtlich der Ausgestaltung des wahrzunehmenden Amtes („Wie") folgt. Sicher ist das aber nicht: Art. 37 Abs. 4 DSGVO lässt sich auch so lesen, dass er den Mitgliedstaaten ausschließlich die Möglichkeit eröffnet, die Funktion des Datenschutzbeauftragten, wie sie die DSGVO vorsieht und ausgestaltet, ohne inhaltliche Gestaltungsfreiheit als Schablone auf weitere Verarbeiter und Auftragsverarbeiter zu erstrecken. Die besseren Gründe streiten dafür, dass der Unionsgesetzgeber das so ausgestalten wollte.

23. Art. 43 (ex Art. 39a) Abs. 1 S. 2: nationale Akkreditierungsstelle

Die nationalen Gesetzgeber regeln, welche nationale Stelle die Zertifizierungsstellen akkreditiert, ihnen also die Berechtigung verleiht, Datenschutzsiegel zu vergeben und Datenschutz-Zertifizierungen durchzuführen (Art. 43 [ex Art. 39a] Abs. 1 DSGVO). Eine Zertifizierung dient als Nachweis, dass die Verantwortlichen die Anforderungen der Datenschutz-Grundverordnung einhalten (Art. 42 [ex Art. 39] Abs. 1 DSGVO). Der Mitgliedstaat teilt mit, ob die Zertifizierungsstellen von der zuständigen Aufsichtsbehörde und/oder der nationalen Akkreditierungsstelle[123] akkreditiert werden (Art. 43 [ex Art. 39a] Abs. 1 S. 2 DSGVO).

[123] In Deutschland handelt es sich dabei um eine beliehene Gesellschaft des Privatrechts, *Bloehs/Frank*, in: dies. (Hrsg.), AkkreditierungsR, 2015, Systematische Einführung, Rn. 19 ff.

a. Einordnung der Öffnungsklausel in das System mitgliedstaatlicher Regelungsspielräume

Die Mitgliedstaaten sind zwar frei in der Auswahl der Akkreditierungsstelle – nicht hingegen bei der Entschließung, ob eine Akkreditierungsstelle überhaupt benannt wird. Art. 43 (ex Art. 39a) Abs. 1 DSGVO enthält insoweit eine obligatorische Öffnungsklausel. Dies korrespondiert mit der Pflicht, Zertifizierungsverfahren zu fördern (Art. 42 [ex Art. 39] Abs. 1, EG 100 [ex EG 77] DSGVO).

b. Inhalt der Öffnungsklausel

Die Öffnungsklausel räumt den Mitgliedstaaten ein Ermessen dahin gehend ein, ob die Aufsichtsbehörde, die nationale Akkreditierungsstelle[124] oder beide gemeinsam für die Akkreditierung der Zertifizierungsstellen verantwortlich sind. Die Öffnungsklausel erschließt den Mitgliedstaaten damit formelle Umsetzungsspielräume.

Materielle Anforderungen an die Akkreditierungsstelle enthält Art. 43 (ex Art. 39a) DSGVO zwar auch. Diese sind aber nicht Bestandteil der Öffnungsklausel. Unabhängig davon hat die nach nationalem Recht autorisierte Akkreditierungsstelle diese Anforderungen einzuhalten bzw. zu prüfen[125].

---

[124] Die nationale Akkreditierungsstelle wird gemäß VO (EG) Nr. 765/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über die Vorschriften für die Akkreditierung und Marktüberwachung im Zusammenhang mit der Vermarktung von Produkten und zur Aufhebung der Verordnung (EWG) Nr. 339/93 des Rates (ABl. EG 2008, L 218/30) im Einklang mit EN-ISO/IEC_17065/2012 und mit den zusätzlichen Anforderungen der zuständigen Aufsichtsbehörde benannt (Art. 43 [ex Art. 39a] Abs. 1 lit. b DSGVO).

[125] Art. 43 (ex Art. 39a) Abs. 2 DSGVO enthält materielle Anforderungen an die Zertifizierungsstelle, um akkreditiert zu werden. Diese Kriterien hat auch die Akkreditierungsstelle bei der Entscheidung über die Anerkennung als Zertifizierungsstelle mit einzubeziehen. Zu diesen Voraussetzungen zählt etwa der die zuständige Aufsichtsbehörde zufriedenstellende Nachweis des Fachwissens und der Unabhängigkeit (lit. a) sowie nicht bestehender Interessenkonflikte (lit. d). Zusätzlich muss sich die Zertifizierungsstelle verpflichten, die Kriterien nach Art. 42 Abs. 5 (ex Art. 39 Abs. 2a), die die Aufsichtsbehörde oder der Europäische Datenschutzausschuss genehmigt hat, einzuhalten, Art. 43 Abs. 2 lit. b (ex Art. 39a Abs. 2 lit. aa). Art. 43 Abs. 2 lit. c (ex Art. 39a Abs. 2 lit. b) verlangt, dass die Stelle Verfahren für die Erteilung, die regelmäßige Überprüfung und den Widerruf von Datenschutzsiegeln und -prüfzeichen festlegt. Schließlich muss die Zertifizierungsstelle transparente Beschwerdeverfahren und -strukturen vorhalten, um Beschwerden zu Verstößen gegen die Zertifizierung behandeln zu lassen, Art. 43 Abs. 2 lit. d (ex Art. 39a Abs. 2 lit. c). Gemäß Art. 43 (ex Art. 39a) Abs. 4 S. 1 DSGVO ist die

Das stellt Art. 43 (ex Art. 39a) Abs. 3 S. 1 DSGVO klar. Die Akkreditierung erfolgt anhand der von der Aufsichtsbehörde oder dem Europäischen Datenschutzausschuss genehmigten Kriterien. Letztere ergänzen die Bestimmungen zu Methoden und Verfahren der Zertifizierungsstellen der VO (EG) Nr. 765/2008, wenn der Mitgliedstaat die nationale Akkreditierungsstelle in die Verantwortung einbezieht (Art. 43 [ex Art. 39a] Abs. 3 S. 2 DSGVO).

c. Vergleich zur Vorgängerrichtlinie

Die Vorschriften zur Zertifizierung, insbesondere zum Europäischen Datenschutzsiegel, sind ein Novum des unionalen Datenschutzrechts. Das gilt entsprechend auch für die Regeln über die Akkreditierungsstelle. Die Regelung findet in der Datenschutzrichtlinie keine Vorbilder.

d. Abgleich mit bestehendem nationalen Recht

Das BDSG enthält bisher keine Regelungen zur Bestimmung einer Akkreditierungsstelle im Rahmen von Zertifizierungsverfahren. Auch das Akkreditierungsstellengesetz[126] legt lediglich fest, welche Stelle als nationale Akkreditierungsstelle gemäß der VO (EG) Nr. 765/2008 anzusehen ist.

24. Art. 49 (ex Art. 44): Ausnahmetatbestände zum Drittstaatentransfer

a. Struktur und Hintergrund

Art. 49 (ex Art. 44) DSGVO regelt Ausnahmefälle für eine Übermittlung in Drittstaaten oder an internationale Organisationen nach Vorgabe der Art. 44 ff. (ex Art. 40 ff.) DSGVO. Übermittlungen in Drittstaaten oder an internationale Organisationen können nach Art. 45 (ex Art. 41) DSGVO entweder aufgrund eines Angemessenheitsbeschlusses der Kommission erfolgen, aufgrund

---

Zertifizierungsstelle für eine angemessene, der Zertifizierung oder deren Widerruf zugrunde liegenden Bewertung verantwortlich. Die Gründe für die Zertifizierung oder deren Widerruf hat sie der Aufsichtsbehörde mitzuteilen, Art. 43 (ex Art. 39a) Abs. 5 DSGVO. Art. 43 Abs. 8, 9 (ex Art. 39a Abs. 7, 8) DSGVO erlauben der Kommission, Tertiärrechtsakte zu spezifischen Anforderungen an die Zertifizierungsverfahren und die Datenschutzsiegel bzw. -prüfzeichen festzulegen.

[126] Gesetz über die Akkreditierungsstelle, BGBl. 2009-I, S. 2625.

geeigneter Garantien i. S. d. Art. 46 (ex Art. 42) DSGVO oder aufgrund von Binding Corporate Rules gem. Art. 47 (ex Art. 43) DSGVO. Art. 49 (ex Art. 44) DSGVO eröffnet den Mitgliedstaaten Spielraum hinsichtlich einer Übermittlung aufgrund wichtiger Gründe des öffentlichen Interesses nach Art. 49 Abs. 1 lit. d i. V. m. Abs. 4 (ex Art. 44 Abs. 1 lit. d i. V. m. Abs. 5) DSGVO, Übermittlung von personenbezogenen Daten aus Registern i. S. d. Art. 49 Abs. 1 lit. g (ex Art. 44 Abs. 1 lit. g) DSGVO und zur Regelung einer Einschränkung der Übermittlung in Drittstaaten oder an internationale Organisationen aus wichtigen Gründen des öffentlichen Interesses i. S. d. Art. 49 Abs. 5 (ex Art. 44 Abs. 5a) DSGVO. Bisher fanden sich die Ausnahmeregelungen in Art. 26 DSRL, die in § 4c BDSG umgesetzt wurden.

b. Qualifikation der Öffnungsklausel

Die Öffnungsklauseln markieren einen fakultativen Regelungsbedarf. Die Bestimmungen des Art. 49 (ex Art. 44) DSGVO richten sich sowohl an öffentliche wie nicht-öffentliche Stellen im Sinne der überkommenen Differenzierung im deutschen Datenschutzrecht. Art. 49 Abs. 1 1 lit. d bzw. g (ex Art. 44 Abs. 1 lit. d bzw. g) DSGVO geben den Mitgliedstaaten die Möglichkeit zur Konkretisierung der Vorgaben der Datenschutz-Grundverordnung. Art. 49 Abs. 5 (ex Art. 44 Abs. 5a) DSGVO gestattet den Mitgliedstaaten eine Beschränkung der Bestimmungen der Datenschutz-Grundverordnung für die Übermittlung in Drittstaaten oder an internationale Organisationen, sofern kein Angemessenheitsbeschluss i. S. d. Art. 45 (ex Art. 41) DSGVO vorliegt.

c. Voraussetzungen der Öffnungsklausel; Handlungsmöglichkeiten

aa) Art. 49 Abs. 1 lit. d, Abs. 4 (ex Art. 44 Abs. 1 lit. d, Abs. 5)

Art. 49 Abs. 1 lit. d, Abs. 4 (ex Art. 44 Abs. 1 lit. d, Abs. 5) DSGVO erlaubt die Übermittlung von personenbezogenen Daten in Drittstaaten oder an internationale Organisationen, wenn sie aus wichtigen Gründen des öffentlichen Interesses notwendig ist. Die wichtigen Gründe des öffentlichen Interesses müssen dabei im Unions- oder mitgliedstaatlichen Recht anerkannt sein, Art. 49 Abs. 4 (ex Art. 44 Abs. 5) DSGVO. Damit eröffnet Art. 49 Abs. 1 lit. d, Abs. 4 (ex Art. 44 Abs. 1 lit. d, Abs. 5) DSGVO die Möglichkeit, das

öffentliche Interesse i. S. d. Art. 49 Abs. 1 lit. d (ex Art. 44 Abs. 1 lit. d) DSGVO zu konkretisieren.
Die englische Formulierung „important reasons of public interest" zeigt, dass die Anforderungen an eine Datenübermittlung höher sind als in Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1 DSGVO, in denen für die Zulässigkeit einer Datenverarbeitung eine Wahrnehmung einer Aufgabe im öffentlichen Interesse ausreicht. In Art. 26 Abs. 1 lit. d Var. 1 DSRL sowie in § 4c Abs. 1 S. 1 Nr. 4 Alt. 1 BDSG findet sich eine ähnliche Formulierung, die auf die Wahrung von wichtigen öffentlichen Interessen[127] hinweist. Die Unterscheidung im Wortlaut eines wichtigen Grundes des öffentlichen Interesse einerseits und zur Wahrung wichtiger öffentlicher Interessen andererseits dürfte rein sprachlicher Natur sein, da sowohl EG 58 DSRL als auch EG 112 (ex EG 87) DSGVO als Beispiele für das Vorliegen eines wichtigen öffentlichen Interesses i. S. d. DSRL bzw. eines wichtigen Grundes, der im öffentlichen Interesse liegt i. S. d. Datenschutz-Grundverordnung den Datenaustausch zwischen Steuer- oder Zollverwaltungen oder zwischen Diensten, die für soziale Sicherheit zuständig sind, nennen. Darüber hinaus nennt EG 112 (ex EG 87) DSGVO ferner den Datenaustausch zwischen Wettbewerbsbehörden, Finanzaufsichtsbehörden und Diensten, die für Angelegenheiten der öffentlichen Gesundheit zuständig sind, als solche Gründe.
Art. 49 Abs. 4 (ex Art. 44 Abs. 5) DSGVO verlangt, dass das öffentliche Interesse i. S. d. Art. 49 Abs. 1 lit. d (ex Art. 44 Abs. 1 lit. d) DSGVO vom Unionsrecht oder dem mitgliedstaatlichen Recht *anerkannt* sein muss, d. h. das öffentliche Interesse muss nicht in einer Sammelnorm zur Aktivierung der Öffnungsklausel festgelegt sein. Im Übrigen erstreckt sich die Öffnungsklausel nur auf die Konkretisierung des *öffentlichen Interesses* und lässt keinen Spielraum, um die Vorgaben des Art. 49 Abs. 1 lit. d (ex Art. 44 Abs. 1 lit. d) DSGVO selbst zu modifizieren oder zu konkretisieren. Weil die Begriffe aus § 4c Abs. 1 S. 1 Nr. 6 Alt. 1 BDSG und Art. 49 Abs. 1 lit. d (ex Art. 44 Abs. 1 lit. d) DSGVO übereinstimmen, besteht kein Handlungsbedarf im nationalen Recht. Damit ersetzt Art. 49 Abs. 1 lit. d (ex Art. 44 Abs. 1 lit. d)

[127] Vgl. Art. 26 Abs. 1 lit. d Var. 1 RL 95/46/EG: „the transfer is necessary (…) on important public interest grounds (…)".

DSGVO die Vorgabe des § 4c Abs. 1 Nr. 6 Alt. 1 BDSG, der nicht aufrechterhalten werden kann, aber auch nicht aufrechterhalten werden muss, um das Datenschutzniveau zu erhalten. Es besteht also eine Handlungsoption der Konkretisierung des öffentlichen Interesses, aber kein Handlungsbedürfnis – auch im Vergleich zur bisherigen Regelung im BDSG, wo diese Konkretisierung nicht erfolgt ist.

bb) Art. 49 Abs. 1 lit. g (ex Art. 44 Abs. 1 lit. g)

Art. 49 Abs. 1 lit. g (ex Art. 44 Abs. 1 lit. g) DSGVO bietet eine Rechtsgrundlage für Übermittlungen solcher personenbezogener Daten in Drittstaaten, die aus Registern erfolgen, deren Inhalt für die Öffentlichkeit bestimmt ist und die entweder für die Öffentlichkeit generell oder für jedermann, der ein berechtigtes Interesse nachweisen kann, zugänglich sind. Die öffentliche Zugänglichkeit soll von den Regelungen des Unionsrechts oder des mitgliedstaatlichen Rechts abhängen. Die Öffnungsklausel ermöglicht also die Regelung der öffentlichen Zugänglichkeit bestimmter Register. Schon nach bisheriger Rechtslage besteht mit § 4c Abs. 1 S. 1 Nr. 6 BDSG (der Art. 26 Abs. 1 lit. f DSRL umsetzt) eine Regelung, die mit den Vorgaben des Art. 49 Abs. 1 lit. g (ex Art. 44 Abs. 1 lit. g) DSGVO korrespondiert. Register i. S. d. § 4c Abs. 1 S. 1 Nr. 6 BDSG sind etwa Handelsregister (§ 9 HGB), oder auch das Grundbuch (§12 GBO).[128] Die Übermittlung von Daten aus einem Register, das nur bei berechtigtem Interesse einsehbar ist, soll nach EG 111 (ex EG 86) DSGVO nur auf Antrag der einsichtsberechtigten Person erfolgen, oder nur dann, wenn die Personen die Empfänger der Übermittlung sind. Diese Klarstellung findet sich bereits in EG 58 DSRL und stellt keine Neuerung der geltenden Rechtslage dar.
Art. 49 Abs. 1 lit. g (ex Art. 44 Abs. 1 lit. g) DSGVO verlangt eine öffentliche Zugänglichkeit nach mitgliedstaatlichem Recht. Hierzu reicht ein Verweis auf die jeweils bestehenden nationalen Regelungen über die Öffentlichkeit des Registers aus. Art. 49 Abs. 1 lit. g (ex Art. 44 Abs. 1 lit. g) DSGVO ersetzt insofern den § 4c Abs. 1 S. 1 Nr. 6 BDSG, und wird, in Verbindung

[128] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 4c, Rn. 8; *Simitis*, in: ders. (Hrsg.), BDSG, 8. Aufl., 2014, § 4c, Rn. 23.

mit der entsprechenden nationalen Norm – z. B. § 9 HGB – neue Rechtsgrundlage für eine Übermittlung personenbezogener Daten aus öffentlich zugänglichen Registern an Drittstaates oder an internationale Organisationen. Insoweit besteht also kein datenschutzrechtlicher Regelungsbedarf – etwaige Regelungen zu Registern sind vielmehr keine datenschutzrechtlichen Bestimmungen.

cc) Art. 49 Abs. 5 (ex Art. 44 Abs. 5a); fakultativer Handlungsbedarf

Art. 49 Abs. 5 (ex Art. 44 Abs. 5a) DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, die Übermittlung von spezifischen Kategorien personenbezogener Daten aus wichtigen Gründen im öffentlichen Interesse einzuschränken, wenn für das Empfängerland kein Angemessenheitsbeschluss der Kommission ergangen ist. Der Erlass einer expliziten Beschränkung ist also nur für solche Fälle möglich, in denen kein Angemessenheitsbeschluss der Kommission vorliegt, und auch nur für die Fälle nötig, in denen die Verarbeitung der in Frage stehenden personenbezogenen Daten nach Maßgabe der Datenschutz-Grundverordnung einerseits und zusätzlich die Übermittlung in Drittstaaten nach Maßgabe der Art. 44 ff. (ex Art. 40 ff.) DSGVO andererseits zulässig wäre. Die englische Formulierung „Member State law may (…) *expressly* set limits (…)“ zeigt auf, dass im Falle einer Aktivierung der Öffnungsklausel eine explizite Regelung nötig wird, in der die spezifischen Datenkategorien, deren Übermittlung beschränkt werden soll, genannt werden. Nicht notwendig ist nach dem Wortlaut des Art. 49 Abs. 5 (ex Art. 44 Abs. 5a) DSGVO eine explizite Nennung der wichtigen öffentlichen Interessen, aus denen die Übermittlung beschränkt werden kann. Beispiele für Arten von Daten i. S. d. Art. 49 Abs. 5 (ex Art. 44 Abs. 5a) DSGVO sind etwa nationale Passdaten oder elektronische Gesundheitsakten.[129]
Eine Beschränkung der Übermittlungen in Drittstaaten für spezifische Datenkategorien enthält das BDSG bisher nicht, obwohl es diese auch nach Art. 26 Abs. 1 DSRL gegenüber den nach der DSRL zu erlaubenden Fällen hätte vorsehen können. Das BDSG übernimmt alleine die Erlaubnistatbestände der DSRL. Art. 49 Abs. 5 (ex Art. 44 Abs. 5a) DSGVO eröffnet damit eine Mög-

[129] Rats-Dok. 10349/14, Rn. 15.

lichkeit der Restriktion, die auch bisher ungenutzt blieb. Eine Inanspruchnahme dieser Öffnungsklausel ist damit nicht notwendig, um das bisherige Datenschutzniveau zu erhalten. Etwas anderes kann alleine mit Blick auf Art. 49 (ex Art. 44) Abs. 1 h DSGVO gelten, der so noch nicht in der DSRL vorhanden war (alleine Art. 26 Abs. 2 DSRL ging in eine ähnliche Richtung und erfuhr in § 26 Abs. 2 BDSG eine konkretisierende Umsetzung). Insoweit könnte das nationale Recht ggf. auch einschränkende Bestimmungen etablieren.

25. Vorbemerkungen zu den Art. 51 ff. (ex Art. 46 ff.) – Kapitel VI und VII: unabhängige Aufsichtsbehörden, Zusammenarbeit und Kohärenzverfahren

a. Einführung – Entwicklung hin zur DSGVO

Im Bereich des aufsichtsrechtlichen Vollzugs des materiellen Datenschutzrechts bleibt manches – wenn auch im Gewand der Verordnung – beim Alten. Vieles aber ändert sich grundlegend: Der Vollzug der Verordnung liegt zwar weiterhin grundsätzlich in den Händen der „völlig unabhängigen" mitgliedstaatlichen Aufsichtsbehörden (Art. 51 ff. DSGVO). Die Zeiten nationaler Datenschutz-Fürstentümer sollen aber verfahrensrechtlich der Vergangenheit angehören.[130] Stattdessen bemüht sich die Datenschutz-Grundverordnung darum, die nationale Datenschutzaufsicht in eine kooperative unionsrechtlich geprägte Aufsichtsstruktur einzupassen. Einerseits regelt sie die Zuständigkeit, Aufgaben und Befugnisse der nationalen Aufsichtsbehörden nunmehr (größtenteils) selbst (Art. 55 ff. DSGVO). Andererseits verpflichtet die Datenschutz-Grundverordnung die Aufsichtsbehörden im Rahmen eines Zusammenarbeits- (Art. 60 [ex Art. 54a] DSGVO) und Kohärenzverfahrens (Art. 63 [ex Art. 57] DSGVO) auf eine enge Kooperation untereinander sowie mit der Union[131] – insbesondere dann, wenn der Verantwortliche mehrere Niederlassungen in der Union unterhält. In diesem Rahmen etabliert die Da-

[130] *Kühling/Martini* (Fn. 1), 452.
[131] Dazu und zum Folgenden *Kühling/Martini* (Fn. 1), 452 f.

tenschutz-Grundverordnung mit dem Europäischen Datenschutzausschuss (EDA) einen neuen Akteur auf der Ebene des unionalen Datenschutzes. Er löst die alte Art. 29-Datenschutzgruppe ab. Seine primäre Aufgabe besteht darin, auf eine einheitliche Anwendung des Datenschutzrechts in der gesamten Union hinzuwirken. Hierfür stattet ihn die Datenschutz-Grundverordnung – ein Novum – mit der Befugnis aus, in Streitfällen *verbindlich* gegenüber den nationalen Aufsichtsbehörden zu entscheiden (Art. 65 Abs. 1 [ex Art. 58a Abs. 1] DSGVO).[132]

Ziel dieser Neukonzeption war neben der besseren Koordinierung und damit Vereinheitlichung des Datenschutzes auch eine Vereinfachung für die Rechtsunterworfenen. Jeder Verarbeiter (mit mehreren Niederlassungen in der Union) soll sich nur noch gegenüber einer Aufsichtsbehörde verantworten müssen. Der von einem Verarbeitungsprozess Betroffene soll sich gleichzeitig – entsprechend dem Grundgedanken des One-Stop-Government-Prinzips – um die Zuständigkeiten und Abstimmungsprozesse nicht zu kümmern brauchen. Er kann sich an seine mitgliedstaatliche Aufsichtsbehörde wenden, um einen effektiven Schutz seines informationellen Selbstbestimmungsrechts zu erreichen.

aa) Überblick unabhängige Aufsichtsbehörden (Art. 51 ff. DSGVO)

Die Datenschutz-Grundverordnung belässt den Mitgliedstaaten bei der Ausgestaltung ihrer Aufsichtsbehörden grundsätzlich einen weiten Ausgestaltungsspielraum. Sie nimmt damit auf deren verfassungsmäßige, organisatorische und administrative Struktur Rücksicht (EG 117 S. 2 [ex EG 92 S. 2] DSGVO). Soweit es dieser „entspricht", können sie namentlich mehrere nationale Aufsichtsbehörden einrichten. Dies stellt Art. 51 Abs. 1 und Abs. 3 (ex Art. 46 Abs. 1 und Abs. 2) DSGVO unmissverständlich klar. Die Bundesrepublik Deutschland kann damit auch unter der Datenschutz-Grundverordnung ihr bisher praktiziertes Modell mehrerer Aufsichtsbehörden sowohl im Bund als auch in den Ländern beibehalten. Dann muss sie aber entsprechende interne Regelungen zum einheitlichen Auftreten *nach außen* und zur *Binnenkoor-*

[132] *Kühling/Martini* (Fn. 1), 452.

dinierung der nationalen Aufsichtsbehörden schaffen. Damit verbinden sich umfassende Handlungsaufträge an die nationalen Gesetzgeber.
Kerncharakteristikum der mitgliedstaatlichen Aufsichtsbehörden ist deren „völlige Unabhängigkeit" (Art. 52 Abs. 1 DSGVO). Die Datenschutz-Grundverordnung führt insoweit die Judikatur des EuGH zur DSRL in Gesetzesform fort. Art. 52 DSGVO konkretisiert die Anforderungen an die aufsichtsbehördliche Unabhängigkeit und stärkt durch die Einräumung unmittelbarer Garantien (etwa Abs. 2) auch die Position der Mitglieder der Aufsichtsbehörde. Dabei erkennt die Datenschutz-Grundverordnung den Bereich der Datenschutzaufsicht als sensibel an und führt ihn ausführlichen und feingliedrigen Regelungen zu. So setzt die Datenschutz-Grundverordnung etwa bereits auf der den Mitgliedern der Aufsichtsbehörden hierarchisch untergeordneten Ebene an und enthält auch für die Bediensteten Maßgaben für die Aufgabenerledigung (z. B. Art. 54 Abs. 2 DSGVO). Die Aufgaben (Art. 57 DSGVO) und Befugnisse (Art. 58 DSGVO) der Aufsichtsbehörden regelt die Datenschutz-Grundverordnung grundsätzlich selbst und umfassend.

bb) Überblick zum Zusammenarbeits- und Kohärenzverfahren (Art. 60 ff. DSGVO)

Die Neuregelung der Organisation der europäischen Datenschutzaufsicht zielte sowohl auf eine bessere Zusammenarbeit der nationalen Aufsichtsbehörden untereinander (*horizontale Koordinierung, sog. Zusammenarbeitsverfahren*, Art. 60 – 62 DSGVO) als auch auf eine verbindliche Vollzugkoordinierung auf europäischer Ebene (*vertikale Koordinierung, sog. Kohärenzverfahren, Art. 63 – 67 DSGVO*).
Der Bedarf nach einer horizontalen Koordinierung (i) ist dabei auch unmittelbare Folge des Ansatzes der Kommission, eine ressourcenschonende Zuständigkeitskonzentration herzustellen (sog. One-Stop-Shop-Prinzip, Art. 51 Abs. 2 DSGVO-KOM). Zwar konnte sich die Kommission mit ihrem strengen Ansatz nicht durchsetzen; geblieben ist jedoch das nach wie vor hohen Koordinierungsbedarf auslösende Konzept der federführenden Aufsichtsbehörde (sog. Lead-Authority, 54a DSGVO-EP): Die federführende Aufsichtsbehörde ist verpflichtet, sich vor der Entscheidung mit den anderen (betroffenen) Aufsichtsbehörden abzustimmen.

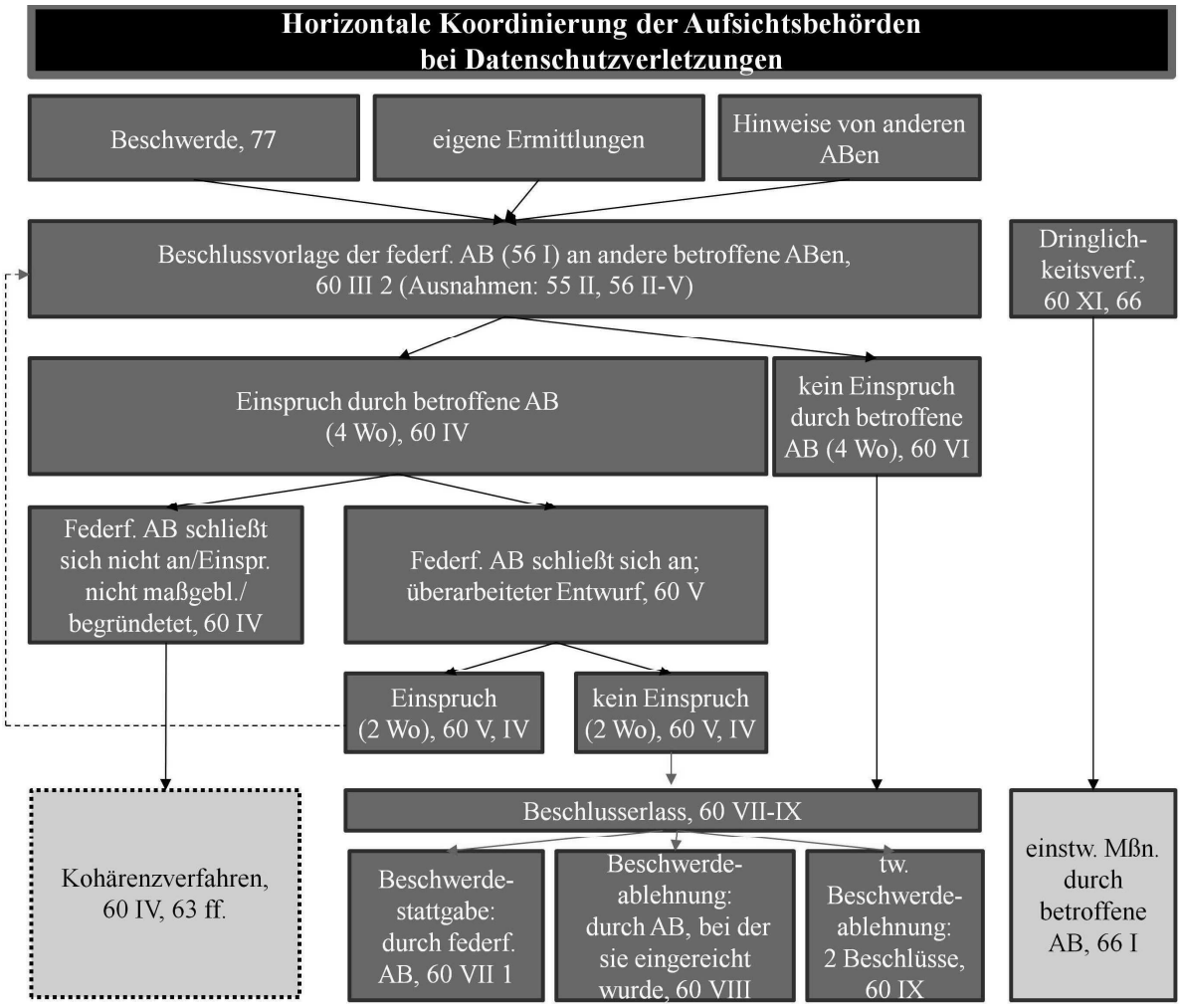
Neben diesem Bedarf der horizontalen Koordinierung tritt in einem auf unionsweit einheitliche Anwendung der Verordnung angelegten System auch die Notwendigkeit einer vertikalen Koordinierung (ii). Einerseits folgt diese aus der Möglichkeit des Scheiterns der horizontalen Koordinierung: Gelingt hier eine Einigung nicht, ist nunmehr der Europäische Datenschutzausschuss (EDA) dazu berufen, eine verbindliche Entscheidung in Form eines Beschlusses (gerichtet an die nationalen Aufsichtsbehörden) zu fällen. Andererseits besteht auch außerhalb des Zusammenarbeitsverfahrens ein Bedarf nach verbindlicher Letztentscheidung auf europäischer Ebene, insbesondere wenn einzelne nationale Aufsichtsbehörden Beschlüsse mit allgemeiner Wirkung treffen, welche die Gefahr in sich bergen, ein einheitliches Datenschutzniveau in der Union zu gefährden. Das gilt zum Beispiel bei der Festlegung von Standard-Datenschutzklauseln und Vertragsklauseln (Art. 64 Abs. 1 lit. d, e DSGVO).

i. Zusammenarbeitsverfahren – horizontale Koordinierung

Das Zusammenarbeitsverfahren (Art. 60-62 DSGVO) als Instrument horizontaler Koordinierung regelt die grenzüberschreitende Zusammenarbeit mehrerer Aufsichtsbehörden in Fällen grenzüberschreitender Datenverarbeitung. Zwei Koordinierungstypen sieht die DSGVO vor: die inhaltliche Zusammenarbeit zwischen der federführenden und den anderen betroffenen Aufsichtsbehörden (Art. 60 DSGVO) auf der einen Seite, die Amtshilfe (Art. 61 DSGVO) und gemeinsame Maßnahmen (Art. 62 DSGVO) auf der anderen Seite (sie sind stets einschlägig, wenn eine (betroffene) Aufsichtsbehörde in einem grenzüberschreitenden Fall tätig wird). Das Verfahren der Zusammenarbeit kommt zum Tragen, wenn ein Sachverhalt, insbesondere wegen mehrerer Niederlassungen des Verantwortlichen, die Zuständigkeit mehrerer Aufsichtsbehörden berührt. Die Aufsichtsbehörde der Hauptniederlassung übernimmt dann die Federführung im aufsichtsbehördlichen Verfahren (Art. 56 Abs. 1 [ex Art. 51a Abs. 1] DSGVO) und arbeitet mit den anderen betroffenen Aufsichtsbehörden konsensorientiert zusammen (Art. 60 Abs. 1 [ex Art. 54a Abs. 1] DSGVO).
Alleine die federführende Aufsichtsbehörde ist dann dazu berufen, das Vorgehen zu steuern und ist vorrangig damit betraut, den Inhalt eines Beschlusses

festzulegen und diesen gegenüber einem Verarbeiter oder Auftragsverarbeiter zu erlassen. Sie hat dabei die inhaltlichen Einwendungen der anderen betroffenen Aufsichtsbehörden zu berücksichtigen. Die federführende Aufsichtsbehörde darf einen Beschluss erst erlassen, wenn ein Konsens zwischen den betroffenen Aufsichtsbehörden (ggf. durch Fiktion, Art. 60 Abs. 6 DSGVO) erzielt wurde. Andernfalls ist eine Entscheidung des EDA im Kohärenzverfahren herbeizuführen. Für den formellen Akt des Beschlusserlasses ist ebenfalls die federführende Aufsichtsbehörde zuständig, es sei denn, der Beschluss besteht in der (teilweisen) Ablehnung einer Beschwerde.

Nicht anwendbar ist das Zusammenarbeitsverfahren nach Art. 60 DSGVO (anders jedoch die Amtshilfe und gemeinsamen Maßnahmen) dann, wenn die Verarbeitung nach Art. 6 Abs. 1 UAbs. 1 lit c und e DSGVO auf der Grundlage einer mitgliedstaatlichen Öffnungsklausel erfolgt. Denn in diesem Fall findet das Konzept der federführenden Aufsichtsbehörde ausnahmsweise (konsequenterweise) keine Anwendung (Art. 55 Abs. 2 DSGVO).



© Martini/Weinzierl

ii. Kohärenzverfahren

Das Kohärenzverfahren der Art. 63 bis 67 (ex Art. 57 bis 63) DSGVO etabliert einen Mechanismus vertikaler Koordination zwischen den nationalen Aufsichtsbehörden (und der Kommission) durch Stellungnahmen und Entscheidungen des EDA (Art. 64, 65 [ex Art. 58, 58a] DSGVO). Es zielt darauf ab, zu einer einheitlichen Anwendung der Datenschutz-Grundverordnung in der gesamten Union beizutragen, wenn das Risiko unterschiedlicher aufsichtsbehördlicher Auslegung der Datenschutz-Grundverordnung besteht (Art. 63, EG 135 S. 1 [ex Art. 57, EG 105 S. 1] DSGVO).

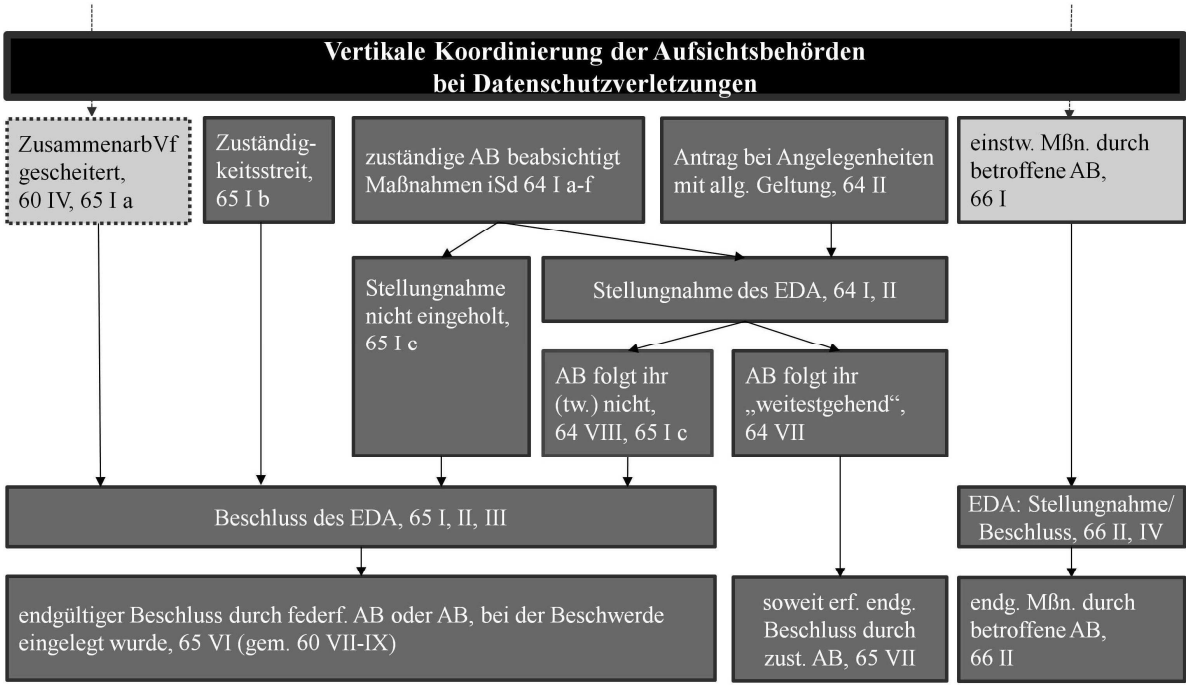
In Grundzügen war es bereits in der DSRL angelegt. Diese sah die sog. Art. 29-Datenschutzgruppe vor, deren Aufgabe es war, die Gleichwertigkeit des Datenschutzes in der Gemeinschaft/Union zu überwachen. Zu diesem

Zweck konnte sie jedoch keine (verbindlichen) Beschlüsse, sondern alleine Stellungnahmen und Empfehlungen abgeben (Art. 30 Abs. 1 – 3 DSRL).
Im Rahmen des Kohärenzverfahrens kommt dem EDA nunmehr die Kompetenz zu, in weiten, abstimmungsrelevanten Bereichen verbindliche Beschlüsse zu treffen (Art. 65 Abs. 1 lit. a bis c DSGVO, sog. Streitbeilegung). Zu einer unmittelbaren Beschlussfassung kommt es in drei Fällen, nämlich wenn:

- die federführende Aufsichtsbehörde im Zusammenarbeitsverfahren einem maßgeblichen und begründeten Einspruch nicht folgt oder sie einen maßgeblichen und begründeten Einspruch verwirft (lit. a),
- es Streit über die Zuständigkeit als federführende Aufsichtsbehörde gibt (lit. b) oder
- eine zuständige Aufsichtsbehörde in Fällen des Art. 64 Abs. 1 DSGVO keine Stellungnahme eingeholt hat oder einer Stellungnahme nach Art. 64 Abs. 1 und 2 nicht folgt (lit. c).

In bestimmten, für das Vollzugskonzept der DSGVO strukturell bedeutsamen Fällen ist der Streitbeilegung ein Stellungnahme-Verfahren vorangestellt (Art. 64 Abs. 1 DSGVO). Dies ist dann der Fall, wenn im Interesse eines unionsweit einheitlichen Datenschutzniveaus nach dem Willen des Verordnungsgebers eine kohärente Tätigkeit der nationalen Aufsichtsbehörden notwendig ist, ohne dass hierüber bereits Meinungsverschiedenheiten zwischen einzelnen Aufsichtsbehörden bestehen. Die Fälle benennt die DSGVO in Art. 64 Abs. 1, namentlich Anwendungsregeln für die Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 4, Kompatibilitäts-Tests für unionsweite Verhaltensregeln (Art. 40 Abs. 7), die Akkreditierung nach Art. 41 Abs. 3 bzw. 43 Abs. 3, die Festlegung von Standard-Datenschutzklauseln gemäß Art. 46 Abs. 2 lit. d und Art. 28 Abs. 8, die Genehmigung von Vertragsklauseln gemäß Art. 46 Abs. 3 lit. a sowie die Annahme verbindlicher interner Vorschriften im Sinne des Art. 47 DSGVO. Daneben greift das Stellungnahme-Verfahren auch dann ein, wenn eine Aufsichtsbehörde, der Vorsitz des EDA oder die Kommission beantragen, dass der EDA eine Angelegenheit mit allgemeiner Geltung oder mit Auswirkungen in mehr als einem Mitgliedstaat vom Ausschuss prüfen möge (Art. 64 Abs. 2 DSGVO). Eine umfassende, lückenlose vertikale Koordination der Datenschutzaufsicht ist dadurch gewährleistet.

Die Stellungnahme, die der EDA abgibt, ist nicht verbindlich (vgl. Art. 288 Abs. 5 AEUV). Will die Aufsichtsbehörde, welche die Stellungnahme eingeholt hat, von ihr jedoch insgesamt oder teilweise abweichen, ergeht ein Beschluss des EDA (Art. 65 Abs. 1 lit. c S. 1 Alt. 2 DSGVO). Gleiches gilt, wenn eine zuständige Aufsichtsbehörde es unter Verstoß gegen Art. 64 Abs. 1 unterlässt, eine Stellungnahme des Ausschusses einzuholen.



© Martini/Weinzierl

b. Regelungsaufträge und regelungsbedürftige Rechtsbeziehungen

aa) Regelungsaufträge - Einrichtung der Aufsichtsbehörden

Die Datenschutz-Grundverordnung konfrontiert das bisherige Aufsichtsregime mit einer Vielzahl von Regelungsaufträgen: Die nationalen Gesetzgeber müssen (eine oder mehrere) unabhängige Datenschutzaufsichtsbehörde(n) schaffen (Art. 51 Abs. 1 und 3 [ex Art. 46 Abs. 1 und 2] DSGVO) und die Vorgaben der Datenschutz-Grundverordnung hinsichtlich der Ausstattung und Charakteristik der Aufsichtsbehörde(n) national umsetzen (Art. 52 Abs. 4 bis 6, Art. 53, Art. 54, Art. 58 Abs. 4 und 5 [ex Art. 47 Abs. 5 bis 7, Art. 48, Art. 49, Art. 53 Abs. 2 und 3] DSGVO). Im Zusammenhang mit dem Kohärenzverfahren ergeben sich weitere Regelungsaufträge, insbesondere die nach

EG 119 (ex EG 93) DSGVO erforderliche Benennung eines einheitlichen Ansprechpartners (sog. zentrale Anlaufstelle) – ferner die Gestaltung der Aufsicht über die Sonderbereiche Rundfunkanstalten und Kirchen. Nicht zuletzt gestattet die Datenschutz-Grundverordnung den Mitgliedstaaten, ihre Datenschutzaufsichtsbehörden mit weiter gehenden als den in der Datenschutz-Grundverordnung vorgesehenen Kompetenzen auszustatten.

bb) Regelungsbedürftige Rechtsbeziehungen – Bereiche einheitlichen Auftretens aller Aufsichtsbehörden der Bundesrepublik nach außen

Im Falle mehrerer nationaler Aufsichtsbehörden besteht Bedarf nach einem einheitlichen Auftreten der deutschen Aufsichtsbehörden nach außen. Er ergibt sich insbesondere aus dem Ziel der effektiven Anwendung der Datenschutz-Grundverordnung. Die Mitgliedstaaten müssen festlegen, welche dieser Behörden den Mitgliedstaat im EDA vertritt (Art. 68 Abs. 4 [ex Art. 64 Abs. 3] DSGVO). Den Aspekt einheitlichen Auftretens betreffen das Auftreten *im* EDA, insbesondere im Kohärenzverfahren (i), das Auftreten *gegenüber dem* EDA (ii), das Auftreten gegenüber einzelnen nationalen Aufsichtsbehörden (iii) sowie gegenüber der Kommission (iv).

i. Auftreten im EDA

Der Bedarf nach einem nach außen hin einheitlichen Auftreten besteht hauptsächlich im EDA. Dies ergibt sich explizit einerseits aus Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO sowie andererseits aus Art. 68 Abs. 4 (ex Art. 64 Abs. 3) DSGVO.
Der EDA genießt eine besondere Rechtsstellung: Er ist eine eigene Einrichtung der Union mit eigener Rechtspersönlichkeit (Art. 68 Abs. 1 [ex Art. 64 Abs. 1a] DSGVO). Er vollzieht – abweichend von dem Grundsatz der Verfahrensautonomie der Mitgliedstaaten, insbesondere dem Vollzug von Unionsrecht durch die Nationalstaaten – selbst und unmittelbar das Unionsrecht durch ein eigenes Organ. Die deutschen Behörden, die an den Handlungen des EDA beteiligt sind, wirken daran als Vollzugseinrichtung der Union mit.
Hinsichtlich des Wirkens des nationalen Vertreters im EDA ist zu unterscheiden zwischen der Wahrnehmung von allgemeinen Aufgaben des Ausschusses und Aufgaben, welche das sog. Kohärenzverfahren betreffen.

(1) Allgemeine Aufgaben, Art. 70 Abs. 1 (ex 66 Abs. 1) mit Ausnahme von lit. a und lit. t (ex lit. aa und lit. d)

Allgemeine Aufgaben des Ausschusses sind solche, die nicht unmittelbar aus dem Kohärenzverfahren folgen (vgl. hierzu Art. 70 Abs. 1 [ex 66 Abs. 1] mit Ausnahme von lit. a und t [ex lit. aa und d] DSGVO). Für diese Fälle sieht Art. 68 Abs. 4 (ex Art. 64 Abs. 3) (sowie Art. 51 Abs. 3 [ex Art. 46 Abs. 2]) DSGVO vor, dass der Mitgliedstaat einen gemeinsamen Vertreter aller nationalen Aufsichtsbehörden zu bestimmen hat. Dieser wird dann im Kollegialorgan EDA als Vertreter aller Aufsichtsbehörden eines Mitgliedstaates tätig.

(2) Im Rahmen des Kohärenzverfahrens (Art. 63 - 66 [ex Art. 57 - 61])

Anders als hinsichtlich der allgemeinen Aufgaben liegt es prima vista bei der Beteiligung im EDA, soweit Aufgaben im Rahmen des Kohärenzverfahrens betroffen sind (Art. 64 Abs. 3, Art. 65 Abs. 1 i. V. m. Art. 70 Abs. 1 lit. a, lit. t [Art. 58 Abs. 3, Art. 58a Abs. 1 i. V. m. Art. 66 Abs. 1 lit. aa, lit. d] DSGVO). Hier scheint EG 119 (ex EG 93) DSGVO eine andere Form der Repräsentation, nämlich die einer zentralen Anlaufstelle, vorzusehen.[133]
Eine derartige Lesart überzeugt jedoch nicht. Auch im Kohärenzverfahren wird der EDA als Kollegialorgan unter Beteiligung der nationalen Aufsichtsbehörden tätig. Entsprechend ist immer, wenn das Handeln im EDA betroffen ist, die Vertretungsregelung des Art. 68 Abs. 4 (ex Art. 64 Abs. 3) DSGVO einschlägig. Denn es besteht in beiden Fällen kein qualitativer Unterschied zwischen dem Handeln des EDA. Stets geht es um eine einheitliche Willensbildung zwischen den Mitgliedstaaten bzw. deren Aufsichtsbehörden (wobei grundsätzlich mit einfacher Mehrheit entschieden wird; vgl. Art. 72 Abs. 1 [ex Art. 68 Abs. 1] DSGVO). Die getroffene Vertretungsregelung nach Art. 68 Abs. 4 (ex Art. 64 Abs. 3) DSGVO umfasst also alle Vertretungen bei Handlungen im EDA als Kollegialorgan (bzw. sollte diese durch einfachgesetzliche Klarstellung erfassen).

[133] EG 119 S. 2 (ex 93 S. 2) sieht vor, dass der Mitgliedstaat eine Aufsichtsbehörde bestimmen soll, „die als zentrale Anlaufstelle für eine wirksame Beteiligung dieser Behörden an dem [Kohärenzverfahren] fungiert und eine rasche und reibungslose Zusammenarbeit mit […] dem Ausschuss […] gewährleistet".

ii. Auftreten gegenüber dem EDA bzw. Auftreten des EDA gegenüber einzelnen Aufsichtsbehörden – zentrale Anlaufstelle

In Fällen, in denen nicht die Einspeisung und die Bündelung des Willens mehrerer nationaler Aufsichtsbehörden im EDA betroffen ist, sondern lediglich eine nationale Aufsichtsbehörde von außen an den EDA herantritt und vice versa, liegen die Dinge anders als in der EDA-internen Kommunikation. Dies ist insbesondere – aber nicht nur – im Kohärenzverfahren der Fall, wenn eine nationale Aufsichtsbehörde dem EDA Informationen zuleiten muss oder soll (so z. B. nach Art. 60 Abs. 7 S. 1, 64 Abs. 1 S. 2, Abs. 2, Abs. 4, Abs. 7, Abs. 8, Art. 65 Abs. 1 lit. b, lit. c, Art. 66 Abs. 1 S. 2, Abs. 3 [ex Art. 54a Abs. 4a S. 1, Art. 58 Abs. 1 S. 2, Abs. 2, Abs. 5, Abs. 8, Abs. 9, Art. 58a Abs. 1 lit. b, lit. d, Art. 61 Abs. 1 S. 2, Abs. 3] DSGVO) bzw. wenn vice versa der EDA Informationen einzelnen, innerstaatlich zuständigen Aufsichtsbehörden zuleiten will oder muss (so z. B. nach Art. 64 Abs. 5 lit. b, Art. 65 Abs. 5 S. 1 [ex Art. 58 Abs. 6 lit. b, Art. 58a Abs. 6 S. 1] DSGVO).
Hierfür ist die in EG 119 (ex EG 93) DSGVO beschriebene *zentrale Anlaufstelle* vorgesehen. Diese soll es dem EDA ermöglichen, ohne Kenntnis der innerstaatlichen Zuständigkeitsverteilung effektiv an einen Mitgliedstaat bzw. dessen Aufsichtsbehörden herantreten zu können. Alleine die jeweilige nationale zentrale Anlaufstelle muss sich dann mit der innerstaatlichen Zuständigkeitsordnung befassen. Diese Aufgabenverteilung dient nicht nur der effektiven Anwendung der Datenschutz-Grundverordnung, sondern ist auch der – aus dem Gedanken der souveränen Gleichheit der Mitgliedstaaten fließenden – völkerrechtlichen Einheitlichkeit des Staates nach außen geschuldet.
Die zentrale Anlaufstelle darf entsprechend den Vorgaben der Datenschutz-Grundverordnung nicht organisatorisch von den Aufsichtsbehörden abgekoppelt und verselbstständigt werden. Stattdessen muss eine Aufsichtsbehörde die Aufgaben der zentralen Anlaufstelle übernehmen und damit als solche fungieren. Die Bundesrepublik kann grundsätzlich entweder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) oder eine Aufsichtsbehörde der Bundesländer zur zentralen Anlaufstelle erheben.
Der gemeinsame Vertreter im EDA muss nicht zwingend mit der zentralen Anlaufstelle personenidentisch sein; dies ist zwar eine zulässige, jedoch keinesfalls eine zwingende Regelungsoption. Für den effektiven Kontakt zwi-

schen dem EDA und den mitgliedstaatlichen Aufsichtsbehörden ist dies auch nicht erforderlich. Eine besondere Effektivitätssteigerung geht mit einer derartigen Personenidentität angesichts der unterschiedlichen Aufgaben nicht einher.

Ob die zentrale Anlaufstelle stets zur Kommunikation zwischen dem EDA und einzelnen Aufsichtsbehörden einzuschalten ist oder ob auch ein direkter Informationsfluss zwischen beiden zulässig ist, ist unklar. EG 119 (ex EG 93) DSGVO beantwortet diese Frage nicht. Gleichwohl folgt aus dem Ziel der Effektivitätssteigerung und dem Grundsatz der Einheitlichkeit des Staates nur, dass sich die einzelnen Aufsichtsbehörden ein Handeln ihrer zentralen Anlaufstelle zurechnen lassen müssen. Damit ist diese zwar stets möglicher Transmitter, nicht jedoch zwingende Zwischenstelle jeglicher Kommunikation. Vielmehr legt der Gedanke der Effektivität nahe, dass jedenfalls jede Aufsichtsbehörde das Recht hat, sich unmittelbar an den EDA zu wenden.[134] Umgekehrt muss sich der EDA nicht an die zentrale Anlaufstelle wenden, kann es aber jederzeit und ohne Begründung tun.

Im Interesse einer effektiven Koordinierung und Aufgabenwahrnehmung kann es sinnvoll sein, den Sitz der zentralen Anlaufstelle in Brüssel, mithin am Sitz der Kommission und im Zweifel auch des EDA, anzusiedeln. Völlig unsensibel ist das rechtlich nicht. Denn mit der Tätigkeit der Anlaufstelle kann, je nach der Ausgestaltung ihrer Befugnisse, auch hoheitliches Tätigwerden verbunden sein. Soll dieses in und von einem anderen Staat aus vorgenommen werden, kann dies (neben politischen) völkerrechtliche Implikationen hervorrufen: Nach dem Grundsatz der Gebietshoheit (bzw. Gebietsausschließlichkeit, und der damit im Zusammenhang stehenden territorialen Souveränität) darf ein Staat Hoheitsakte grundsätzlich nur auf seinem eigenen

[134] In diese Richtung deutet auf den ersten Blick auch der Wortlaut von Art. 64 (ex Art. 58) DSGVO. Dieser verwendet Formulierungen wie „übermittelt die zuständige Aufsichtsbehörde“, „Jede Aufsichtsbehörde“, „die betroffene Aufsichtsbehörde“. Er meint damit aber – entsprechend der Vorstellungswelt der Datenschutz-Grundverordnung „ein Land, eine Aufsichtsbehörde“ – nicht die nach innerstaatlichem Recht zuständige oder jede nach innerstaatlichem Recht eingesetzte Aufsichtsbehörde, sondern die Gesamtheit der mitgliedstaatlichen Aufsichtsbehörden, vgl. hierzu unten S. 212.

Territorium vornehmen.[135] Dass dieses Verbot solche Hoheitsakte nicht umfasst, die zwar im Ausland gesetzt werden, ihre Wirkung aber alleine im Inland entfalten, wird nur teilweise vertreten.[136] Ausnahmen vom Grundsatz der Gebietshoheit lassen sich insbesondere durch völkerrechtliche Verträge begründen (so z. B. geschehen im Rahmen des Wiener Übereinkommens über diplomatische Beziehungen oder in Sitzstaatsabkommen mit internationalen Organisationen). Abhängig von der Ausgestaltung der Befugnisse der zentralen Anlaufstelle kann also eine Zustimmung des Sitzstaates für die Ausübung ihrer Tätigkeit erforderlich werden. Es empfiehlt sich insoweit jedenfalls, vorherige Konsultationen mit dem potenziellen Sitzstaat aufzunehmen.

iii. Auftreten gegenüber anderen nationalen Aufsichtsbehörden im Bereich der Zusammenarbeit (Art. 60 ff. [ex Art. 54a ff.])

Regelungsbedarf besteht nicht nur für das Verhältnis zwischen den nationalstaatlichen Aufsichtsbehörden und dem EDA, sondern auch für das Verhältnis zwischen nationalen Aufsichtsbehörden und den Aufsichtsbehörden anderer Mitgliedstaaten im Verfahren der Zusammenarbeit (Art. 60 ff. [ex Art. 54a ff.] DSGVO). Für solche Mitgliedstaaten, die mehrere Aufsichtsbehörden kennen, enthält die Datenschutz-Grundverordnung auf den ersten Blick keine Regelung des Auftretens nach außen. Art. 68 Abs. 4 (ex Art. 64 Abs. 3) DSGVO ist nur auf ein Handeln im EDA anwendbar; EG 119 (ex EG 93) DSGVO bezieht sich seinem Wortlaut nach nur auf das Kohärenzverfahren (nach Art. 63 ff. DSGVO), nicht aber auf die Zusammenarbeit nach Art. 60 ff. (ex Art. 54a ff.) DSGVO.
Gleichwohl ist der Gedanke der zentralen Anlaufstelle auch für die Fälle der Zusammenarbeit, mithin den Kontakt zwischen Aufsichtsbehörden verschiedener Mitgliedstaaten auf horizontaler Ebene, anzuwenden. Insoweit spricht EG 119 S. 2 (ex EG 93 S. 2) DSGVO auch davon, dass die zentrale Anlaufstelle dazu dient, eine rasche und reibungslose Zusammenarbeit mit anderen Aufsichtsbehörden – also im horizontalen Verhältnis – zu gewährleisten.

---

[135] *Breuer*, Auslandswirkung von Hoheitsakten, in: Schöbener (Hrsg.), Völkerrecht, 2014, S. 34 f.; *Hobe*, Einführung in das Völkerrecht, 10. Aufl., 2014, S. 96; PCIJ, Lotus Case (France v. Turkey), Entsch. v. 07.09.1927, PCIJ Series A, No. 10 (1927).
[136] *Breuer* (Fn. 135), S. 35.

Insbesondere in diesem horizontalen Verhältnis kommt der zentralen Anlaufstelle auch eine herausragende Bedeutung zu. Denn es kann den Aufsichtsbehörden der anderen Mitgliedstaaten ungleich weniger als dem EDA zugemutet werden, die jeweiligen innerstaatlichen Kompetenzregelungen eines anderen Mitgliedstaates zu kennen. Aufsichtsbehörden der anderen Mitgliedstaaten sind für eine effektive Zusammenarbeit auf einen schnellen und reibungslosen Kontakt über eine als Scharnier fungierende zentrale Anlaufstelle angewiesen.
Dabei gilt auch hier, dass die zentrale Anlaufstelle jedenfalls aus unionaler Perspektive in den Kontakt einbezogen werden kann, dies aber nicht sein muss.

iv. Auftreten gegenüber der Kommission

Neben dem Verhältnis zu dem EDA bedarf womöglich auch das Rechtsverhältnis zwischen (nationaler) Aufsichtsbehörde und der Kommission einer Regelung. Hierauf deutet der Umstand hin, dass die Aufsichtsbehörden im Rahmen des Zusammenarbeits- und des Kohärenzverfahrens aufgerufen sind, ggf. auch mit der Kommission zusammenzuarbeiten (Art. 51 Abs. 2, Art. 63 [ex Art. 46 Abs. 1a, Art. 57 Abs. 1] DSGVO). Auch ist es nach EG 119 S. 2 (ex EG 93 S. 2) DSGVO Aufgabe der zentralen Anlaufstelle, eine rasche und reibungslose Zusammenarbeit mit der Kommission zu gewährleisten. In die gleiche Richtung weist EG 123 S. 2 (ex EG 96 S. 2) DSGVO: Danach arbeiten die Aufsichtsbehörden sowohl untereinander als auch mit der Kommission zusammen, um die Bestimmungen der Datenschutz-Grundverordnung zu überwachen und zu ihrer einheitlichen Anwendung beizutragen.
Gleichwohl kommt der Kommission im Zusammenarbeits- und Kohärenzverfahren keine entscheidende Bedeutung zu. Die Kommission tritt den nationalen Aufsichtsbehörden nie unmittelbar gegenüber bzw. arbeitet nie mit diesen unmittelbar zusammen. So nimmt die Kommission gemäß Art. 68 Abs. 5 (ex Art. 64 Abs. 4) DSGVO ohne Stimmrecht an den Tätigkeiten und Sitzungen des EDA teil (ebenso EG 139 S. 6 [ex EG 110 S. 6] DSGVO); ihr wird lediglich eine beratende Funktion zuteil. Aus Art. 64 Abs. 2 (ex Art. 58 Abs. 2) DSGVO (Antragsrecht) und Art. 70 Abs. 1 S. 2 (ex Art. 66 Abs. 1 S. 2) DSGVO (Ersuchen der Kommission) ergibt sich nichts anderes. Beide Vor-

schriften beziehen sich auf das Verhältnis zwischen Kommission und EDA, nicht aber auf das zwischen Aufsichtsbehörde und Kommission.
Die Formulierungen des Art. 51 Abs. 2, Art. 63 (ex Art. 46 Abs. 1a, Art. 57 Abs. 1) DSGVO und EG 119 und 123 (ex EG 93 und 96) DSGVO sind wohl noch der Entwurfsfassung der Europäischen Kommission vom 25.1.2012 (KOM(2012), 11 endgültig) geschuldet. Dieser sah in Art. 59 f. DSGVO-E – kaum überraschend – weitergehende Befugnisse der Kommission, insbesondere zur Stellungnahme und zur Aussetzung einer geplanten Maßnahme, vor. In das Ergebnis des Trilogs haben diese Vorschriften jedoch nicht Eingang gefunden.
Da die nationalen Aufsichtsbehörden nicht unmittelbar gegenüber der Kommission auftreten, bedarf es einer entsprechenden Regelung somit nicht.

v. Zwischenfazit

In allen skizzierten Konstellationen stellt sich die Frage nach einer föderalen Abstimmung und einem einheitlichen Auftreten der deutschen Aufsichtsbehörden nach außen. Der Mitgliedstaat muss auf beide Problemlagen eine Antwort finden. Er muss insbesondere durch eigene Regelungen die Bestimmung des Vertreters und einer zentralen Anlaufstelle, die inhaltliche Entscheidungskoordination und die Bindung des Vertreters an den ermittelten aufsichtsbehördlichen Willen in seiner Regelung adressieren.

cc) Regelungsbedürftige Rechtsbeziehungen – Binnenkoordinierung der nationalen Aufsichtsbehörden

Errichtet ein Mitgliedstaat mehrere nationale Aufsichtsbehörden, besteht neben der unmittelbar durch die Datenschutz-Grundverordnung vorgegebenen Aufgabe der Regelung des Auftretens nach außen der Bedarf nach einer Binnenkoordinierung der nationalen Aufsichtsbehörden. Zu regeln ist die innerstaatliche Vorabstimmung der Aufsichtsbehörden sowohl im Rahmen des Zusammenarbeitsverfahrens (also der Außenbeziehung vermittels einer zentralen Anlaufstelle) als auch des Kohärenzverfahrens (also insbes. hinsichtlich der Tätigkeit des gemeinsamen Vertreters im EDA). Dabei sind Regeln zu finden unter anderem in Bezug auf die Beteiligung, die Abstimmung und die

Bindung an und von Entscheidungen sowie den Grad und die Form der etwaigen Institutionalisierung der Koordination.

b. Regelungsansatz einer zukünftigen Regelung der Datenschutzaufsicht im nationalen Recht

EG 8 (ex EG 6a) DSGVO eröffnet den Mitgliedstaaten in Übereinstimmung mit der Rechtsprechung des EuGH[137] ausdrücklich die Möglichkeit, – trotz der unmittelbaren Wirkung der Verordnung (Art. 288 Abs. 2 AEUV) – die Regelungen der Datenschutz-Grundverordnung unter gewissen Bedingungen zu wiederholen.[138]

aa) Nationale Regelung und echte Normwiederholungen

Gerade für den Bereich der Datenschutzaufsicht ist es erwägenswert, von Normwiederholungen Gebrauch zu machen, um das Regelungssystem der Aufsichtsbehörden durch das nationale Recht verständlich und konsistent zu kodifizieren. Andernfalls erschließen sich die Aufsichtsstrukturen in ihrer Gesamtheit nur durch ein Nebeneinander von Datenschutz-Grundverordnung und nationalem Datenschutzgesetz, was gerade für den Rechtsanwender eine undurchsichtige Gesetzeslage erzeugt. Eine weitere Stütze findet dieses Ergebnis in EG 121 (ex EG 95) DSGVO, der entsprechende mitgliedstaatliche Regelungen impliziert.
Normwiederholungen sind insbesondere sub specie der Anforderungen an die Mitglieder der Aufsichtsbehörde (Art. 53 DSGVO) und die Aufgaben und Befugnisse der Aufsichtsbehörden (Art. 57, 58 DSGVO) denkbar. Die Zulässigkeit einer Normwiederholung ändert nichts daran, dass die Normierungs- und verbindliche Auslegungsbefugnis alleine auf europäischer Ebene liegt. Der Schein geschaffener Normklarheit kann insofern trügen. Von der Möglichkeit zur Normwiederholung sollte zurückhaltend Gebrauch gemacht werden.

---

[137] Vgl. EuGH, Rs. 272/83, Kommission/Italien, Slg. 1985, 1057 Rn. 27; erforderlich ist dann jedoch ein Hinweis auf den unionsrechtlichen Ursprung der betroffenen nationalen Regelungen.
[138] Ausführlicher hierzu oben auf S. 6 f.

bb) Nationale Regelung und scheinbare Normwiederholungen

Von der Frage nach der Zulässigkeit einer Normwiederholung abzuschichten sind solche Fälle, in denen die Regelungen der Datenschutz-Grundverordnung nur scheinbar alle innerstaatlichen Fälle regeln, tatsächlich aber eine eigene Regelung im mitgliedstaatlichen Recht notwendig ist. Dies ist zum Beispiel der Fall bei den Zuständigkeitsregelungen nach Art. 55 und 56 DSGVO. Hier regelt die Datenschutz-Grundverordnung bei Staaten, die mehrere nationale Aufsichtsbehörden vorsehen nur die Zuständigkeit der Aufsichtsbehörden eines Mitgliedstaates an sich. Dieser selbst muss hingegen Regelungen schaffen, nach denen die so bestehende Zuständigkeit innerstaatlich distribuiert wird (s. unten S. 212). Tut er dies, liegt also bereits kein Fall der Normwiederholung vor – auch dann nicht, wenn der Mitgliedstaat die Regelungen der Datenschutz-Grundverordnung übernimmt, um sein innerstaatliches Zuständigkeitssystem auszugestalten. Gleiches gilt für die Fragen der Zusammenarbeit und Abstimmung mehrerer nationaler Aufsichtsbehörden untereinander mangels Anwendbarkeit der Art. 60-62 DSGVO für eine innerstaatliche (Vor-)Koordination.

c. Die personelle Gestalt der Aufsichtsbehörde

Die Datenschutz-Grundverordnung unterscheidet mit Blick auf die für die Aufsichtsbehörde tätigen Personen zwischen den Mitgliedern der Aufsichtsbehörden (aa) und den Bediensteten (bb; vgl. Art. 54 Abs. 1 lit. f, Abs. 2, Art. 62 Abs. 1 [ex Art. 49 Abs. 1 lit. f, Abs. 2, Art. 56 Abs. 1] DSGVO). Für beide Personengruppen hält sie jeweils spezifische Regelungen bereit[139]. Außerdem rekurriert die Datenschutz-Grundverordnung in EG 120 (ex EG 94), EG 121 S. 3 (ex EG 95 S. 3) sowie Art. 52 Abs. 5 (ex Art. 47 Abs. 6) DSGVO auf das „Personal“. Dieser Terminus dürfte jedoch synonym zu den „Bediensteten“ zu verstehen sein, da die englische Textfassung nicht zwischen den beiden Begriffen differenziert, sondern stets den Ausdruck „staff“ verwendet.

[139] Z. B. Art. 52 Abs. 2 und 3, Art. 53 (ex Art. 47 Abs. 2 und 3, Art. 48) DSGVO einerseits, Art. 62 Abs. 4 und 5 (ex Art. 56 Abs. 3a und 3b) DSGVO andererseits.

aa) Mitglieder der Aufsichtsbehörden

Die „Mitglieder der Aufsichtsbehörden“ zeichnen sich durch ihre Leitungsfunktion aus. Ihnen kommt eine exponierte Stellung zu. Deshalb sieht die Datenschutz-Grundverordnung für die Mitglieder auch wesentlich ausführlichere und striktere Regelungen vor als für die Bediensteten.

bb) Bedienstete (und „Personal“)

Die Bediensteten sind den Mitgliedern der Aufsichtsbehörden unterstellt (vgl. den EG 121 S. 3 [ex EG 95 S. 3] DSGVO). Ihnen kommt für die Aufgabenwahrnehmung der Aufsichtsbehörde eine wichtige Funktion zu. Dies verdeutlicht der Umstand, dass die Datenschutz-Grundverordnung auch die Amtsausübung der Bediensteten betreffenden Regelungen unterwirft (vgl. Art. 54 Abs. 1 lit. f [ex Art. 49 Abs. 1 lit. f] DSGVO) und sie zur Verschwiegenheit verpflichtet (Art. 54 Abs. 2 [ex Art. 49 Abs. 2] DSGVO). Mithin nehmen die Bediensteten keine allein randständigen Aufgaben wahr, sondern sind kraft ihrer Einbindung in Aufsichtsfunktionen ein sensibler Baustein der inhaltlichen Arbeit der Aufsichtsbehörde. Anderenfalls wäre das in der Datenschutz-Grundverordnung enthaltene differenzierte Regelungsregime auch nicht nötig. „Bediensteter“ im Sinne der Datenschutz-Grundverordnung sind also nicht der Pförtner oder andere nicht in die Wahrnehmung von Aufsichtsaufgaben eingebundener Beschäftigte.

26. Art. 51 (ex Art. 46): Aufsichtsbehörde

a. Inhalt der Öffnungsklausel

Art. 51 (ex Art. 46) DSGVO leitet das Kapitel über die unabhängigen Aufsichtsbehörden ein. Der Regelungsgehalt der Vorschrift erschließt sich aber nur in ihrem Regelungskontext, korrespondiert sie doch mit den umliegenden Vorschriften des sechsten Kapitels (insbesondere den Art. 54 und 52 [ex Art. 49 und 47] DSGVO).

aa) Art. 51 Abs. 1 (ex Art. 46 Abs. 1)

Art. 51 Abs. 1 (ex Art. 46 Abs. 1) DSGVO verpflichtet die Mitgliedstaaten, eine (oder mehrere) unabhängige Aufsichtsbehörde(n) für die Überwachung der Einhaltung der Datenschutz-Grundverordnung vorzusehen. Für den Mitgliedstaat bedeutet dies zunächst, dass er entsprechende Zuständigkeitsvorschriften vorsehen muss.

In engem Zusammenhang mit Art. 51 Abs. 1 (ex Art. 46 Abs. 1) DSGVO verlangt Art. 54 Abs. 1 lit. a (ex Art. 49 Abs. 1 lit. a) DSGVO, dass die Mitgliedstaaten die unabhängige(n) Aufsichtsbehörde(n) „durch Rechtsvorschriften" errichten müssen. Damit hebt die Datenschutz-Grundverordnung nicht notwendig auf ein Gesetz im formellen Sinne ab, sodass es grundsätzlich keines Parlamentsgesetzes bedarf, wie EG 41 (ex EG 31a) DSGVO klarstellt. Jedoch ergibt sich das Erfordernis einer formell-gesetzlichen Regelung nationalstaatlich aus dem Parlamentsvorbehalt: Wer für die Wahrnehmung der Aufgabe des Grundrechtsschutzes der informationellen Selbstbestimmung zuständig ist, berührt die Grundrechte Betroffener.

Ist dem Mitgliedstaat aufgrund der Ermächtigung des Art. 51 Abs. 1 (ex Art. 46 Abs. 1) DSGVO auch die Errichtung *mehrerer* unabhängiger Aufsichtsbehörden möglich,[140] schließt das nicht nur eine Aufspaltung der Zuständigkeit nach örtlichen, sondern auch nach sachlichen Gesichtspunkten ein. Gangbar ist unter föderalen Gesichtspunkten also eine Verteilung der Aufsicht auf unterschiedliche Behörden anhand thematischer Aspekte (Aufsicht über öffentliche und nicht-öffentliche Akteure) und nach örtlichen Gliederungen.[141]

Die Vorgängervorschrift zu Art. 51 Abs. 1 (ex Art. 46 Abs. 1) DSGVO findet sich in Art. 28 Abs. 1 S. 1 DSRL. Auch hiernach sollen eine oder mehrere öffentliche Stellen als Kontrollstelle(n) fungieren, um zu überwachen, ob die zur Umsetzung der Datenschutzrichtlinie erlassenen Vorschriften befolgt werden.

---

[140] Zur Begründung siehe EG 117 (ex 92): „Die Mitgliedstaaten sollten mehr als eine Aufsichtsbehörde errichten können, wenn dies ihrer verfassungsmäßigen, organisatorischen und administrativen Struktur entspricht.".

[141] *von Lewinski*, DuD 2012, 564 (566 f.).

Wie bereits unter dem Regime der Datenschutzrichtlinie es ist der Bundesrepublik Deutschland daher möglich, ihr gegenwärtig praktiziertes, sich aus dem föderalen Gedanken ergebendes Modell mehrerer, nach örtlicher und sachlicher Zuständigkeit gegliederter Aufsichtsbehörden beizubehalten. Allerdings hat sie dann – damit einhergehend – auch die Vorgaben des Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO zu beachten.

i. Begriff der Aufsichtsbehörde im Sinne der Datenschutz-Grundverordnung – öffentlicher und nicht-öffentlicher Bereich

Den Begriff der „Aufsichtsbehörde" im Sinne der Datenschutz-Grundverordnung definiert Art. 4 Nr. 21 (ex Art. 4 Abs. 19) als „eine von einem Mitgliedstaat gemäß Artikel 51 (ex Art. 46) eingerichtete unabhängige staatliche Stelle".[142] Die „Aufsichtsbehörde" ist nicht, wie im nationalen Recht bisher üblich, nur für die Aufsicht über den nicht-öffentlichen Bereich zuständig. Stattdessen versteht die Datenschutz-Grundverordnung den Begriff synonym zu dem der „Kontrollstelle" in Art. 28 der Datenschutzrichtlinie. Die Datenschutz-Grundverordnung verfolgt damit, wie auch die Datenschutzrichtlinie, ein einheitliches Konzept der Aufsicht; Aufsichtsbehörde meint dementsprechend die Aufsicht über die Verarbeitung *im öffentlichen und nicht-öffentlichen Bereich*. Dies ergibt sich mittelbar auch aus Art. 55 Abs. 2 (ex Art. 51 Abs. 2) DSGVO. Diese Vorschrift bezeichnet die Behörden, welche Verarbeitungstätigkeiten kontrollieren, die auf Öffnungsklauseln für den öffentlichen Bereich zurückgehen, ausdrücklich als „Aufsichtsbehörden". Aufsichtsbehörden im Sinne der Datenschutz-Grundverordnung sind – gemessen am gegenwärtig in der Bundesrepublik etablierten Aufsichtssystem – somit sowohl die BfDI, die von den Ländern nach § 38 BDSG eingerichteten Aufsichtsbehörden als auch die nach Landesrecht mit der Aufsicht über den öffentlichen Bereich betrauten Stellen.[143]

[142] Siehe auch den Klammerzusatz in Art. 51 Abs. 1 DSGVO.
[143] Wobei inzwischen nur noch der Freistaat Bayern für die Aufsicht über den öffentlichen und den nicht-öffentlichen Bereich zwei verschiedene Stellen eingerichtet hat.

ii. Sonderregelungen für journalistische Einrichtungen

Die Datenschutz-Grundverordnung ist auch für Sonderregelungen im Bereich journalistischer Einrichtungen offen. So können die Mitgliedstaaten nach Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO (hierzu EG 153 [ex EG 121] DSGVO) von den Vorschriften über die unabhängige Aufsichtsbehörde abweichen, soweit dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen. Dies erlaubt grundsätzlich Sonderregelungen, wie sie heute etwa § 42 Abs. 1 BDSG für die Deutsche Welle vorsieht.

iii. Sonderregelungen für Religionsgemeinschaften

Ebenso wie für journalistische Einrichtungen erlaubt die Datenschutz-Grundverordnung auch Sonderregelungen für Kirchen und religiöse Vereinigungen oder Gemeinschaften. Für diese besteht unter gewissen Voraussetzungen die Möglichkeit, sie der Kontrolle durch eine spezifische unabhängige Aufsichtsbehörde zu unterwerfen (Art. 91 Abs. 2 i. V. m. Abs. 1 [ex Art. 85 Abs. 2 i. V. m. Abs. 1] DSGVO sowie EG 165 [ex EG 128] DSGVO). Dies ermöglicht grundsätzlich Sonderregelungen, wie sie heute etwa (auf Grundlage von Art. 137 Abs. 3 WRV i. V. m. Art. 140 GG) in §§ 18 ff. DSG-EKD vorgesehen sind. Danach bestellt die Evangelische Kirche in Deutschland, ihre Gliedkirchen und ihre gliedkirchlichen Zusammenschlüsse je für ihren Bereich Beauftragte für den Datenschutz. Die Vorschriften des BDSG finden auf sie jedenfalls im Bereich der kirchlichen Tätigkeit keine Anwendung.[144]

bb) Art. 51 Abs. 3 (ex Art. 46 Abs. 2)

Installiert der Mitgliedstaat mehrere unabhängige Aufsichtsbehörden, muss er gemäß Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO *eine* Aufsichtsbehörde bestimmen, die diese Behörden im EDA[145] vertritt (a.) und ein Verfahren implementieren, das die Einhaltung der Regeln für das Kohärenzverfahren

[144] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 2, Rn. 14a; vgl. zu dem Meinungsstand hierzu *Preuß*, ZD 2015, 217 (220 ff.).
[145] Der Europäische Datenschutzausschuss löst die Datenschutzgruppe ab, vgl. *Härting*, BB 2012, 459 (460 f.); EG 139 S. 4 (ex 110 S. 4) DSGVO.

nach Art. 63 (ex Art. 57) DSGVO durch die nationalen Aufsichtsbehörden sicherstellt (b.). Diese Regelungen zielen insbesondere auf eine reibungsfreie Abstimmung unter den nationalen Aufsichtsbehörden des jeweiligen Mitgliedstaates.[146] Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO enthält somit in zweifacher Hinsicht eine Öffnungsklausel. Wie Art. 51 Abs. 1 (ex Art. 46 Abs. 1) DSGVO legt sie den Mitgliedstaaten eine obligatorische Regelungsverpflichtung auf.

i. Vertretung beim Europäischen Datenschutzausschuss

Wenn ein Mitgliedstaat mehrere unabhängige Aufsichtsbehörden errichtet, muss er bestimmen, welche dieser Behörden die anderen im EDA vertritt. Art. 68 Abs. 4 (ex Art. 64 Abs. 3) DSGVO begründet insoweit eine mit der Verpflichtung des Art. 51 Abs. 3 Hs. 1 (ex Art. 46 Abs. 2 Hs. 1) DSGVO korrespondierende Regelung.
Die Vorschrift des Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO hat im Verlaufe der Gesetzgebungsgeschichte Wandlungen erfahren:

[146] *Kahler*, RDV 2013, 69 (72 f.) bemängelt, dass auf Basis der gegenwärtigen Rechtslage nur eine unzureichende Koordination zwischen den verschiedenen Datenschutzbeauftragten der Bundesländer bestehe.

DSGVO-KOM vom 25.01.2012, - KOM(2012) 11 endg. -	**DSGVO-EP vom 12.03.2014 - 7427/1/14 REV 1-**	**DSGVO-Rat vom 26.03.2015 - 7466/15 -**	**DSGVO-Trilog vom 15.12.2015 - 15039/15 ANNEX -**	**VO (EU) 2016/679 – DSGVO vom 27.04.2016**
Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority which **functions as a single contact point for the effective participation of** those authorities in the European Data Protection Board […].		Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority **which shall represent** those authorities in the European Data Protection Board […].	Where in a Member State more than one supervisory authority are established, that Member State shall designate the supervisory authority **which shall represent** those authorities in the European Data Protection Board […].	Where more than one supervisory authority is established in a Member State, that Member State shall designate the supervisory authority **which is to represent** those authorities in the Board […].

Vergleich des Art. 68 Abs. 4 (ex Art. 64 Abs. 3) DSGVO in der Gesetzgebungsgeschichte:

DSGVO-KOM vom 25.01.2012, - KOM(2012) 11 endg. -	**DSGVO-EP vom 12.03.2014 - 7427/1/14 REV 1-**	**DSGVO-Rat vom 26.03.2015 - 7466/15 -**	**DSGVO-Trilog vom 15.12.2015 - 15039/15 ANNEX -**	**VO (EU) 2016/679 – DSG-VO vom 27.04.2016**
Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, **they shall nominate the head of one of those supervisory authorities as joint representative.**		Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, (…) **a joint representative shall be appointed in accordance with the national law of that Member State.**	Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, **a joint representative shall be appointed in accordance with the national law of that Member State.**	Where in a Member State more than one supervisory authority is responsible for monitoring the application of the provisions pursuant to this Regulation, **that Member State shall designate the supervisory authority which is to represent those authorities in the Board and shall set out the mechanism to ensure compliance by the other authorities with the rules relating to the consistency mechanism referred to in Article 63**

(1) Inhaber des Bestimmungsrechts

Wem das Bestimmungsrecht darüber zukommt, welche der nationalen Aufsichtsbehörden diese im EDA vertritt, ist nicht ganz trivial. In Betracht kommen die Aufsichtsbehörden selbst oder der nationale Gesetzgeber.

Die Datenschutzrichtlinie überließ es gemäß Art. 29 RL 95/46/EG den Aufsichtsbehörden selbst, einen gemeinsamen Vertreter zu bestimmen, der die nationale Sichtweise in das Koordinierungsgremium einbringt:[147] Auf Basis des Art. 29 sowie EG 65 RL 95/46/EG besteht eine Datenschutzgruppe.[148] In dieses Gremium muss die Aufsichtsbehörde eines jeden Mitgliedstaates einen Vertreter abordnen (Art. 29 Abs. 2 RL 95/46/EG); für den Fall, dass er von der ihm eingeräumten Möglichkeit Gebrauch macht, mehrere Aufsichtsbehörden zu installieren, ordnet die Vorschrift die Entsendung eines gemeinsamen Vertreters an, den die Aufsichtsbehörden des jeweiligen Mitgliedstaates in gemeinschaftlichem Zusammenwirken „ernennen".

Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO gesteht diese Kreations-Kompetenz nunmehr – offener – explizit dem „Mitgliedstaat" zu. Die Norm scheint den Begriff des „Mitgliedstaats" in Abgrenzung zu dem der „Aufsichtsbehörde" zu gebrauchen. Die Bezugnahme der Wendung „dieser Mitgliedstaat" auf den Satzanfang unterstreicht das.

Gleichzeitig ist nicht eindeutig, dass mit dieser Abkehr des Wortlauts auch eine materielle Änderung der Rechtslage intendiert ist. Denn die Befugnis, den eigenen Vertreter zu bestimmen, stärkt die Unabhängigkeit der Aufsichtsbehörden, die der Datenschutz-Grundverordnung ein besonderes regulatorisches Anliegen ist.[149] Aufgrund der Ausweitung der Befugnisse des EDA – verglichen mit der beratenden Funktion der Datenschutzgruppe (vgl. Art. 29 Abs. 1 RL 95/46/EG) – erlangt dieser Aspekt umso größere Bedeutung. Entsprechend könnte man auch daran denken, dass insoweit abweichend vom

[147] Vgl. auch *Brühann*, in: Grabitz/Hilf (Hrsg.), EU-Recht, 57. Erg.-Lfg., 2015, Art. 29 Datenschutzrichtlinie, Rn. 6.

[148] Gemäß EG 139 S. 4 DSGVO wird sie auf Grundlage der Datenschutz-Grundverordnung durch den Europäischen Datenschutzausschuss ersetzt.

[149] *Brühann* (Fn. 147), Art. 29 Datenschutzrichtlinie, Rn. 6. Kritisch aber *Wolff*, Rechtsvorgaben für die Besetzung der Art. 29-Gruppe, 2015, S. 12 f.

Wortlaut des Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO die Aufsichtsbehörden selbst einen gemeinsamen Vertreter bestimmen.[150]

(α) Entstehungsgeschichte

Ein Blick auf die Entstehungsgeschichte der Datenschutz-Grundverordnung macht deutlich, dass die Änderung des Anknüpfungspunktes für das Bestimmungsrecht mit Bedacht erfolgte. Nur der Entwurf der Kommission und des Parlaments deutete in Art. 64 Abs. 3 DSGVO-E an, das Bestimmungsrecht den Aufsichtsbehörden vorbehalten zu wollen. Die inhaltlich ähnliche Vorschrift des Art. 46 Abs. 2 DSGVO-E übertrug dieses Recht demgegenüber von Anbeginn dem Mitgliedstaat. So war dann während der weiteren Beratungen stets vom Bestimmungsrecht des *Mitgliedstaats* die Rede. Auch die Erwägungsgründe enthalten keinen Hinweis darauf, dass das Bestimmungsrecht den Aufsichtsbehörden zustehen soll. Hätte der europäische Gesetzgeber das Bestimmungsrecht den Aufsichtsbehörden selbst zuweisen wollen, hätte er dies in der textlichen Fassung der Datenschutz-Grundverordnung unmissverständlich zum Ausdruck bringen müssen.[151] Zudem spricht die – verglichen mit der Datenschutzgruppe festzustellende – Befugnisausweitung des EDA auch umgekehrt dafür, das Bestimmungsrecht nicht länger den Aufsichtsbehörden zuzugestehen, sondern es den Mitgliedstaaten, genauer den mitgliedstaatlichen Parlamenten, zuzuweisen, da diese durch das Volk demokratisch herausgehoben legitimiert sind.

(ß) Zwischenergebnis

Auf Basis des insoweit eindeutigen Wortlauts von Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO kommt dem jeweiligen Mitgliedstaat, nicht den Aufsichts-

[150] Hierfür wohl *Die brandenburgische Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht*, in: Deutscher Bundestag, Ausschuss Digitale Agenda, Ausschussdrucksache 18(24)92, S. 5 f., 11.

[151] Zwar ist Art. 68 Abs. 4 (ex Art. 64 Abs. 3) DSGVO in sprachlicher Hinsicht offener, gleichwohl weist auch er das Bestimmungsrecht nicht eindeutig den nationalen Aufsichtsbehörden zu. Das eine klare Übertragung des Bestimmungsrechts an die Aufsichtsbehörden möglich ist, beweist nicht zuletzt die Regelung des Art. 29 RL 95/46/EG. Einen weiteren Kontrapunkt bildet etwa auch Art. 40 Abs. 5 EBA-VO.

behörden selbst das Recht zu, den Vertreter zu benennen.[152] Dies bedeutet hingegen nicht zwingend, dass der Mitgliedstaat die Vertretungsregelung nicht wiederum an die Aufsichtsbehörden weiterdelegieren könnte. Dies kann nämlich von seinem Bestimmungsrecht umfasst sein.[153]

(2) Regelungsform

Die Datenschutz-Grundverordnung lässt offen, in welcher Form der Mitgliedstaat die Vertretung im EDA regeln muss. Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO spricht lediglich von „bestimmen", Art. 68 Abs. 4 DSVGVO von der Benennung „im Einklang mit den Rechtsvorschriften dieses Mitgliedstaats". Auch nach EG 41 (ex EG 31a) DSGVO[154] trifft die DSGVO hierzu keine Vorgabe.

Auch der Parlamentsvorbehalt scheint eine formal-gesetzliche Regelung nicht zu erzwingen. Denn die Vertretungsregelung betrifft primär nur das Verhältnis der unabhängigen Aufsichtsbehörden untereinander; es handelt sich nicht um eine Zuständigkeitsregelung im engeren Sinne. Dritte und deren Rechte sind lediglich mittelbar betroffen.

Gleichwohl ist es angezeigt, die Vertretungsregelung nationalstaatlich in Form eines Parlamentsgesetzes zu verankern.[155] Eine formell-gesetzliche Regelung stärkt nicht zuletzt die aufsichtsbehördliche Unabhängigkeit. Würde die Exekutive die Vertretungsregelung festlegen, bestünde die Gefahr, dass sie in erheblichem Maße Einfluss auf die Aufsichtsbehörden ausüben könnte. Dies überschritte wohl die Grenzen des Art. 52 (ex Art. 47) DSGVO sowie diejenigen, die der EuGH gezogen hat[156].[157] Nicht zuletzt schafft eine parlamentsgesetzliche Vertretungsregelung größere Rechtssicherheit und -klarheit.

---

[152] So wohl auch *Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, in: Deutscher Bundestag, Ausschuss Digitale Agenda, Ausschussdrucksache 18(24)93, S. 8.
[153] Siehe unten S. 142.
[154] Vgl. S. 8.
[155] Im Ergebnis auch *Schaar*, PinG 2016, 62 (64).
[156] EuGH, MMR 2010, 352; ZD 2012, 563.
[157] Vgl. auch *Nguyen*, ZD 2015, 265 (266).

ii. Sicherstellung der Einhaltung der Regeln für das Kohärenzverfahren nach Art. 63 (ex Art. 57)

Der Mitgliedstaat, der mehrere unabhängige Aufsichtsbehörden installiert, muss mit Hilfe eines Verfahrens sicherstellen, dass die Aufsichtsbehörden die Regeln für das Kohärenzverfahren nach Art. 63 (ex Art. 57) DSGVO einhalten. Nähere Vorgaben, wie dieses Verfahren ausgestaltet sein muss, enthält die Datenschutz-Grundverordnung nicht. Dem Mitgliedstaat kommt mithin ein Handlungsspielraum zu. Einzig das Ziel, die Sicherstellung der Einhaltung der Regeln für das Kohärenzverfahren nach Art. 63 (ex Art. 57) DSGVO durch die Behörden, ist dem Mitgliedstaat vorgegeben. In Übereinstimmung mit EG 119 (ex EG 93) DSGVO muss dieses Verfahren durch Rechtsvorschrift festgelegt werden. [158]

cc) Art. 51 Abs. 4 (ex Art. 46 Abs. 3)

Art. 51 Abs. 4 (ex Art. 46 Abs. 3) DSGVO enthält keine Öffnungsklausel. Die Vorschrift ermächtigt die Mitgliedstaaten nicht zum Erlass einer gesetzlichen Regelung, sondern statuiert lediglich eine Unterrichtungspflicht der Mitgliedstaaten.

b. Bisherige Ausgestaltung im nationalen Recht

aa) Art. 51 Abs. 1 (ex Art. 46 Abs. 1)

Bereits gegenwärtig verfügt die Bundesrepublik Deutschland über mehrere unabhängige Aufsichtsbehörden auf Ebene des Bundes und der Länder. Ihre Existenz folgt verfassungsrechtlich aus der Staatlichkeit der Länder in einem föderalen System.

Das BDSG regelt die Aufsicht für die *öffentlichen Stellen des Bundes* (§ 22 BDSG) und ermächtigt die Länder, die Aufsicht für *nicht-öffentliche* Stellen zu regeln (§ 38 Abs. 6 BDSG).[159] Die Aufsicht über ihre *öffentlichen Stellen der Länder* regeln diese aus ihrer eigenen Kompetenz heraus. Dabei haben alle Länder mit Ausnahme Bayerns die Aufsicht über öffentliche Stellen des

[158] Dass das aus Sicht des Unionsrechts nicht notwendig ein formelles Gesetz bedingt, macht EG 41 (ex 31a) DSGVO deutlich.

[159] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 38, Rn. 29.

Landes und nicht-öffentliche Stellen in einer Hand vereint[160] (siehe zum Beispiel § 24 Abs. 1 S. 1, 2 RhPfDSG).
Anders als in § 38 Abs. 6 BDSG durch die Wendung „die Landesregierung" scheinbar vorgegeben, sehen die Länder die Zuständigkeit der Aufsichtsbehörden allerdings nicht durch Rechtsverordnung, sondern grundsätzlich durch Gesetz vor.[161] Bei den unabhängigen Aufsichtsbehörden handelt es sich (bis auf Bayern[162]) um den jeweiligen Landesdatenschutzbeauftragten.[163] Sie kontrollieren die Datenverarbeitung nicht-öffentlicher Stellen.
Die Zuständigkeitszuschreibung an diese Aufsichtsbehörden basiert jedoch auf der (alten) Datenschutzrichtlinie sowie dem BDSG. Sie bedarf der Anpassung an die Datenschutz-Grundverordnung, damit die deutschen Aufsichtsbehörden deren Einhaltung überwachen können.

bb) Art. 51 Abs. 3 (ex Art. 46 Abs. 2)

Die Notwendigkeit einer Vertretung Deutschlands auf der europäischen Bühne der Datenschutzaufsicht ist nicht als solche ein Novum: Sie bestand bereits für die Art. 29-Datenschutzgruppe. Für die Bestimmung des gemeinsamen Vertreters in der Datenschutzgruppe existiert bisher keine nationale gesetzliche Grundlage. Die derzeitige Praxis besteht darin, dass die Aufsichtsbehörden ihren Vertreter einstimmig wählen. Die deutsche Abgesandte in der Datenschutzgruppe ist derzeit die BfDI. Ihr Stellvertreter ist derjenige Beauftragte für Datenschutz und Informationsfreiheit, der in der Konferenz der Datenschutzbeauftragten turnusgemäß den Vorsitz innehat.[164]

---

[160] *Gola/Klug/Körffer* (Fn. 159), § 38, Rn. 29.
[161] So und zur Unschädlichkeit dieses Vorgehens *Petri*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 38, Rn. 16; anders aber in Bremen, vgl. die Bekanntmachung über Zuständigkeiten nach dem Bundesdatenschutzgesetz vom 31. März 1992 (Brem.ABl. S. 219).
[162] In Bayern ist gemäß Art. 34 BayDSG das Landesamt für Datenschutzaufsicht zuständig.
[163] § 31 Abs. 1 LDSG BW; § 33 Abs. 1 BlnDSG; § 23 Abs. 1a BbgDSG; § 1 BDatenSchZustBek (Brem.ABl. S. 219); § 24 HmbDSG; § 24 Abs. 4 HDSG; § 33a DSG MV; § 22 Abs. 6 NDSG; § 22 Abs. 5 S. 2 DSG NRW; § 24 Abs. 1 S. 2 LDSG Rh-Pf; § 28a SDSG; § 30a SächsDSG; § 22 Abs. 2 DSG LSA; § 39 Abs. 3 LDSG SH; § 42 ThürDSG.
[164] *Anonymous*, Data Protection Authorities, http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm (5.2.2016).

Eine Kooperationspflicht für die nationalen Aufsichtsbehörden enthält das BDSG in seinem § 26 Abs. 4. Die Datenschutz-Grundverordnung verdichtet diese Regelungen.[165]

c. Regelungsmöglichkeiten hinsichtlich der Vertretung beim EDA

Wer die Vertretung Deutschlands beim EDA bestimmt, hängt maßgeblich von der Verteilung der föderalen Kompetenzen zwischen Bund und Ländern ab. Als Anknüpfungspunkt kommen auf den ersten Blick sowohl die Außenvertretungskompetenz als auch die allgemeinen Regelungen zur Gesetzgebungs- und zur Verwaltungskompetenz in Betracht.

aa) Kompetenzverteilung zwischen Bund und Ländern

i. Außenvertretungskompetenz als Grundlage?

Art. 32 Abs. 1 GG verleiht dem Bund eine Verbandskompetenz für die Pflege auswärtiger Beziehungen zu anderen Staaten.[166] Spezialregelungen zur allgemeineren Norm des Art. 32 GG enthalten die Art. 23 und 24 GG.[167] Art. 32 GG bezieht sich nur auf die *Vertragsschluss*kompetenz; für die *Gesetzgebungs*kompetenz betreffend auswärtige Angelegenheiten hält Art. 73 Abs. 1 Nr. 1 Alt. 1 GG eine gesonderte Vorschrift vor.[168] Abweichend von der Grundregel des Art. 30, 70 Abs. 1 GG weist Art. 73 Abs. 1 Nr. 1 Alt. 1 GG dem Bund die ausschließliche Gesetzgebungskompetenz für auswärtige Angelegenheiten zu.

Eine auswärtige Angelegenheit ist nicht automatisch jeder Tatbestand mit Auslandsbezug.[169] Nach Ansicht des Bundesverfassungsgerichts sind „unter auswärtigen Angelegenheiten im Sinn von Art. 73 Nr. 1 GG […] diejenigen Fragen zu verstehen, die für das Verhältnis der Bundesrepublik Deutschland zu anderen Staaten oder zwischenstaatlichen Einrichtungen, insbesondere für

---

[165] Vgl. *von Lewinski*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 26, Rn. 35.
[166] *Nettesheim*, in: Maunz/Dürig (Hrsg.), GG, 49. Erg.-Lfg., Art. 32, Rn. 23. Siehe auch BVerfGE 1, 351 (369).
[167] *Nettesheim* (Fn. 166), Art. 32, Rn. 24.
[168] *Hillgruber*, in: Schmidt-Bleibtreu/Hofmann/Henneke (Hrsg.), GG, 13. Aufl., 2014, Art. 32, Rn. 2; *Pieroth*, in: Jarass/Pieroth (Hrsg.), GG, 13. Aufl., 2014, Art. 73, Rn. 3.
[169] BVerfGE 100, 313 (368).

die Gestaltung der Außenpolitik, Bedeutung haben."[170] Hierzu sollen auch Vertretungen der Bundesrepublik bei anderen Völkerrechtssubjekten zählen.[171]

Im Falle der Vertretung der deutschen Aufsichtsbehörden im EDA ist nur mittelbar die Vertretung der Bundesrepublik Gegenstand. Der Vertreter im Ausschuss bündelt die Stimmen der übrigen deutschen Aufsichtsbehörden und spricht auch für sie mit einer Stimme. Das ist Ausfluss des Regelungsauftrages in Art. 51 Abs. 3 und Art. 68 Abs. 4 (ex Art. 46 Abs. 2 und Art. 64 Abs. 3) DSGVO, der sich an die Mitgliedstaaten richtet. So gesehen artikuliert der Vertreter beim EDA zwar eine gesamtdeutsche aufsichtsbehördliche Position des Mitgliedstaates. Er wirkt aber bei dem unmittelbaren Vollzug des Unionsrechts durch eine „Einrichtung der Union mit eigener Rechtspersönlichkeit" (Art. 68 Abs. 1 [ex Art. 64 Abs. 1a] DSGVO) mit. Zugleich ist dabei nicht die Vertretung der Bundesrepublik Deutschland als Völkerrechtssubjekt zu anderen Staaten oder sonstigen Völkerrechtssubjekten betroffen, sondern – ausweislich des klaren Wortlauts des Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO – die Vertretung der Aufsichtsbehörden, falls ein Mitgliedstaat mehrere Aufsichtsbehörden kennt. Ob das nach Sinn und Zweck von Art. 73 Abs. 1 Nr. 1 Alt. 1 GG umfasst ist, darf kritisch hinterfragt werden. Art. 73 Abs. 1 Nr. 1 Alt. 1 GG darf insbesondere kein Instrument sein, die Kompetenzverteilung zwischen Bund und Ländern zu unterlaufen.[172]

ii. Gesetzgebungskompetenz für die Sachmaterie „Datenschutz" und das Verwaltungsverfahren

Die Gesetzgebungskompetenz für die inhaltliche Ausgestaltung des Datenschutzrechts ergibt sich in Deutschland aus der Kompetenz für den durch die datenschutzrechtliche Regelung betroffenen Sachgegenstand.[173] Weder dem

---

[170] BVerfGE 100, 313 (368 f.). Weniger präzise noch BVerfGE 33, 52 (60).

[171] *Uhle*, in: Maunz/Dürig (Hrsg.), GG, 58. Erg.-Lfg., Art. 73, Rn. 41 m. w. N.

[172] BVerfGE 100, 313 (368).

[173] *Polenz*, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes, in: Kilian/Heussen (Hrsg.), Computerrechts-Handbuch, 32. EL, 2013, Rn. 25 ff. Siehe auch *von Lewinski*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, Einleitung, Rn. 68 ff.; ausführlich auch *Simitis*, in: ders. (Hrsg.), BDSG, 8. Aufl., 2014, § 1, Rn. 1 ff. Vgl. ergänzend auch die Begründung des Gesetzentwurfs zum Bundesdatenschutzgesetz 1977, BT-Drs. 7/1027, S. 16.

Bund noch den Ländern steht insoweit die alleinige Kompetenz zu. Dementsprechend bestehen sowohl Bundes- als auch Länderkompetenzen. Insbesondere kommt dem Bund keine gesetzgeberische „Leitfunktion" zu.[174] Immerhin kann der Bund auf der Grundlage des Art. 74 Abs. 1 Nr. 11 GG jedoch in breitem Maße gesetzgeberisch tätig werden.[175]

Für den Datenschutz im Bereich der Aufsicht über die *öffentlichen Stellen* ergibt sich die Gesetzgebungskompetenz aus der Kompetenz zur Regelung des Verwaltungsverfahrens.[176] Für die Datenschutzaufsicht ist daher die Gesetzgebungskompetenz zwischen Bund und Länder geteilt.

Führen die Länder ihre Landesgesetze – hinsichtlich der Datenschutzaufsicht über ihre öffentlichen Stellen – aus, regeln sie auch selbst kraft eigenen Gesetzgebungsrechts das Verwaltungsverfahren. Führen die Länder das BDSG – im Bereich der *nicht-öffentlichen Stellen* – als eigene Angelegenheit aus, regeln sie auch selbst die Einrichtung der Behörden und das Verwaltungsverfahren (Art. 84 Abs. 1 S. 1 GG). Die Regelung der Datenschutzaufsicht ist Teil des Verwaltungsverfahrensrechts. Der Bund darf aber abweichende Regelungen erlassen (Art. 84 Abs. 1 S. 2 GG), von denen wiederum die Länder abweichen dürfen (Art. 84 Abs. 1 S. 2 Hs. 2 GG). Versteht man den Vertreter der Aufsichtsbehörden als Teil eines Exekutivorgans, so erscheint die Herleitung des nationalen Bestimmungsrechts hinsichtlich des nationalen Vertreters anhand der grundgesetzlichen Verteilung der Verwaltungskompetenzen zumindest denkbar. Daraus ergibt sich dann das Gebot einer koordinierten Rechtssetzung von Bund und Ländern. Als Rechtsform für das koordinierte Zusammenwirken von Bund und Ländern hinsichtlich der Vertretungsregelung ist der Staatsvertrag prädestiniert.

Bei dem Vertreter der deutschen Aufsichtsbehörden im EDA handelt es jedoch *nicht* um den klassischen Fall des Vollzugs von Unionsrechts durch den Mitgliedstaat, der in Deutschland nach den Art. 83 ff. GG[177] zu beurteilen ist. Der Vertreter im EDA agiert vielmehr als Teil eines unionalen Exekutivorgans. Ein Rekurs auf die Art. 83 ff. GG kommt dann unter Umständen allen-

[174] *Simitis* (Fn. 173), § 1, Rn. 2.
[175] *Wolff* (Fn. 149), S. 18.
[176] *Simitis* (Fn. 173), § 1, Rn. 8.
[177] Dazu *Suerbaum*, in: Epping/Hillgruber (Hrsg.), BeckOK GG, 27. Ed., 2015, Art. 83, Rn. 6.

falls deshalb in Betracht, weil der EDA als „verlängerter Arm“ des nationalen Gesetzesvollzugs fungiert.
Ob die Vertretung Deutschlands in einem unionalen Exekutivorgan nach den Verwaltungskompetenzen des Grundgesetzes (mithin Art. 83 ff. GG) bestimmt werden kann, ist aber zweifelhaft, übt der EDA doch *unionale* und keine mitgliedstaatliche Verwaltungstätigkeit aus, auf welche die Art. 83 ff. GG zugeschnitten sind. Ähnlich wie die mitgliedstaatlichen Vertreter im Rat (Art. 16 Abs. 2 EUV), handeln die Vertreter der mitgliedstaatlichen Aufsichtsbehörden im EDA, neben dieser Funktion, zugleich für ein Unionsorgan.[178]

iii. Annexkompetenz des Bundes

Die Zusammenschau der unterschiedlichen Regeln des Grundgesetzes[179] belegt, dass grundsätzlich der Bund für die Außenvertretung zuständig ist. Den Bund trifft auch die Einstandspflicht gegenüber anderen Völkerrechtssubjekten bezüglich der Erfüllung der übernommenen Verpflichtungen.[180]
Um die sich aus der Datenschutz-Grundverordnung ergebenden Pflichten, konkret die Entsendung eines aufsichtsbehördlichen Vertreters, erfüllen zu können, und anknüpfend an die Kompetenz des Bundes zur Außenvertretung, lässt sich unter Umständen eine Annexkompetenz des Bundes herleiten, die ihn (allein) zur Regelung ermächtigt.[181] Auf diese Weise könnte der Bund eine praktikable Vertretungsregelung schaffen und sicherstellen, dass die deutschen Aufsichtsbehörden in jedem Fall im EDA vertreten werden.[182] Mittelbar könnte der Bund damit auch die Handlungsfähigkeit des EDA selbst garantieren. Den Länderbelangen lässt sich im Rahmen des Gesetzgebungsverfahrens über ein Zustimmungserfordernis des Bundesrates (Zustimmungsgesetz) Rechnung tragen. Ergänzend können die Interessen der Länder

---

[178] Den Ratsvertretern kommt eine „Doppelfunktion“ zu, vgl. *Calliess*, in: Calliess/Ruffert (Hrsg.), EUV/AEUV, 4. Aufl., 2011, Art. 16 EUV, Rn. 6 f.; siehe auch *Kühling/Martini* (Fn. 1), 453.
[179] Vgl. S. 136 f.
[180] *Wolff* (Fn. 149), S. 10.
[181] So etwa *Wolff* (Fn. 149), S. 19 f.
[182] Vgl. abermals *Wolff* (Fn. 149), S. 19.

auf der inhaltlichen Ebene durch im Gesetz verankerte Mitbestimmungsrechte gestärkt werden.[183] Für ein ebensolches Modell könnte insbesondere auch die Vorschrift des Art. 23 Abs. 1 S. 2 GG streiten: Der Bund darf durch Gesetz mit Zustimmung des Bundesrates Hoheitsrechte übertragen. Allerdings ist die Vorschrift nicht unmittelbar, sondern allenfalls in ihrem Rechtsgedanken anwendbar: Sie meint grundsätzlich das Zustandekommen unionaler Regeln, welche mit einer Übertragung von Kompetenzen einhergehen (vgl. die im Integrationsverantwortungsgesetz genannten Fälle, etwa der Zustimmung des deutschen Vertreters im Rat zu Brückenklauseln zur Kompetenzerweiterung etc.), nicht aber die Realisierung bereits übertragener Hoheitsrechte.[184] Die Ausübung der Rechte im EDA betrifft diesen Fall der inhaltlichen Ausfüllung solcher Rechtsakte, für die Deutschland bereits Hoheitsrechte übertragen hat. Allenfalls lässt sich argumentieren, dass die Union kraft der ihr übertragenen Kompetenz auch die inhaltliche Ausfüllung der Mandate regeln hätte dürfen, die der EDA wahrnimmt, z. B. die BDfDI als Vertreterin Deutschlands hätte bestimmen können. Das tut die Datenschutz-Grundverordnung jedoch nicht. Sie regelt die Bestimmung eines nationalen Vertreters nicht selbst, sondern überlässt ihre Beantwortung dem Recht der Mitgliedstaaten („im Einklang mit den Rechtsvorschriften dieses Mitgliedstaats“, Art. 68 Abs. 4 DSGVO). Womöglich lässt sich aber in dem – auf der Grundlage des Art. 51 Abs. 3 DSGVO geforderten – Akt der Bestimmung des Vertreters der Aufsichtsbehörden die Konkretisierung einer Übertragung von Hoheitsrechten an eine EU-Einrichtung, namentlich die Ausfüllung der Aufgaben des EDA, verstehen (welche ihrerseits auf einer von Hoheitsrechten an die EU, namentlich Art. 16 Abs. 2 AEUV beruht). Denn der EDA übt seinerseits unionsrechtliche Hoheitsrechte im Vollzug aus, an denen der deutsche Vertreter mitwirkt.

iv. Zwischenergebnis

Die Verteilung der Kompetenz zur Bestimmung eines Vertreters im EDA trifft auf eine diesen Fall nicht ganz eindeutig regelnde verfassungsrechtliche Kompetenzverteilungsregelung. Eine ungeschriebene Bundeskompetenz un-

[183] *Wolff* (Fn. 149), S. 19.
[184] *Streinz*, in: Sachs (Hrsg.), GG, 7. Aufl., 2014, Art. 23 GG, Rn. 85.

terliegt als Ausnahmeregelung einem gesteigerten Rechtfertigungsbedarf.[185] Ob eine Annexkompetenz des Bundes letztlich trägt oder aber in unzulässiger Weise originäre Landeskompetenzen überspielt, bedürfte einer ergänzenden ausführlicheren Prüfung, die den Rahmen der in diesem Gutachten möglichen Analyse überschreitet.

Für die Kompetenz zur Bestimmung der zentralen Anlaufstelle entschärft Art. 55 Abs. 2 (ex Art. 51 Abs. 2) DSGVO die Verteilungsproblematik ein Stück weit: Machen die Mitgliedstaaten von ihren Öffnungsklauseln im öffentlichen Bereich Gebrauch, findet danach nämlich das Verfahren der federführenden Aufsichtsbehörde und der zentralen Anlaufstelle keine Anwendung. Vielmehr ist dann die nationale Aufsichtsbehörde des jeweiligen Kompetenzträgers die zuständige Behörde. Ein kompetenzieller Koordinierungsbedarf entsteht dann nicht. Allerdings ist von dieser Regelung nur ein kleiner Ausschnitt der Kompetenzüberlagerungsproblematik betroffen und die Problematik nicht als solche gelöst.

bb) Regelungsmodell

Hinsichtlich der Ausgestaltung der Vertretungsregelung stehen dem Bund und den Ländern mehrere Regelungsoptionen offen. Das gilt sowohl für die Bestimmung des Vertreters im EDA (i.), die Entscheidungskoordination zwischen den Aufsichtsbehörden (ii.), eine mögliche Bindung des Vertreters (iii.), eine organisationsrechtliche Verstetigung eines Koordinierungsgremiums und der Vertretungsstrukturen (iv.). Bei der Wahl zwischen ihnen ist sowohl den Belangen der Aufsichtsbehörde des Bundes als auch denen der Länder sowie dem politischen Interesse an einer wirksamen Vertretung nationaler Interessen auf der europäischen Bühne des Aufsichtsvollzugs in ausreichendem und angemessenem Maße Rechnung zu tragen.

i. Bestimmung des Vertreters

Für die inhaltliche Ausgestaltung des nationalen Systems der Aufsichtsstrukturen im Unionsrechtsverbund ist von zentraler Bedeutung, wer die Bundes-

[185] Prägnant *Seiler*, in: Epping/Hillgruber (Hrsg.), BeckOK GG, 27. Ed., 2015, Art. 70, Rn. 22.

republik im EDA vertritt bzw. wie der Vertreter ermittelt wird. Insoweit sind unterschiedliche Ausgestaltungen denkbar.

(1) Delegation der Entscheidung an die Aufsichtsbehörden: Wahl eines Vertreters durch die Aufsichtsbehörden

In Betracht kommt die Delegation der Entscheidung über die Bestimmung des Vertreters an die Aufsichtsbehörden. Diese würden dann ihren Vertreter selbst wählen. Dies entspräche dem Status quo unter der Datenschutzrichtlinie in Bezug auf die Vertretung Deutschlands in der Artikel-29-Datenschutzgruppe.[186]
Die Datenschutz-Grundverordnung bricht mit diesem Regelungsprinzip und weist den Regelungsauftrag den Mitgliedstaaten zu (Art. 51 Abs. 3 DSGVO).[187] Die Mitgliedstaaten müssen dies jedoch nicht zwingend „durch Gesetz“ tun. Auch unter dem verfassungsrechtlichen Gesichtspunkt der Wesentlichkeit ist die Bundesrepublik nicht gehindert, die Regelung (gleichsam wieder „zurück“) in die Hände der Aufsichtsbehörden zu legen. Der Vorteil einer solchen Regelung bestünde insbesondere darin, dass sie die aufsichtsbehördliche Unabhängigkeit weiter stärkt. Im Rahmen dieses Modells müsste der Gesetzgeber zudem das nähere Prozedere der Wahl festlegen. Dies betrifft vor allem die Frage, ob der Vertreter einstimmig zu bestimmen ist, oder ob ein Mehrheitsprinzip Anwendung findet. Ein Konsensprinzip kann Entscheidungsfindungen verzögern und im schlimmsten Fall entsteht eine Blockadesituation, welche die Bestimmung eines Vertreters verhindert. Das Risiko dürfte allerdings gering sein, da keine Beschlussfassung über kontroverse Sachfragen, sondern lediglich über die formale Repräsentation nach außen erfolgt.[188] Den Gegenpol zur einstimmigen Wahl bildet das Mehrheitsprinzip. Neben den Herausforderungen, die eine Mehrheitswahl mit sich bringen

[186] Vgl. S. 131. Zu beachten ist allerdings, dass kein Stimmungleichgewicht dadurch entsteht, dass in einem Bundesland mehrere Aufsichtsbehörden bestehen und auf diese Weise dem Bundesland vermittelt durch die Aufsichtsbehörden ein größeres Stimmgewicht zukommt, vgl. *Wolff* (Fn. 149), S. 12.
[187] Dazu bereits oben S. 131.
[188] Zur inhaltlichen Willensbildung vgl. unten auf S. 146 ff.

kann,[189] sieht sich der Bund womöglich einer übermäßig starken Länderrepräsentation gegenüber. Die Aufsichtsbehörden der Länder könnten, ohne vertiefte Berücksichtigung der Position der BfDI, und damit gewissermaßen an dieser vorbei, den deutschen Vertreter beim EDA bestimmen. Sieht der Gesetzgeber ein Bestimmungsrecht der Aufsichtsbehörden vor, sprechen aus der Interessenperspektive des Bundes folglich gute Gründe dafür, für die Wahl das Einstimmigkeitsprinzip zu implementieren.

(2) Rotationsprinzip

Eine zweite denkbare gesetzgeberische Regelungsoption ist das sog. Rotationsprinzip. Ähnlich wie beispielsweise der Vorsitz der Fachministerkonferenzen oder die Präsidentschaft im Bundesrat würde die Vertretung rotieren. Die Dauer der Vertretungsperiode würde im Zweifel der Gesetzgeber festlegen. Die Reihenfolge könnte eine Anleihe an der Königsteiner Vereinbarung und der Praxis der Rotation des Vorsitzes in Fachministerkonferenzen und im Düsseldorfer Kreis nehmen (wobei der Bund in diese aufgenommen werden müsste).[190] Ob das Rotationsprinzip der Repräsentation den Aufgaben der BfDI hinreichend gerecht wird, lässt sich unterschiedlich werten. Vor allem leidet ein Rotationsverfahren an dem Nachteil, im Regelfall keine Professionalisierung der Strukturen und damit keine optimale Repräsentation deutscher Interessen auf der europäischen Bühne zuzulassen.[191]

(3) Modell des (gesetzlich bestimmten) ständigen Vertreters

Statt einer Wahl durch die Aufsichtsbehörden selbst oder eines Rotationsprinzips könnte auch das Gesetz selbst bzw. ein Staatsvertrag eine der Aufsichtsbehörden, beispielsweise die BfDI, als ständige Vertreterin installieren. In diesem Fall kann ein Mitglied einer Aufsichtsbehörde eines Landes als ihr

---

[189] Siehe etwa die Diskussion um die verfassungsrechtliche Zulässigkeit des Glücksspielkollegiums, vgl. unten S. 153.

[190] Zur Wahl des Präsidenten und des Vizepräsidenten des Bundesrates nach der Königsteiner Vereinbarung siehe *Herzog*, § 59 Zusammensetzung und Verfahren des Bundesrates, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, 3. Aufl., 2005 Rn. 11 und 13.

[191] Vgl. auch *Kühling/Martini* (Fn. 1), 453.

Stellvertreter fungieren. Die Stellvertreterrolle könnte zwischen den Aufsichtsbehörden der Länder rotieren.
Das Modell des ständigen Vertreters birgt im Unterschied zum Rotationsprinzip den Vorteil einer hohen Kontinuität in der Amtswahrnehmung. Es ist einerseits geeignet, die innerdeutsche Zusammenarbeit mit Bezug zur Vertretung zu vereinfachen; gleichzeitig kann es dazu beitragen, den Einfluss im EDA zu steigern. In Mitgliedstaaten, die nicht mehrere Aufsichtsbehörden einrichten, werden einzelne Vertreter auch über mehrere Jahre an der Arbeit des EDA teilnehmen. Diese nehmen im Zweifel schon aufgrund ihrer Erfahrung eine Führungsrolle in Verhandlungen ein. Eine rotierende deutsche Vertretung kann demgegenüber schnell ins Hintertreffen geraten, da persönliches Wissen und Erfahrung schwer institutionalisierbar sind.

(4) Doppelspitzen-Lösung

Eine vierte Möglichkeit besteht in einer „Doppelspitzen-Lösung“. Diese entspräche weitgehend dem Modell eines ständigen Vertreters – mit der Ergänzung, dass das jeweilige Mitglied der Aufsichtsbehörde des Landes kein Stellvertreter, sondern gleichberechtigter (Mit-)Vertreter ist. Nicht ganz eindeutig ist aber, ob die Grundlage der Datenschutz-Grundverordnung ein solches Modell trägt. Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO legt den Mitgliedstaaten die Verpflichtung auf, „die Aufsichtsbehörde, die diese Behörden im Europäischen Datenschutzausschuss vertritt“, zu bestimmen. Die Verwendung des Singulars impliziert, dass nur *einer* Aufsichtsbehörde die Aufgabe der Vertretung des Mitgliedstaates zukommt.[192] Auch Art. 68 Abs. 4 (ex Art. 64 Abs. 3) DSGVO geht davon aus, dass lediglich „ein gemeinsamer Vertreter“ benannt wird. Diese Wortwahl ist ihrem Sinn nach aber wohl dem

[192] Bei einer Doppelspitzen-Lösung kann zusätzlich das Problem einer einheitlichen Stimmabgabe virulent werden. Für die Abstimmung im Bundesrat statuiert das Grundgesetz in Art. 51 Abs. 3 S. 2 GG, dass die Vertreter eines Landes ihre Stimmen nur einheitlich abgeben dürfen. Siehe hierzu auch BVerfGE 106, 310 ff. Verfügt ein Mitgliedstaat nur über eine Stimme, kann diese ihrem Wesen nach nur einheitlich abgegeben werden. Es können sich aber Konflikte ergeben, wenn sich die beiden Vertreter nicht inhaltlich auf eine Position einigen können und divergierende Standpunkte einnehmen. Dann stellt sich die Frage, wessen Abstimmungsverhalten das maßgebliche ist. Eine Doppelspitzen-Lösung kann insofern Konflikte erzeugen; ein Modell der Stellvertretung ist insofern vorzugswürdig.

Bemühen geschuldet, sicherzustellen, dass die jeweilige Aufsichtsbehörde aus dem jeweiligen Mitgliedstaat nur über *eine Stimme* verfügt. Entsänden die Aufsichtsbehörden sämtlicher Mitgliedstaaten zwei Vertreter mit Stimmrecht, wäre das mit dem in der Datenschutz-Grundverordnung angelegten Modell „one country, one vote“ fraglos nicht vereinbar.
Die Entsendung mehrerer aufsichtsbehördlicher Vertreter (mit nur einer Stimme) aus einem Mitgliedstaat schließt dies aber nicht unbedingt aus. Für die Arbeitsfähigkeit des EDA wäre es freilich kontraproduktiv (für die interne Abstimmung und Ausbalancierung der Interessen des Bundes und der Länder demgegenüber sehr geeignet). Aber nicht nur das: Da auch die Präsenz in einem Abstimmungsprozess das Gewicht einzelner Mitgliedstaaten verschieben kann, sprechen die besseren Gründe dagegen, dass die Datenschutz-Grundverordnung die Entsendung mehrerer gleichberechtigter Vertreter – sei es mit, sei es ohne Stimmrecht –zulässt. Eine Vertretungsregelung schließt das aber nicht aus. Ein Mitgliedstaat darf sich mit anderen Worten im Wechsel durch jeweils unterschiedliche Personen vertreten lassen.

(5) Zwischenfazit; fallspezifische Vertretungsregelung

Die Datenschutz-Grundverordnung lässt es zu, den Aufsichtsbehörden die Wahl des gemeinsamen Vertreters nach dem Konsensprinzip selbst zu überlassen oder die BfDI als ständige Vertreterin zu installieren, die wechselnd von einem Mitglied einer Aufsichtsbehörde der Länder als Stellvertreter unterstützt wird.
Diese beiden zu bevorzugenden Modelle bieten in gleichem Maße Raum für die Implementierung fallspezifischer Vertretungsregelungen.[193] In Anlehnung an Art. 23 Abs. 6 GG ist es auf Grundlage beider Modelle möglich, für einen konkreten Fall auch einen anderen als den üblichen Vertreter – insbesondere ein Mitglied einer Aufsichtsbehörde der Länder, in dessen Aufsichtsbereich ein Unternehmen ansässig ist – zu entsenden. Das ermöglicht eine inhaltliche Entscheidungskoordination nach Betroffenheit und unternehmensspezifischem Fachwissen, erhöht allerdings das Risiko einer regulatory capture.

[193] Auf inhaltlicher Ebene wird dies durch eine gegenstandsbezogene Koordinierung rückgespiegelt, siehe dazu sogleich auf den folgenden Seiten.

ii. Entscheidungskoordination zwischen den Aufsichtsbehörden des Bundes und der Länder

Ist der Vertreter der Bundesrepublik beim EDA benannt, bedarf es auch eines Verfahrens, das es erlaubt, den Willen der BfDI und den der verschiedenen Aufsichtsbehörden der Länder zu koordinieren, damit der Vertreter diesen in seiner Stimme bündeln und im EDA artikulieren kann. Der Vertreter Deutschlands im EDA muss inhaltlich an den Willen der übrigen Aufsichtsbehörden rückgebunden werden; er darf nicht allein seine Position repräsentieren. Stattdessen tritt er gleichsam als Sprecher bzw. Bevollmächtigter für alle deutschen Aufsichtsbehörden auf.
Eine Abstimmung der aufsichtsbehördlichen Position in Bezug auf Sachfragen kann auf unterschiedliche Weise erfolgen. Eine Grobeinteilung der bestehenden gesetzgeberischen Optionen kann danach erfolgen, ob eine pauschale (1) oder aber eine gegenstandsbezogene Regelung (2) zur Koordinierung der aufsichtsbehördlichen Standpunkte bezweckt ist.

(1) Pauschale Regelung

Bei einer *pauschalen Regelung* verliefe die Abstimmung der aufsichtsbehördlichen Auffassung zu inhaltlichen Belangen stets in gleicher Weise. Denkbar sind insbesondere Entscheidungen anhand des Konsens- oder des Mehrheitsprinzips.[194] Unter Geltung eines Konsensprinzips müssten sich alle Aufsichtsbehörden auf eine inhaltliche Position einigen. Würde man hingegen ein Mehrheitsprinzip implementieren, verträte der Vertreter Deutschlands beim EDA die aufsichtsbehördliche Mehrheitsmeinung. Nachteilig an einer derart pauschalen Regelung ist, dass sie keine Flexibilität bietet und für die durchaus verschiedenen thematischen Aufgaben des EDA (gerade auch in föderaler Hinsicht) womöglich nicht hinreichend differenziert ist.

[194] Die Vor- und Nachteile solcher Modelle wurden bereits zuvor auf S. 142 beschrieben.

(2) Gegenstandsbezogene Regelung entsprechend dem Leitmodell des Art. 23 GG

Eine *gegenstandsbezogene Regelung* ebnet den Weg zu einem differenzierten System der Entscheidungskoordination. Die Abstimmung der aufsichtsbehördlichen Position könnte sich in Abhängigkeit vom konkreten inhaltlichen Entscheidungsgegenstand und somit anhand der Betroffenheit der unterschiedlichen Aufsichtsbehörden auf eine unterschiedliche Art und Weise vollziehen.[195] Für ein derartiges Modell kann etwa Art. 23 GG Pate stehen, der in seinen Abs. 2 bis 7 die Mitwirkung der deutschen gesetzgebenden Organe, des Bundestages und des Bundesrates, in Angelegenheiten der Europäischen Union regelt. Die Norm etabliert ein differenziertes Beteiligungssystem, welches das EUZBBG[196] und das EUZBLG[197] einfach-gesetzlich ausformen. So enthält Abs. 5 spezifische Mitwirkungsrechte des Bundesrates, die sich danach richten, wie stark und welche Länderbelange betroffen sind.[198] Gesteigert wird die Mitwirkung des Bundesrates schließlich durch die in Abs. 6 enthaltene Regelung: In dem dort genannten Fall übt ein vom Bundesrat benannter Vertreter der Länder die mitgliedstaatlichen Rechte aus.[199] Allerdings betont das GG auch an dieser Stelle die Notwendigkeit einer Kooperation von Bund und Ländern. Gemäß Art. 23 Abs. 6 S. 2 GG muss eine Beteiligung und Abstimmung mit der Bundesregierung erfolgen.
Hinsichtlich der Vertretung Deutschlands beim EDA ist eine vergleichbare Regelung denkbar.[200] Überträgt man die Grundstrukturen des Art. 23 GG auf

---

[195] Vgl. auch ausführlich *Wolff* (Fn. 149), S. 21 ff.
[196] Gesetz über die Zusammenarbeit von Bundesregierung und Deutschem Bundestag in Angelegenheiten der Europäischen Union vom 4.7.2013, BGBl. I S. 2170.
[197] Gesetz über die Zusammenarbeit von Bund und Ländern in Angelegenheiten der Europäischen Union vom 12.3.1993, BGBl. I S. 313.
[198] Vgl. *Hillgruber*, in: Schmidt-Bleibtreu/Hofmann/Henneke (Hrsg.), GG, 13. Aufl., 2014, Art. 23, Rn. 73.
[199] Beispielsweise kann ein Länderminister die Bundesrepublik Deutschland im Ministerrat (Art. 16 Abs. 2 EUV) vertreten, § 6 Abs. 2 EUZBLG.
[200] Ein solches Modell wohl für die Vertretungsregelung nach Art. 68 Abs. 4 (ex Art. 64 Abs. 3) DSGVO befürwortend *die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*, in: Deutscher Bundestag, Ausschuss Digitale Agenda, Ausschussdrucksache 18(24)93, S. 8. Ähnlich auch *Roßnagel*, in: Deutscher Bundestag, Ausschuss Digitale Agenda, Ausschussdrucksache 18(24)94, S. 11.

die Vertretung der deutschen Aufsichtsbehörden beim EDA, so lässt sich die BfDI als primärer Vertreter Deutschlands installieren.[201] Inhaltlich muss sie die Auffassung der Aufsichtsbehörden der Bundesländer in einem abgestuften Maße beachten. Dieses richtet sich nach dem Ausmaß, in dem Länderbelange betroffen sind. In bestimmten Fällen kann zudem die Entsendung eines der Aufsichtsbehörde eines Landes angehörigen Vertreters angezeigt sein.[202] In diesem Fall obläge es, in Anlehnung an Art. 23 Abs. 5 GG,[203] den Aufsichtsbehörden der Länder, einen gemeinsamen Vertreter zu benennen, der die Bundesrepublik Deutschland insgesamt vertritt bzw. den gemeinsamen benannten Vertreter entsprechend dem gemeinsam gebildeten Willen der Länder zu binden.

Ein solches Modell verlangt aber auch nach einer entsprechenden Vorkoordination der Aufsichtsbehörden der Länder. Soll die BfDI als Vertreterin aller deutschen Aufsichtsbehörden den Standpunkt der Aufsichtsbehörden der Länder beachten und in das EDA transportieren, müssen zunächst die Länder ihr gegenüber einen einheitlichen Willen artikulieren. Der diesbezügliche Willensbildungsprozess kann auch hier grundsätzlich nach dem Konsens- oder dem Mehrheitsprinzip erfolgen. Gemäß Art. 52 Abs. 3 S. 1 GG entscheidet der Bundesrat mit Stimmmehrheit, sodass die Koordinierung des Länderwillens im Rahmen des Art. 23 GG gegenwärtig (wenn auch in anderem Regelungskontext) auch hier nach dem Mehrheitsprinzip erfolgt.

Das verfassungsrechtlich verankerte Prinzip eigenverantwortlicher Aufgabenwahrnehmung steht einer Mehrheitsentscheidung der verschiedenen Aufsichtsbehörden nicht zwingend entgegen:[204] Sowohl die Bundesrepublik selbst als auch der EDA sind auf eine wirksame Vertretung der deutschen Aufsichtsbehörden angewiesen. Das Erfordernis einer konsensualen Einigung der Aufsichtsbehörden der Länder würde hingegen eine zeitnahe inhaltliche

---

[201] So gesehen besteht ein enger Zusammenhang zwischen dem soeben beschriebenen ersten und dem vorliegenden zweiten Fragenkreis; eine isolierte Betrachtung der einzelnen Aspekte ist nur schwer möglich.

[202] Vgl. auch *von Lewinski*, Datenschutzaufsicht in Europa als Netzwerk (Entwurfsfassung vom 24.2.2015), in: Ziekow (Hrsg.), Verwaltung in Netzwerken, 2016 (in Vorbereitung), S. 7.

[203] Zur Bestimmung des Vertreters im Rahmen des Art. 23 Abs. 6 GG siehe *Scholz*, in: Maunz/Dürig (Hrsg.), GG, 2015, Art. 23, Rn. 177.

[204] Zur Problematik um die Verfassungsmäßigkeit des Glücksspielkollegiums siehe auf S. 153.

Abstimmung und damit eine effektive Vertretung bzw. unionsweite Koordinierung der Aufsichtsbehörden nachhaltig erschweren. Mit der Zustimmung zu den Europäischen Verträgen hat die Bundesrepublik Deutschland der damit verbundenen Einschränkung des Prinzips eigenverantwortlicher Aufgabenwahrnehmung rechtlich grundsätzlich den Weg bereitet.[205]

iii. Bindung des Vertreters an den ermittelten Willen

Implementiert der Gesetzgeber ein abgestuftes Beteiligungsregime, muss er sicherstellen, dass der Vertreter der deutschen Aufsichtsbehörden, den Willen der anderen Aufsichtsbehörden auch tatsächlich vertritt. Der aufsichtsbehördliche Wille bindet den Vertreter lediglich im Innen-, nicht aber im Außenverhältnis. Dieser Bindung kann sich der Vertreter nicht durch eine eigenmächtige Entscheidung entziehen; er muss der Willensbekundung der Aufsichtsbehörden der anderen Länder entsprechen. Diese Verpflichtung folgt aus dem Grundsatz des bundesfreundlichen Verhaltens.[206] Der Vertreter verfügt dann nicht über ein freies, sondern über ein imperatives Mandat.
Die Datenschutz-Grundverordnung lässt ein Modell zu, das den Vertreter im Außenverhältnis mit unbegrenzter Vertretungsmacht ausstattet, ihn jedoch im Innenverhältnis Bindungen unterwirft. Sie trifft insoweit keine Vorgaben, achtet insbesondere – auch ausweislich des EG 117 (ex EG 92) DSGVO – ausdrücklich die mitgliedstaatlichen Strukturen, soweit die Zielsetzungen der Verordnung dadurch nicht beeinträchtigt werden. Der föderale Staatsaufbau ist ein wichtiges verfassungsmäßiges Strukturelement der Bundesrepublik. Gerade diesem föderalen Gedanken will die Bundesrepublik durch die Installation mehrerer Aufsichtsbehörden Rechnung tragen. Die Gestaltung der Aufsicht über die eigenen Landesbehörden ist insbesondere Ausdruck der Staatlichkeit der Länder. Eine Einschränkung der Vertretungsmacht des deutschen Vertreters beim EDA im Innenverhältnis, die sich aus der Notwendigkeit der Einbindung der Aufsichtsbehörden der Bundesländer in den Entscheidungsprozess ergibt, ist somit möglich und erforderlich.

---

[205] Daraus eine Annexkompetenz des Bundes für die Vertretung folgernd *Wolff* (Fn. 149), S. 19.
[206] Vgl. in Bezug auf Art. 23 GG *Scholz* (Fn. 203), Art. 23, Rn. 174.

iv. Organisationsrechtliche Verstetigung eines nationalen aufsichtsbehördlichen Gremiums? – Vergleich zu Referenzmodellen in anderen Rechtsbereichen

Bei der Neugestaltung der aufsichtsrechtlichen Zusammenarbeit muss der Gesetzgeber die Frage beantworten, ob er ein Gremium installieren will, das die Kooperation und Koordination der verschiedenen nationalen Aufsichtsbehörden organisatorisch verstetigt. Ein solches Gremium könnte hinsichtlich des gemeinsamen Auftretens der deutschen Aufsichtsbehörden nach außen im unionalen Datenschutz zur wichtigen Schaltzentrale avancieren. Gegenwärtig fungiert als organisationsrechtlich verstetigtes Gremium einer Verständigung der Aufsichtsbehörden der Düsseldorfer Kreis. Hier koordinieren sich die Datenschutzbeauftragten des Bundes und der Länder im Rahmen einer Konferenz.

Die Ausgestaltung eines organisatorisch verstetigten Koordinierungsmechanismus ist, unter Zugrundelegung bereits bestehender Strukturen, auf unterschiedliche Art und Weise denkbar. Bestehende (Aufsichts-)Modelle können dabei als Referenzmuster dienen. Allerdings ist im Hinblick auf die Spezifika der Datenschutzaufsicht stets zu prüfen, inwieweit sich ein bereits in anderen Bereichen praktiziertes Modell tatsächlich bruchfrei übertragen lässt, da hier – insoweit anders als in den Referenzfällen – eine Kooperation von Bund und allen Ländern erforderlich ist.

(1) Das Modell der Medienaufsicht

Eine Koordinierung aufsichtlicher Aufgabenwahrnehmung in einem föderalen Bundesstaat hat – im Hinblick auf die bundesweiten Ausstrahlungswirkungen landesaufsichtlicher Maßnahmen in einem bundesweit und immer stärker unionsweit agierenden Medienumfeld – vergleichsweise früh das Recht der Medienaufsicht etabliert. Die Medienaufsicht nehmen in der Bundesrepublik Deutschland die Landesmedienanstalten wahr (§§ 36 ff. RStV). Sie sind rechtsfähige Anstalten des öffentlichen Rechts[207] und unterliegen nur einer Rechts-, aber keiner Fachaufsicht[208]. Ihre Zusammenarbeit koordinieren be-

[207] *Fechner*, Medienrecht, 15. Aufl., 2014, 10. Kap. Rn. 199.
[208] *Fechner* (Fn. 207), 10. Kap. Rn. 201.

sondere Gremien mit apokrypher Struktur, die in einer verstetigten Form den Koordinierungsbedarf unter den Aufsichtsbehörden organisieren. Der RStV hat zu diesem Zweck vier Gremien etabliert: die Kommission für Zulassung und Aufsicht (ZAK), die Gremienvorsitzendenkonferenz (GVK), die Kommission zur Ermittlung der Konzentration im Medienbereich (KEK) und die Kommission für Jugendmedienschutz (KJM). Die Einrichtungen fungieren als Organe der jeweiligen Landesmedienanstalten (§ 35 Abs. 2 S. 2 RStV)[209] und sind dabei plural mit Vertretern der unterschiedlichen Landesmedienanstalten besetzt. Dem Begriff des „Organs" kommt im vorliegenden Fall aber nur eine schwache Aussagekraft zu. Sie erschöpft sich mehr oder weniger darin, zu verdeutlichen, dass die Kommissionen selbst nicht nach außen auftreten, [210] insbesondere nicht selbst Verwaltungsträger sind.[211] Am plastischsten lassen sie sich als sog. „Wanderorgan" charakterisieren.[212] Die Organe im Sinne des § 35 Abs. 2 RStV verfügen über eine gemeinsame Geschäftsstelle (§ 35 Abs. 7 RStV).[213] Ihre dem Gedanken der Staatsferne des Rundfunks geschuldete Unabhängigkeit sichert § 35 Abs. 8 RStV. Besondere Wirkmacht erlangen die Beschlüsse der Kommissionen dadurch, dass sie die anderen Organe der Landesmedienanstalten binden (§ 35 Abs. 9 S. 5 RStV). Die Kommissionen entscheiden mit der Mehrheit ihrer gesetzlichen Mitglieder (§ 35 Abs. 9 S. 1 RStV). Außerhalb der Kommissionen kooperieren und koordinieren sich die Landesmedienanstalten über die Arbeitsgemeinschaft der Landesmedienanstalten.[214]

Konzeptionell scheint das Modell der Rundfunkregulierung für die neue Gestaltung der Aufsichtsbehörden unter der Datenschutz-Grundverordnung gut geeignet: Das Prinzip des koordinierten Zusammenwirkens, die Bindung an

---

[209] Vgl. auch *Grünwald*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl., 2015, § 35 RStV, Rn. 5 f. Dies für die KEK verneinend aber *Westphal*, Föderale Privatrundfunkaufsicht im demokratischen Verfassungsstaat, 2007, S. 309. Stattdessen sieht *Westphal* (Fn. 209), S. 360, die KEK als neue Organisationsform, nämlich als „zentrale Länderkommission".

[210] *Schuler-Harms*, in: Hahn/Vesting (Hrsg.), BeckOK RundfunkR, 3. Aufl., 2012, § 35 RStV, Rn. 48.

[211] Vgl. BayVGH, Beschl. v. 3.4.2007 – 7 C 06.3009 –, juris, Rn. 6.

[212] *Gröpl*, ZUM 2009, 21 (22).

[213] Ausführlicher zur Geschäftsstelle *Gröpl* (Fn. 212), 23 ff.

[214] Vgl. hierzu *Fechner* (Fn. 207), 10. Kap. Rn. 210.

Entscheidungen, das verankerte Mehrheitsprinzip; die Unabhängigkeit der Aufsichtsbehörden, welche die Datenschutz-Grundverordnung vorsieht, steht in einer gedanklichen Nähe zur Staatsferne, dem das Rundfunkmodell verpflichtet ist.
Eine Übertragung des Modells der Rundfunkaufsicht auf die Vertretung der deutschen Datenschutzaufsichtsbehörden ist jedoch – abgesehen von den strukturellen Besonderheiten des Rundfunkrechts, insbesondere des Prinzips der Staatsferne – bereits deshalb nicht in jeder Hinsicht möglich, weil die Zuständigkeit für die Medienaufsicht alleine bei den Ländern liegt; eine Abstimmung mit dem Bund ist dort nicht erforderlich. Es macht das Modell der Medienaufsicht aber nicht generell als eine Blaupause für die Gestaltung einer künftigen nationalen Datenschutzkommission untauglich, wenn sich Bund und Länder auf eine solche Gestaltung verständigen.

(2) Glücksspielkollegium (§ 9a Abs. 5-8 GlüStV)

Ein der Medienaufsicht strukturell ähnliches Modell praktiziert auch das Glücksspielrecht. Aufgrund des unionsrechtlichen Erfordernisses kohärenter Ausgestaltung der Glücksspielregelungen überträgt der GlüStV dem Glücksspielkollegium in § 9a Abs. 5 S. 1 GlüStV eine Koordinierungsfunktion. Seine Aufgabe besteht darin, für alle Länder die Erlaubnis zur Ausübung des Glücksspiels zu erteilen und die Aufgabe in der Glücksspielaufsicht mit Wirkung für alle Länder auszuüben (§ 9a Abs. 5 S. 1 i. V. m. Abs. 1 bis 3 GlüStV). In seiner Ausgestaltung kommt die Glücksspielkommission der organisationsrechtlichen Kategorie einer Mehrländereinrichtung sehr nahe.[215] Das Kollegium ist weder dem Bund noch einem Land zuzuordnen.[216] Seine Geschäftsstelle besteht jedoch gemäß § 9a Abs. 7 S. 1 GlüStV auf Grundlage des hessischen Rechts. Ausweislich des § 9a Abs. 5 S. 2 GlüStV fungiert das Glücksspielkollegium als Organ der Glücksspielaufsichtsbehörden der Länder. Diese treten auch nach außen auf, sind jedoch an die Beschlüsse des Kollegiums gebunden (vgl. § 9a Abs. 8 S. 4 GlüStV). Das Gremium fasst seine

[215] Vgl. *Martini*, Die IMK als Gegenstand des Informationsrechts, 2015, S. 19.
[216] Siehe dazu *Martini* (Fn. 215), S. 20.

Beschlüsse mit einer Mehrheit von mindestens zwei Dritteln der Stimmen seiner Mitglieder (§ 9a Abs. 8 S. 1 GlüStV).

Ob das Glücksspielkollegium verfassungskonform ist, ist unklar. Nach Ansicht insbesondere des HessVGH widerspricht es dem Bundesstaats- und dem Demokratieprinzip.[217] Als neuralgischer Punkt erweist sich vor allem die Entscheidungsfindung im Glücksspielkollegium. Dass das Kollegium nicht einstimmig entscheidet, lässt es nach Einschätzung des HessVGH in unzulässiger Weise auf einer „dritten Ebene" der Staatlichkeit agieren, da es weder dem Bund noch in eines der Länder eingegliedertes Organ sei.[218] Insbesondere erlaube das Mehrheitsprinzip die Überstimmung einzelner Länder, in denen die Entscheidung des Glücksspielkollegiums in der Folge ohne Anbindung an das Staatsvolk des jeweiligen Landes ausgeführt werden könne.[219]

Wie im Rahmen der Medienaufsicht sind an der Glücksspielaufsicht durch die Glücksspielkommission nur die Länder kompetenziell beteiligt. Die Notwendigkeit der Kooperation mit einer Stelle des Bundes besteht im Glücksspielrecht, anders als im Rahmen der Datenschutzaufsicht, nicht. Das schränkt die Tauglichkeit des Regelungsmodells, welches das Glücksspielrecht gewählt hat, als Referenzmodell für das Datenschutzrecht – soweit es sich als verfassungsrechtlich zulässig erweist – ein, schließt sie aber nicht aus.

(3) Fachministerkonferenzen

Als übergreifende Gremien der Kooperation und Koordination zur Abstimmung gemeinsamer Handlungsstrategien haben sich in der Bundesrepublik über inzwischen sechs Jahrzehnte hinweg Fachministerkonferenzen etabliert. Sie bilden ein Beratungs- und Beschlussgremium der jeweiligen Fachminister der Bundesländer unter dem Beisein des jeweiligen Bundesministers. Derartige Fachministerkonferenzen sind keine gemeinschaftlichen Behörden oder

[217] HessVGH, NVwZ 2016, 171 (172 ff.). Anders aber BayVerfGH, BeckRS 2015, 52905, Rn. 139 ff.
[218] HessVGH, NVwZ 2016, 171 (172 f.).
[219] HessVGH, NVwZ 2016, 171 (174).

gemeinsame Organe der Länder, sondern viel eher Arbeitsgemeinschaften[220] mit im Jahresrhythmus rotierendem Vorsitz.[221]
Als Anleihe für die Ausgestaltung der Vertretung Deutschlands im EDA eignen sich die Fachministerkonferenzen jedoch nur bedingt. Zum einen handelt es sich um informelle Gremien, die sich rechtlich nur eingeschränkt greifen lassen. Die Beschlüsse der Fachministerkonferenzen sind zwar politisch bedeutsam, zeitigen für die durch die jeweiligen Minister vertretenen Länder aber – anders als Beschlüsse des EDA – in der Regel keine rechtliche Bindung.[222], insbesondere keine rechtlich bindenden Beschlüsse. Außerdem handelt es sich primär um eine Korporationsform *der Länder*.[223] So verfügt der jeweilige Bundesminister regelmäßig nur über einen Gaststatus,[224] der es ihm nicht erlaubt, an der Abstimmung teilzunehmen. Abstimmungsbefugt sind alleine die Länder; sie entscheiden im Konsensprinzip.[225] Eine (für die Datenschutzaufsicht erforderliche) Beschlusskooperation zwischen Bund und Ländern ist somit gerade nicht intendiert.

(4) Gremium Europäischer Regulierungsstellen für elektronische Kommunikation (GEREK)

Als Gremium zur Koordination der Regulierungsbehörden kennt das Telekommunikationsrecht das sog. GEREK. Es erfährt durch die VO (EG) 1211/2009 seine nähere Ausgestaltung. Das deutsche Recht adressiert es in den § 3 Nr. 9c, § 12 Abs. 2 Nr. 1 S. 1, Nr. 2 S. 1, Nr. 4, § 13 Abs. 4 TKG.
Das GEREK besteht aus einem Regulierungsrat, in dem jeweils ein Mitglied pro Mitgliedstaat vertreten ist (Art. 4 Abs. 1 und 2 VO (EG) 1211/2009). Das zu entsendende Mitglied ist gemäß Art. 4 Abs. 2 VO (EG) 1211/2009 dabei der „Leiter oder ein nominierter hochrangiger Vertreter der in jedem Mitgliedstaat errichteten nationalen Regulierungsbehörde, die die Hauptverant-

[220] So in Bezug auf die Innenministerkonferenz *Martini* (Fn. 215), S. 28 f.
[221] *Rudolf*, § 141 Kooperation im Bundesstaat, in: Isensee/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, 3. Aufl., 2005, Rn. 39.
[222] Erneut in Bezug auf die Innenministerkonferenz *Martini* (Fn. 215), S. 11 ff.
[223] Vgl. *Rudolf* (Fn. 221), Rn. 37.
[224] *Rudolf* (Fn. 221), Rn. 40.
[225] Vgl. zur Innenministerkonferenz *Martini* (Fn. 215), S. 12.

wortung für die Beaufsichtigung des laufenden Marktgeschehens im Bereich der elektronischen Kommunikationsnetze und -dienste trägt“. Zudem verfügt jeder Mitgliedstaat über ein stellvertretendes Mitglied. Dieses wird nach Art. 4 Abs. 2 UAbs. 3 VO (EG) 1211/2009 von den nationalen Regulierungsbehörden benannt.

Als Referenzfall für die Koordinierung der Datenschutzaufsicht ist das GEREK insofern nur bedingt geeignet, als das Telekommunikationsrecht der ausschließlichen Gesetzgebungskompetenz des Bundes unterfällt. Insofern verhält sich die Situation umgekehrt wie im Medienrecht und im Glücksspielrecht. Jenseits der kompetenziellen Unterschiede kann sich die Koordinationsfunktion des GEREK aber rechtspolitisch in Grenzen als Referenzmodell für eine Neugestaltung der Zusammenarbeit unter den Datenaufsichtsbehörden eignen.

(5) Kartellbehördlicher Informationsaustausch (§ 50a Abs. 1 GWB i. V. m. § 50 Abs. 2 GWB)

Einen interessanten denkbaren Referenzfall zur Ausgestaltung aufsichtsrechtlicher Koordinationsstrukturen markiert das Kartellrecht, genauer § 50a Abs. 1 GWB und § 50 Abs. 2 GWB. Das gilt insbesondere im Hinblick auf die vergleichbare kompetenzielle Ausgangssituation: Im Bereich des Kartellrechts überschneiden sich teilweise landesrechtliche und bundesrechtliche Kompetenzen. § 50a GWB etabliert eine Regelung zum Informationsaustausch zwischen der nationalen Kartellbehörde und der Europäischen Kommission sowie den Kartellbehörden der anderen EU-Mitgliedstaaten. Die Vorschrift betrifft neben dem Bundeskartellamt auch die Landeskartellbehörden.[226] § 50a Abs. 1 S. 2 GWB ordnet eine entsprechende Geltung des § 50 Abs. 2 GWB an. Hieraus folgt, dass beim Tätigwerden der Landeskartellbehörden der Geschäftsverkehr über das Bundeskartellamt läuft.[227] So wird das Bundeskartellamt zum „zentrale[n] Ansprechpartner“ der Bundesrepublik für Europäische Kommission und die Kartellbehörden der übrigen Mitgliedstaa-

[226] *Rehbinder*, in: Immenga/Mestmäcker (Hrsg.), Wettbewerbsrecht, 5. Aufl., 2014, § 50a GWB, Rn. 4.

[227] Vgl. auch *Becker*, in: Loewenheim/Meessen/Riesenkampff (Hrsg.), Kartellrecht, 2. Aufl., 2009, § 50a GWB, Rn. 1.

ten.[228] Die Landeskartellbehörden werden vom Bundeskartellamt vertreten und können diesem daher Weisungen erteilen.[229]
Eine ergänzende Regelung hält § 50 Abs. 2 S. 3 GWB bereit, der dem Bundeskartellamt die Vertretung Deutschlands im Beratenden Ausschuss für Kartell- und Monopolfragen zuweist. Eine Partizipation der Landeskartellbehörden ist jedoch im Wege der Teilnahme als Experten möglich.[230]
Allerdings koordinieren sich Bund und Länder in diesem Bereich nicht in einer organisatorisch verstetigten Form, die uneingeschränkt als Blaupause für den vorliegenden Fall eines nationalen aufsichtsbehördlichen Gremiums im Datenschutzrecht dienen könnte.
Findet sich gegenwärtig auch kein der Koordination der Datenschutzaufsichtsbehörden exakt vergleichbarer Referenzfall, können die im Ansatz vergleichbaren Strukturen der Entscheidungskoordination, die sich im föderalen System der Bundesrepublik Deutschland etabliert haben, doch rechtspolitisch eine Grundlage für eine eklektizistische Neugestaltung der datenschutzaufsichtlichen Entscheidungskoordination zwischen Bund und Ländern bilden.

27. Art. 52 (ex Art. 47): Unabhängigkeit

a. Inhalt der Regelung

Während Art. 51 Abs. 1 (ex Art. 46 Abs. 1) DSGVO das Erfordernis begründet, eine unabhängige Aufsichtsbehörde zu installieren, gestaltet Art. 52 (ex Art. 47) DSGVO dieses Unabhängigkeitskriterium näher aus. Seine Präzisierung erfährt die aufsichtsbehördliche Unabhängigkeit vor allem durch die ersten drei Absätze des Art. 52 (ex Art. 47) DSGVO.

aa) Art. 52 Abs. 1 (ex Art. 47 Abs. 1)

Art. 52 Abs. 1 (ex Art. 47 Abs. 1) DSGVO verlangt von der Aufsichtsbehörde das Handeln in „völliger Unabhängigkeit“. Damit bemüht Art. 52 Abs. 1 (ex Art. 47 Abs. 1) DSGVO letztlich die gleiche Wendung wie zuvor bereits

[228] *Rehbinder*, in: Immenga/Mestmäcker (Hrsg.), Wettbewerbsrecht, 5. Aufl., 2014, § 50 GWB, Rn. 8.
[229] *Rehbinder* (Fn. 228), § 50 GWB, Rn. 8.
[230] *Rehbinder* (Fn. 228), § 50 GWB, Rn. 9 m. w. N.

Art. 28 Abs. 1 UAbs. 1 der Datenschutzrichtlinie.[231] Primärrechtlich überwölben Art. 16 Abs. 2 S. 2 AEUV und Art. 8 Abs. 3 GrCh die geforderte Unabhängigkeit der Aufsichtsbehörden.

bb) Art. 52 Abs. 2 (ex Art. 47 Abs. 2)

Den Programmsatz völliger Unabhängigkeit der Aufsichtsbehörde, den Art. 52 Abs. 1 (ex Art. 47 Abs. 1) DSGVO proklamiert, füllt der zweite Absatz der Norm mit Blick auf die einzelnen Mitglieder der Aufsichtsbehörde(n) inhaltlich aus. Er verbürgt den Mitgliedern Weisungsfreiheit und damit ihre sachliche Unabhängigkeit. Diese soll verhindern, dass andere Stellen die Mitglieder der Aufsichtsbehörde(n) inhaltlich bei der Erfüllung ihrer Aufgaben und der Ausübung ihrer Befugnisse steuern. Aus EG 118 (ex EG 92a) DSGVO wird allerdings deutlich, dass diese sachliche Unabhängigkeit der Mitglieder der Aufsichtsbehörde(n) ihre Entscheidungen nicht von gerichtlicher Kontrolle freistellt. Sie verfügen mithin nicht über ein exekutives Letztentscheidungsrecht.
Die Mitglieder der Aufsichtsbehörde müssen ihre Tätigkeit eigenverantwortlich wahrnehmen. Sie dürfen ihre Aufgabenwahrnehmung und Befugnisausübung also nicht selbst aus eigener Entscheidung materiell an eine andere Stelle abgeben.

cc) Art. 52 Abs. 3 (ex Art. 47 Abs. 3)

Dem normativen Konzept gestufter Konkretisierung folgend spezifiziert Absatz 3 die Anforderungen, denen die Mitglieder der Aufsichtsbehörde im Interesse ihrer Unabhängigkeit genügen müssen. Die Vorschrift verbietet es den Mitgliedern der Aufsichtsbehörden, Handlungen vorzunehmen, die nicht mit ihrem Amt vereinbar sind, und eine andere entgeltliche oder unentgeltliche Tätigkeit neben ihrem Amt auszuüben, die mit diesem nicht kompatibel ist. Wie sich aus EG 121 (ex EG 95) DSGVO ergibt, muss der Mitgliedstaat dies durch Rechtsvorschrift[232] regeln.

---

[231] Vgl. auch *von Lewinski*, ZG 2015, 228 (231).
[232] Vgl. zum Verständnis dieser Wendung in der Datenschutz-Grundverordnung oben S. 8.

dd) Art. 52 Abs. 4 (ex Art. 47 Abs. 5)

Damit die Aufsichtsbehörden die ihnen übertragenen Aufgaben und Befugnisse effektiv erfüllen können, legt Art. 52 Abs. 4 (ex Art. 47 Abs. 5) DSGVO den Mitgliedstaaten die Verpflichtung auf, die Aufsichtsbehörden mit hinreichenden personellen, technischen und finanziellen Ressourcen, Räumlichkeiten und Infrastrukturen auszustatten. So will die Vorschrift den tatsächlichen Vollzug des in der Datenschutz-Grundverordnung enthaltenen materiellen Datenschutzrechts verbürgen. Die Bereitstellung ausreichender finanzieller und personeller Mittel vermittelt den Aufsichtsbehörden auch zu einem gewissen Grad institutionelle Unabhängigkeit.[233]
In welcher Handlungsform der Mitgliedstaat dem Handlungsauftrag des Art. 52 Abs. 4 (ex Art. 47 Abs. 5) DSGVO nachkommt, stellt die Datenschutz-Grundverordnung ihm frei.

ee) Art. 52 Abs. 5 (ex Art. 47 Abs. 6)

Der Aufsichtsbehörde gesteht Art. 52 Abs. 5 (ex Art. 47 Abs. 6) DSGVO das Recht zu, das eigene Personal selbst auswählen zu dürfen. Mit seinem zweiten Halbsatz knüpft Absatz 5 (ex 6) ein Stück weit an die vorherigen Absätze an und sieht vor, dass das Personal einzig den Mitgliedern der Aufsichtsbehörde untersteht. Beides müssen die Mitgliedstaaten gewährleisten.

ff) Art. 52 Abs. 6 (ex Art. 47 Abs. 7)

Die „goldenen Zügel“ finanzieller Abhängigkeit können auf die sachliche Unabhängigkeit ausstrahlen. Gleichwohl stellt Art. 52 Abs. 6 (ex Art. 47 Abs. 7) DSGVO – entsprechend den Erwägungen in EG 118 (ex EG 92a) DSGVO – die Aufsichtsbehörde(n) nicht von einer Finanzkontrolle vollkommen frei. Diese darf aber ihre Unabhängigkeit nicht beeinträchtigen. Außerdem muss die Aufsichtsbehörde über eigene, öffentliche, jährliche Haushaltspläne verfügen. Diese beiden Aspekte formuliert Art. 52 Abs. 6 (ex Art. 47 Abs. 7) DSGVO als Handlungsauftrag an die Mitgliedstaaten. So

[233] Vgl. die Aussagen von *Thomé*, VuR 2015, 130 (132).

gesehen sichert Art. 52 Abs. 6 (ex Art. 47 Abs. 7) DSGVO den Aufsichtsbehörden auch eine „gewisse finanzielle Unabhängigkeit“[234].
Wie auch in Absatz 4 (ex Absatz 5) verbindet sich mit der Handlungsanweisung an die Mitgliedstaaten nicht zugleich die Verpflichtung, auch in gesetzgeberischer Hinsicht tätig werden zu müssen.

b. Einordnung in das System der Öffnungsklauseln

Eine Öffnungsklausel enthalten die ersten drei Absätze des Art. 52 (ex Art. 47) DSGVO nicht explizit. Sie knüpfen vielmehr an Art. 51 Abs. 1 (ex Art. 46 Abs. 1) DSGVO an, der seinerseits die Mitgliedstaaten zur Errichtung einer oder mehrerer unabhängiger Aufsichtsbehörden verpflichtet. Art. 52 Abs. 1-3 (ex Art. 47 Abs. 1-3) DSGVO sind daher im Zusammenhang mit Art. 51 Abs. 1 (ex Art. 46 Abs. 1) DSGVO zu lesen. Sie enthalten verbindliche inhaltliche Zielvorgaben für den Mitgliedstaat hinsichtlich der Art und Weise, in dem er die nationalen Aufsichtsbehörde(n) auszugestalten hat. Die Aufsichtsbehörde(n), welche der Mitgliedstaat geschaffen hat, muss den von Art. 52 Abs. 1 bis 3 (ex Art. 47 Abs. 1 bis 3) DSGVO aufgestellten Anforderungen zwingend entsprechen. Mit Art. 52 Abs. 3 (ex Art. 47 Abs. 3) DSGVO korrespondiert Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f) DSGVO. Dieser erfordert eine Regelung des Mitgliedstaats durch Rechtsvorschrift.
Die Absätze 4 bis 6 (ex 5 bis 7) legen dagegen ausdrücklich den Mitgliedstaaten Handlungsanweisungen auf („jeder Mitgliedstaat bzw. die Mitgliedstaaten stellt bzw. stellen sicher, dass…“). Diese in den Absätzen jeweils enthaltenen Öffnungsklauseln sind, bereits aufgrund der sprachlichen Fassung der Normen, obligatorischer Natur.

c. Vergleich zur Datenschutzrichtlinie

Die Datenschutzrichtlinie übte sich im Vergleich zur Datenschutz-Grundverordnung sub specie des Unabhängigkeitsstatus in deutlich stärkerer normativer Zurückhaltung, welche die Aufsichtsbehörden genießen. So findet sich weder für Art. 52 Abs. 3 (ex Art. 47 Abs. 3) DSGVO noch für die Absätze 4 bis 6 (ex 5 bis 7) eine Parallelvorschrift in der Datenschutzrichtlinie.

[234] *Nguyen* (Fn. 157), 266.

Auch eine dem Art. 52 Abs. 2 (ex Art. 47 Abs. 2) DSGVO entsprechende Vorschrift enthält die Datenschutzrichtlinie nicht. Allerdings ist die Weisungsfreiheit Teil des Erfordernisses „völliger Unabhängigkeit", den bereits Art. 28 Abs. 1 RL 95/46/EG forderte.[235] Eine mit EG 118 (ex EG 92a) DSGVO vergleichbare Regelung hält die Datenschutzrichtlinie dagegen in Art. 28 Abs. 3 bereit.

Art. 52 Abs. 1 (ex Art. 47 Abs. 1) DSGVO entspricht weitgehend Art. 28 Abs. 1 RL 95/46/EG. Neu ist nur, dass die Datenschutz-Grundverordnung neben den „Aufgaben" nun auch ausdrücklich auf die „Befugnisse" Bezug nimmt. Dies dient aber wohl vornehmlich der Klarstellung, dass auch die Befugnisausübung in Unabhängigkeit geschieht.

Darüber, wie die Wendung „völliger Unabhängigkeit" zu verstehen ist, bestand lange Zeit keine Einigkeit. Im Jahr 2010 konturierte der EuGH den Begriff und qualifizierte dabei die Unabhängigkeit der deutschen Aufsichtsbehörden als unzureichend.[236] Nachdem die Datenschutz-Grundverordnung den Terminus ebenfalls adaptiert, erlangt die Ausdeutung des EuGH auch für sie Relevanz.[237]

Der EuGH versteht „völlige Unabhängigkeit" in dem Sinne, dass es den für die Überwachung der Verarbeitung personenbezogener Daten im nicht-öffentlichen Bereich zuständigen Kontrollstellen möglich sein muss, „ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, die in Frage stellen könnte, dass die genannten Kontrollstellen ihre Aufgabe erfüllen, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen,."[238] Unterwirft der Staat die Aufsichtsbehörde ihrerseits einer Aufsicht, verletzt dies nach Ansicht des EuGH die Garantie „völliger

[235] So etwa *Brühann*, in: Grabitz/Hilf (Hrsg.), EU-Recht, 57. Erg.-Lfg., 2015, Art. 28 Datenschutzrichtlinie, Rn. 6, der allerdings von der Weisungsfreiheit der *Kontrollstelle* spricht.
[236] EuGH, Urt. v. 9.3.2010 – C-518/07 –, MMR 2010, 352.
[237] Vgl. *Born*, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, 2014, S. 42; *Nguyen* (Fn. 157), 266.
[238] EuGH, Urt. v. 9.3.2010 – C-518/07 – juris, Rn. 30.

Unabhängigkeit“.[239] Nicht eindeutig entnehmen lässt sich dem Urteil aber noch, ob alle Formen von Aufsicht damit unvereinbar sind. Eine Unterscheidung anhand der verschiedenen im deutschen Recht bekannten Formen der Aufsicht – Rechts-, Fach- und Dienstaufsicht – trifft es nicht. In einem späteren Urteil stellte der EuGH jedoch klar, dass auch die Dienstaufsicht nicht in Einklang mit dem Erfordernis „völliger Unabhängigkeit“ der Aufsichtsbehörde(n) steht.[240]

Die Aussagen des EuGH gelten sowohl für die Aufsicht über den öffentlichen als auch über den nicht-öffentlichen Bereich.[241] Folglich zwingt die Rechtsprechung des EuGH dazu, die Aufsichtsbehörden von einer Rechts-, Fach- und Dienstaufsicht freizustellen.

d. Bisherige Ausgestaltung im nationalen Recht

aa) Art. 52 Abs. 1 (ex Art. 47 Abs. 1)

i. Die Zulässigkeit ministerialfreier Räume nach deutschem Recht

Eine Form behördlicher Unabhängigkeit, wie sie der EuGH dem Terminus „völliger Unabhängigkeit“ entnimmt, firmiert in der deutschen Dogmatik unter dem Terminus des „ministerialfreien Raums“. Dies bezeichnet solche Zonen, in denen „Verwaltungsstellen den sachlichen Weisungen des zuständigen Ressortministers nicht oder nur eingeschränkt unterliegen“[242]. Ob bzw. inwieweit derartige ministerialfreie Räume mit dem Grundgesetz vereinbar sind, ist Gegenstand einer lebhaften Diskussion.[243] In bestimmten Grenzen ist die Zulässigkeit ministerialfreier Räume aber anerkannt.[244] Die Ausgestaltung der Aufsichtsbehörden als ministerialfreie Räume ist ebenfalls rechtlich nicht zu beanstanden.[245]

---

[239] EuGH, Urt. v. 9.3.2010 – C-518/07 –, juris, Tenor 1 sowie Rn. 37.
[240] EuGH, Urt. v. 16.10.2012 – C-614/10 –, juris, Rn. 48 ff. Anders aber *Born* (Fn. 237), S. 41; siehe auch die Nachweise bei *Ziebarth*, CR 2013, 60 (66).
[241] *Dammann*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 22, Rn. 20.
[242] *Pieroth*, in: Jarass/Pieroth (Hrsg.), GG, 13. Aufl., 2014, Art. 86, Rn. 3.
[243] Siehe nur *Ibler*, in: Maunz/Dürig (Hrsg.), GG, 52. Erglfg., Art. 86, Rn. 57 ff.
[244] Vgl. die Angaben und Nachweise bei *Pieroth* (Fn. 242), Art. 86, Rn. 4.
[245] Ausführlich *Ziebarth* (Fn. 240), 61 ff.

ii. Reaktion des deutschen Gesetzgebers auf die Rechtsprechung des EuGH zur „völligen Unabhängigkeit“

Auf die Rechtsprechung des EuGH zur „völligen Unabhängigkeit“ reagierte der *Bundesgesetzgeber* mit einer Nachjustierung des BDSG.[246] So hat er insbesondere § 22 Abs. 4 S. 3 BDSG gestrichen und § 22 Abs. 5 S. 1 BDSG geändert (vgl. Art. 1 des Änderungsgesetzes). Mit dieser Änderung des BDSG bezweckte er – neben einer unionsrechtskonformen Anpassung des nationalen Rechts – auch eine Stärkung der Datenschutzaufsicht insgesamt.[247] Damit genügt das BDSG nunmehr den Vorgaben des Art. 28 RL 95/46/EG.[248] Auch die *Länder* haben ihre Datenschutzgesetze angepasst.[249] In Rheinland-Pfalz stellte der Landesgesetzgeber etwa die Konformität mit Art. 28 Abs. 1 RL 95/46/EG dadurch her, dass er der Aufsichtsbehörde (dies ist gemäß § 24 Abs. 1 S. 2 LDSG Rh-Pf der Landesbeauftragte für den Datenschutz und die Informationsfreiheit) die Stellung einer obersten Landesbehörde einräumte (vgl. § 23 Abs. 3 LDSG Rh-Pf).[250]

Genügt das Datenschutzrecht des Bundes und der Länder nunmehr den in der EuGH-Rechtsprechung herausgearbeiteten Erfordernissen zur „völligen Unabhängigkeit“ der Aufsichtsbehörde(n), so entspricht die gegenwärtige Ausgestaltung der aufsichtsbehördlichen Unabhängigkeit auch den insoweit bestehenden Vorgaben der Datenschutz-Grundverordnung; Anpassungsbedarf besteht für das deutsche Recht nicht.

---

[246] Vgl. Das Zweite Gesetz zur Änderung des Bundesdatenschutzgesetzes – Stärkung der Unabhängigkeit der Datenschutzaufsicht im Bund durch Errichtung einer obersten Bundesbehörde vom 25.2.2015, BGBl. I S. 162. Knapp zum diesbezüglichen Gesetzgebungsverfahren sowie den Gesetzesänderungen im Einzelnen, *von Lewinski* (Fn. 231), 232 ff. Siehe auch *Roßnagel*, ZD 2015, 106 ff.

[247] Siehe BT-Drucks. 18/2848, S. 11.

[248] Vgl. auch *von Lewinski* (Fn. 231), 242 f., der zugleich aber auch auf Konfliktpotenziale hinweist.

[249] Siehe hierzu *Born* (Fn. 237), S. 53 ff.

[250] Vgl. LT-Drucks. 15/5135.

bb) Art. 52 Abs. 2 (ex Art. 47 Abs. 2)

Die BfDI ist nach § 22 Abs. 4 S. 2 BDSG unabhängig und nur dem Gesetz unterworfen.[251] In bewusster Anlehnung der Vorschrift an den die Rechtsstellung der Richter regelnden Wortlaut des Art. 97 Abs. 1 GG verdeutlicht das BDSG damit, dass die BfDI sog. sachliche Unabhängigkeit genießt.[252] Diese äußert sich insbesondere darin, dass sie keinerlei Weisungen befolgen muss, welche ihre inhaltliche Tätigkeit betreffen.[253] Diese gesetzliche Ausgestaltung entspricht den Vorgaben des Art. 52 Abs. 2 (ex Art. 47 Abs. 2) DSGVO. Ein Umsetzungsbedarf besteht insoweit nicht.
Inwieweit eine Dienstaufsicht die Unabhängigkeit der Aufsichtsbehörde beeinträchtigt, ist umstritten.[254] Jedoch ist der EuGH der Auffassung, dass eine Dienstaufsicht nicht mit der Richtlinienvorgabe „völliger Unabhängigkeit" (Art. 28 RL 95/46/EG) vereinbar ist.[255] An dieser Sichtweise dürfte der EuGH wohl auch auf Grundlage der Datenschutz-Grundverordnung festhalten. Soweit die nationalen Datenschutzgesetze die Aufsichtsbehörden einer Dienstaufsicht unterstellen, sind diese unionsrechtswidrig.[256]

cc) Art. 52 Abs. 3 (ex Art. 47 Abs. 3)

Die bundesgesetzliche Norm des § 23 Abs. 2 BDSG zur Rechtstellung der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bildet nur einen Teil des Regelungsgehalts ab, den Art. 52 Abs. 3 (ex Art. 47 Abs. 3) DSGVO etabliert, geht teilweise aber auch über ihn hinaus. Das BDSG untersagt der BfDI pauschal die Ausübung einer anderen entgeltlichen Tätigkeit, ohne dass es darauf ankommt, ob diese mit der aufsichtsbehördli-

[251] Selbiges gilt etwa auch für den rheinland-pfälzischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit, § 23 Abs. 1 S. 1 LDSG Rh-Pf.
[252] Siehe *Dammann* (Fn. 241), § 22, Rn. 16 f., vgl. auch *Born* (Fn. 237), S. 56.
[253] *Dammann* (Fn. 241), § 22, Rn. 16.
[254] Siehe die Nachweise bei *Ziebarth* (Fn. 240), S. 66.
[255] Siehe oben auf S. 159.
[256] Vgl. für das BDSG *Dammann*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 23, Rn. 1. Der rheinland-pfälzische Landesbeauftragte für den Datenschutz und die Informationsfreiheit untersteht gemäß § 23 Abs. 1 S. 2 RhPfLDSG der Dienstaufsicht des Landtagspräsidenten. Dementsprechend konfligiert eine Dienstaufsicht über den rheinland-pfälzischen Landesbeauftragten für den Datenschutz und die Informationsfreiheit gemäß § 23 Abs. 1 S. 2 RhPfLDSG mit Art. 52 Abs. 1 und 2 (ex Art. 47 Abs. 1 und 2) DSGVO.

chen Tätigkeit vereinbar ist. Insoweit enthält das BDSG sogar striktere Vorgaben als Art. 52 Abs. 3 (ex Art. 47 Abs. 3) DSGVO.
Ein Verbot, eine unentgeltliche Tätigkeit auszuüben, die mit dem Amt nicht zu vereinbaren ist, enthält § 23 Abs. 2 BDSG hingegen nicht. Ebenfalls legt das BDSG der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nicht auf, sämtliche mit dem Amt nicht zu vereinbarenden Handlungen zu unterlassen.

dd) Art. 52 Abs. 4 (ex Art. 47 Abs. 5)

Eine dem Art. 52 Abs. 4 (ex Art. 47 Abs. 5) DSGVO entsprechende Regelung enthält das BDSG nicht (mehr)[257].

ee) Art. 52 Abs. 5 (ex Art. 47 Abs. 6)

Auch in Bezug auf Art. 52 Abs. 5 (ex Art. 47 Abs. 6) DSGVO hält das BDSG keine analoge Regelung bereit. Die thematisch in diesen Kontext gehörende Vorschrift des § 22 Abs. 5 S. 4 BDSG a. F. wurde gestrichen. Sie wäre mit Art. 52 Abs. 5 (ex Art. 47 Abs. 6) DSGVO nicht zu vereinbaren gewesen.

ff) Art. 52 Abs. 6 (ex Art. 47 Abs. 7)

Das BDSG regelt die Finanzkontrolle der Aufsichtsbehörde(n) nicht. Es besteht also mit Blick auf den Regelungsauftrag der DSGVO auf nationaler Ebene Regelungsbedarf.

28. Art. 53 (ex Art. 48): Allgemeine Bedingungen für die Mitglieder der Aufsichtsbehörde

a. Inhalt der Regelung

aa) Art. 53 Abs. 1 (ex Art. 48 Abs. 1)

Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO etabliert Vorgaben hinsichtlich der Ernennung der Mitglieder der Aufsichtsbehörden – und zwar in zweierlei

[257] Eine ähnliche Regelung bezogen auf Personal- und Sachausstattung enthielt § 22 Abs. 5 S. 3 BDSG a. F.

Hinsicht: Das Ernennungsverfahren muss transparent sein. Transparenz bedeutet in diesem Zusammenhang vor allem Nachvollziehbarkeit für den Bürger.[258] Des Weiteren darf die Ernennung nur durch eine in Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO genannte Stelle erfolgen (vgl. auch den EG 121 [ex EG 95] DSGVO).[259]

bb) Art. 53 Abs. 2 (ex Art. 48 Abs. 2)

Art. 53 Abs. 2 (ex Art. 48 Abs. 2) DSGVO stellt Anforderungen an die Mitglieder der Aufsichtsbehörde. Hierdurch will die Datenschutz-Grundverordnung sicherstellen, dass die Mitglieder geeignet sind, die aufsichtsbehördlichen Aufgaben in angemessener Weise auszuüben.

cc) Art. 53 Abs. 3 (ex Art. 48 Abs. 3)

Die Tatbestände für die Beendigung des Amts eines Mitglieds der Aufsichtsbehörde enthält Art. 53 Abs. 3 (ex Art. 48 Abs. 3) DSGVO.

dd) Art. 53 Abs. 4 (ex Art. 48 Abs. 4)

Art. 53 Abs. 4 (ex Art. 48 Abs. 4) DSGVO knüpft an den vorangegangenen Absatz an und konkretisiert die Möglichkeit einer Amtsenthebung der Mitglieder der Aufsichtsbehörden. Ein zulässiger Enthebungsgrund liegt hiernach zunächst dann vor, wenn das Mitglied der Aufsichtsbehörde eine schwere Verfehlung begangen hat. Den Begriff der „schweren Verfehlung“ definiert die Datenschutz-Grundverordnung nicht. Mit Blick auf die Stärkung der aufsichtsbehördlichen Unabhängigkeit sind an die Annahme einer solchen „schweren Verfehlung“ erhöhte Anforderungen zu stellen. Eine „schwere Verfehlung“ liegt wohl jedenfalls dann vor, wenn sie das Vertrauen in den Amtsträger dergestalt erschüttert, dass er seine Aufgaben nicht länger glaubhaft wahrnehmen kann. Dies ergibt ein Vergleich zum zweiten möglichen Grund für eine Amtsenthebung. Dieser ist nämlich dann gegeben, wenn das Mitglied die Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht

[258] Vgl. auch die eine andere Thematik betreffende Norm des Art. 5 Abs. 1 lit. a (ex Art. 5 Abs. 1 lit. a) DSGVO.
[259] Zur Auswahl des Personals der Aufsichtsbehörde siehe den dritten Satz des EG 121 (ex 95).

mehr erfüllt. Diese in Bezug genommenen Voraussetzungen ergeben sich dabei aus Art. 53 Abs. 2 (ex Art. 48 Abs. 2) DSGVO.
Keine Aussage trifft Art. 53 Abs. 4 (ex Art. 48 Abs. 4) DSGVO zu derjenigen Stelle, die die Entlassung vornimmt. Auch Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO regelt nicht die für die Entlassung zuständige Stelle. Der Gedanke des actus contrarius streitet aber dafür, die Entlassung durch die ernennende Stelle (Art. 53 Abs. 1 [ex Art. 48 Abs. 1] DSGVO) vornehmen zu lassen.

b. Einordnung in das System der Öffnungsklauseln und Regelungsaufträge

aa) Art. 53 Abs. 1 (ex Art. 48 Abs. 1)

Der Regelungsauftrag, den Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO und EG 121 (ex EG 95) DSGVO den Mitgliedstaaten mit auf den Weg gibt, ist obligatorischer Natur. Ausweislich des Art. 54 Abs. 1 lit. c (ex Art. 49 Abs. 1 lit. c) DSGVO muss die Regelung durch Rechtsvorschrift getroffen werden.[260] Den Mitgliedstaaten kommt allerdings ein Spielraum zu, wie sie das Ernennungsverfahren genau ausgestalten und welche der in Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO genannten Stellen sie mit der Ernennung beauftragen.

bb) Art. 53 Abs. 2 (ex Art. 48 Abs. 2)

Art. 53 Abs. 2 (ex Art. 48 Abs. 2) DSGVO verlangt, anders insoweit als Abs. 1, von den Mitgliedstaaten nicht explizit eine eigene Regelung. Allerdings ergibt sich aus Art. 54 Abs. 1 lit. b (ex Art. 49 Abs. 1 lit. b) DSGVO, dass die Mitgliedstaaten die von Art. 53 Abs. 2 (ex Art. 48 Abs. 2) DSGVO an die Mitglieder der Aufsichtsbehörde gestellten Anforderungen durch Rechtsvorschrift regeln müssen (vgl. auch EG 121 [ex EG 95] DSGVO). Eine nationale Regelung muss insbesondere die Voraussetzungen des Art. 53 Abs. 2 (ex Art. 48 Abs. 2) DSGVO konkretisieren und operabel gestalten.

[260] Vgl. zum Verständnis dieser Wendung in der Datenschutz-Grundverordnung oben S. 8.

cc) Art. 53 Abs. 3 (ex Art. 48 Abs. 3)

Art. 53 Abs. 3 (ex Art. 48 Abs. 3) DSGVO formuliert keinen ausdrücklichen Auftrag an die Mitgliedstaaten, die Beendigungsgründe gesetzlich vorzusehen. Jedoch geht die Vorschrift davon aus, dass sich die Amtsenthebung nach mitgliedstaatlichem Recht bestimmt. Der Mitgliedstaat muss somit jedenfalls die Amtsenthebung regeln. Außerdem korrespondiert Art. 54 Abs. 1 lit. d und f (ex Art. 49 Abs. 1 lit. d und f) DSGVO partiell mit Art. 53 Abs. 3 (ex Art. 48 Abs. 3) DSGVO und legt dem Mitgliedstaat die Verpflichtung auf, die Amtszeit des Mitglieds sowie die Regeln für die Beendigung des Beschäftigungsverhältnisses durch Rechtsvorschrift zu regeln.

dd) Art. 53 Abs. 4 (ex Art. 48 Abs. 4)

Auch Art. 53 Abs. 4 (ex Art. 48 Abs. 4) DSGVO gibt dem Mitgliedstaat nicht explizit auf, gesetzgeberisch tätig zu werden. Mit Blick auf den engen thematischen Zusammenhang zu Art. 53 Abs. 2 und 3 (ex Art. 48 Abs. 2 und 3) DSGVO und unter Berücksichtigung der EG 8 und 121 (ex EG 6a und 95) DSGVO ist jedoch eine gesetzliche Ausgestaltung durch das nationale Recht geboten.

c. Vergleich zur Datenschutzrichtlinie

Eine dem Art. 53 Abs. 1 bis 4 (ex Art. 48 Abs. 1 bis 4) DSGVO jeweils entsprechende Vorschrift enthält die Datenschutzrichtlinie nicht.

d. Bisherige Ausgestaltung im nationalen Recht

aa) Art. 53 Abs. 1 (ex Art. 48 Abs. 1)

Gegenwärtig sieht § 22 Abs. 1 S. 1 BDSG die Wahl der BfDI durch den Deutschen Bundestag *ohne Aussprache* vor. Den Vorschlag macht die Bundesregierung. Die Ernennung erfolgt schließlich gemäß § 22 Abs. 1 S. 3 BDSG durch den Bundespräsidenten als das Staatsoberhaupt[261] i. S. d. Art. 53 Abs. 1 Spstr. 3 (ex Art. 48 Abs. 1 Spstr. 3) DSGVO.

[261] *Herzog*, in: Maunz/Dürig (Hrsg.), GG, 54. Erg.-Lfg., Art. 54, Rn. 3. Ausführlich *Nettesheim*, § 61 Amt und Stellung des Bundespräsidenten in der grundgesetzlichen Demokratie, in: Isen-

i. Arbeitsteiligkeit des Ernennungs- und Auswahlverfahrens

Ob das Verfahren der Ernennung auch arbeitsteilig in der Weise erfolgen kann, dass das Vorschlagsrecht und die Ernennung unterschiedlichen Personen zufällt, lässt Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO offen. Wäre es anders, wäre das deutsche Verfahren einer Trias aus Vorschlag – Wahl – Ernennung mit unterschiedlichen Beteiligten mit der Datenschutz-Grundverordnung nicht vereinbar.
Ihrem Sinn nach will die Datenschutz-Grundverordnung den Mitgliedstaaten in Art. 53 (ex Art. 48) DSGVO weitgehende Gestaltungsfreiheit einräumen, insbesondere auf die verfassungsrechtlichen Besonderheiten jedes Mitgliedstaats Rücksicht nehmen (vgl. EG 117 S. 2 [ex EG 92 S. 2] DSGVO). Unter diesem Gesichtspunkt ist eine Personenidentität aller an dem Verfahren der Ernennung Beteiligten nicht notwendig.

iii. Verzicht auf eine Aussprache

Dass das gegenwärtige Verfahren der Ernennung ohne Aussprache erfolgt, verträgt sich nicht ohne Weiteres mit dem Gebot der Transparenz des Verfahrens, welches Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO statuiert. Der Verzicht auf eine Aussprache ist von dem Gedanken getragen, die Person des zu Ernennenden vor einer persönlichen Beschädigung in der Öffentlichkeit zu bewahren und damit die Dignität des Amtes nicht zu beschädigen. Die gleichen Beweggründe veranlassen die Verfassung dazu, den Bundespräsidenten ohne Aussprache zu wählen. Dieses Prozedere stellt die Person des künftigen Amtsinhabers, nicht eine Tätigkeit oder Agenda in den Mittelpunkt.
Der Gedanke der Transparenz des Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO bezieht sich nach seinem Sinn nicht auf die Transparenz im Hinblick auf die *Person* des zu Ernennenden, sein Amtsverständnis oder eine Programmatik. Sie bezieht sich vielmehr auf das *Verfahren*, in dem die Ernennung erfolgt. Dies bedingt nicht zwingend eine öffentliche Aussprache über die Motive zur Ernennung. Insbesondere verbände sich damit womöglich das Risiko, dass ein Ernennungsverfahren, das auf programmatische Aussagen eines künftigen

see/Kirchhof (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, 3. Aufl., 2005, Rn. 12 ff.

Amtsinhabers rekurriert, inhaltlich die Unabhängigkeit des Mitglieds der Aufsichtsbehörde gefährdet. Denn an seinen inhaltlichen Aussagen vor Amtsantritt müsste sich jeder Amtsinhaber in der Öffentlichkeit auch messen lassen.

iv. Zwischenergebnis

Das gegenwärtige Ernennungsverfahren für die BfDI genügt den Vorgaben des Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO; ein Änderungsbedarf für den nationalen Gesetzgeber besteht nicht.[262]

bb) Art. 53 Abs. 2 (ex Art. 48 Abs. 2)

Das BDSG hält keine dem Art. 53 Abs. 2 (ex Art. 48 Abs. 2) DSGVO entsprechende Regelung bereit. Es regelt in § 22 Abs. 1 S. 2 BDSG alleine das (Mindest-)Alter;[263] die Art. 53 Abs. 2 und Art. 49 Abs. 1 lit. b (ex Art. 48 Abs. 2 und Art. 49 Abs. 1 lit. b) DSGVO rufen aber insbesondere auch nach materiellen Anforderungen (z. B. fachliche Qualifikation). Da der Mitgliedstaat insoweit eine gesetzliche Regelung treffen muss, besteht gesetzgeberischer Handlungsbedarf.

cc) Art. 53 Abs. 3 (ex Art. 48 Abs. 3)

Die Amtszeit der BfDI regelt § 22 Abs. 3 BDSG. Die Beendigungstatbestände für das Amt enthält § 23 Abs. 1 S. 2 und 3 BDSG. Die Norm bildet eben jene Beendigungstatbestände ab, die auch Art. 53 Abs. 3 (ex Art. 48 Abs. 3 DSGVO vorsieht. Folglich ist eine Anpassung des BDSG mit Blick auf Art. 53 Abs. 3 (ex Art. 48 Abs. 3) BDSG nicht erforderlich.

---

[262] Siehe aber auch *Kahler* (Fn. 146), 72 f. der eine Wahl bzw. Ernennung der Landesbeauftragten für Datenschutz und die Informationsfreiheit durch die *Landesparlamente* für nicht ausreichend mit Blick auf die Datenschutz-Grundverordnung hält.

[263] Es lässt sich hinterfragen, ob das Mindestalter von 35 Jahren – weil pauschal ohne Rücksicht auf die Person des Bewerbers auf das Lebensalter abstellend – mit dem unionsrechtlichen Verbot der Altersdiskriminierung im Einklang zu bringen ist. Die Verordnung knüpft an Ausbildung, Erfahrung und Fähigkeiten an. Ein Mindestlebensalter ist zugleich aber Teil der Lebenserfahrung, die Voraussetzung für eine fachliche Bewältigung der Aufgabe ist.

dd) Art. 53 Abs. 4 (ex Art. 48 Abs. 4)

Die Gründe, auf deren Grundlage die BfDI ihres Amtes enthoben werden kann, spezifiziert § 23 Abs. 1 S. 3 BDSG. Hiernach bedarf es Gründe, „die bei einer Richterin auf Lebenszeit oder einem Richter auf Lebenszeit die Entlassung aus dem Dienst rechtfertigen". Die insoweit maßgebliche Regelung im Deutschen Richtergesetz markiert § 21 DRiG.[264] § 21 DRiG bildet die nach Art. 53 Abs. 4 (ex Art. 48 Abs. 4) DSGVO zulässigen Amtsenthebungsgründe nicht zutreffend ab; vor allem sind die Gründe für eine Amtsenthebung in der Norm, verglichen mit Art. 53 Abs. 4 (ex Art. 48 Abs. 4) DSGVO, zu weit gefasst. Hinsichtlich der Amtsenthebungsgründe trifft den Gesetzgeber folglich die Pflicht, das BDSG dem Art. 53 Abs. 4 (ex Art. 48 Abs. 4) DSGVO entsprechend anzupassen.
Die zuständige Stelle für die Entlassung der BfDI ist gemäß § 23 Abs. 1 S. 3 BDSG der Bundespräsident. Insoweit besteht für den nationalen Gesetzgeber kein Änderungsbedarf.

29. Art. 54 (ex Art. 49): Errichtung der Aufsichtsbehörde

a. Art. 54 Abs. 1 (ex Art. 49 Abs. 1)

Art. 54 Abs. 1 (ex Art. 49 Abs. 1) DSGVO spezifiziert die Vorgaben des Art. 53 (ex Art. 48) DSGVO zur Ausgestaltung der Aufsichtsbehörde. Er formuliert gesetzgeberische Handlungsaufträge an die Mitgliedstaaten („jeder Mitgliedstaat sieht durch Rechtsvorschriften Folgendes vor:"),[265] die der Mitgliedstaat zu erfüllen hat. Der materielle Gehalt der jeweils zu erlassenden Regelung ergibt sich zum größten Teil in detaillierter Weise aus den umliegenden Normen. Teilweise enthalten die Tatbestände des Art. 54 Abs. 1 (ex Art. 49 Abs. 1) DSGVO aber auch eigene inhaltliche Regelungen.

---

[264] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 23, Rn. 2, weisen aber einschränkend darauf hin, dass eine entsprechende Anwendung des jeweiligen Tatbestands in § 21 DRiG überhaupt möglich sein muss.
[265] Vgl. zum Verständnis dieser Wendung in der Datenschutz-Grundverordnung oben S. 8.

Norm des Art. 54 Abs. 1 (ex Art. 49 Abs. 1) DSGVO	Korrespondierende inhaltlicher Anknüpfungspunkt in der DSGVO	Eigene weiter gehende inhaltliche Regelung?
Lit. a	Art. 51 Abs. 1 (ex Art. 46 Abs. 1) DSGVO	(-)
Lit. b	Art. 53 Abs. 2 (ex Art. 48 Abs. 2) DSGVO	(-)
Lit. c	Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO	(-)
Lit. d	Art. 53 Abs. 3 (ex Art. 48 Abs. 3) DSGVO	(+), s. u.
Lit. e	(-)	(+), s. u.
Lit. f	Art. 52 Abs. 3 (ex Art. 47 Abs. 3) DSGVO Art. 53 Abs. 3 und 4 (ex Art. 48 Abs. 3 und 4) DSGVO	(+), s. u.

aa) Art. 54 Abs. 1 lit. d (ex Art. 49 Abs. 1 lit. d)

Mit Aussagen zur Amtszeit der Mitglieder der Aufsichtsbehörden trifft Art. 54 Abs. 1 lit. d (ex Art. 49 Abs. 1 lit. d) DSGVO eine ergänzende inhaltliche Regelung. Die Norm fordert, die Amtszeit der Mitglieder der Aufsichtsbehörden durch Rechtsvorschrift vorzusehen; die Mindestdauer muss vier Jahre betragen. Bis auf die Berücksichtigung dieser Maßgabe sind die Mitgliedstaaten bei der Festlegung der Amtszeit frei. Zusätzlich trifft Art. 54 Abs. 1 lit. d (ex Art. 49 Abs. 1 lit. d) DSGVO im zweiten Halbsatz eine Ausnahmeregelung für die Handhabung der ersten Amtszeit nach Inkrafttreten der Datenschutz-Grundverordnung.
Die Datenschutzrichtlinie 95/46/EG traf keine Aussage zur Amtszeit der Mitglieder der Aufsichtsbehörden. Dagegen sieht § 22 Abs. 3 S. 1 BDSG vor, dass die Amtszeit der BfDI fünf Jahre beträgt. Diese Regelung genügt den Anforderungen des Art. 54 Abs. 1 lit. d (ex Art. 49 Abs. 1 lit. d) DSGVO, sodass der nationale Gesetzgeber in Deutschland insoweit keine Anpassung vornehmen muss.

bb) Art. 54 Abs. 1 lit. e (ex Art. 49 Abs. 1 lit. e)

Art. 54 Abs. 1 lit. e (ex Art. 49 Abs. 1 lit. e) DSGVO überlässt es dem Mitgliedstaat festzulegen, ob und wie oft eine Wiederernennung der Mitglieder

der Aufsichtsbehörde möglich ist. Allerdings verlangt die Norm den Mitgliedstaaten ab, eine diesbezügliche Regelung zu treffen.
Auch zu diesem Aspekt traf die bisherige Datenschutzrichtlinie keine Aussage. Das BDSG gestattet in § 22 Abs. 3 S. 2 BDSG eine einmalige Wiederwahl der BfDI.[266] Folglich zwingt Art. 54 Abs. 1 lit. e (ex Art. 49 Abs. 1 lit. e) DSGVO die Bundesrepublik Deutschland nicht zur Änderung der aktuellen Rechtslage.

cc) Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f)

Der Regelungsauftrag des Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f) DSGVO nimmt auf Art. 52 Abs. 3 (ex Art. 47 Abs. 3) DSGVO Bezug. Dieser bezieht sich in seinem Anwendungsbereich aber nur auf die laufende Amtszeit der Mitglieder der Aufsichtsbehörden. Insoweit reicht Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f) DSGVO weiter: Die Norm erfasst auch mit dem Amt unvereinbares Verhalten, das *nach* der Amtszeit liegt. Für den Mitgliedstaat entsteht dadurch jedenfalls zusätzlicher Regelungsbedarf.
Sowohl die Datenschutzrichtlinie als auch das BDSG treffen bisher keine den Vorgaben des Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f) DSGVO entsprechende Aussage im Hinblick auf *nach* der Amtszeit des Beauftragten liegendes Verhalten. Diese Lücke muss der deutsche Gesetzgeber bis zum Inkrafttreten der Datenschutz-Grundverordnung schließen. Anleihe könnte er hier bei den neuen Regelungen zur Karenzzeit für Bundesminister und Parlamentarische Staatssekretäre nehmen.[267]
In persönlicher Hinsicht geht Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f) DSGVO ebenfalls weiter als Art. 52 Abs. 3 (ex Art. 47 Abs. 3) DSGVO und Art. 53 Abs. 3 und 4 (ex Art. 48 Abs. 3 und 4) DSGVO: Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f) DSGVO adressiert auch die Bediensteten der Aufsichtsbehörde.
Das BDSG sieht für die Bediensteten der Aufsichtsbehörde bislang keine korrespondierenden Vorschriften vor. Allerdings enthält das Bundesbeamtengesetz diesbezügliche Regelungen, welche auch für die Bediensteten der BfDI

[266] Eine Wiederwahl zu einem späteren Zeitpunkt kommt jedoch in Betracht; *Dammann* (Fn. 241), § 22, Rn. 13.
[267] Vgl. hierzu *Scheffczyk*, ZRP 2015, 133.

gelten (vgl. § 22 Abs. 5 S. 3 BDSG). Die Entlassungsgründe ergeben sich dabei aus den §§ 30 ff. BBG. Die Entlassungsgründe für die Bediensteten der Aufsichtsbehörde müssen nicht den inhaltlichen Vorgaben des Art. 53 Abs. 3 und 4 (ex Art. 48 Abs. 3 und 4) DSGVO genügen, da die Bediensteten dort nicht angesprochen sind. Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f) DSGVO verlangt insoweit daher lediglich, dass das mitgliedstaatliche Recht die Entlassungsgründe gesetzlich fixiert. Allerdings muss auch geregelt werden, wer für die Entlassung zuständig ist. Um die unionsrechtlich gebotene Unabhängigkeit zu wahren, ist es angezeigt, diese Zuständigkeit in die Hände der BfDI zu legen. Insoweit bedarf es wohl einer Regelung, die § 129 BBG entspricht, um die Unabhängigkeit auch insoweit sicherzustellen, als nur der Bundesdatenschutzbeauftragte selbst (oder das in EG 121 S. 3 [ex EG 95 S. 3] DSGVO erwähnte neutrale Gremium)[268] das Personal des Bundesdatenschutzbeauftragten entlassen kann. Folglich besteht insoweit für den nationalen Gesetzgeber Umsetzungsbedarf.

Schließlich verlangt Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f) DSGVO dem nationalen Gesetzgeber ab, „die Bedingungen im Hinblick auf die Pflichten […] der Bediensteten jeder Aufsichtsbehörde, die Verbote von Handlungen, beruflichen Tätigkeiten und Vergütungen während und nach der Amtszeit, die mit diesen Pflichten unvereinbar sind“ festzulegen. Derartige Regelungen finden sich in den §§ 60 ff. BBG und dem Bundesdisziplinargesetz. Den deutschen Gesetzgeber trifft insofern wohl keine Anpassungspflicht.

b. Art. 54 Abs. 2 (ex Art. 49 Abs. 2)

Art. 54 Abs. 2 (ex Art. 49 Abs. 2) DSGVO ordnet eine Verschwiegenheitsverpflichtung der Mitglieder und Bediensteten jeder Aufsichtsbehörde gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten an. Enthält das Unionsrecht keine entsprechende Regelung, muss der Mitgliedstaat tätig werden, um durch die Verpflichtung auf die Verschwiegenheit die sachangemessene Aufgabenerfüllung der Aufsichtsbehörde zu sichern. Der Anwendungsbereich der

[268] Art. 52 Abs. 5 DSGVO fügt sich mit EG 121 DSGVGO nur bedingt zusammen. Beide scheinen nicht aufeinander abgestimmt. Im Kollisionsfall gebührt dem verfügenden Teil der Datenschutz-Grundverordnung der Vorrang.

Norm erstreckt sich sowohl auf die Dienstzeit als auch auf die Zeit nach Beendigung des Amtes.
Eine ähnliche Regelung enthielt bereits Art. 28 Abs. 7 RL 95/46/EG. Ausführlich gestaltet gegenwärtig § 23 Abs. 4 bis 6 BDSG die Verschwiegenheitsverpflichtung der BfDI aus – vor allem durch Absatz 5. Für die Bediensteten hält das BDSG keine derart ausführlichen Regelungen bereit. Das Gesetz adressiert sie einzig in § 23 Abs. 4 S. 2 BDSG. Allerdings begründet § 67 BBG (i. V. m. § 22 Abs. 5 S. 3 BDSG) eine Verschwiegenheitspflicht für die bediensteten Beamten der BfDI. Eine Überführung einer § 67 BBG entsprechenden Regelung in das BDSG ist nicht angezeigt. Allenfalls empfiehlt es sich, zum Zwecke der Klarstellung einen Verweis auf die Norm in das BDSG einzufügen. Ein durch Art. 54 Abs. 2 (ex Art. 49 Abs. 2) DSGVO hervorgerufener Änderungsbedarf besteht insoweit nicht.

30. Art. 55 (ex Art. 51): Zuständigkeit

a. Inhalt der Regelung

Art. 55 (ex Art. 51) DSGVO steckt die Zuständigkeitsgrenzen der Aufsichtsbehörden ab. Er koppelt sie an die mitgliedstaatliche Gebietshoheit. Daraus ergeben sich zugleich mittelbar auch Zuständigkeitsüberlappungen. Insbesondere Verarbeitungstätigkeiten nicht-öffentlicher Stellen können die Gebietshoheit mehrerer Mitgliedstaaten berühren. Für diesen Fall ordnet Art. 56 (ex Art. 51a) DSGVO das Konzept einer federführenden Aufsichtsbehörde sowie ein umfassendes Verfahren der Zusammenarbeit und Kohärenz (Art. 60 ff. [ex Art. 54a ff.] DSGVO) an.
Eine wichtige Ausnahme formuliert Art. 55 Abs. 2 (ex Art. 51 Abs. 2) DSGVO: Macht der Mitgliedstaat von der Öffnungsklausel in Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO[269] Gebrauch, erlaubt er also die Verarbeitung von Daten im öffentlichen Interesse, ist (nur) die Aufsichtsbehörde des betroffenen Mitgliedstaates zuständig. Das Verfahren der Zusammenarbeit in Art. 60 ff. (ex Art. 54a ff.) DSGVO sowie das Prinzip der zentralen Anlauf-

[269] Dazu S. 27 ff.

stelle (vgl. EG 128 [ex EG 98] DSGVO) finden dann keine Anwendung (s. hierzu S. 242). Denn entscheidend für die Beurteilung der Rechtmäßigkeit der Verarbeitung sind dann primär mitgliedstaatliche Rechtsnormen. Hierüber können alleine die Aufsichtsbehörden des entsprechenden Mitgliedstaates befinden. Das macht auch EG 128 (ex EG 98) DSGVO deutlich.

Die Vorschrift des Art. 55 Abs. 2 (ex Art. 51 Abs. 2) DSGVO folgt einer einleuchtenden Logik: Gestalten die Mitgliedstaaten aufgrund ihres nationalen Spielraums ihr Recht individuell, entsteht kein Harmonisierungsbedarf, den das Zusammenarbeits- und Kohärenzverfahren befriedigen könnte. Die Regelung ist die konsequente Folge des unionsrechtlichen Respekts vor der mitgliedstaatlichen Regelungsautonomie. Von Art. 55 Abs. 2 (ex Art. 51 Abs. 2) DSGVO kann auf die Mitgliedstaaten ein strategischer Anreiz ausgehen, möglichst umfänglich von den Öffnungsklauseln für ihre Behörden und sonstigen öffentlichen Stellen Gebrauch zu machen, um sich zumindest insoweit aus dem „Klammergriff" des unionsrechtlichen Abstimmungsbedarfs zu befreien.

Auch die Überwachung der von *Gerichten* im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen nimmt Art. 55 Abs. 3 (ex Art. 51 Abs. 3) DSGVO ausdrücklich von dem Zuständigkeitsradius der Aufsichtsbehörden aus. Dies soll – ausweislich des zweiten Satzes des EG 20 (ex EG 16a) DSGVO – die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschließlich ihrer Beschlussfassung schützen. Die Mitgliedstaaten können jedoch besondere Stellen in ihrem Justizsystem mit der Aufsicht über diese Datenverarbeitungsvorgänge betrauen (EG 20 S. 3 [ex EG 16a S. 3] DSGVO).

b. Einordnung in das System der Öffnungsklauseln

Ob Art. 55 Abs. 3 (ex Art. 51 Abs. 3) DSGVO als (ungeschriebene) fakultative Öffnungsklausel oder Bereichsausnahme zu qualifizieren ist, ist unklar. Die besseren Gründe sprechen für ein Verständnis als Bereichsausnahme: Die Datenschutz-Grundverordnung nimmt insoweit ihren Regelungsanspruch zurück und nimmt die originär rechtsprechende Tätigkeit von dem Regelungsregime der Verordnung aus.

c. Vergleich zur Datenschutzrichtlinie

Die Datenschutzrichtlinie sah keine dem Art. 55 Abs. 3 (ex Art. 51 Abs. 3) DSGVO entsprechende, generelle Ausnahme von der Zuständigkeit der Kontrollstelle für die Tätigkeit der Gerichte im Rahmen ihrer justiziellen Tätigkeit vor (vgl. Art. 28 DSRL). Hingegen nimmt sie die Verarbeitung personenbezogener Daten durch den Staat im strafrechtlichen Bereich bereits vom Anwendungsbereich aus (Art. 3 Abs. 2 Spstr. 2 a. E. DSRL). Da die Richtlinie 95/46/EG nicht unmittelbar galt, hielt sie auch keine dem Art. 55 Abs. 2 (ex Art. 51 Abs. 2) DSGVO korrespondierende Ausnahmeregelung vor.

d. Bisherige Ausgestaltung im nationalen Recht

Das BDSG unterwirft Bundesgerichte der Kontrolle der BfDI nur, soweit sie in Verwaltungsangelegenheiten tätig werden (§ 24 Abs. 3 BDSG). Die Regelung entspricht Art. 55 Abs. 3 (ex Art. 51 Abs. 3) DSGVO und kann daher bestehen bleiben.[270] Entsprechende Regelungen enthalten auch die Landesdatenschutzgesetze, wie z. B. § 24 Abs. 2 RhPfDSG, wonach die Gerichte der Kontrolle des Landesbeauftragten für den Datenschutz und die Informationsfreiheit nur unterliegen, soweit sie in Verwaltungsangelegenheiten tätig werden. Eine eigene Kontrollstruktur der Gerichte selbst sieht weder das Bundes- noch das Landesrecht vor.

31. Art. 56 (ex Art. 51a): Zuständigkeit der federführenden Aufsichtsbehörde

a. Inhalt der Regelung

Art. 56 (ex Art. 51a) DSGVO greift das Konzept der Lead Authority auf. Die federführende Aufsichtsbehörde sorgt bei grenzüberschreitenden Verarbei-

[270] Ggf. ist sie aber nicht in einem die Umsetzung der Datenschutz-Grundverordnung normierenden BDSG-neu zu verankern, sondern in den weiterbestehenden Regelungen des nationalen Datenschutzrechtes für Fälle, welche die Datenschutz-Grundverordnung nicht erfasst. Denn die Datenschutz-Grundverordnung regelt ihre Unanwendbarkeit für diesen Bereich bereits selbst. Soweit der Bundesgesetzgeber ein mit Auffangfunktion ausgestattetes nationales Datenschutzrecht vorsieht, wäre eine entsprechende Ausnahme der Zuständigkeit in dieses zu überführen.

tungen für eine Koordinierung der betroffenen Aufsichtsbehörden (Art. 4 Abs. 22 DSGVO). Die Kommission favorisierte demgegenüber ursprünglich – in konsequenter Umsetzung des One-Stop-Shop-Prinzips – die Main-Establishment-Rule. Danach wäre alleine die Aufsichtsbehörde zuständig, in deren Hoheitsgebiet sich die verantwortliche Stelle niedergelassen hat (Art. 51 Abs. 2 DSGVO-KOM). Bei mehreren Niederlassungen einer verantwortlichen Stelle wäre dann diejenige Aufsichtsbehörde allein zuständig, in deren Mitgliedstaat die Hauptniederlassung gelegen ist. Bereits das Europäische Parlament hat dies mit dem Ziel der Gewährung eines effektiven Rechtsschutzes für den von der Datenverarbeitung betroffenen Einzelnen zugunsten des Lead Authority-Konzepts aufgegeben.[271]

Art. 56 (ex Art. 51a) DSGVO enthält keine Öffnungsklauseln. Da die entsprechenden Regelungen in der Verordnung grundsätzlich abschließend sind,[272] besteht kein Umsetzungsbedarf. Anderes gilt allenfalls im Hinblick auf die innerstaatliche Umsetzung des Modells als Folge eines Nebeneinanders mehrerer Aufsichtsbehörden.[273]

b. Vergleich zur Datenschutzrichtlinie

Art. 28 Abs. 6 DSRL kannte kein dem Art. 56 (ex Art. 51a) DSGVO vergleichbares, differenziertes Regelungsmuster. Er sah lediglich vor, dass eine Kontrollstelle die Kontrollstelle eines anderen Mitgliedstaats um die Ausübung ihrer Befugnisse ersuchen kann (UAbs. 1 S. 2) sowie, dass die Kontrollstellen für die zur Erfüllung ihrer Kontrollaufgaben notwendige gegenseitige Zusammenarbeit sorgen, insbesondere durch den Austausch sachdienlicher Informationen (UAbs. 2).

---

[271] Vgl. *Nguyen* (Fn. 157), 266.

[272] Soweit nicht Ausnahmen nach Art. 85, 91 (ex Art. 80, 85) DSGVO für Journalismus und Religionsgemeinschaften nutzbar gemacht werden.

[273] Siehe zur Diskussion um die Abstimmung der innerstaatlichen Zuständigkeit S. 219.

32. Art. 57 (ex Art. 52): Aufgaben

a. Inhalt der Regelung

Art. 57 (ex Art. 52) DSGVO regelt die Aufgaben der Aufsichtsbehörden abschließend[274] und unmittelbar durch das Unionsrecht. In weiten Teilen verweist er dabei auf weitere Artikel der Datenschutz-Grundverordnung, welche die einzelnen Aufgaben etablieren bzw. spezifizieren. Sie enthalten teilweise Öffnungsklauseln, die mittelbar auf die in Art. 57 Abs. 1 (ex Art. 52 Abs. 1) DSGVO geregelten Aufgaben einwirken.

Alleine Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab) DSGVO formuliert einen unmittelbaren Vorbehalt zugunsten des Mitgliedstaates. Er gibt ihnen einen Beratungsauftrag der Aufsichtsbehörden mit auf den Weg: Sie müssen im Einklang mit dem Recht des Mitgliedstaates das nationale Parlament, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung beraten (englisch: „each supervisory authority shall on its territory [,…] (c [ex ab]) advise …“). Dabei handelt es sich nicht lediglich um ein Beratungsrecht, sondern – entsprechend der Funktion der Festlegung in Art. 57 (ex Art. 52) DSGVO – um eine Beratungspflicht. Dafür streitet auch der Wortlaut der Klausel; „muss“ bzw. „shall“ bezeichnet generell eine Verpflichtung, nicht nur ein Recht. So ist eine Vielzahl von Aufgaben des Art. 57 Abs. 1 (ex Art. 52 Abs. 1) DSGVO – wie die, sich mit Beschwerden von betroffenen Personen zu befassen lit. f (ex lit. b) – nur als echte Rechtspflicht denkbar. Ein Beratungsanspruch der in Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab) DSGVO genannten Institutionen korrespondiert mit der Beratungspflicht nicht notwendig. Vielmehr adressiert der unionsrechtliche Pflichtenkatalog alleine die Aufsichtsbehörden als Pflichtenträger, ohne ein damit korrespondierendes Recht der Begünstigten zu etablieren.

[274] Wobei Abs. 1 lit. v (ex k) durch seine offene Formulierung gleichwohl Raum lässt für in lit. a bis u (ex jb) nicht angesprochene Aufgaben.

Art. 57 Abs. 2 (ex Art. 52 Abs. 4) DSGVO knüpft inhaltlich an Absatz 1 lit. f (ex Absatz 1 lit. b) an und zielt darauf, das Einreichen von Beschwerden zu vereinfachen. Die Vorschrift enthält keine Öffnungsklausel.
Keine Öffnungsklausel enthält auch Art. 57 Abs. 3 (ex Art. 52 Abs. 5) DSGVO. Die Norm ist lediglich beschreibender Natur und legt dem Mitgliedstaat keine Pflichten auf. Diese ergeben sich bereits aus der Norm selbst. Selbiges gilt auch für Art. 57 Abs. 4 (ex Art. 52 Abs. 6) DSGVO.

b. Einordnung in das System der Öffnungsklauseln

Regelungsspielraum belässt Art. 57 Abs. 1 (ex Art. 52 Abs. 1) DSGVO den Mitgliedstaaten nur im Hinblick auf lit. c (ex lit. ab). Der Spielraum, den Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab) DSGVO den Mitgliedstaaten einräumt, bezieht sich dabei nicht auf das „Ob“, sondern auf das „Wie“ der Beratungsmaßnahmen – die Öffnungsklausel ist damit grundsätzlich obligatorischer Natur. Die Beratungsmaßnahmen folgen in ihrer Ausgestaltung dem Muster, den der Nationalstaat als Teil seiner Institutionenordnung für das Verhältnis zwischen Parlament, Regierung sowie anderen Einrichtungen vorsieht. Der Mitgliedstaat ist also nicht gezwungen, bestehende nationalstaatliche Regelungen zur Erfüllung der aufsichtsbehördlichen Beratungspflicht zu verletzen. Die Wendung „im Einklang“ ist auch insoweit bewusst defensiver als die denkbare Alternativformulierung „nach Maßgabe“ (des Rechts des Mitgliedstaats).
Soweit ersichtlich, löst die Beratungspflicht der Aufsichtsbehörden keine Friktionen mit dem nationalen Verfassung- oder Verwaltungsrecht aus, die einer nationalstaatlichen Regelung bedürfen. Über die Verankerung einer Beratungspflicht hinaus braucht die Bundesrepublik Deutschland insoweit nicht unbedingt zusätzliche Regelungen zu treffen; sie darf es aber.

c. Vergleich zur Datenschutzrichtlinie

Auf der Grundlage der Richtlinie 95/46/EG waren die Kontrollstellen bei der Ausarbeitung von Rechtsverordnungen oder Verwaltungsvorschriften anzuhören, die den Schutz der Rechte und Freiheiten von Personen bei der Verarbeitung personenbezogener Daten betreffen (Art. 28 Abs. 2 DSRL). Die Datenschutzrichtlinie sah also ein Anhörungsrecht vor. Legt man Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab) DSGVO dahin gehend aus, dass diesem auch

ein Anspruch auf Beratung innewohnt, geht die Datenschutz-Grundverordnung insoweit über die Datenschutzrichtlinie hinaus. Die Beratungspflicht ohne korrespondierenden Anspruch deckt sich jedoch grundsätzlich mit dem Anhörungsrecht.

d. Bisherige Ausgestaltung im nationalen Recht

Die Aufgaben der BfDI hat der Bundesgesetzgeber bislang überwiegend in § 26 Abs. 2 BDSG, die der Aufsichtsbehörden der Länder in § 38 BDSG geregelt.

aa) § 38 BDSG

§ 38 Abs. 1 S. 2 BDSG legt der Aufsichtsbehörde die Aufgabe auf, die verantwortliche Stelle sowie den betrieblichen Datenschutzbeauftragten zu beraten und zu unterstützen (Abs. 1 S. 2).[275] Die Beratung und Unterstützung kann sowohl proaktiv als auch im Nachgang an eine gestellte Anfrage erfolgen.[276] § 38 Abs. 1 S. 1 BDSG schränkt den Beratungsumfang ein: Sie erfolgt mit Rücksicht auf die typischen Bedürfnisse der Normadressaten.
Beratungsadressaten sind auf Basis des Normwortlauts jedenfalls die verantwortliche Stelle und der betriebliche Datenschutzbeauftragte. Ob die Aufsichtsbehörde auch den Betroffenen beraten darf, ist weniger klar. Der Betroffene ist qua Normwortlauts nicht Adressat des § 38 Abs. 1 S. 2 BDSG. Mangels Regelungslücke scheidet auch eine analoge Anwendung der Norm aus:[277] Für die Rechtsstellung der Betroffenen hat der Bund in § 21 BDSG mit dem Anrufungsrecht eine grundsätzlich abschließende Regelung getroffen; ähnlich verhält es sich im Hinblick auf die landesrechtlichen Regelungen.[278] Ob eine Beratung des Betroffenen gleichwohl zulässig ist, hängt da-

[275] Sehr ausführlich zur aufsichtsbehördlichen Beratung *Born* (Fn. 237), S. 220 ff.
[276] *Born* (Fn. 237), S. 221.
[277] *Born* (Fn. 237), S. 238.
[278] Siehe insbesondere § 24 Abs. 1 S. 1 BlnDSG; § 23 BbgDSG; § 27 Abs. 1 S. 1 BremDSG; § 30 Abs. 1 S. 1 DSG M-V; § 22 Abs. 1 S. 1 DSG NRW; § 24 Abs. 1 S. 1 Rh-PfLDSG; § 26 Abs. 1 S. 1 SaarlDSG; § 22 Abs. 1 S. 1 DSG LSA; § 39 Abs. 2 S. 1 SchlHDSG.

von ab, wie man die grundgesetzlichen Vorgaben in Bezug auf staatliche Informationstätigkeit versteht.[279]
Ob § 38 Abs. 1 S. 2 BDSG eine Beratungspflicht der Aufsichtsbehörde statuiert und in der Konsequenz ein Anspruch der Beratungsadressaten auf Beratung besteht, ist umstritten.[280] Weitet man den Blick und bezieht in die Betrachtung auch die übrigen Normen des BDSG ein, so folgt aus § 38 Abs. 1 S. 2 BDSG jedenfalls für diejenigen Fälle, in denen das BDSG dem betrieblichen Datenschutzbeauftragten das Recht gewährt oder ggf. sogar die Pflicht auferlegt, sich an die Aufsichtsbehörde zu wenden, auch ein korrespondierender Anspruch auf eine Beratung.[281]

bb) § 26 Abs. 2 BDSG

§ 26 Abs. 2 S. 3 BDSG gesteht der BfDI das Recht zu, sich jederzeit an den Deutschen Bundestag zu wenden. Daneben genießt die BfDI nach § 26 Abs. 3 S. 1 BDSG das Recht, die Bundesregierung und den in § 12 Abs. 1 BDSG genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes zu geben und sie in Fragen des Datenschutzes zu beraten. Umgekehrt sieht das BDSG in § 26 Abs. 2 S. 1 besondere Pflichten der BfDI gegenüber dem Parlament und der Regierung vor: Sie hat auf Anforderung des Deutschen Bundestages oder der Bundesregierung, Gutachten zu erstellen und Berichte zu erstatten.[282]

---

[279] Vgl. einerseits *von Lewinski*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 38 BDSG, Rn. 23, und andererseits *Born* (Fn. 237), S. 238 f.
[280] Eine Beratungspflicht verneinend etwa *Petri* (Fn. 161), § 38, Rn. 37. Eine solche bejahend dagegen *Gola/Klug/Körffer* (Fn. 159), § 38, Rn. 7a.
[281] Vgl. *Hillenbrand-Beck*, Aufsichtsbehörden, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 816 (Rn. 96).
[282] Für den Kompetenzbereich der Länder sehen die Datenschutzgesetze ähnliche Regelungen vor. Nach § 24 Abs. 4 RhPfDSG hat der Landesbeauftragte für den Datenschutz und die Informationsfreiheit das Recht, den Landtag, die Landesregierung und ihre Mitglieder sowie die übrigen öffentlichen Stellen zu beraten. Nach § 24 Abs. 5 S. 1 RhPfDSG können der Landtag und seine Ausschüsse sowie die Landesregierung den Landesbeauftragten für den Datenschutz und die Informationsfreiheit mit der Erstattung von Gutachten und Berichten zu Fragen des Datenschutzes betrauen. Es besteht also ebenfalls ein Beratung- bzw. Anhörungsrecht sowie eine Pflicht, Gutachten und Berichte zu erstellen.

i. Beratungsadressaten

Das BDSG sieht als Adressat des Beratungsrechtes die Bundesregierung sowie sonstige Stellen nach § 12 Abs. 1 BDSG i. V. m. § 2 Abs. 1 BDSG vor. § 2 Abs. 1 S. 1 BDSG erfasst erweiterte, der Exekutive zuordenbare Stellen, wie die Behörden des Bundes. Auch bundesunmittelbare Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie deren Vereinigungen – ungeachtet ihrer Rechtsform – fallen hierunter. Gleichzeitig ist hiervon auch das nationale Parlament, mithin der Bundestag (samt Fraktionen) erfasst.[283] Denn § 2 Abs. 1 S. 1 BDSG erstreckt den Kreis der Beratungsadressaten auf andere öffentlich-rechtlich organisierte Einrichtungen des Bundes. Damit erfasst das BDSG einen Adressatenkreis, auf den auch die Datenschutz-Grundverordnung die Beratungspflicht erstreckt.

Ob es sich mit der Datenschutz-Grundverordnung vereinbaren lässt, dass das BDSG auch die Judikative zu den Beratungsadressaten zählt, ist nicht ganz gesichert. So erfasst § 26 Abs. 3 S. 1, § 12 Abs. 1, § 2 Abs. 1 S. 1 BDSG die Organe der Rechtspflege. Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab) DSGVO nimmt die *Judikative* demgegenüber nicht explizit mit in den Kreis der Beratungsadressaten auf. Allenfalls lässt sich die Judikative unter „andere Einrichtungen und Gremien“ fassen. Dem widerstreitet aber, dass sowohl die Legislative als auch die Spitze der Exekutive explizit genannt sind. Die Wendung „andere Einrichtungen und Gremien“ bezieht sich wohl nur auf solche Stellen, die diesen beiden Staatsgewalten (oder nur der Exekutive) zuzuordnen sind. Erfasst sind Stellen der Justiz dann allenfalls insoweit, als sie Verwaltungsaufgaben wahrnehmen.

Andererseits lässt sich aus Art. 55 Abs. 3 (ex Art. 51 Abs. 3) DSGVO im Umkehrschluss entnehmen, dass die Aufsichtsbehörden grundsätzlich auch für die Überwachung von Gerichten zuständig sind, soweit nicht der Bereich originärer gerichtlicher Rechtsprechungstätigkeit berührt ist. Es ist nicht ersichtlich, warum Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab) DSGVO hier eine weiter gehende Ausnahme vorsehen und die Gerichte insgesamt aus der Beratungspflicht ausnehmen sollte. Diese sind folglich auch mögliche Beratungsadressaten. Der Adressatenkreis, den das BDSG in seinem § 26 vorsieht,

[283] *Gola/Klug/Körffer* (Fn. 144), § 2, Rn. 17a.

lässt sich insoweit mit den Vorgaben der Datenschutz-Grundverordnung vereinbaren.
Insoweit darf die Bundesrepublik Deutschland die Regelung in ihrem nationalen Datenschutzrecht auch neben der ausdifferenzierten Regelung der Datenschutz-Grundverordnung als Konkretisierung des Art. 57 Abs.1 lit. c (ex Art. 52 Abs. 1 lit. ab) DSGVO aufrechterhalten.

ii. Weiter und undefinierter Adressatenkreis – Beratungspflicht vs. Beratungsrecht

Das BDSG fasst den Kreis derer, welche die BfDI im Rahmen ihres Anhörungsrechts beraten darf, unkonturiert weit. Dies birgt bei Annahme eines Anspruchs auf Beratung nach der Datenschutzgrundverordnung die Gefahr in sich, dass die Beratungsaufgaben die Möglichkeiten der Aufsichtsbehörde übersteigen. Jedoch lässt sich aus der Datenschutz-Grundverordnung kein genereller Beratungsanspruch entnehmen. Der Kreis der Beratungsadressaten kann daher grundsätzlich weit gefasst werden. Erforderlich ist lediglich eine Begrenzung mit Bezug auf solche Stellen, hinsichtlich derer eine echte Beratungspflicht besteht, d. h. die einen Anspruch auf Beratung geltend machen können.
Folglich ist die Trennung des BDSG hinsichtlich solcher Stellen, bei denen die BfDI ein *Anhörungs- (bzw. Beratungs-)recht* hat und solcher, die eine *Beratung* verlangen können, mit den Grundlinien der Datenschutz-Grundverordnung vereinbar. Gleichwohl empfiehlt es sich, die Regelungen im BDSG dem Grundgedanken der Datenschutz-Grundverordnung anzupassen, die von einer Beratungspflicht (ohne korrespondierenden Anspruch) ausgeht.
Insoweit sollte das BDSG in einem ersten Schritt den Kreis derjenigen Stellen regeln, hinsichtlich derer die BfDI ein Recht, aber keine einklagbare Pflicht, zur Beratung hat. § 12 Abs. 1 BDSG i. V. m. § 2 Abs. 1 BDSG bildet hierfür eine taugliche Grundlage. Ein solches Beratungsrecht enthält § 26 Abs. 3 BDSG. Das BDSG sollte ferner bestimmen, welchen dieser Stellen auf deren Verlangen hin eine Beratung zu erteilen ist. Hierfür ist wiederum der Kreis der in § 26 Abs. 3 S. 1 BDSG genannten Stellen tauglich.

Ob eine *ipso iure* bestehende Beratungspflicht aufgenommen werden soll, bleibt dem Gesetzgeber überlassen. Dies scheint jedoch wenig sinnvoll, da die BfDI bereits durch das Beratungsrecht über einen weit reichenden Handlungsspielraum verfügt.

33. Art. 58 (ex Art. 53): Befugnisse

Während Art. 57 (ex Art. 52) DSGVO den Kreis der Aufgaben der Aufsichtsbehörde absteckt, regelt Art. 58 (ex Art. 53) DSGVO deren Befugnisse. In dieser Trennung spiegelt sich das rechtsstaatliche Bedürfnis nach einer klaren ordnungsrechtlichen Binnenkategoriendifferenzierung zwischen Aufgabe und Befugnis.

a. Regelungsreichweite des Art. 58 Abs. 1 - 3 (ex Art. 53 Abs. 1 - 1c)

Der Befugniskatalog des Art. 58 Abs. 1 bis 3 (ex Art. 53 Abs. 1 bis 1c) DSGVO wirft eine Grundfrage auf: Folgen die Befugnisse der Aufsichtsbehörde bereits aus der Datenschutz-Grundverordnung selbst oder ist zunächst ein nationaler Umsetzungsakt erforderlich? Ersteres ist der Fall.
Dies lässt sich aus der Entstehungsgeschichte ablesen. Der Entwurf der Kommission formulierte noch: „Jede Aufsichtsbehörde ist befugt“, Art. 53 Abs. 1 DSGVO-E KOM – hiernach sollte die Befugnis unmittelbar aus der Datenschutz-Grundverordnung folgen. Etwas unklar ist der Entwurf des Europäischen Parlaments, der niederlegt, dass „[j]ede Aufsichtsbehörde […] im Einklang mit dieser Verordnung befugt“ ist. Dies ließe sich auch so verstehen, dass die Befugnis dem nationalen Recht zu entnehmen und selbst „im Einklang mit der Verordnung“ auszuüben ist. Jedenfalls der Entwurf des Rates sah dann explizit ein Umsetzungsbedürfnis vor. Er ordnete an: „Jeder Mitgliedstaat regelt durch Gesetz, dass seine Aufsichtsbehörde mindestens über die folgenden Untersuchungsbefugnisse verfügt“. Gleichwohl haben die Parteien des Trilog-Verfahrens diesen Regelungsansatz wieder aufgegeben. In der DSGVO heißt es in Abs. 1 nun: „Each supervisory authority shall have all of the following investigative powers“ bzw. in der deutschen Sprachfassung: „Jede Aufsichtsbehörde verfügt über sämtliche folgenden Untersuchungsbefugnisse“. Damit distanziert sich die Endfassung der Datenschutz-Grundverordnung von dem Entwurf des Rates: Die Befugnisse müssen nicht

erst eingeräumt werden, sondern bestehen unmittelbar aus der Datenschutz-Grundverordnung selbst heraus. Gleiches gilt für Abs. 2 und 3 (ex Abs. 1b und Abs. 1c). Auch ein systematischer Vergleich mit Art. 58 Abs. 5 (ex Art. 53 Abs. 3) DSGVO führt zu demselben Ergebnis. Dort gibt die Verordnung – anders als in Abs. 1 – den Mitgliedstaaten einen unmissverständlichen Regelungsauftrag mit auf den Weg. Die Befugnis der Aufsichtsbehörden, Verstöße gegen die Datenschutz-Grundverordnung selbst vor die Gerichte der Mitgliedstaaten zu bringen, sieht danach „jeder Mitgliedstaat (…) durch Rechtsvorschriften vor".

Die Regelung der Befugnisse der Aufsichtsbehörden durch die Datenschutz-Grundverordnung selbst entspricht auch der Mission der Verordnung, das Datenschutzrecht und dessen Vollzug innerhalb der Union zu vereinheitlichen. Dieses Ziel formuliert EG 129 S. 1 (ex EG 100 S. 1) DSGVO für die Befugnisse der Aufsichtsbehörden explizit.[284] Weite mitgliedstaatliche Umsetzungsspielräume der Aufsichtsbehörden im Bereich der Eingriffsbefugnisse wären ihm abträglich. Einerseits könnten Unternehmen und Einzelne nicht mehr davon ausgehen, dass die Aufsichtsbehörden in der gesamten Union mit den gleichen Kompetenzen ausgestattet sind, sondern müssten stets nationale Gesetze und damit auch Rechtsexperten in den Blick nehmen. Andererseits wäre eine Abstimmung in Kooperations- und Kohärenzverfahren unbillig erschwert. Denn den Aufsichtsbehörden der anderen Mitgliedstaaten wäre es nicht möglich, z. B. Entscheidungen über ein Vorgehen im EDA stets den gleichen Rahmen an Befugnissen der zur Umsetzung von Entscheidungen berufenen nationalen Aufsichtsbehörden zugrunde zu legen. Diesen Unwägbarkeiten beugt eine Festlegung der Befugnisse unmittelbar in der Datenschutz-Grundverordnung wirksam vor. Ein Umsetzungsbedarf und eine Umsetzungsmöglichkeit bestehen daher grundsätzlich nicht.

Nur im Rahmen einzelner Befugnisse hat das Unionsrecht Einfallstore für das nationale Recht geöffnet. Das gilt v. a. für Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db) DSGVO: Der Zugang der Aufsichtsbehörde zu den Geschäftsräumen des Verantwortlichen und des Auftragsverarbeiters erfolgt nur gemäß

[284] „Um die einheitliche Überwachung und Durchsetzung dieser Verordnung in der gesamten Union sicherzustellen, sollten die Aufsichtsbehörden in jedem Mitgliedstaat dieselben Aufgaben und wirksamen Befugnisse haben".

dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats. Die Regelung ist Ausdruck divergierender Auffassungen in den Mitgliedstaaten darüber, ob für derartige Maßnahmen stets ein Gerichtsbeschluss erforderlich ist.[285] Der Bundesrepublik Deutschland steht es auf der Grundlage dieser Öffnungsklausel frei, die mit Blick auf Art. 13 GG als verfassungsrechtlich zwingend oder sachgerecht wahrgenommenen mitgliedstaatlichen Anforderungen an den Richtervorbehalt für den Zugang zu Geschäftsräumen zu regeln. Das insoweit im nationalen Recht bereits bestehende Regime kann daher bestehen bleiben.

b. Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db)

aa) Inhalt der Regelung

Art. 58 Abs. 1 bis 3 (ex Art. 53 Abs. 1 bis 1c) DSGVO regelt die Untersuchungs-, Abhilfe-, Genehmigungs- und beratenden Befugnisse der Aufsichtsbehörde. Im Rahmen dieser Befugnisse kommt dem Mitgliedstaat grundsätzlich kein Regelungsspielraum zu.[286] Abs. 1 lit. f (ex Abs. 1 lit. db) DSGVO verleiht der Aufsichtsbehörde die Befugnis, gemäß dem Verfahrensrecht der Union oder dem Verfahrensrecht des Mitgliedstaats Zugang zu den Geschäftsräumen, einschließlich aller Datenverarbeitungsanlagen und -geräte, des Verantwortlichen und des Auftragsverarbeiters zu erhalten.

bb) Einordnung in das System der Öffnungsklauseln

Bei Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db) DSGVO handelt es sich um eine fakultative Öffnungsklausel: Die Mitgliedstaaten können von ihr Gebrauch machen, müssen es aber nicht. Aus dem nationalen Recht, insbesondere aufgrund des Schutzes der Unverletzlichkeit der Wohnung aus Art. 13 GG, kann sich eine verfassungsrechtliche Handlungspflicht ergeben.

---

[285] Vgl. *Nguyen* (Fn. 157), (269).

[286] Zu beachten ist, dass nach Art. 90 Abs. 1 (ex Art. 84 Abs. 1) DSGVO die Mitgliedstaaten die Befugnisse der Aufsichtsbehörden nach Art. 58 Abs. 1 lit. e und f (ex Art. 53 Abs. 1 lit. da und db) DSGVO gegenüber Berufsgeheimnisträgern oder einer gleichwertigen Geheimhaltungspflicht Unterliegenden besonders regeln können, soweit die betroffenen Daten im Rahmen der zur Geheimhaltung verpflichtenden Tätigkeit erworben wurde.

cc) Vergleich zur Datenschutzrichtlinie

Zutrittsrechte sah die Datenschutzrichtlinie nur im Ansatz vor. Art. 28 Abs. 3 Spstr. 1 RL 95/46/EG bestimmte, dass die Kontrollstelle über Untersuchungsbefugnisse, wie das Recht auf Zugang zu Daten, verfügt.

dd) Bisherige Ausgestaltung im nationalen Recht

Das BDSG trennt zwischen den Rechten der Bundesdatenschutzbeauftragten für den Datenschutz und die Informationsfreiheit (im Hinblick auf die Verarbeitung von Daten durch öffentliche Stellen des Bundes) und den Rechten der (durch Landesrecht einzurichtenden) Aufsichtsbehörden für die Verarbeitung von Daten durch nicht-öffentliche Stellen.
Hinsichtlich öffentlicher Stellen des Bundes sieht es deren Verpflichtung vor, Zutritt zu allen Diensträumen sowie Auskunft zu Fragen und Einsicht in alle Unterlagen, insbesondere in die gespeicherten Daten und in die Datenverarbeitungsprogramme, zu gewähren (§ 24 Abs. 1 und Abs. 4 S. 2 Nr. 1, 2 BDSG). Hinsichtlich nicht-öffentlicher Stellen bestimmt § 38 Abs. 4 BDSG, dass die von der Aufsichtsbehörde mit der Kontrolle beauftragten Personen befugt sind, während der Betriebs- und Geschäftszeiten Grundstücke und Geschäftsräume der Stelle zu betreten und dort Prüfungen und Besichtigungen vorzunehmen.

ee) Umsetzung und Anpassung

i. Umsetzungsrahmen nach der DSGVO

Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db) DSGVO lässt die Frage unbeantwortet, ob sich der nationale Umsetzungsspielraum nur auf *formale* Kriterien, wie einen gerichtlichen Beschluss, oder auch auf *materielle*, wie das Vorliegen eines (hinreichenden) Verdachtes bezieht.

(1) Formelle Voraussetzungen

Die Gestaltung der formellen Voraussetzungen für die Zugangsverschaffung ist zweifelsfrei von dem Spielraum der Öffnungsklausel gedeckt, den die Verordnung dem nationalen Recht belässt. Denn seine Existenz gründet sich gerade auf die unterschiedlichen formellen Voraussetzungen der Mitglied-

staaten für den Zugang zu einem Grundstück oder das Betreten eines Hauses.[287] Diese Zielrichtung kommt insbesondere in der Formulierung „procedural law“ („Verfahrensrecht“) zum Ausdruck. Entsprechend gestattet EG 129 S. 5 (ex EG 100 S. 5) DSGVO den Mitgliedstaaten explizit, das Erfordernis einer gerichtlichen Anordnung vorzusehen.[288] Der allgemeinen Schutzklausel des Abs. 4 (ex Abs. 2) dürfte diesbezüglich keine darüber hinausgehende Bedeutung zukommen.

(2) Materielle Voraussetzungen

Ob die Mitgliedstaaten auch materielle Voraussetzungen für den Zutritt regeln dürfen, ist weniger gesichert. Dies folgt bereits daraus, dass sowohl der Entwurf der Kommission als auch der des Parlamentes materielle Voraussetzungen (wenn auch in geringem Umfang) selbst regelten.[289] Jedenfalls für die ursprünglichen Entwürfe der Kommission und des Rates lässt sich daraus wohl schließen, dass diese materiellen Voraussetzungen abschließend wären.
Andererseits enthalten beide Entwürfe einen Vorbehalt nicht nur zugunsten des „Verfahrensrecht[es] der Mitgliedstaaten“, sondern allgemein hinsichtlich des „Recht[es] der Mitgliedstaaten“. Dies konfligiert jedoch mit dem Ziel der Vollharmonisierung auch im Bereich der Eingriffsbefugnisse: Die Datenschutz-Grundverordnung nimmt grundsätzlich für sich in Anspruch, den Datenschutz und die konfligierenden Interessen selbst in einen ausgewogenen Ausgleich zu bringen.
Wie die Datenschutz-Grundverordnung selbst[290] auszulegen ist, die insoweit der Fassung des Rates entspricht, ist unklar. Einerseits enthält die Befugnis, sich Zutritt zu verschaffen, als solche keinerlei Hinweise auf materielle Vo-

[287] Siehe auch *Nguyen* (Fn. 157), 269.
[288] “Investigatory powers as regards access to premises should be exercised in accordance with specific requirements in national procedural law, such as the requirement to obtain a prior judicial authorisation.”
[289] Die Kommission sah in Art. 53 Abs. 2 lit. b DSGVO-E vor, dass der Zugang nur zulässig ist, „sofern Grund zu der Annahme besteht, dass dort Tätigkeiten ausgeführt werden, die gegen diese Verordnung verstoßen“. Das Parlament hingegen sah vor, dass der Zugang „ohne Vorankündigung“ erfolgen darf; eine Gefahr des Verstoßes sah es nicht vor.
[290] Die Datenschutz-Grundverordnung hat im Vergleich zum Trilog-Ergebnis noch eine Anpassung erfahren: Nunmehr verweist sie nicht mehr auf das Unionsrecht an sich, sondern auf das Verfahrensrecht des Unionsrechts.

raussetzungen – weder positiver noch negativer Art. Gleichzeitig unterwirft sie auch die sonstigen Eingriffsbefugnisse nach Abs. 1 lit. a - e (ex Abs. 1 lit. a - da) keinen materiellen Schranken. Vielmehr sieht sie nur bei der Zutrittsverschaffungsbefugnis ausnahmsweise einen Vorbehalt zugunsten des Rechts der Mitgliedstaaten vor, der dem Wortlaut nach nur für das „procedural law", also das Verfahrensrecht gilt. Hiernach dürften die Mitgliedstaaten materielle Voraussetzungen nicht regeln.

Diese Auslegung sieht sich jedoch mehreren Einwänden ausgesetzt: Zum einen ist nicht gesichert, dass sich „procedural law" tatsächlich alleine auf das Verfahrensrecht im rein formalen Sinne bezieht oder ob darunter nicht auch Vorgaben zum Beispiel hinsichtlich eines Verdachtsgrades zu fassen sind. Schon im deutschen Recht lassen sich die Grenzen nicht immer klar ziehen. Die deutsche Strafprozessordnung regelt etwa nicht nur das Erfordernis, einen Durchsuchungsbeschluss zu erlassen (§ 105 Abs. 1 StPO), sondern auch dessen materielle Voraussetzungen (§§ 102 f. StPO). Auch im europäischen Vergleich verschwimmen die Grenzen. So kennt zum Beispiel das englische Verfahrensrecht Institutionen wie das *statute of limitations*, das bei uns als Verjährungsrecht klassisches materielles Zivilrecht ist. Die Grenzen sind also nicht trennscharf.

Zum anderen legt auch die Formulierung des EG 129 S. 3 (ex EG 100 S. 3) DSGVO ein weites Verständnis des Begriffs „Verfahrensrecht" nahe. Danach sollen die Befugnisse der Aufsichtsbehörden in Übereinstimmung mit den angemessenen Verfahrensgarantien des Unionsrechts und des nationalen Rechts ausgeübt werden. Diese Verfahrensgarantien beziehen sich aber nicht auf den Rechtsschutz nach der Ausführung, sondern – wie die weitere Aufzählung „unparteilich, fair und in angemessener Zeit" deutlich macht – auf die Durchführung selbst. Unter diese Verfahrensgarantien fasst der anschließende Satz, also EG 129 S. 4 (ex EG 100 S. 4) DSGVO, auch den Grundsatz der Verhältnismäßigkeit: „in particular each measure should be appropriate, necessary and proportionate […]". Der Grundsatz der Verhältnismäßigkeit als eine Verfahrensgarantie legt ein weites Verständnis des Begriffs „Verfahrensrecht" nahe.

Diese Gesamtschau ergibt, dass der Begriff des „Verfahrensrechts" in Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db) DSGVO auch materielle Voraussetzungen für eine Zutrittsverschaffung umfasst.

Welche Rolle insoweit noch der allgemeinen Schutzklausel nach Art. 58 Abs. 4 (ex Art. 53 Abs. 2) DSGVO zukommt, bleibt dann unklar. Diese erfasst nicht nur den Rechtsschutz gegen die (erfolgten) Maßnahmen ("propriate safeguards, including effective judicial remedy and due process"), sondern auch geeignete Garantien, die sich auf die Durchführung der Maßnahme selbst beziehen.

ii. Umsetzungsleitlinien und -rahmen

Manche der Regelungsspielräume, welche die Datenschutz-Grundverordnung für die Zukunft eröffnet, schöpft das deutsche Recht in seiner gegenwärtigen Form bereits aus. Bei anderen deckt sich der Regelungsinhalt mit dem, den die Datenschutz-Grundverordnung etabliert.

Das BDSG eröffnet namentlich heute die Möglichkeit einer unangekündigten Betriebsprüfung ohne Gerichtsbeschluss (§ 38 Abs. 4 BDSG). Die Regelung verfolgt das Ziel, einer Beweisverschleierung entgegenzuwirken. Hiervon abzuweichen, scheint nicht angezeigt. Dies gilt jedenfalls dann, wenn Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db) DSGVO so auszulegen ist, dass er sich nur auf (reine [!]) Geschäftsräume bezieht. Denn dann greift nach der Lesart des BVerfG weder der Richtervorbehalt des Art. 13 Abs. 2 GG noch die Schrankenregelung des Art. 13 Abs. 7 GG (für sonstige Eingriffe).[291] Vielmehr ist die reine Betretung kein Eingriff i. S. v. Art. 13 Abs. 7 GG und deshalb nur an Art. 2 Abs. 1 GG zu messen[292] und in den Grenzen des § 38 Abs. 4 S. 1 BDSG verfassungsrechtlich zulässig.

Problematisch kann dies alleine deshalb sein, weil das Recht zur Zutrittsverschaffung über ein reines Betretungs- und Besichtigungsrecht der Verwaltung hinausgeht – insofern als der Verantwortliche Zutritt auch zu Datenverarbeitungsanlagen und -geräten gewähren muss. Jedoch scheint hier das BVerfG einen auch für derartige Ausdehnungen des Betretungsrechtes offenen Ansatz gewählt zu haben: In den Mittelpunkt seiner Ausführungen stellt es „die sachlichen Notwendigkeiten der Verwaltung des modernen Staates"[293] und nimmt auf diese besonders Bedacht. Hierunter zählt als Äquivalent zur Buchprüfung

[291] BVerfGE 32, 54 (73, 75f.); *Gola/Klug/Körffer* (Fn. 159), § 38, Rn. 22.
[292] Ibid.; auch BVerwGE 121, 345, 351 = NJW 2005, 454 (455 f.).
[293] BVerfGE 32, 54 (75).

bei der Außenprüfung des Finanzamtes (§§ 193 f. AO) bei der Datenschutzprüfung die Einsicht in Datenverarbeitungsanlagen und -geräte. Eine andere Auslegung ist deshalb nicht angezeigt.
Erfasste die Zutrittsbefugnis der Aufsichtsbehörden jedoch auch Wohnräume oder geschäftlich genutzte Wohnräume, wäre die Lage gänzlich anders zu beurteilen. Die Verschaffung des Zutritts zu Wohnungen und gemischt genutzten Wohnungen (insbesondere auch zu Datenverarbeitungsanlagen und -geräten) stellt eine Durchsuchung i. S. d. Art. 13 Abs. 2 GG dar und löst den Richtervorbehalt aus.
Die deutsche Fassung des Art. 58 Abs. 1 lit. f (ex Art. 53 Abs.1 lit. db) DSGVO ist auf Geschäftsräume beschränkt. Nach der englischen Fassung ist dies weniger eindeutig. Denn danach sind „any premises of the controller and the processor“ erfasst. Problematisch ist aber, dass weder „controller“ noch „processor“ nach den Legaldefinitionen in Art. 4 Abs. 7 und 8 (ex Art. 4 Abs. 5 und 6) DSGVO einen zwingenden wirtschaftlichen Bezug haben, so dass nicht sicher ist, dass tatsächlich (gemischt genutzte) Wohnungen ausgeschlossen sind. Auch der sachliche Anwendungsbereich klärt dies nicht. Denn die grundsätzliche Anwendbarkeit nach Art. 2 Abs. 1 sowie die Bereichsausnahme durch Art. 2 Abs. 2 lit. c (ex Art. 2 Abs. 2 lit. d) DSGVO („durch natürliche Personen zu persönlichen oder familiären Zwecken“) schließen nicht aus, dass Daten in einschlägiger Weise in (gemischt genutzten) Wohnungen verarbeitet werden. Insoweit bestünde – nach dem Gedanken effektiver Durchsetzung des unionalen Datenschutzrechts – grundsätzlich eine Verpflichtung des nationalen Gesetzgebers, dem Datenschutzbeauftragten die Möglichkeit einzuräumen, eine richterliche Anordnung für ein Betreten von Wohnungen zum Zwecke der Zutrittsverschaffung in (gemischt genutzte) Wohnungen beantragen zu können. Deutschland darf dann aber – auch wenn man die englischsprachige Fassung zugrunde legt – von seinem verfahrensrechtlichen Regelungsspielraum Gebrauch machen.
Gleichzeitig dürften die Beschränkungen hinsichtlich der Geschäftszeiten (§ 38 Abs. 4 S. 1 BDSG) jedenfalls dem Begriff des „Verfahrensrechts“ unterfallen und entsprechend beibehalten werden. Auch die vorgenommene Beschränkung auf das zur Erfüllung der der Aufsichtsbehörde übertragenen Aufgaben Erforderliche ist mit der Datenschutz-Grundverordnung vereinbar. Dies unterfällt noch der Regelungsbefugnis aus Art. 58 Abs. 1 lit. f (ex

Art. 53 Abs. 1 lit. db) DSGVO, jedenfalls aber der Schutzklausel nach Art. 58 Abs. 4 (ex Art. 53 Abs. 2) DSGVO (jeweils i. V. m. EG 129 S. 4 [ex EG 100 S. 4] DSGVO).
Welcher Verdachtsgrad die Aufsichtsbehörden zur Zutrittsverschaffung berechtigt, liegt primär in der Regelungsbefugnis des nationalen Gesetzgebers, soweit er eine wirksame Durchsetzung des Unionsrechts sicherstellt.

c. Art. 58 Abs. 3 lit. b (ex Art. 53 Abs. 1c lit. aa)

aa) Inhalt der Regelung

Auch Art. 58 Abs. 3 lit. b (ex Art. 53 Abs. 1c lit. aa) DSGVO eröffnet den Mitgliedstaaten einen Regelungsspielraum: Die Aufsichtsbehörde hat das Recht, zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an das nationale Parlament, die Regierung des Mitgliedstaats oder im Einklang mit dem Recht des Mitgliedstaates an sonstige Einrichtungen und Stellen sowie an die Öffentlichkeit zu richten.

bb) Einordnung in das System der Öffnungsklauseln

Auch bei Art. 58 Abs. 3 lit. b (ex Art. 53 Abs. 1c lit. aa) DSGVO handelt es sich um eine fakultative Öffnungsklausel. Die Mitgliedstaaten müssen die sonstigen Einrichtungen und Stellen nicht weiter konkretisieren. Tun sie dies nicht, bleibt die Befugnis der Aufsichtsbehörde nach der Datenschutz-Grundverordnung unbeschränkt.

cc) Vergleich zur Datenschutzrichtlinie

Die Befugnis, von sich aus oder auf Anfrage Stellungnahmen an bestimmte Stellen zu richten, sieht die Datenschutzrichtlinie nicht explizit vor. Jedoch gesteht sie den Kontrollstellen das Recht zu, eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten oder die Parlamente oder andere politische Institutionen zu befassen (Art. 28 Abs. 3 UAbs. 1 Spstr. 2 DSRL). Hierin ist das Recht zur Stellungnahme jedenfalls als Minus enthalten.

dd) Bisherige Ausgestaltung im nationalen Recht

§ 26 Abs. 1 S. 1 BDSG legt der BfDI auf, den Deutschen Bundestag und die Öffentlichkeit über wesentliche Entwicklungen des Datenschutzes zu unterrichten. Die BfDI kann der Bundesregierung und den in § 12 Abs. 1 BDSG genannten Stellen des Bundes Empfehlungen zur Verbesserung des Datenschutzes geben und sie in Fragen des Datenschutzes beraten (§ 26 Abs. 3 BDSG).
Für die Aufsichtsbehörden der Länder sieht z. B. § 24 Abs. 4 RhPfDSG ein Beratungsrecht hinsichtlich des Landtags, der Landesregierung und ihrer Mitglieder sowie der übrigen öffentlichen Stellen vor. § 24 Abs. 8 RhPfDSG normiert, dass der LfDI die Bürgerinnen und Bürger in Fragen des Datenschutzes und der Datensicherheit berät und informiert.

ee) Umsetzung und Anpassung

i. Umsetzungsrahmen nach der DSGVO

(1) Die Öffentlichkeit

Worauf sich das Recht zur Abgabe von Stellungnahmen „im Einklang mit dem Recht des Mitgliedstaats“ bezieht, ist nicht eindeutig. Der Satzbau lässt Auslegungsspielräume offen.
Der Passus lässt sich so verstehen, dass sich die Öffnungsmöglichkeit nur auf die sonstigen Einrichtungen und Stellen bezieht, die Öffentlichkeit hingegen stets erfasst ist.
Dies entspricht aber nicht unbedingt der englischsprachigen Fassung. Dort sind die sonstigen Einrichtungen und Stellen und die Öffentlichkeit ohne das sog. *Serial comma* oder auch *Oxford comma* aufgezählt (“or, in accordance with national law, to other institutions and bodies as well as to the public”). Dies lässt sich so verstehen, dass sich die Öffnungsklausel auf beide Alternativen bezieht.
Andererseits sind die Alternativen der anderen Einrichtungen und der Öffentlichkeit so wesensverschieden, dass nicht einleuchtend ist, warum beide gleichermaßen unter einer Öffnungsklausel stehen sollen. Dem Grundgedanken der Datenschutz-Grundverordnung und dem Sinn der Öffnungsklausel

entspricht es mehr, dass sie den Mitgliedstaaten einen Konkretisierungsspielraum einrichten möchte, welche sonstigen Stellen und Einrichtungen von diesem Recht zur Stellungnahme betroffen sind. Diese Konkretisierungsleistung würde die Datenschutz-Grundverordnung überfordern. Entsprechend gesteht sie das Bestimmungsrecht den Mitgliedstaaten zu. Soweit Adressat nicht die Spitze einer der zwei genannten Gewalten sein soll, ist also der nationale Gesetzgeber berufen, zu entscheiden, welche Einrichtungen und Stellen dies sein sollen. Auch die Entstehungsgeschichte der Regelung stützt diese Lesart. Denn der Entwurf der Kommission und des Parlaments sah in Art. 53 Abs. 1 lit. j DSGVO-E vor, dass der Aufsichtsbehörde das Recht zukommt, „das nationale Parlament, die Regierung oder sonstige politische Institutionen sowie die Öffentlichkeit über Fragen im Zusammenhang mit dem Schutz personenbezogener Daten zu informieren“. Alleine die „sonstigen politischen Institutionen“ wurden im Folgenden in „sonstige Einrichtungen und Stellen“ umbenannt und dabei unter den Öffnungsvorbehalt gestellt.
Die besseren Gründe streiten also dafür, die Aufzählung derart zu lesen, dass die Öffentlichkeit stets und nicht erst nach Ermächtigung durch den nationalen Gesetzgeber zulässiger Adressat von Stellungnahmen der Aufsichtsbehörde ist. Im Übrigen bestimmt der nationale Gesetzgeber die sonstigen Einrichtungen und Stellen.

(2) „Sonstige Einrichtungen und Stellen“

Was „sonstigen Einrichtungen und Stellen“ im Sinne des Art. 58 Abs. 3 lit. b (ex Art. 53 Abs. 1c lit. aa) DSGVO meint, bestimmt die Verordnung nicht näher. Das heißt aber nicht, dass den Mitgliedstaaten insoweit vollständige Gestaltungsfreiheit zukommt. Die Zielsetzung der Verordnung, wirksamen Datenschutz herzustellen, kann ihm Grenzen ziehen. Ob die Wendung „sonstige Einrichtungen und Stellen“ alleine andere Mitglieder der Exekutive als die Regierungen (insbesondere unabhängige Stellen wie die Zentralbanken und nach deutschem Recht den Wehrbeauftragten, aber auch Gerichte in ihrer nicht rechtsprechenden Tätigkeit) oder auch Private (insbesondere Unternehmen) erfasst, ist klärungsbedürftig.
Einen ersten Anhaltspunkt bietet die englische Fassung, die von „and other institutions and bodies“ spricht. Der Bezug zu den Einrichtungen des Parla-

ments und der Regierung macht dabei deutlich, dass es sich auch um öffentliche Einrichtungen handeln muss (sog. *argumentum eiusdem generis*), nicht um beliebige Einrichtungen. Dies ist auch aus der Systematik der Regelung des Art. 58 Abs. 3 (ex Art. 53 Abs. 1c) DSGVO heraus folgerichtig. Denn lit. a erlaubt es, den Verantwortlichen nach dem Verfahren der vorherigen Zurateziehung (Art. 36 [ex Art. 34] DSGVO) zu beraten. Schüfe lit. b (ex lit. aa) eine Öffnung für die Berechtigung zur Beratung bzw. Abgabe von Stellungnahmen ohne das Verfahren des Art. 36 (ex Art. 34) DSGVO, wäre lit. a seines Anwendungsbereiches praktisch beraubt. Hieraus folgt, dass es sich bei „sonstigen Einrichtungen und Stellen“ nur um öffentliche Stellen handelt.

Den Umfang der öffentlichen Einrichtungen und Stellen, die der nationale Gesetzgeber einbeziehen kann, beschränkt die Öffnungsklausel dagegen nicht unmittelbar. Die Datenschutz-Grundverordnung zieht insoweit auch keine sonstigen Grenzen. Denn die Stellungnahmen können zwar einerseits auf eigene Initiative der Aufsichtsbehörde abgegeben werden. Sie sind aber nicht geeignet, die Unabhängigkeit z. B. der nationalen Zentralbank (Art. 130 S. 1 AEUV) zu gefährden, da sie nicht rechtlich verbindlich sind. Andererseits spricht auch nichts dafür, den Kreis der öffentlichen Stellen zu begrenzen, denen eine Anfragebefugnis eingeräumt werden kann. Denn die Anfragebefugnis vermittelt keinen Anspruch darauf, eine Stellungnahme zu erhalten. Das Recht, Stellungnahmen abzugeben, räumt die Datenschutz-Grundverordnung den Aufsichtsbehörden alleine im Interesse wirksamen Persönlichkeitsschutzes ein. Diese sind damit, auch wegen ihrer durch die Datenschutz-Grundverordnung vorgesehenen Unabhängigkeit, nicht verpflichtet, Anfragen nach Stellungnahmen nachzukommen.

ii. Umsetzungsleitlinien und -rahmen nach dem Grundgesetz

Die Ausgestaltung des nationalen Umsetzungsspielraums wirft insbesondere im Hinblick auf die nationale Kompetenzverteilung sowie die Zweckmäßigkeit der Regelung Fragen auf.

(1) Kompetenzen

Das Datenschutzrecht folgt keinem einheitlichen Kompetenztitel.[294] Die Regelungskompetenz ergibt sich aus der Rechtsmaterie, die jeweils von der Regelung betroffen ist, z. B. das Recht der Wirtschaft bei der Regelung von Datenschutzregelungen für nicht-öffentliche Stellen. Hinsichtlich der öffentlichen Verwaltung folgt die Zuständigkeit der Zuständigkeit des Kompetenzträgers für das Verwaltungsverfahrensrecht. Das Recht der öffentlichen Stellen des Bundes regelt der Bund, das der Länder generell die Länder.[295] Folglich hat der Bund die Kompetenz, für den BfDI weitere Adressaten und Anspruchsberechtigte Einrichtungen festzulegen, die Länder haben ein entsprechendes Recht für ihre Datenschutzbeauftragten und Einrichtungen.

(2) Zweckmäßigkeit

Soweit – wie hier angenommen – ein Anfragerecht nicht gleichzeitig einen Anspruch auf eine Stellungnahme begründet, spricht nichts dagegen, den Kreis der erfassten Stellen weit zu ziehen. Der Kreis nach § 26 Abs. 3 BDSG kann deshalb jedenfalls beibehalten werden. Gleiches gilt auch für die entsprechenden Vorschriften der Länder, wie § 24 Abs. 4 RhPfDSG.

d. Art. 58 Abs. 4 (ex Art. 53 Abs. 2)

aa) Inhalt der Regelung

Art. 58 Abs. 4 (ex Art. 53 Abs. 2) DSGVO schützt die Rechte der betroffenen Personen bei der Ausübung der Befugnisse der Aufsichtsbehörde: Die Ausübung der der Aufsichtsbehörde übertragenen Befugnisse erfolgt vorbehaltlich geeigneter Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren gemäß dem Unionsrecht und dem Recht des Mitgliedstaats im Einklang mit der Charta der Grundrechte der Europäischen Union. Die Mitgliedstaaten haben das Recht und die Pflicht, den von den Befugnissen Betroffenen, Verfahrensrechte und Rechtsbehelfe zur Sicherung ihrer Rechtspositionen einzuräumen. Grundsätzlich genießen die Mit-

[294] Vgl. *Kühling/Seidel/Sivridis* (Fn. 44), S. 50. Dazu auch bereits S. 137.
[295] Vgl. *Polenz* (Fn. 173), Rn. 26.

gliedstaaten insoweit weitgehende Regelungsfreiheit. Allerdings darf die Einräumung von Rechtsbehelfen und Verfahrensrechten nicht faktisch die Befugnisse der Aufsichtsbehörden aushöhlen. Diese Grenze ist aber erst dann überschritten, wenn der Schutz Betroffener, den die Mitgliedstaaten herstellen, die wirksame Durchsetzung der unionsrechtlich eingeräumten Befugnisse entweder unmöglich macht oder in einer für die Zielsetzung der Datenschutz-Grundverordnung unzumutbaren Weise beeinträchtigt. Die Verfahrensrechte und Rechtsbehelfsmöglichkeiten, welche das nationale Datenschutzrecht den Adressaten von Befugnissen bisher eingeräumt hat, überschreiten diese Schwelle nicht. Sie dürfen aufrechterhalten bleiben.

bb) Einordnung in das System der Öffnungsklauseln

Art. 58 Abs. 4 (ex Art. 53 Abs. 2) DSGVO etabliert eine obligatorische Öffnungsklausel: Die Mitgliedstaaten müssen die Ausübung der Befugnisse der Aufsichtsbehörde in geeignete Garantien einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren einbetten. Verfahrensrechtliche Vorschriften der Mitgliedstaaten dürfen über die Anforderungen nach der Datenschutz-Grundverordnung hinausgehen (EG 129 S. 8 [ex EG 100 S. 8] DSGVO).

cc) Vergleich zur Datenschutzrichtlinie

Seinen regulatorischen Vorläufer findet Art. 58 Abs. 4 (ex Art. 53 Abs. 2) DSGVO in Art. 28 Abs. 3 UAbs. 2 DSRL. Er sah lediglich vor, dass gegen beschwerende Entscheidungen der Kontrollstelle der Rechtsweg offensteht. Die Beachtung spezifischer verfahrensrechtlicher Vorgaben sowie sonstiger Garantien regelte die Datenschutzrichtlinie nicht. Dies entspricht dem Gedanken der Verfahrensautonomie der Mitgliedstaaten.

dd) Bisherige Ausgestaltung im nationalen Recht

Hinsichtlich der Kontrolle der *öffentlichen* Stellen sehen die Datenschutzgesetze bisher nur in geringem Umfang verfahrensrechtliche Vorschriften vor. Dies gilt sowohl für das BDSG in §§ 22 ff. als auch z. B. für § 25 RhPfDSG.
Hinsichtlich der Kontrolle der *nicht-öffentlichen* Stellen normiert § 38 BDSG u. a. ein Aussageverweigerungsrecht bei drohender Selbstbelastung und eine

entsprechende Hinweispflicht (Abs. 3 S. 2, 3). Hinsichtlich der weiteren Eingriffsbefugnisse (Abs. 5) findet ergänzend das allgemeine Verwaltungsrecht Anwendung.[296] Rechtsschutz eröffnet die Verwaltungsgerichtsordnung insbesondere in Form der Anfechtungs- und der Feststellungsklage, § 42 Abs. 1, § 43 VwGO.

ee) Umsetzung und Anpassung

Bund und Länder dürfen in ihrem Kompetenzbereich zur Sicherung verfahrensrechtlicher Garantien weitere Anforderungen an das Handeln der Aufsichtsbehörden implementieren; zwingender Ergänzungsbedarf besteht jedoch nicht.
Die Vorschriften der Verwaltungsverfahrensgesetze des Bundes und der Länder zum Verfahren und zur Form des Erlasses von Verwaltungsakten genügen den Anforderungen der Datenschutz-Grundverordnung. So sichert §§ 20 f. VwVfG u. a. die Unparteilichkeit (EG 129 S. 4 [ex EG 100 S. 4] DSGVO) und §§ 37 Abs. 1, 28 Abs. 1, 39 Abs. 1 VwVfG die Bestimmtheit, Anhörung und Begründung (EG 129 S. 7 [ex EG 100 S. 7] DSGVO). Die Pflicht zur Rechtsbehelfsbelehrung (EG 129 S. 7 [ex EG 100 S. 7] DSGVO) ist § 58 VwGO zu entnehmen.
Auch die gerichtliche Überprüfung (EG 129 S. 9 [ex EG 100 S. 9] DSGVO) ist durch § 42 Abs. 1, § 43 VwGO eröffnet.

e. Art. 58 Abs. 5 (ex Art. 53 Abs. 3)

aa) Inhalt der Regelung

Art. 58 Abs. 5 (ex Art. 53 Abs. 3) DSGVO gibt den Mitgliedstaaten einen Regelungsauftrag mit auf den Weg: Sie müssen ihren Aufsichtsbehörden die Befugnis einräumen, Verstöße gegen die Datenschutz-Grundverordnung den Justizbehörden zur Kenntnis zu bringen und „gegebenenfalls“ die Einleitung eines gerichtlichen Verfahrens zu betreiben oder sich sonst daran zu beteiligen, um die Bestimmungen der Datenschutz-Grundverordnung durchzusetzen.

[296] *Gola/Klug/Körffer* (Fn. 159), § 38, Rn. 25.

Welcher Regelungsgehalt dem Wort *„gegebenenfalls“* in dem Regelungskontext des Art. 58 Abs. 5 (ex Art. 53 Abs. 3) DSGVO beizumessen ist, lässt Rätsel offen. Die Wendung könnte einerseits bedeuten, dass das Recht, ein Verfahren einzuleiten und sich an einem Verfahren zu beteiligen, gewährt werden muss, jedoch auf besondere Konstellationen beschränkt werden kann. Insbesondere lässt sich die Wendung so verstehen, dass die Aufsichtsbehörde das Recht hat, ein solches Verfahren anzustrengen, wenn sie dies „im Einzelfall“ für sinnvoll erachtet und einen Verstoß den Justizbehörden in dieser Weise zur Befassung durch eigene Klage vorlegen will. Die Aufsichtsbehörden erhielten dann ein besonderes Klagerecht. Es wäre vergleichbar mit der Klagebefugnis der Aufsichtsbehörden nach § 17 Abs. 1 RhPfAGVwGO. Andererseits könnte es aber auch so verstanden werden, dass die Mitgliedstaaten eine umfassende Freiheit haben, entsprechende Rechte vorzusehen.
Die englische Fassung legt das erstere Verständnis, also ein zwingendes behördliches Klagerecht, nahe. Danach sollen die Aufsichtsbehörden das Recht auf Verfahrenseinleitung- und Beteiligung haben, „where appropriate“, wo es also angemessen, sachgemäß oder zweckdienlich ist. Auch scheint EG 129 S. 1 (ex EG 100 S. 1) a. E. DSGVO von einer Parallelität beider Rechte auszugehen und dem Mitgliedstaat kein Wahlrecht einzuräumen. Hiernach haben die Aufsichtsbehörden „– unbeschadet der Befugnisse der Strafverfolgungsbehörden nach Recht der Mitgliedstaaten – die Befugnis, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und Gerichtsverfahren anzustrengen“.[297] Dies deckt sich mit der englischen Fassung des EG.[298]
Hingegen stünde der Ansatz eines Wahlrechts des Mitgliedstaates in der Tradition der Datenschutzrichtlinie (vgl. Art. 28 Abs. 3 Spstr. 3). Gleichzeitig entspricht dies dem Gedanken der Verfahrensautonomie der Mitgliedstaaten.
In eine andere Richtung scheint das Safe-Harbor-Urteil des EuGH zu weisen. Dort führt der Gerichtshof aus, dass die Kontrollstelle „nach Art. 28 Abs. 3

[297] Hingegen hat das Trilog-Ergebnis noch mehr in Richtung eines Wahlrechtes tendiert: „die Befugnis, Verstöße gegen diese Verordnung den Justizbehörden zur Kenntnis zu bringen und/oder Gerichtsverfahren anzustrengen“.
[298] „and without prejudice to the powers of prosecutorial authorities under Member State law, to bring infringements of this Regulation to the attention of the judicial authorities and engage in legal proceedings“.

UnterAbs. 1 dritter Gedankenstrich der Richtlinie 95/46 im Licht insbesondere von Art. 8 Abs. 3 der Charta ein Klagerecht haben [muss]". Insoweit sei es „Sache des nationalen Gesetzgebers, Rechtsbehelfe vorzusehen, die es der betreffenden nationalen Kontrollstelle ermöglichen, die von ihr für begründet erachteten Rügen vor den nationalen Gerichten geltend zu machen, damit diese, wenn sie die Zweifel der Kontrollstelle an der Gültigkeit der Entscheidung der Kommission teilen, um eine Vorabentscheidung über deren Gültigkeit ersuchen."[299] Dies lässt sich womöglich so verstehen, dass die Kontrollstellen ein bereits aus dem Primärrecht folgendes umfassendes Klagerecht auch zu nationalen Gerichten haben. Der Zusammenhang, in dem diese Ausführungen stehen, macht jedoch deutlich, dass dies nicht zwingend so zu lesen ist. Der EuGH führt lediglich aus, dass es der Kontrollstelle möglich sein muss, selbst eine gerichtliche Entscheidung über die Rechtmäßigkeit einer nach Art. 25 Abs. 6 der Datenschutzrichtlinie ergangenen Entscheidung der Kommission herbeizuführen. Er verlangt ein Klagerecht zum nationalen Gericht, damit dieses dann die Frage dem EuGH (nach Art. 267 AEUV) vorlegen kann (und so nach dem Gedanken der „Rechtsunion" jeder Akt der Unionseinrichtungen einer Rechtmäßigkeitskontrolle unterzogen werden kann[300]). Insofern betrachtet der EuGH nur einen sehr kleinen Ausschnitt der Klagemöglichkeiten der Kontrollstelle und sagt insbesondere nichts darüber aus, ob diese auch ein Klagerecht *gegen einzelne Verarbeiter von Daten* haben müssen. Um letzteres Recht geht es aber in Art. 58 Abs. 5 (ex Art. 53 Abs. 3) DSGVO.[301] Das Gebot, dem EuGH eine Kontrolle von Rechtsakten, die auf der Grundlage unionsrechtlicher Rechtsakte ergehen, zu ermöglichen, impliziert nicht zwingend ein Klagerecht der Aufsichtsbehörden gegen einzelne Datenverarbeiter.

Ob der EuGH das genauso sieht, ist nach dem Schrems-Urteil jedoch sehr fraglich. Entsprechend hat der Ausschuss für Innere Angelegenheiten dem

[299] EuGH, Rs. C-362/14, Urteil v. 6.10.2015 – „Schrems", Rn. 65.
[300] EuGH, Rs. C-362/14, Urteil v. 6.10.2015 – „Schrems", Rn. 60 ff.
[301] Das Ziel des EuGH, für die Aufsichtsbehörden die Möglichkeit zu schaffen, die Handlungen insbesondere der Kommission einer Rechtmäßigkeitskontrolle zu unterziehen kann insbesondere auch dadurch erreicht werden, dass diesen ein Klagerecht nach Art. 263 AEUV eingeräumt wird; siehe dazu unten S. 264.

Bundesrat vorgeschlagen, das BDSG um einen § 38b zu ergänzen, der entsprechende Klagerechte etabliert.[302]

bb) Einordnung in das System der Öffnungsklauseln

Art. 58 Abs. 5 (ex Art. 53 Abs. 3) DSGVO ist eine obligatorische Öffnungsklausel (vgl. die Formulierung: „Jeder Mitgliedstaat regelt durch Rechtsvorschrift, dass…“) hinsichtlich ihrer ersten Alternative; den Regelungsauftrag auf beide Alternativen zu erstrecken, ist aber ebenso gut vertretbar. Die Verordnung bleibt hier sibyllinisch. In Bezug auf darüber hinausgehende Befugnisse ist die Öffnungsklausel fakultativ.

cc) Vergleich zur Datenschutzrichtlinie

Die Datenschutzrichtlinie sah ebenfalls bereits die Einräumung eines Klage- oder Anzeigerechts der Kontrollstellen vor (Art. 28 Abs. 3 UAbs. 1 Spstr. 3 DSRL). Neu ist hingegen, dass die Datenschutz-Grundverordnung den Kontrollstellen auch das Recht einräumt, sich an Verfahren zu beteiligen. Jedoch stand die Datenschutzrichtlinie der Gewährung dieses Rechts nicht im Wege, da die Rechte, welche Art. 28 Abs. 3 UAbs. 1 DSRL aufzählt, nicht abschließend sind.

dd) Bisherige Ausgestaltung im nationalen Recht

Das BDSG sieht bislang keine explizierten Rechte des BfDI vor, selbst gerichtliche Verfahren anzustrengen. Die §§ 22-26 BDSG schweigen sich insoweit aus. § 21 BDSG sieht lediglich ein Anrufungsrecht in die umgekehrte Richtung – gegenüber dem BfDI – vor. Die Aufsichtsbehörden haben das Recht, den Verstoß bei den für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen (§ 38 Abs. 1 S. 6 BDSG).
Daneben kommt sowohl der BfDI als auch den Aufsichtsbehörden nach § 44 Abs. 2 BDSG das Strafantragsrecht hinsichtlich des in § 44 Abs. 1 BDSG normierten Straftatbestandes zu.

[302] BR-Drucks. 171/1/16 vom 2.5.2016.

Im Landesrecht gestaltet sich die Lage unterschiedlich. Ein Strafantragsrecht für landesgesetzliche Straftatbestände sehen nur Berlin und Bayern vor, Rheinland-Pfalz demgegenüber z. B. nicht (vgl. § 37 RhPfDSG).[303]
Verbraucherschutzverbänden gesteht der Gesetzgeber aber umfängliche Verbandsklagerechte bei der zivilrechtlichen Durchsetzung verbraucherschützender Vorschriften des Datenschutzrechts zu.[304] § 12a UKlaG spricht nunmehr den Datenschutzbehörden ein Anhörungsrecht zu. Dieses Anhörungsrecht ist jedoch nicht selbstständiger Natur, sondern akzessorisch zum Verbandsklagerecht der Verbraucherschutzverbände. Es wird nur wirksam, wenn die Verbände von diesem Recht Gebrauch machen. Dem Art. 58 Abs. 5 Hs. 2 Alt. 2 (ex Art. 53 Abs. 3 Hs. 2 Alt. 2) DSGVO scheint das aber zu genügen. Denn er verbürgt den Aufsichtsbehörden *alternativ* zum selbständigen Klagerecht ein akzessorisches Beteiligungsrecht am Verfahren zu.

ee) Umsetzung und Anpassung

§ 36 Abs. 1 S. 6 BDSG gesteht den Aufsichtsbehörden das Recht zu, Verstöße gegen Vorschriften über das Datenschutzrecht bei den zuständigen Stellen anzuzeigen. § 44 Abs. 2 BDSG normiert für alle Aufsichtsbehörden das Strafantragsrecht hinsichtlich Straftaten nach § 44 Abs. 1 BDSG. Soweit Landesdatenschutzgesetze, wie das RhPfDSG kein Strafantragserfordernis vorsehen, kommt lediglich eine Berufung auf das Jedermann-Recht zur Strafanzeige bei der Polizei oder Staatsanwaltschaft in Betracht (§ 158 Abs. 1 S. 1 Var. 1 StPO). Hierunter fallen aber nach der Grundvorstellung der StPO wohl nur natürliche und juristische Personen, nicht auch Behörden. Insofern besteht gesetzgeberischer Handlungsbedarf.
Ob auch ein Klagerecht der Behörden bzw. ein zwingendes gerichtliches Verfahrensbeteiligungsrecht nach Art. 58 Abs. 5 (ex Art. 53 Abs. 3) DSGVO vorzusehen ist, ist offen. Der Wortlaut der Vorschrift und das Verständnis des EuGH legen das nahe (vgl. S. 198).

---

[303] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 44, Rn. 9.
[304] Siehe das Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts vom 17.2.2016, BGBl. I vom 23.2.2016, S. 233 ff.; vgl. auch den Gesetzesentwurf unter BT-Drucks. 18/4631.

f. Art. 58 Abs. 6 (ex Art. 53 Abs. 4)

aa) Inhalt der Regelung

Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO gewährt jedem Mitgliedstaat das Recht, durch Rechtsvorschriften seiner Aufsichtsbehörde weitere als die in Abs.1 bis 3 (ex Abs. 1 bis 1c) aufgeführten Befugnisse zu übertragen. Die Ausübung dieser Befugnisse darf allerdings zugleich nicht die effektive Durchführung der Bestimmungen des Kapitels VII („Zusammenarbeit und Kohärenz“) der Datenschutz-Grundverordnung beeinträchtigen.

bb) Vergleich zur Datenschutzrichtlinie

Dass den Kontrollstellen weitere Befugnisse übertragen werden können, galt auch unter der Datenschutzrichtlinie. Diese regelte nur, dass die Kontrollstellen „insbesondere“ gewisse Befugnisse aus Art. 28 Abs. 3 UAbs. 1 DSRL haben müssen. Die Aufzählung der Befugnisse war nicht abschließend.

cc) Bisherige Ausgestaltung im nationalen Recht

Die Befugnisse der Aufsichtsbehörden, also der Datenschutzbeauftragten von Bund und Ländern, regeln bislang §§ 23-26 BDSG sowie § 38 BDSG und die Datenschutzgesetze der Länder, wie z. B. §§ 24, 25 RhPfDSG.

dd) Umsetzung und Anpassung

Will der Gesetzgeber die über die Befugnisse aus der Datenschutz-Grundverordnung hinausgehen Befugnisse der Aufsichtsbehörden gemäß den §§ 24-26 und 38 BDSG auch weiter bestehen lassen, darf und muss er dies regeln. Dabei empfiehlt es sich, die Befugnisse an die Terminologie der Datenschutz-Grundverordnung anzupassen.[305]

[305] Siehe dazu unten S. 419 ff. u. 461 ff.

34. Art. 59 (ex Art. 54): Tätigkeitsbericht

a. Inhalt der Regelung

Art. 59 S. 2 (ex Art. 54 S. 1) DSGVO legt den Aufsichtsbehörden auf, jährlich einen Tätigkeitsbericht anzufertigen. Dieser ist insbesondere der Öffentlichkeit zugänglich zu machen (S. 3). Der Tätigkeitsbericht ist dem nationalen Parlament, der Regierung und anderen nach dem Recht der Mitgliedstaaten bestimmten Behörden zu übermitteln (S. 2). In der Wendung „nach dem Recht der Mitgliedstaaten“ verbirgt sich zugleich eine Öffnungsklausel. Ihr Gehalt ist insoweit unklar, als nicht deutlich wird, inwieweit der nationale Gesetzgeber nur das „Wie“ oder auch das „Ob“ (also den Adressatenkreis) der Übermittlung regeln darf.
Als zwingende Adressaten benennt die Vorschrift das Parlament und die Regierung. Insoweit ist die Öffnungsklausel obligatorisch. Spielraum bleibt hinsichtlich der Ausfüllung der Wendung „anderen […] Behörden“. Ein Vergleich mit der ähnlichen Öffnungsklausel des Art. 58 Abs. 3 lit. b (ex Art. 53 Abs. 1c lit. aa) DSGVO legt nahe, dass dem nationalen Gesetzgeber insoweit Konkretisierungsspielraum auch bezüglich des „Ob“ zukommt. Ein Spielraum, der sich alleine auf das „Wie“ der Übermittlung beschränkt, wäre nur bedingt sinnvoll. Insoweit ist die Öffnungsklausel fakultativer Natur.

b. Vergleich zur Datenschutzrichtlinie

Der Tätigkeitsbericht ist kein Novum der Datenschutz-Grundverordnung. Bereits nach Art. 28 Abs. 5 DSRL hat jede Kontrollstelle regelmäßig einen Bericht über ihre Tätigkeit vorzulegen. Dieser Bericht ist zu veröffentlichen.

c. Bisherige Ausgestaltung im nationalen Recht

Das BDSG legt bereits sowohl der BfDI als auch den Aufsichtsbehörden die Verpflichtung auf, einen Tätigkeitsbericht vorzulegen: Nach § 26 Abs. 1 S. 1 BDSG hat die *BfDI* dem Deutschen Bundestag alle zwei Jahre einen Tätigkeitsbericht zu erstatten. Die *Aufsichtsbehörde* veröffentlicht regelmäßig, spätestens alle zwei Jahre, einen Tätigkeitsbericht (§ 38 Abs. 1 S. 7 BDSG).

d. Umsetzung und Anpassung

Die Regelungen zur Veröffentlichungsfrist sind nach Inkrafttreten der Datenschutz-Grundverordnung grundsätzlich hinfällig und aufzuheben. Denn die Datenschutz-Grundverordnung legt diese selbst fest und eröffnet keinen mitgliedstaatlichen Regelungsspielraum. Auch den Verpflichtungsinhalt und den Adressatenkreis verfügt die Datenschutz-Grundverordnung grundsätzlich abschließend. Insoweit ist alleine festzulegen, welche nach der Öffnungsklausel zusätzlichen Adressaten der Tätigkeitsbericht haben soll und wie dieser zu übermitteln ist. Daneben ist mit Blick auf Parlament und Regierung nach EG 8 (ex EG 6a) DSGVO eine klarstellende Regelung zulässig, die eine Einordnung in den Regelungskontext ermöglicht (und wegen der mit Unsicherheiten verbundenen Auslegung der Öffnungsklausel auch zu empfehlen). Regelungen für die Tätigkeitsberichte sind zwar nicht auf ein einzelnes, nach außen wirkendes Verwaltungshandeln gerichtet, sondern übergreifender Natur und statuieren keine materiellen Kompetenzen der Aufsichtsbehörden (wie zum Beispiel Beratungsaufträge). Sie sind aber gleichwohl Teil des Verwaltungsverfahrens.

Folglich kann der Bundesgesetzgeber hinsichtlich seiner Behörden, also der BfDI, alleine regeln (Art. 86 S. 1 GG), wie und welchen anderen Behörden des Bundes der Bericht zu übermitteln ist. Neben dem Bundestag und der Bundesregierung sollten hier weitere oberste Bundesbehörden und Bundesoberbehörden als Adressaten aufgenommen werden, soweit sie selbst datenintensive Tätigkeiten ausüben. Zu denken ist hier an den Bundesrechnungshof (BRH) sowie das Bundesamt für Verfassungsschutz (BfV), das Bundeskriminalamt (BKA) und den Bundesnachrichtendienst (BND). Zwingend ist dies jedoch nicht.

Hinsichtlich der Landesdatenschutzbeauftragten ist die Regelungskompetenz des Bundes weniger eindeutig. Denn der Tätigkeitsbericht erfasst sowohl deren Handeln in Ausführung von Bundes- als auch von Landesgesetzen. Der Bund ist allerdings auf der Grundlage des Art. 83 Abs. 1 S. 1 GG alleine für erstere das Verwaltungsverfahren zu regeln kompetent.[306] In dieser Mischlage könnte, da der Tätigkeitsbericht grundsätzlich einheitlich erstellt wird, dem

[306] Hierauf durfte sich die aktuelle Regelung des § 38 Abs. 1 S. 7 BDSG stützen lassen.

Bund allenfalls als Annex auch für die Tätigkeiten in Ausführung von Landesgesetzen die Regelungskompetenz zustehen. Gleichwohl erscheint dies nicht unbedingt zwingend. Der Bund kann seine Kompetenz wahrnehmen, ohne dass er in originäre Kompetenzrechte der Länder übergreifen muss.[307] Der Bund darf mithin Regelungen über die Adressaten der Veröffentlichung nach Art. 59 S. 2 (ex Art. 54 S. 2) DSGVO für den Bereich der Aufsicht über die nicht-öffentliche Datenverarbeitung treffen, die Länder für den öffentlichen Bereich.

35. Art. 60 ff. (ex Art. 54a ff.): Zusammenarbeit zwischen der federführenden Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden

a. Regelungsbedarf für das Zusammenarbeitsverfahren auf nationaler Ebene

aa) Kein Regelungsbedarf für das Zusammenarbeitsverfahren selbst

Die Art. 60 bis 62 (ex Art. 54a bis 56) DSGVO regeln das sog. Zusammenarbeitsverfahren (vgl. dazu bereits oben S. 110). Dieses dem Kohärenzverfahren in weiten Bereichen strukturell vorgelagerte (aber auch eigenständige) Verfahren zielt auf klare Zuständigkeitsregelungen bei grenzüberschreitenden Sachverhalten (vgl. Art. 60 Abs. 1 S. 1 [ex Art. 54a Abs. 1 S. 1] DSGVO) sowie auf eine Abstimmung und gegenseitige Unterstützung der Aufsichtsbehörden in solchen Fällen. Hierzu etabliert es einen Mechanismus der Abstimmung und Zusammenarbeit zwischen den nationalen Aufsichtsbehörden. Aus den Regelungen ergibt sich unmittelbar kein Umsetzungsbedarf. Die Datenschutz-Grundverordnung regelt das Verfahren der Zusammenarbeit abschließend.

---

[307] So entspricht es auch der bisherigen Regelungstradition. Sowohl im BDSG als auch in den LDSG finden sich entsprechend (übereinstimmende) Regelungen zum Tätigkeitsbericht des Landesdatenschutzbeauftragten (vgl. z. B. für das Land Rheinland-Pfalz § 29 Abs. 2 RhPfLDSG). Bayern hat die Aufsicht über die öffentlichen und die nicht-öffentlichen Stellen beispielsweise institutionell getrennt.

bb) Regelungsbedarf für nationales Begleitverfahren

Wiewohl die Datenschutz-Grundverordnung das Verfahren der Zusammenarbeit weitreichend prädeterminiert, besteht ein Regelungsbedarf für ein nationales Begleitverfahren zum Verfahren der Zusammenarbeit, wenn – wie in der Bundesrepublik – mehr als eine nationale Aufsichtsbehörde existiert. Die Vorschriften der Datenschutz-Grundverordnung treffen insoweit keine Regelung. Regelungsbedürftige Aspekte einer nationalen Begleitregelung sind sowohl das Außenverhältnis (s. bereits S. 119) als auch das Innenverhältnis, mithin die Binnenkoordination der nationalen Aufsichtsbehörden.

i. Teilweiser Anwendungsausschluss des Zusammenarbeitsverfahrens

Konstellationen der Aufsicht über *öffentliche* Stellen lösen typischerweise keine Zuständigkeitskonflikte und damit den Bedarf nach Zusammenarbeit (und Kohärenz) aus. Das ergibt sich aus Art. 55 Abs. 2 und EG 128 (ex Art. 51 Abs. 2 und EG 98) DSGVO: Machen die Mitgliedstaaten insoweit von ihren Öffnungsklauseln des Art. 6 Abs. 1 UAbs. 1 lit. c oder e DSGVO Gebrauch, ist alleine die Aufsichtsbehörde des Mitgliedstaates zuständig. *Innerhalb* des Mitgliedstaates ist dann (kraft der Befugnis zur Regelung der Aufsicht über die eigenen Behörden) alleine das Land regelungsbefugt und betroffen, dessen öffentliche Stelle betroffen ist.
Anders verhält es sich demgegenüber regelmäßig hinsichtlich der Aufsicht über *nicht-öffentliche* Stellen. Für diese Fälle ist es sachgerecht, zwischen den deutschen Aufsichtsbehörden ein Zuständigkeitskonzept entsprechend dem Konzept der Betroffenheit und Federführung nach der Datenschutz-Grundverordnung zu etablieren.

ii. Herleitung des Bedarfs nach einer nationalen Regelung im Außen- und Innenverhältnis

Das Bedürfnis nach einer Regelung des Außen- und Innenverhältnisses einer Mehrzahl von Aufsichtsbehörden in einem Mitgliedstaat stellt sich nur dann, wenn die Art. 60 ff. DSGVO auf diese nicht unmittelbar anwendbar sind. Wären alle nationalen Aufsichtsbehörden „betroffene Aufsichtsbehörden“ i. S. v. Art. 60, Art. 4 Nr. 22 (ex Art. 54a, Art. 4 Nr. 19a) DSGVO und damit jeweils einzeln von der federführenden Aufsichtsbehörde zu kontaktieren,

bräuchte es keine Abstimmung nach außen hin und innerhalb eines Mitgliedstaates. Anders verhält es sich, wenn die deutschen Aufsichtsbehörden in ihrer Gesamtheit als die „betroffene Aufsichtsbehörde“ i. S. d. Vorschrift zu sehen sind. In letzterem Fall müssten sie dann, mit Hilfe der zentralen Anlaufstelle, nach außen hin mit einer Stimme sprechen und ihr Vorgehen nach innen hin koordinieren.

Auf den ersten Blick können dabei auch einzelne von mehreren nationalen Aufsichtsbehörden „betroffene Aufsichtsbehörden“ i. S. v. Art. 4 Nr. 22 (ex Art. 4 Nr. 19a) DSGVO sein. Denn bei diesen kann jeder eine Beschwerde einreichen, so dass Art. 4 Nr. 22 lit. c (ex Art. 4 Nr. 19a lit. c) DSGVO sie als „betroffen“ erklärt. Gleichwohl dürfte der Begriff nicht in diesem Sinne zu verstehen sein, sondern nur *die Aufsichtsbehörden eines Mitgliedstaates als Gesamtheit* adressieren, soweit eine der dort etablierten Aufsichtsbehörden nach Art. 4 Nr. 22 (ex Art. 4 Nr. 19a) DSGVO betroffen ist. Bereits der Wortlaut des lit. a legt dies nahe. Dieser knüpft an die Niederlassung des Verantwortlichen *im Hoheitsgebiet des Mitgliedstaates dieser Aufsichtsbehörde* an.[308] Entscheidend ist danach eine Betrachtung auf der Ebene des Mitgliedstaates (so auch lit. b). Die Datenschutz-Grundverordnung betrachtet den Mitgliedstaat insoweit als Einheit. Innerstaatliche Fragmentierungen der Zuständigkeitsbereiche muss der Mitgliedstaat selbst nach außen hin z. B. durch eine zentrale Anlaufstelle ausgleichen, ohne die effektive Durchsetzung des Unionsrechts zu gefährden. Andernfalls würde der Mitgliedstaat die hieraus erwachsenden Schwierigkeiten auf die Aufsichtsbehörden der anderen Mitgliedstaaten überwälzen.

Folglich sind nicht mehrere innerstaatliche Aufsichtsbehörden i. S. v. Art. 4 Nr. 21 i. V. m. Art. 60 (ex Art. 4 Nr. 19 i. V. m. Art. 54a) DSGVO Betroffene, sondern alleine die Gesamtheit der Aufsichtsbehörden. Es bedarf also einer innerstaatlichen Vorabstimmung, damit sich ein einheitlicher Wille gegenüber der Kontakt aufnehmenden federführenden Aufsichtsbehörde vermittels der zentralen Anlaufstelle bilden und artikulieren kann.

---

[308] Engl.: „supervisory authority concerned' means a supervisory authority which is concerned by the processing, because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority”.

iii. Regelungsbedarf am Beispiel von drei Fallszenarien

Hat ein Mitgliedstaat mehr als eine Aufsichtsbehörde geschaffen und greift das Zusammenarbeitsverfahren nach Art. 60 DSGVO, löst dies einen umfassenden Abstimmungsbedarf zwischen den unterschiedlichen berührten Aufsichtsträgern insbesondere dann aus, wenn nicht-öffentliche Stellen Daten verarbeiten und die Stelle nicht nur eine (Haupt-)Niederlassung, sondern weitere Niederlassungen unterhält.
Die einfachste Konstellation ist diejenige eines grenzüberschreitenden Sachverhalts, der nur *eine* Aufsichtsbehörde der Bundesrepublik Deutschland betrifft (Fall 1). Schwieriger wird es, bei grenzüberschreitenden Sachverhalten, die *mehrere* Aufsichtsbehörden der Bundesländer tangieren (Fall 2). Davon zu unterscheiden sind *rein innerstaatliche Sachverhalte*, bei denen mehrere Aufsichtsbehörden der Bundesländer berührt sind (Fall 3). In diesen Konstellationen ist der Regelungsbereich der in der Datenschutz-Grundverordnung verankerten Regeln zur Zusammenarbeit nur mittelbar berührt. Denn diese adressieren grundsätzlich die Mitgliedstaaten als solche. Neben diesen sind solche Fälle virulent, in denen *besondere Aufsichtsbehörden* betroffen sind [unten (4)].

(1) Fall 1: Grenzüberschreitender Sachverhalt, der nur eine Aufsichtsbehörde der Länder betrifft

Soweit alleine ein Landesdatenschutzbeauftragter mit einer ausländischen Aufsichtsbehörde zusammenarbeiten muss, ist zu klären, inwieweit die zentrale Anlaufstelle eine Mittlerrolle einnehmen muss und ob bzw. welche Befugnisse ihr zukommen. Relevant wird dies bspw., wenn ein Unternehmen in Polen seine Haupt-, in München seine Zweitniederlassung hat oder umgekehrt die Hauptniederlassung in München, eine Zweitniederlassung in Polen angesiedelt ist.
Gegebenenfalls ist ein Mechanismus vorzusehen, der über Streitfälle der Beteiligung (hier hinsichtlich des „Ob“) anderer nationaler Aufsichtsbehörden – insbesondere im Hinblick auf die Präzedenzwirkung für künftige Fälle – befindet.

(2) Fall 2: Grenzüberschreitender Sachverhalt, der mehrere Aufsichtsbehörden der Länder betrifft

Sind mehrere Aufsichtsbehörden der Länder berührt, stellen sich grundsätzlich die gleichen Herausforderungen wie bei Fall 1. Ein solcher Fall tritt bspw. ein, wenn ein Unternehmen nicht nur wie in München, sondern auch noch in Mainz eine Zweitniederlassung besitzt.
Die Lage ist dann um einen wesentlichen Aspekt reicher: Es ist zu klären, wie die Abstimmung zwischen den nationalen Aufsichtsbehörden, also den verschiedenen zuständigen Landesdatenschutzbeauftragten, zu erfolgen hat. Es fragt sich, ob die betroffenen Aufsichtsbehörden nur nach Anfall zusammenarbeiten oder in einer verstetigten Form. Die Aufsichtsbehörden müssten einen Modus innerstaatlicher Meinungsbildung (also dem „Wie" der Beteiligung) finden. Insbesondere stellt sich die Frage nach der Beteiligung der nicht-betroffenen Aufsichtsbehörden im einzelnen Fall.

(3) Fall 3: rein innerstaatlicher Sachverhalt, der mehrere Aufsichtsbehörden der Länder betrifft

Handelt es sich um einen rein innerstaatlichen Sachverhalt, der mehrere Aufsichtsbehörden der Länder berührt, wenn also bspw. ein Unternehmen nur innerhalb Deutschlands ansässig ist und dabei in München seine Haupt-, in Mainz eine Zweitniederlassung hat, ist nicht Art. 60 (ex Art. 54a) DSGVO berührt, sondern Art. 51 Abs. 3 und Art. 68 Abs. 4 (ex Art. 46 Abs. 2 und Art. 64 Abs. 3) DSGVO. In diesem Fall stellt sich alleine die Frage nach der innerdeutschen Abstimmung zwischen den betroffenen bzw. allen nationalen Aufsichtsbehörden.[309]

(4) Betroffenheit besonderer Aufsichtsbehörden

Als besondere Problematik tritt in all diesen Konstellationen die Frage hinzu, wie besondere Aufsichtsbehörden etwa der Religionsgemeinschaften und der

[309] Diese Konstellation erfasst die Datenschutz-Grundverordnung unmittelbar allerdings nicht, vgl. sogleich auf S. 212. Trotzdem muss der Mitgliedstaat auch hier eine entsprechende Regelung treffen (siehe dazu auf S. 215).

Deutschen Welle in innerdeutsche Abstimmungs- und Vertretungsmechanismen eingebunden werden.[310]

iv. Im Außenverhältnis: Zentrale Anlaufstelle

Für die Fälle 1 und 2 bedarf es einer Regelung, auf welchem Weg die ausländische Aufsichtsbehörde an die betroffene deutsche Aufsichtsbehörde herantreten kann.
Das Verhältnis zu den anderen Mitgliedstaaten bzw. deren Aufsichtsbehörden sowie zur Kommission ist dabei von der Regelung der Vertretung im EDA (vgl. S. 136 ist nicht umfasst (vgl. hierzu bereits oben S. 119). Insoweit liegt es nahe, die aus EG 119 (ex EG 93) DSGVO fließende Pflicht, eine *zentrale Anlaufstelle* zu errichten, nicht alleine dem Wortlaut entsprechend auf das Kohärenzverfahren nach Art. 63 ff. (ex Art. 57 ff.) DSGVO (mithin im engeren Sinne) zu beziehen, sondern auch auf die Regelungen der Zusammenarbeit nach Art. 60 (ex Art. 54a) (i. V. m. Art. 56 Abs. 1, 4 [ex Art. 51a Abs. 1, 2c] DSGVO) bis Art. 62 (ex Art. 56) DSGVO. Hier treten sich die einzelnen Aufsichtsbehörden unmittelbar – gleichsam im horizontalen Verhältnis – gegenüber. Insbesondere in diesen Fällen ist es für die Effektivität der Durchführung grenzüberschreitender aufsichtsrechtlicher Verfahren unerlässlich, dass in jedem Mitgliedstaat eine zentrale Anlaufstelle als einheitlicher Ansprechpartner besteht. Denn andernfalls würde die innerunionale Zusammenarbeit dadurch gefährdet, dass es der kontaktsuchenden Aufsichtsbehörde obliegt, sich selbst Klarheit über die innerstaatliche Zuständigkeitsordnung zu verschaffen; siehe hierzu unten, S. 217.

v. Im Innenverhältnis

Auch im Innenverhältnis besteht binnenkoordinierender Regelungsbedarf zwischen den einzelnen nationalen Aufsichtsbehörden. So muss geklärt wer-

[310] EG 128 (ex 98) DSGVO erweckt prima facie den Eindruck, als sei in diesen Fällen alleine die für diese Sonderfälle vorgesehene Aufsichtsbehörde zuständig. Das Verfahren der Zusammenarbeit entfiele dann. Allerdings korrespondiert EG 128 (ex 98) DSGVO mit der Sondernorm des Art. 55 Abs. 2 (ex Art. 51 Abs. 2) DSGVO. Diese nimmt alleine auf die Öffnungsklausel des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO Bezug, nicht aber auf die Öffnungsklauseln für Medien und die Kirchen, insbesondere Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO, auf die die Sondernormen für deren Aufsicht zurückgehen.

den, wie die zentrale Anlaufstelle einzurichten ist und über welche Befugnisse sie verfügt.
Sowohl im Fall 1 als auch im Fall 2 bedarf es – ggf. in unterschiedlichem Umfang – einer innerstaatlichen Vorabstimmung (1). In Fall 3 stellt sich die Frage, inwieweit aus dem Unionsrecht oder gegebenenfalls dem nationalen Recht auch in rein innerstaatlichen Sachverhalten ähnliche Koordinierungs- und Zusammenarbeitsverpflichtungen erwachsen (2).

(1) Bei grenzüberschreitendem Sachverhalt

Liegt ein grenzüberschreitender Sachverhalt – wie in den Fällen 1 und 2 – vor, ist das Zusammenarbeitsverfahren nach Art. 60 ff. DSGVO grundsätzlich einschlägig. Da es jedoch nur die in einem Mitgliedstaat bestehenden Aufsichtsbehörden in ihrer Gesamtheit adressiert (vgl. oben ii., S. 207), ist für diese neben einer gemeinsamen Regelung des Außenverhältnisses grundsätzlich auch eine Binnenkoordination erforderlich.
Inwieweit bzw. in welchen Bereichen des Zusammenarbeitsverfahrens eine interne Vorabstimmung erforderlich ist, erschließt sich nicht auf den ersten Blick. Die Bereiche mit Vorabstimmungsbedarf lassen sich dabei in drei Gruppen gliedern:

(α) Abstimmung hinsichtlich der innerstaatlichen Zuständigkeit/Betroffenheit einzelner Aufsichtsbehörden

Aus Sicht der Datenschutz-Grundverordnung ist für das Zusammenarbeitsverfahren die Identifizierung der betroffenen und federführenden Aufsichtsbehörde von zentraler Bedeutung. Gleichzeitig regelt die Datenschutz-Grundverordnung nicht auch die Betroffenheit oder Federführung zwischen verschiedenen Aufsichtsbehörden eines Mitgliedstaates. Diese muss deshalb – um die innerdeutsche Zuständigkeitsordnung zu wahren – durch nationales Recht geregelt (materielle Regelung) und in einem innerstaatlichen Abstimmungssystem (Regelung des Verfahrens bzw. formelle Regelung) auf die einzelnen innerstaatlichen Aufsichtsbehörden weiterverteilt werden. Relevant ist dies in den Fällen 1 und 2 zum Beispiel für die Erteilung von Auskünften (Art. 60 Abs. 1 S. 2 [ex Art. 54a Abs. 1 S. 2] DSGVO), die Gewährung von

Amtshilfe und die Durchführung gemeinsamer Maßnahmen (Art. 62 Abs. 2 [ex Art. 56 Abs. 2] DSGVO).[311]

(β) Abstimmung des Vorgehens einzelner oder mehrerer nationaler Aufsichtsbehörden

Über die innerstaatliche Verteilung der Zuständigkeiten hinaus ergibt sich auch der Bedarf nach einer Abstimmung des Vorgehens einzelner oder mehrerer nationaler Aufsichtsbehörden. Davon betroffen sind beispielsweise: die Erarbeitung eines Standpunktes (Art. 60 Abs. 3 S. 2 [ex Art. 54a Abs. 2 S. 2] DSGVO), die Entscheidung über die Einlegung (Art. 60 Abs. 4 [ex Art. 54a Abs. 3] DSGVO) oder Nichteinlegung (Art. 60 Abs. 6 [ex Art. 54a Abs. 4] DSGVO) eines Einspruchs, die teilweise Ablehnung einer Beschwerde (Art. 60 Abs. 9 [ex Art. 54a Abs. 4bb] DSGVO), außerdem die Ablehnung eines Amtshilfeersuchens (Art. 61 Abs. Abs. 4 [ex Art. 55 Abs. 4] DSGVO) und die Einladung von Bediensteten einer unterstützenden Aufsichtsbehörde (Art. 62 Abs. 4 [ex Art. 56 Abs. 3a] DSGVO).
In Fall 2 ist insoweit ein Abstimmungsbedarf evident. Hier müssen zumindest die (zwei oder mehr) *betroffenen Aufsichtsbehörden* ein einheitliches Vorgehen abstimmen, um dieses dann der federführenden Aufsichtsbehörde zu kommunizieren. Denn Letztere kann nicht darauf verwiesen werden, selbst mehrere – aus innerstaatlichen Rechtsordnung eines Mitgliedstaates herrührende – unterschiedliche Meinungen zu der Vorgehensweise mit in ihre Entscheidungsfindung einzustellen. Vielmehr erstreckt sich auch hier die unions- bzw. völkerrechtliche Perspektive auf den Mitgliedstaat als Ganzes. Dessen Aufsichtsbehörden müssen als Betroffene einen einheitlichen Willen artikulieren.
In Fall 1 und Fall 2 bedarf es einer Klärung, ob auch nach der innerstaatlichen Zuständigkeitsordnung *nicht betroffene* Aufsichtsbehörden in den Abstimmungsvorgang einzubeziehen sind. Dies mag auf den ersten Blick abwegig erscheinen, da die innerstaatliche Zuständigkeitsordnung gerade eine einzelne oder mehrere, aber nicht alle Aufsichtsbehörden zur Entscheidung beruft. Gleichwohl sprechen insbesondere eine gewisse Bindungswirkung von im

[311] Siehe hierzu S. 219.

Verfahren der Zusammenarbeit ergehenden Entscheidungen und die Verantwortlichkeit Deutschlands im Außenverhältnis für das Handeln der einzelnen Aufsichtsbehörden dafür, alle nationalen Aufsichtsbehörden in die Entscheidungsfindung einzubeziehen.[312]

(γ) (Selbst-)Kontrolle der nationalen Aufsichtsbehörden

Alleine die innerstaatliche Verteilung der Zuständigkeiten (und Abstimmung der Entscheidungen) genügt noch nicht, um eine effektive Durchführung des Zusammenarbeitsverfahrens zu verbürgen. Vielmehr besteht wegen der Verantwortlichkeit Deutschlands im Außenverhältnis ein Bedarf zur sicheren Koordinierung der übernommenen deutschen Verpflichtungen, die innerstaatlich an einzelne Aufsichtsbehörden weitergeleitet werden. Solche Verpflichtungen sind zum Beispiel das In-Kenntnis-Setzen des EDA und anderer Aufsichtsbehörden (Art. 60 Abs. 7 S. 1 Hs. 2 [ex Art. 54a Abs. 4a S. 1 Hs. 2] DSGVO), die Informationsübermittlung (Art. 60 Abs. 1 S. 2 [ex Art. 54a Abs. 1 S. 2] DSGVO) sowie das Ergreifen geeigneter Maßnahmen bei der Amtshilfe (Art. 61 Abs. 2 S. 1 [ex Art. 55 Abs. 2 S. 1] DSGVO) und die Information über Ergebnisse und Fortgang der Amtshilfe (Art. 60 Abs. 5 [ex Art. 55 Abs. 5] DSGVO).[313]

(δ) Haftungsregelung

Regelungsbedarf besteht nicht nur für die Koordinierung der primären Verantwortung für die Aufgabenerfüllung, sondern auch für eine daran anknüpfende innerdeutsche Verteilung der Haftungsrisiken.

- Haftung nach der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung lässt den Mitgliedstaat der einladenden Aufsichtsbehörde für Schäden haften, die Bedienstete einer unterstützenden Aufsichtsbehörde im Einsatz verursachen (Art. 62 Abs. 4 [ex Art. 56 Abs. 3a] DSVO). Diese Haftung trifft nach der Datenschutz-Grundverordnung unab-

[312] Siehe hierzu S. 222.
[313] Siehe hierzu unten S. 227.

hängig von der innerstaatlichen Zuständigkeitsverteilung die Bundesrepublik als Völkerrechtssubjekt.[314] Gleichzeitig sind nach der innerstaatlichen Zuständigkeitsordnung im Falle der gemeinsamen Maßnahmen jedoch (vorrangig) die Aufsichtsbehörden einzelner Länder einladende Aufsichtsbehörde. Hier ist zu überlegen, ob und in welchem Umfang eine Haftung auf die Länder übertragen werden muss.
Gleiches gilt in dem umgekehrten Fall, in dem Bedienstete einer deutschen Aufsichtsbehörde im Ausland Schaden verursachen für die Erstattung des von dem empfangenden Mitgliedstaat geleisteten Schadensersatzes (Art. 62 Abs. 5 S. 2 [ex Art. 56 Art. 3b S. 2] DSGVO).

- Allgemeine Haftung insbesondere bei Vertragsverletzungsverfahren

Ob es einer spezifischen Regelung zum Regress bei einer Verurteilung der Bundesrepublik und der Anordnung eines Zwangsgeldes bzw. Pauschbetrages (Art. 260 Abs. 2 UAbs. 2 AEUV) bedarf, ist ebenfalls klärungsbedürftig; siehe hierzu S. 238.

(2) Bei rein innerstaatlichen Sachverhalten

Anders als die Fälle 1 und 2[315] behandelt Fall 3[316] einen rein innerstaatlichen Sachverhalt. Hier stellt sich die Frage, ob das Zusammenarbeitsverfahren grundsätzlich Anwendung findet bzw. inwieweit anderweitiger Bedarf für eine Regelung der Abstimmung zwischen den innerstaatlichen Aufsichtsbehörden besteht.
Das Verfahren der Zusammenarbeit (und das Kohärenzverfahren, s. u.) sind alleine in grenzüberschreitenden Sachverhalten anwendbar. Denn nur dann kann es eine betroffene und eine federführende Aufsichtsbehörde i. S. d. Art. 60 (ex Art. 54a) DSGVO geben. Beide können nicht im selben Mitgliedstaat liegen. In Fall 3 ergibt sich ein innerstaatlicher Abstimmungsbedarf

[314] Vgl. allgemein zur Haftungszuordnung Schlussanträgen des GA Geelhoed in der Rs. C-129/00, Slg. 2003, S. I-14637 (Komm./Italien), Rn. 50 ff.
[315] Dazu S. 209.
[316] Dazu S. 210.

damit nicht unmittelbar aus den Vorschriften der Datenschutz-Grundverordnung zum Zusammenarbeits(- und Kohärenz-)verfahren.
Gleichwohl ergibt er sich mittelbar aus ihr. Denn die Verpflichtung zur effektiven Einhaltung der materiellen Vorgaben der Datenschutz-Grundverordnung besteht auch in rein innerstaatlichen Sachverhalten.[317] Damit verbindet sich die Verpflichtung, innerhalb eines Mitgliedstaates, in dem die Aufsicht mehreren Behörden anvertraut ist, für eine kohärente Anwendung des Datenschutzrechts zu sorgen. Eine Zersplitterung der Rechtsanwendung innerhalb (der Aufsichtsbehörden) eines Mitgliedstaates ist geeignet, das Funktionieren des europäischen Binnenmarktes zu beeinträchtigen. Dies gefährdet den in der Union angestrebten einheitlichen Datenschutz (EG 135 S. 1 [ex EG 105 S. 1] DSGVO: „einheitliche Anwendung dieser Verordnung in der gesamten Union“).
Dem lässt sich nicht entgegenhalten, dass auch auf europäischer Ebene Unterschiede in der Rechtsanwendung dadurch entstehen können, dass in einer Vielzahl der Fälle nur die Aufsichtsbehörde eines Mitgliedstaates zuständig und betroffen sein wird, so dass keine europaweite Abstimmung des Vorgehens dieser Aufsichtsbehörde nötig ist. Denn die anderen Aufsichtsbehörden haben in jedem Fall die Möglichkeit, nach Art. 64 Abs. 2 (ex Art. 58 Abs. 2) DSGVO den EDA einzuschalten.[318]
Es besteht damit auf nationaler Ebene für Fall 3 der Bedarf, ein Verfahren der Zusammenarbeit (und der Kohärenz) zu etablieren. Dafür ist jedenfalls eine Regelung erforderlich, die einen dem Art. 60 Abs. 3-7 (ex Art. 54a Abs. 2 - 4a) DSGVO entsprechenden Abstimmungserfolg gewährleistet. Daneben ist wohl auch ein Entscheidungsmechanismus für solche Fälle vorzusehen, in

[317] Die Heranziehung des Art. 16 Abs. 2 S. 1 a. E. AEUV als Rechtsgrundlage setzt nicht voraus, dass in jedem Einzelfall, der von dem auf dieser Rechtsgrundlage ergangenen Rechtsakt erfasst wird, tatsächlich ein Zusammenhang mit dem freien Verkehr zwischen Mitgliedstaaten besteht; vgl. EuGH Urteil vom 20. Mai 2003, Rs. C-465/00, C-138/01 und C-139/01, Österreichischer Rundfunk, Randnr. 41 – noch zu Artikel 100a EG-Vertrag.
[318] Selbstverständlich nur, soweit eine Angelegenheit allgemeine Geltung oder Auswirkungen in mehr als einem Mitgliedstaat hat. Dies ist aber bei einer drohenden zersplitternden Rechtsanwendung wohl stets zu bejahen.

denen sich die betroffenen Aufsichtsbehörden nicht auf ein gemeinsames Vorgehen einigen können.[319]

b. Ansätze für die Gewährleistung des Verfahrens der Zusammenarbeit

Nähere Vorgaben, wie die zur Lösung aufgrund mehrerer mitgliedstaatlicher Aufsichtsbehörden entstehenden Fragen[320] zu etablierenden Verfahren ausgestaltet sein müssen, trifft die Datenschutz-Grundverordnung nicht. Sie belässt insoweit den Mitgliedstaaten grundsätzlich weiten Handlungsspielraum. Dabei ist dem Mitgliedstaat das Ziel vorgegeben, die Einhaltung der Regeln für das Kohärenzverfahren durch die Behörden sicherzustellen. Es ist eine zwingende Folge des Gedankens der Effektivität und der Prinzipien der Zusammenarbeit und lässt sich insoweit auch auf das Verfahren der Zusammenarbeit übertragen.

aa) Im Außenverhältnis: Zentrale Anlaufstelle für das Verfahren der Zusammenarbeit

Das Herzstück des Begleitverfahrens zum Verfahren der Zusammenarbeit ist die Einrichtung einer zentralen Anlaufstelle.[321] Alleine diese ermöglicht eine reibungsfreie Selbstkoordinierung in der Arbeit der nationalen Aufsichtsbehörden auf horizontaler Ebene.

Für die Bestimmung der zentralen Anlaufstelle empfehlen sich ähnliche Überlegungen wie bei der Bestimmung des Vertreters im EDA (siehe dazu S. 141). Auch hier gilt: Sachgerecht ist die Bestimmung einer ständigen Instanz, welche die Aufgaben als Ansprechpartner in institutionalisierter Form wahrnimmt.

Eine „Doppelspitzenlösung“[322] scheidet mit Blick auf das Gebot der wirksamen Erfüllung mitgliedstaatlicher Regelungspflichten aus. Denn in den anderen Mitgliedstaaten und bei den sonstigen Kontaktpartnern der zentralen Anlaufstelle kann dieses Modell Unsicherheiten über die genaue Zuständigkeit

[319] Siehe hierzu unten S. 228.
[320] Siehe oben S. 206.
[321] Vgl. oben S. 119.
[322] Dazu bereits S. 144.

und Zurechnung auszulösen. Es ist eine *einzelne* zentrale Anlaufstelle vorzusehen.

Diese muss eine der nach nationalem Recht gebildeten Aufsichtsbehörden sein. So formuliert EG 119 S. 2 (ex EG 93 S. 2) DSGVO: „Insbesondere sollte dieser Mitgliedstaat eine Aufsichtsbehörde bestimmen, die als zentrale Anlaufstelle […] fungiert". Dabei ist nicht nur nach dem Wortlaut, sondern auch entsprechend dem Grundgedanken der Unabhängigkeit der Aufsichtsbehörden jedenfalls ausgeschlossen, dass eine *außerhalb* der Aufsichtsbehörden stehende Person oder Einrichtung als zentrale Anlaufstelle fungiert. Gleichzeitig scheint es nicht von vorneherein ausgeschlossen, dass nicht eine Aufsichtsbehörde, sondern ein Bediensteter einer Aufsichtsbehörde als zentrale Anlaufstelle fungiert. Doch deutet auch hier der Wortlaut des EG 119 (ex EG 93) DSGVO klar in eine andere Richtung. Dies kommt noch deutlicher in der englischen Fassung zum Ausdruck, in der es heißt: „That Member State should in particular designate the supervisory authority which functions as a single contact point". Sie lässt für die Ernennung einer anderen Stelle oder Person als einer Aufsichtsbehörde als zentrale Anlaufstelle keinen Raum. Gleichzeitig schließt dies nicht aus, dass sich diese dauerhaft von einer Person als Ansprechpartner vertreten lässt. Entscheidend ist die Zurechenbarkeit zu einer Aufsichtsbehörde und damit die Gewährleistung der Unabhängigkeit.

Dabei ist jedoch einerseits *nicht* erforderlich, dass die Aufsichtsbehörde, die als zentrale Anlaufstelle firmiert, mit dem Vertreter im EDA zwingend (personen-)identisch ist. Dies kann den Koordinierungsaufwand und mögliche Reibungsverluste reduzieren. Jedoch sind solche nur in geringem Umfang zu befürchten, da sich die Aufgaben von Vertreter und zentraler Anlaufstelle stark unterscheiden. Andererseits ist nicht erforderlich, dass ununterbrochen dieselbe nationale Aufsichtsbehörde die zentrale Anlaufstelle repräsentiert. Zwar würde dies die Ansprechbarkeit durch Dritte vereinfachen und Unsicherheiten beseitigen. Es ermöglicht auch eine Professionalisierung der Aufsichtsstrukturen. Gleichwohl zeigt die Offenheit der Datenschutz-Grundverordnung für die verfassungsmäßige, organisatorische und administrative Struktur der Mitgliedstaaten (vgl. EG 117 S. 2 [ex EG 92 S. 2] DSGVO), dass die Mitgliedstaaten insoweit über Regelungsfreiheit verfügen.

Empfehlenswert ist gleichwohl eine Regelung mit weitgehender (organisationsrechtlicher) Verstetigung (wenn auch ohne Identität mit dem Vertreter im

EDA). Zu denken ist etwa daran, eine Aufsichtsbehörde der Länder dauerhaft als zentrale Anlaufstelle einzurichten. Dieser könnte dann zugleich die Koordinierung eines nationalen Zusammenarbeits- und Kohärenzverfahrens auferlegt werden.

bb) Im Innenverhältnis

Im Hinblick auf die Gestaltung der zentralen Anlaufstelle im Innenverhältnis kommt den Mitgliedstaaten ein weiter Regelungsspielraum zu. Klärungsbedürftig ist insoweit die innerstaatliche Zuständigkeit in materieller und formeller Hinsicht (i.), die Abstimmung der Aufsichtsbehörden (ii.), die (Selbst-)Kontrolle der nationalen Aufsichtsbehörden (iii.) und die Behandlung rein innerstaatlicher Sachverhalte (v.).[323]

i. Abstimmung bzgl. der innerstaatlichen Zuständigkeit/Betroffenheit einzelner Aufsichtsbehörden

Da die Zuständigkeitsregelungen der DSGVO auf das Verhältnis mehrere nationale Aufsichtsbehörden untereinander nicht anwendbar sind, muss eine nationale Regelung Zuständigkeitsfragen sowohl in materieller (1) als auch in formeller (2) Hinsicht beantworten.

(1) Materielle Regelung

Weitreichende Freiheiten genießt der Mitgliedstaat insbesondere im Hinblick auf die materielle Regelung der innerstaatlichen Zuständigkeiten, die den Aufsichtsbehörden übertragen sind. Die Datenschutz-Grundverordnung legt den Mitgliedstaaten nicht die Verpflichtung auf, das Konzept von betroffenen und federführenden Aufsichtsbehörden auch auf nationaler Ebene anzuwenden. Dies ergibt sich bereits daraus, dass nicht alleine eine Aufgliederung der

[323] Zur Regelung der Haftung kann auf das zu Art. 62 Abs. 4 [ex Art. 56 Abs. 3a] DSVO und Art. 62 Abs. 5 S. 2 [ex Art. 56 Art. 3b S. 2] DSGVO unten gesagte verwiesen werden, s. S. 236. Einer spezifischen Regelung zum Regress bei einer Verurteilung der Bundesrepublik und der Anordnung eines Zwangsgeldes bzw. Pauschbetrages (Art. 260 Abs. 2 UAbs. 2 AEUV) bedarf es nicht, da insoweit das Lastentragungsgesetz (§§ 1, 3 LastG) Anwendung findet (vgl. S. 238).

Zuständigkeiten nach örtlichen-, sondern auch nach sachlichen Erwägungen zulässig ist.
Gleichwohl spricht rechtspolitisch Vieles dafür, die Regelungen zur Zuständigkeit der Datenschutz-Grundverordnung grundsätzlich als Blaupause für die nationalen Aufsichtsbehörden zu nutzen, insbesondere soweit auch innerhalb Deutschlands – ebenso wie innerhalb der Union – eine örtlich(-sachliche) Zuständigkeitsverteilung geschaffen wird. So verhält es sich heute zwischen den Bundesländern. Nach Art. 30, 83 GG bzw. nach den allgemeinen Grundsätzen territorialer Souveränität sind die Aufsichtsbehörden der Länder grundsätzlich örtlich für das Gebiet ihrer Bundesländer zuständig (vgl. auch § 38 Abs. 6 BDSG).
So liegt es de lege ferenda insbesondere nahe, auch für die Bestimmung der innerstaatlichen Zuständigkeiten und Beteiligungsrechte die Kategorien der betroffenen und der federführenden Aufsichtsbehörde zu übernehmen. Hierzu bedarf es einer Art. 4 Nr. 22 bzw. Art. 60 Abs. 1 (ex Art. 4 Nr. 19a bzw. Art. 54a Abs. 1) DSGVO nachempfundenen Regelung. Sie stellt auch eine Kohärenz der Regelungskonzepte zwischen der Datenschutz-Grundverordnung und den mitgliedstaatlichen Ausgestaltungsregelungen her.
Gleichzeitig müsste diese Regelung an die hergebrachte Trennung der Zuständigkeiten – je nach Betroffenheit öffentlicher und nicht-öffentlicher Stellen – angepasst werden.
Hiernach wäre die *BfDI* betroffen, wenn:

- der Verantwortliche oder der Auftragsverarbeiter eine öffentliche Stelle des Bundes ist oder
- eine Beschwerde bei ihr eingereicht wurde.

Die Aufsichtsbehörden der *Länder* wären betroffen, wenn:

- der Verantwortliche oder der Auftragsverarbeiter eine öffentliche Stelle des Landes ist.[324]

[324] In den Fällen, in denen die Aufsicht der Länder über ihre öffentlichen Stellen berührt ist, machen die Länder regelmäßig von der Öffnungsklausel in Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO Gebrauch. In diesen Fällen findet das Prinzip der zentralen Anlaufstelle nach der DSGVO gerade keine Anwendung (EG 128 S. 1 [ex 98 S. 1]); vgl. auch S. 242. Das macht eine innerstaatliche Koordinierung unionsrechtlich, nicht aber unbedingt innerstaatlich entbehrlich.

- der Verantwortliche oder der Auftragsverarbeiter eine nicht-öffentliche Stelle ist und im Hoheitsgebiet des Landes dieser Aufsichtsbehörde niedergelassen ist,
- diese Verarbeitung durch eine nicht-öffentliche Stelle erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz in diesem Land hat oder haben kann oder
- eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde.

Für die *Federführung* würde gelten: Federführend ist

- die *BfDI*, wenn der Verantwortliche oder der Auftragsverarbeiter eine öffentliche Stelle des Bundes ist,
- die Aufsichtsbehörde *des Landes*, wenn der Verantwortliche oder der Auftragsverarbeiter eine öffentliche Stelle des Landes ist,
- in allen anderen Fällen / wenn der Verantwortliche oder der Auftragsverarbeiter eine nicht-öffentliche Stelle ist, *die Aufsichtsbehörde der Hauptniederlassung oder der einzigen Niederlassung des Verantwortlichen oder des Auftragsverarbeiters.*

(2) Formelle Regelung: Verfahren der Zuständigkeitsbestimmung

Für die Abstimmung der innerstaatlichen Zuständigkeit bieten sich zwei Lösungswege an.
Einerseits könnte die zentrale Anlaufstelle zur Entscheidung berufen werden, andererseits könnten die Aufsichtsbehörden gemeinsam Zuständigkeitsfragen klären müssen.
Die zentrale Anlaufstelle fungiert grundsätzlich als Transmitter für den Kontakt zwischen den ausländischen Aufsichtsbehörden bzw. zentralen Anlaufstellen und den einzelnen deutschen Aufsichtsbehörden. Die Übertragung der Entscheidung über die Zuständigkeit auf die Anlaufstelle würde die für die Entscheidung benötigte Abstimmungszeit auf ein Minimum reduzieren und so dem Bedürfnis nach sachgerechter Informationsweiterleitung und Koordinierung mit den Aufsichtsbehörden anderer Mitgliedstaaten am besten ge-

---

Denn klärungsbedürftige Sachverhalte können sowohl öffentliche Stellen als auch nicht-öffentliche Stellen gleichermaßen betreffen.

recht. Die Ausstattung der zentralen Anlaufstelle mit der Befugnis zur Festsetzung der Zuständigkeiten ist grundsätzlich rechtlich umsetzbar. Der Bund könnte eine entsprechende Regelung im Rahmen seiner Kompetenz zur Regelung des Verwaltungsverfahrens bzw. der Behördeneinrichtung (Art. 84 Abs. 1 S. 2 GG) für die Aufsicht über nicht-öffentliche Stellen treffen. Für die Aufsicht über öffentliche Stellen müssten die Länder die Befugnis der zentralen Anlaufstelle durch Staatsvertrag übertragen.
Denkbar wäre es aber auch, die deutschen Datenschutzbehörden in ihrer Gesamtheit über Zuständigkeitskonflikte befinden zu lassen. Die zentrale Anlaufstelle träfe dann bei Unsicherheiten – ebenso wie alle Aufsichtsbehörden – die Verpflichtung, eine Entscheidung herbeizuführen. Die Ausgestaltung könnte sich an das Kohärenzverfahren anlehnen (vgl. Art. 65 Abs. 1 lit. b [ex Art. 58a Abs. 1 lit. b] DSGVO[325]).

ii. Abstimmung des Vorgehens einzelner oder mehrerer nationaler Aufsichtsbehörden

Hinsichtlich der Abstimmung des Vorgehens einzelner oder mehrerer Aufsichtsbehörden stellen sich verschiedene Teilfragen. Sie betreffen insbesondere die Beteiligung an der Abstimmung (1), die Mitwirkungsberechtigung von Bund und Ländern an der Entscheidungsfindung (2) und den Modus der Programmierung (3).

(1) Beteiligung an der Abstimmung – Gliederung nach Gegenstand der Entscheidung

Ob nur die betroffenen Aufsichtsbehörden oder die Gesamtheit der Aufsichtsbehörden eine Abstimmungsentscheidung trifft, ist eine der Kernfragen des Koordinierungsprozesses. Handelt es sich um einen grenzüberschreitenden Sachverhalt, bei dem nur eine Aufsichtsbehörde der Länder betroffen ist, ist nach der allgemeinen Zuständigkeitsordnung nur diese zur Entscheidung

[325] Nach dem Wortlaut kann hier nur die Frage nach der federführenden Aufsichtsbehörde, nicht aber nach der Betroffenheit einer Aufsichtsbehörde an sich geklärt werden. Die Frage der Betroffenheit wird aber wohl a maiore a minus mit geregelt werden können, da auch diese entscheidend für das Zusammenarbeits- und Kohärenzverfahren ist.

berufen (Fall 1).[326] Sind bei grenzüberschreitenden Sachverhalten mehrere Aufsichtsbehörden in ihrer Zuständigkeit berührt, sind grundsätzlich alle am Abstimmungsverfahren zu beteiligen (Fall 2).[327]

α) Option 1: Abstimmung alleine unter den betroffenen Aufsichtsbehörden

Eine Lösung kann dahin gehen, *alleine unter den betroffenen Aufsichtsbehörden* eine Abstimmung vorzusehen (insoweit wäre dies bei der Aufsicht über öffentliche Stellen regelmäßig ausschließlich die BfDI oder ein einzelner Landesdatenschutzbeauftragter). Diese Lösung folgt der Logik der innerstaatlichen Zuständigkeitsverteilung. Denn in diesen Fällen sind diese an sich in der Sache zuständig und es drängt sich insoweit zumindest aus nationaler Perspektive kein Grund auf, deren Vollzugsentscheidungen von anderen Aufsichtsbehörden mitbestimmen zu lassen. Darüber hinaus beschleunigt dieser Lösungsweg den Entscheidungsprozess.

β) Option 2: Abstimmung zwischen allen LfDIs (und ggf. auch des BfDI)

Andererseits könnte in allen Fällen – jedenfalls, wenn die Aufsicht über nicht-öffentliche Stellen betroffen ist – eine Entscheidung zwischen *allen LfDIs* (und ggf. auch des BfDI) herbeigeführt werden. Für eine solche Lösung streitet die mittelbare Rückwirkung derartiger Vollzugsentscheidungen auf die anderen mitgliedstaatlichen Aufsichtsbehörden. Die Datenschutz-Grundverordnung fordert eine weitestgehend einheitliche Anwendung des Datenschutzrechts. Entscheidungen im Bereich des Zusammenarbeitsverfahrens tendieren dazu – wiewohl nur für den konkreten Fall getroffen (und vergleichsweise schwächer als im Kohärenzverfahren) – grenzüberschreitende Vereinheitlichungstendenzen auszulösen. Dies gilt insbesondere dann, wenn im Fall der Divergenz mit der federführenden Aufsichtsbehörde eine Entscheidung des EDA herbeigeführt wird (Art. 65 Abs. 1 lit. c [ex Art. 58a Abs. 1 lit. d] DSGVO). Der Ansatz, alle nationalen Aufsichtsbehörden bzw.

[326] Dazu S. 209.
[327] Dazu S. 210.

jedenfalls die potenziell betroffenen mit in den nationalen Entscheidungsfindungsprozess einzubeziehen, kann insofern durchaus sinnvoll sein.

γ) Option 3: Betrauung alleine der (innerstaatlich) federführenden Aufsichtsbehörde

Denkbar ist es auch, *alleine die (innerstaatlich) federführende Aufsichtsbehörde* mit der Meinungsfindung zu betrauen. Es ließe sich dann ein Gleichlauf mit den Regelungen der Datenschutz-Grundverordnung herstellen. Sie legt die Aufgabe, einen Beschlussentwurf zu konzipieren und diesen dann mit den anderen betroffenen Aufsichtsbehörden abzustimmen, in die Hände der federführenden Aufsichtsbehörde.
Andere an sich betroffene Aufsichtsbehörden könnten im Rahmen einer weitergehenden innerstaatlichen Zuständigkeitskonzentration von der Zuständigkeit ausgeschlossen werden und die Entscheidung alleine bei der federführenden Aufsichtsbehörde zur Behandlung verbleiben. Damit verbände sich aber ein intensiver Eingriff in das grundsätzlich einer örtlichen Zuständigkeitsregelung folgende föderale System.

δ) Rechtspolitische Kurzbewertung

Die von Entscheidungen im Zusammenarbeitsverfahren ausgehende Rückwirkung auf zukünftige Entscheidung ist verglichen mit solchen im Kohärenzverfahren eher gering. Vor allem trägt die Beschränkung des Kreises der einzubeziehenden Aufsichtsbehörden zur effizienten Aufgabenwahrnehmung bei. Die Berücksichtigung der Interessen nicht unmittelbar berührter Aufsichtsbehörden lässt sich durch Mitwirkungsrechte, insbesondere ein Recht zur Stellungnahme kompensieren. Alle drei Lösungen scheinen, soweit sie kompetenziell verfassungskonform angeordnet werden, sowohl mit dem nationalen Verfassungsrecht im Übrigen als auch mit der Datenschutz-Grundverordnung vereinbar.

(2) Mitwirkungsberechtigung von Bund und Ländern an der Entscheidungsfindung

Ein innerstaatliches Koordinierungsregime muss eine Lösung für die Frage vorhalten, ob und ggf. wann Bund und/oder Länder in den Kreis der potenziell entscheidungsberufenen Stellen einbezogen werden sollen.
Insoweit lassen sich zwei Fälle unterscheiden: Handeln in Bezug auf oder mit Auswirkung auf die Aufsicht über (α) öffentliche Stellen des Bundes und öffentliche Stellen der Länder und (β) nicht-öffentliche Stellen.

α) Handeln mit Auswirkung auf die Aufsicht über öffentliche Stellen des Bundes und öffentliche Stellen der Länder

Soweit ein Vorgehen im Zusammenarbeitsverfahren (wobei hier wegen des weitreichenden Ausschlusses von Art. 60 [ex Art. 54a] DSGVO grundsätzlich nur Art. 61 und 62 [ex Art. 55 und 56] DSGVO in Betracht kommen) nur die öffentlichen Stellen eines Landes oder des Bundes betrifft, liegt es prima vista nahe, nur der entsprechenden Aufsichtsbehörde ein Mitspracherecht einzuräumen. Die Datenschutz-Grundverordnung steht dem nicht entgegen. Sie trägt eine Nichteinbeziehung in die Abstimmung grundsätzlich mit. Denn EG 128 (ex EG 98) DSGVO sieht vor, dass im Fall des Ausschlusses von Art. 60 (ex Art. 54a) DSGVO auch das Verfahren der Kohärenz und damit das Prinzip der zentralen Anlaufstelle unangewendet bleibt. In diesem Fall steht aus unionsrechtlicher Perspektive die effektive Anwendung der Verordnung also zurück.
Die Nichteinbeziehung findet eine verfassungsrechtliche Rechtfertigung darin, dass in diesen Fällen die Länder bzw. der Bund die alleinige Gesetzgebungskompetenz und Kompetenz zur Regelung des Verwaltungsverfahrens innehaben. Gleichzeitig ist – anders als im Kohärenzverfahren – die faktische Ausstrahlung und Bindungswirkung von Entscheidungen und Stellungnahmen im Zusammenarbeitsverfahren eher gering. Es ist deshalb nicht zwingend erforderlich, auch den Bund und alle Bundesländer an der Willensbildung zu beteiligen.

β) Handeln mit Auswirkung auf die Aufsicht über nicht-öffentliche Stellen des Bundes und nicht-öffentliche Stellen der Länder

Soweit die Aufsicht über nicht-öffentliche Stellen betroffen ist, liegt die Sache insoweit anders, als der Bund von einer Ausstrahlungswirkung auf den Vollzug nicht betroffen sein kann. Denn er ist vom Vollzug der Aufsicht über die nicht-öffentlichen Stellen gänzlich ausgeschlossen. Gleichwohl steht ihm hier die materielle Gesetzgebungsbefugnis (insbesondere aus Art. 74 Abs. 1 Nr. 11 GG) für die durch das Verwaltungsverfahren ausgelösten inhaltlichen Fragen zu. Insofern hat er zumindest eine sachliche Kompetenz auf seiner Seite. Dies kann es sachlich angezeigt erscheinen lassen, den Bund hier nicht von vorneherein vom Kreis der Mitwirkungsberechtigten auszuschließen.

(3) Modus der Programmierung – Konsens- oder Mehrheitsprinzip

Das Abstimmungsverfahren bedarf einer Entscheidungsregel für diejenigen Fälle, in denen die zur Entscheidung Berufenen unterschiedliche Positionen vertreten. In Betracht kommen das Konsensprinzip oder das Mehrheitsprinzip, ggf. unterstützt durch ein Quorum.
Die souveräne Gleichheit der Länder streitet für die Anwendung des Konsensprinzips. Immerhin ist die Wahrnehmung der Aufsicht integraler Teil der Staatlichkeit der Länder. Das Konsensprinzip droht das innerstaatliche Abstimmungsverfahren aber schwerfällig und zeitraubend werden zu lassen. Entscheidungen müssen indes ggf. in kürzester Zeit, jedenfalls im Zeitraum von ein bis zwei Monaten getroffen werden. Eine auf Konsens zielende Abstimmung läuft Gefahr, in diesem Zeitraum kein Ergebnis hervorzubringen. Die Praktikabilität und Effektivität des Verfahrens leiden.
Dies spricht dafür, das Mehrheitsprinzip anzuwenden. Verfassungsrechtlich ist eine solche Mehrheitsentscheidung im Hinblick auf den verfassungsrechtlichen Grundsatz eigenverantwortlicher Aufgabenwahrnehmung[328] rechtfertigungsbedürftig. Zulässig ist eine Mehrheitsentscheidung nur, wenn die Wahrnehmung auf der Grundlage von in Art. 23 GG eingegangenen Verpflichtungen nicht anders als durch eine Überformung sonst grundsätzlich

[328] Dazu auch bereits S. 204.

bestehender Kompetenzwahrnehmungen möglich ist. Für das Abstimmungsverfahren der Datenschutz-Grundverordnung liegen diese Voraussetzungen wohl vor, ist doch davon auszugehen, dass die fristgebundene Koordinierung, welche die Verordnung den Mitgliedstaaten abverlangt, in einem Verfahren der Einstimmigkeit, das jedem Land eine Veto-Position verleiht, kaum gelingen kann.[329]

iii. (Selbst-)Kontrolle der nationalen Aufsichtsbehörden

Aufsichtsbefugnisse der zentralen Anlaufstelle wären einer effektiven Durchführung der Datenschutzaufsicht in Deutschland zuträglich. Denn sie könnten sicherstellen, dass nicht die Bundesrepublik als Ganze ihre Pflichten aus der Datenschutz-Grundverordnung gegenüber den ausländischen Aufsichtsbehörden bzw. deren zentralen Anlaufstellen verletzt. Insoweit müsste der zentralen Anlaufstelle zumindest eine Rechtsaufsichtsfunktion zukommen. Dann könnte sie kontrollieren, ob die mitgliedstaatlichen Aufsichtsbehörden ihre (mittelbar) aus der Datenschutz-Grundverordnung stammenden Verpflichtungen, insbesondere zur Amtshilfe (Art. 61 Abs. 2 [ex Art. 55 Abs. 2] DSGVO) etc., einhalten.

Mit dem Gedanken der Unabhängigkeit nach Art. 52 DSGVO wäre das wohl vereinbar. Denn er schließt Beschränkungen der Unabhängigkeit innerhalb des Aufsichtssystems eines Mitgliedstaates nicht aus. Dies gilt insbesondere, soweit sie der Gestaltung einer effektiven Aufsichtsstruktur zu dienen bestimmt sind und der Mitgliedstaat von seinem nach Art. 51 Abs. 3 DSGVO bestehenden Regelungsspielraum Gebrauch macht. Ein Teil des Begleitverfahrens, welches Art. 51 Abs. 3 S. 2 DSGVO fordert, kann auch eine Binnenkontrolle der Aufsichtsbehörden untereinander sein.

Gleichwohl kommt dem Bund eine solche Kompetenz zur Etablierung derartiger Aufsichtsbefugnisse nach dem Grundgesetz nicht zu. Zwar steht dem Bund nach Art. 84 Abs. 3 S. 1 GG bereits die Rechtsaufsicht über die Ausführung der Bundesgesetze durch die Länder zu. Doch lässt sich diese Kompe-

[329] Nicht nur die Etablierung des Mehrheitsprinzips, sondern auch eine Verstetigung der Abstimmung und der institutionellen Rahmenbedingungen kann einen Beitrag zur Effizienzsteigerung und Professionalisierung der Koordinationsverfahren darstellen. Zu den Regelungsmöglichkeiten der organisationsrechtlichen Verstetigung siehe S. 150.

tenz hier (obgleich die Landesbeauftragten für den Datenschutz und Informationsfreiheit aufgrund ihrer unabhängigen Stellung zumeist oberste Landesbehörden sind) nicht fruchtbar machen. Denn Gegenstand ist hier nicht die generelle Aufsicht über die Ausführung, sondern die Koordinierung von Kompetenzträgern. Betroffen ist nicht die generelle Aufsicht über die Ausführung und es ist auch nicht gesagt, dass der Bund die zentrale Anlaufstelle stellen wird. Vielmehr ist Regelungsgegenstand eine Frage des Verfahrens, die der Bund nach Art. 84 Abs. 1 S. 2 GG regeln darf, soweit seine materielle Gesetzgebungskompetenz für nicht-öffentliche Stellen reicht. Gleichwohl könnte hierauf auch verzichtet werden, um die Unabhängigkeit der einzelnen Aufsichtsbehörden zu stärken.

iv. Rein innerstaatliche Sachverhalte

Wie eine Regelung für die Abstimmung zwischen mehreren deutschen Aufsichtsbehörden für einen rein innerstaatlichen Sachverhalt (Fall 3)[330] aussehen könnte, ist eine intrikate Frage. Grundsätzlich greift hier ein weiter Regelungsspielraum des nationalen Gesetzgebers.
Denn das „Wie“ der Abstimmung ist ihm freigestellt. Denkbar ist es, – um ein Maximum an Abstimmung zu erreichen – bereits auf der ersten Stufe der Abstimmung stets eine Abstimmung zwischen allen nationalen Aufsichtsbehörden herbeizuführen. Dies ist aber wenig praktikabel und auch verfassungsrechtlich, wegen des weitreichenden Einflusses auf die Gesetzesanwendung durch andere Bundesländer, problematisch.
Überzeugender ist es, das System des Art. 60 Abs. 3-6 (ex Art. 54a Abs. 2-4) DSGVO auf die nationalen Ebene zu übertragen – entweder, indem es selbst entsprechend im BDSG-neu geregelt wird, oder indem die Regelung der Datenschutz-Grundverordnung für entsprechend anwendbar erklärt wird. Flankierend müsste dann wohl auch ein System für den Erlass von Beschlüssen nach Art. 60 Abs. 7 - 9 (ex Art. 54a Abs. 4a - 4bb) DSGVO aufgenommen werden. Auch deshalb ist die erstgenannte Lösung vorzuziehen.

[330] Siehe S. 210.

c. Regelungskompetenz für die einzelnen Ansätze

aa) Im Außenverhältnis: Errichtung zentrale Anlaufstelle

Die Errichtung einer zentralen Anlaufstelle weist kompetenzrechtlich eine strukturelle Ähnlichkeit mit der Errichtung des gemeinsamen Vertreters nach Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO auf. Auch hier besteht ein großer Außenbezug der Regelung. Gleichwohl unterfällt auch die Errichtung der zentralen Anlaufstelle wohl nicht unmittelbar den auswärtigen Angelegenheiten. Bund und die Länder bewegen sich in einem komplexen Kompetenzfeld geteilter Zuständigkeiten.[331]
Die Kompetenzproblematik schwächt sich jedoch für den Bereich der Errichtung der zentralen Anlaufstelle ein Stück weit aufgrund der Vorschrift des Art. 55 Abs. 2 (ex Art. 51 Abs. 2) DSGVO sowie des EG 128 S. 1 (ex EG 98 S. 1) DSGVO ab: Machen der Bund oder die Länder von der Öffnungsklausel des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO für den öffentlichen Bereich Gebrauch, sind hierauf bezogene Aufsichtstätigkeiten nicht dem Verfahren der Zusammenarbeit und der Kohärenz und damit dem Prinzip der zentralen Anlaufstelle unterworfen.

bb) Im Innenverhältnis

Nicht anders liegt es im Innenverhältnis. Betroffen ist hier stets das gesamte Aufsichtshandeln der Aufsichtsbehörden. Dieses stützt sich bei den Aufsichtsbehörden der Länder teilweise auf Sachkompetenzen des Bundes, teilweise auf solche der Länder.

d. Sonderfälle

In die nationale Aufsichtsstruktur sind die Sonderfälle der Religionsgemeinschaften und der Deutschen Welle (DW) nur mittelbar einbezogen. Ob und wie sie in das System der nationalen Koordinierung einbezogen werden können bzw. müssen, ist unklar.

---

[331] Dazu im Einzelnen S. 136 ff.

aa) Journalismus / Deutsche Welle

Hinsichtlich der Deutschen Welle erlaubt Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO weitreichende Abweichungen von Kapitel VII (Zusammenarbeit und Kohärenz) der Datenschutz-Grundverordnung. Die Verordnung äußert sich nicht ganz eindeutig dazu, ob das auch ein Herauslösen aus dem Zusammenarbeitsverfahren umschließt, der Datenschutzbeauftragte der Deutschen Welle also nicht in das nationale Begleitverfahren eingebunden wird. Auf den ersten Blick scheint dies sehr weitreichend, insbesondere mehr als ein Ausschluss denn als ein Abweichen von den betreffenden Vorschriften. Doch ist dies wohl die konsequente Folge der Regelung, welche die Datenschutz-Grundverordnung mit der Eröffnung eines nationalen Regelungsauftrages getroffen hat. Jede Einbindung journalistischer Stellen in das nationale Begleitverfahren würde deren Unabhängigkeit empfindlich treffen.
Gleichwohl scheint auch eine Einbindung nicht ganz ausgeschlossen, die weitestgehende Alleinentscheidungsbefugnisse vorsieht, z. B. bezüglich des Vorgehens des Datenschutzbeauftragten der Deutschen Welle. Das würde jedenfalls in der Außenbeziehung Deutschlands die Einheitlichkeit des Ansprechpartners wahren.

bb) Religionsgemeinschaften

Ob dies auch für Kirchen und Religionsgemeinschaften zutrifft, ist ungleich schwieriger zu beantworten. Deren eigenständige Datenschutzregelungen dürfen zwar nach Art. 91 Abs. 1 (ex Art. 85 Abs. 1) DSGVO weiter angewandt, müssen aber mit der Datenschutz-Grundverordnung in Einklang gebracht werden.
Art. 91 Abs. 2 (ex Art. 85 Abs. 2) DSGVO gebietet eine Aufsicht durch eine unabhängige Aufsichtsbehörde, erlaubt aber zugleich Abweichungen: Die Aufsichtsbehörde darf „spezifischer Art sein“ (Art. 91 Abs. 2 DSGVO). Womöglich verbindet sich damit auch ein Regelungsspielraum des Mitgliedstaats, diese Aufsichtsbehörden nicht zwingend in das System des Kohärenzmechanismus einbinden zu müssen, den die DSGVO etabliert. Allerdings muss diese Aufsichtsbehörde „die in Kap. VI niedergelegten Bedingungen erfüllen“ (Art. 91 Abs. 2 DSGVO). Dazu gehört die Teilnahme am Verfahren der Zusammenarbeit und der Kohärenz aber nicht. Denn diese regelt das Kap.

VII, nicht das Kap. VI. Das deutet auf ein beredtes Schweigen des Unionsgesetzgebers hin: Die Sonderstellung rechtfertigt wohl eine Ausnahme von der Einbeziehung in den aufsichtsrechtlichen Koordinierungsmechanismus.

36. Art. 61 (ex Art. 55): Gegenseitige Amtshilfe

Die Vorschriften über die Amtshilfe lösen für die Mitgliedstaaten keinen Umsetzungsbedarf aus. Insbesondere begründen sie keinen Regelungsauftrag für die Mitgliedstaaten. Vielmehr ist eine einheitliche europäische Regelung erforderlich. Insoweit ist es folgerichtig, dass Art. 61 Abs. 9 (ex Art. 55 Abs. 10) DSGVO der Kommission eine Kompetenz nach Art. 291 AEUV einräumt, um das Verfahren zu regeln.
§ 38 Abs. 1 S. 6 BDSG legt im bisherigen deutschen Recht den Aufsichtsbehörden die Verpflichtung auf, den Aufsichtsbehörden anderer Mitgliedstaaten der Europäischen Union auf Ersuchen ergänzende Hilfe zu leisten. Wegen der Dopplung mit der nach Art. 56 Abs. 4 i. V. m. Art. 60 Abs. 2 i. V. m. Art. 57 Abs. 1 lit. g (ex Art. 51a Abs. 2c i. V. m. Art. 54a Abs. 1a i. V. m. Art. 52 Abs. 1 lit. c) DSGVO bestehenden Pflicht zur Amtshilfe streiten mit Blick auf das Normwiederholungsverbot grundsätzlich gute Gründe für eine Aufhebung der Vorschrift. Jedoch formuliert Abs. 1 einen Handlungsauftrag an die Mitgliedstaaten, für den Fall, dass die nationalen Aufsichtsbehörden nicht in der Lage sind, effektiv mit denen der anderen Mitgliedstaaten zusammenzuarbeiten („Die Aufsichtsbehörden […] treffen Vorkehrungen für eine wirksame Zusammenarbeit“). Eine derartige Anweisung an die Mitgliedstaaten enthält auch Art. 52 Abs. 4 (ex Art. 47 Abs. 5) DSGVO; Art. 61 Abs. 1 (ex Art. 55 Abs. 1) DSGVO geht über diese Forderung nicht hinaus. Im Ergebnis ist daher eine Beibehaltung der Vorschrift im nationalen Recht – ggf. ergänzt um weitere Vorkehrungen für eine wirksame Zusammenarbeit – empfehlenswert.

37. Art. 62 (ex Art. 56): Gemeinsame Maßnahmen der Aufsichtsbehörden

a. Inhalt der Regelung

Art. 62 (ex Art. 56) DSGVO legt den Aufsichtsbehörden gemeinsame Maßnahmen „einschließlich gemeinsamer Untersuchungen und gemeinsamer Durchsetzungsmaßnahmen“ in grenzüberschreitenden Sachverhalten auf. Er sieht ein Recht der Aufsichtsbehörden vor, an gemeinsamen Maßnahmen in einem anderen Mitgliedstaat teilzunehmen (Abs. 2 S. 1). Nach Art. 55 Abs. 1 (ex Art. 51 Abs. 1) DSGVO gilt hierbei grundsätzlich, dass nur die Aufsichtsbehörde des Mitgliedstaates, in dem die Maßnahme stattfindet, ihre Befugnisse nach der Datenschutz-Grundverordnung ausüben darf.
Hiervon macht Art. 62 Abs. 3 S. 1 (ex Art. 56 Abs. 3 S. 1) zwei bedeutende Ausnahmen: Ein einladender Mitgliedstaat kann im Rahmen von gemeinsamen Maßnahmen der Aufsichtsbehörde eines anderen teilnehmenden Mitgliedstaates Untersuchungsbefugnisse übertragen (Hs. 1). Darüber hinaus kann vorgesehen werden, dass es den Mitgliedern oder Bediensteten der unterstützenden Aufsichtsbehörde gestattet ist, ihre Untersuchungsbefugnisse nach dem Recht ihres eigenen Mitgliedstaats auszuüben (Hs. 2). Dies bedeutet, dass einerseits exekutive Hoheitsrechte i. S. e. „jurisdiction to enforce“ auf ausländische Behörden übertragen werden. Dazu kann auch die „jurisdiction to prescribe“ auf den entsendenden Staat übertragen werden, wenn den entsandten Mitarbeitern der Aufsichtsbehörde im Empfängerstaat gestattet wird, nach ihren eigenen nationalen Untersuchungsbefugnissen zu handeln.
Insbesondere Letzteres hat eine im Unionsrecht bisher – soweit ersichtlich – nicht da gewesene Öffnung der nationalen Rechtssysteme und des Zurückfahrens von Souveränität zur Folge. So legt § 93 Abs. 1 IRG[332] zum Beispiel nur fest, dass Ermittlern aus anderen Staaten die Durchführung von Ermittlungsmaßnahmen übertragen werden kann – der ausländische Ermittler ist jedoch an die Ermittlungsbefugnisse des einladenden Staates gebunden (vgl. Art. 13

[332] Grundlage hierfür ist Art. 13 Übereinkommen über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der EU, 2000/C 197/01.

Abs. 3 (b) des Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der EU).
Schließlich verfügt Art. 62 Abs. 3 S. 3 (ex Art. 56 Abs. 3 S. 3) DGVO, dass die Mitglieder oder Bediensteten der unterstützenden Aufsichtsbehörde dem Recht des Mitgliedstaats der einladenden Aufsichtsbehörde unterliegen. Dies muss wohl so verstanden werden, dass dies gilt, soweit nicht nach Art. 62 Abs. 3 S. 1 Hs. 2 (ex Art. 56 Abs. 3 S. 1 Hs. 2) DSVGO das Recht der Untersuchungsbefugnisse des entsendenden Mitgliedstaates anwendbar ist. Damit stellt die Datenschutz-Grundverordnung in der Sache klar, dass die entsandten Mitglieder und Bediensteten der unterstützenden Aufsichtsbehörde keine Art diplomatischer oder konsularischer Immunität genießen. So gelten insbesondere die strafrechtlichen Vorschriften des empfangenden Staates.

b. Einordnung in das System der Öffnungsklauseln

Ob die Öffnungsklausel des Art. 62 Abs. 3 S. 1 Hs. 1 (ex Art. 56 Abs. 3 S. 1 Hs. 1) DSGVO fakultativer oder obligatorischer Natur ist, ist nicht eindeutig. Denn in Abgrenzung zu der Öffnungsklausel aus Hs. 2 („soweit dies nach dem Recht des Mitgliedstaates der einladenden Aufsichtsbehörde zulässig ist“), enthält Hs. 1 keine derartige weite Formulierung, die auch das „Ob“ einer Übertragung miteinbezieht. Die Öffnungsklausel erfasst hinsichtlich der Übertragung von Untersuchungsbefugnissen alleine das „Wie“. Diese wird dadurch obligatorisch, da das „Ob“ ohne Regelungen zum „Wie“ nicht praktikabel ist.
Hingegen ist Hs. 2 ausweislich des klaren Wortlauts insgesamt fakultativer Natur. Dies entspricht auch dem Zweck der Regelung. Denn eine gemeinsame Maßnahme in einem Mitgliedstaat ist auch dann möglich, wenn die Mitglieder und Bediensteten der entsendenden Aufsichtsbehörde hinsichtlich der Untersuchungsbefugnisse dem Recht des empfangenden Mitgliedstaates unterliegen. Dies erschwert die Tätigkeit nur insoweit, als die Mitglieder und Bediensteten sich dem ihnen grundsätzlich unbekannten Recht des empfangenden Mitgliedstaates anpassen müssen. Gleichzeitig sind die wesentlichen Untersuchungsbefugnisse bereits unmittelbar durch Art. 58 (ex Art. 53) DSGVO selbst und damit unionseinheitlich geregelt.

c. Vergleich zur Datenschutzrichtlinie

Die Datenschutzrichtlinie enthielt keine dem Art. 62 (ex Art. 56) DSGVO vergleichbaren Regelungen. Art. 28 Abs. 6 UAbs. 1 DSRL bestimmte – ohne Ausnahmen zuzulassen –, dass jede Kontrollstelle alleine im Hoheitsgebiet ihres Mitgliedstaats für die Ausübung der ihr übertragenen Befugnisse zuständig ist. Eine Kontrollstelle kann die Kontrollstelle eines anderen Mitgliedstaates daher lediglich um die Ausübung ihrer Befugnisse ersuchen.

d. Bisherige Ausgestaltung im nationalen Recht

Bisher sah das BDSG alleine eine Verpflichtung zur grenzüberschreitenden Amtshilfe vor, so in (§ 26 Abs. 4 S. 2 i. V. m.) § 38 Abs. 1 S. 5 BDSG.

e. Umsetzung und Anpassung

aa) Übertragung von Untersuchungsbefugnissen, Art. 62 Abs. 3 S. 1 Hs. 1 (ex Art. 56 Abs. 3 S. 1 Hs. 1)

Eine Übertragung von Ermittlungs- bzw. Untersuchungsbefugnissen ist im deutschen Recht kein absolutes Novum. Anders als bei Erlass des § 93 IRG steht bei Art. 62 Abs. 3 S. 1 Hs. 1 (ex Art. 56 Abs. 3 S. 1 Hs. 1) DSGVO das „Ob“ der Übertragung bereits aufgrund der unmittelbar geltenden Datenschutz-Grundverordnung fest. Die nationale Regelung kann also nur noch das „Wie“, insbesondere das einzuhaltende Verfahren regeln. § 93 IRG enthält hierfür jedoch kein Regelungsvorbild, da dort das „Wie“ nicht näher ausgestaltet ist. Die Zuständigkeit gibt die Datenschutz-Grundverordnung insoweit vor, als dass diese „der Aufsichtsbehörde“ zufällt. Dies meint jedoch die Gesamtheit der deutschen Aufsichtsbehörden – notwendig ist damit eine innerstaatliche Zuständigkeitsverteilung.

i. Kompetenz für die Regelungen betreffend (Zuständigkeit und Verfahren) der Übertragung

Die innerstaatliche Kompetenzverteilung wirft die Frage auf, ob das „Wie“ der Einräumung des Rechts an ausländische Behörden, in Deutschland hoheitlich tätig zu werden, den auswärtigen Angelegenheiten (Art. 73 Abs. 1 Nr. 1 GG) unterfällt oder ein Teil des Verwaltungsverfahrens (Art. 83, 84

Abs. 1 S. 1 GG) ist.[333] Ersteres umfasst das Recht, jene Fragestellungen zu normieren, die sich aus der Stellung der Bundesrepublik Deutschland zu anderen Völkerrechtssubjekten ergeben.[334] Das Recht zur Regelung des Verwaltungsverfahrens umschließt hingegen die Art und Weise des Verwaltungshandelns, insbesondere die Art der Prüfung und Vorbereitung der Entscheidung.[335]

Die Datenschutz-Grundverordnung regelt mit der Anordnung des „Ob" die grundsätzliche Beziehung der Bundesrepublik zu den anderen Mitgliedstaaten bereits selbst. Das „Wie" ist hingegen eine interne Angelegenheit, die sich nur mittelbar auf die Beziehung zu anderen Staaten auswirkt. Es ist deshalb Teil des das „Ob" ausgestaltenden Verwaltungsverfahrens.

Damit kommt, soweit nicht die Aufsicht über die öffentlichen Stellen des Bundes betroffen ist, grundsätzlich den Ländern die Regelungskompetenz zu (Art. 30, 83 GG). Der Bund kann das Verfahren hinsichtlich der Aufsicht über nicht-öffentliche Stellen nach Art. 84 Abs. 1 S. 2 GG jedoch gleichfalls selbst regeln. Die Kompetenz zur Regelung des Verfahrens über die Aufsicht öffentlicher Stellen der Länder liegt stets bei diesen.

ii. Vorschlag zur Regelung der Zuständigkeit beim Bund und bei den Ländern

Die Zuständigkeit für die Erlaubniserteilung liegt nach Art. 62 Abs. 3 S. 1 (ex Art. 56 Abs. 3 S. 1) DSGVO grundsätzlich bei der Aufsichtsbehörde. Soweit jedoch, wie in Deutschland, mehrere Aufsichtsbehörden errichtet werden, ist zu klären, welche dieser Aufsichtsbehörden für die Erteilung zuständig sein soll.

---

[333] Hinsichtlich Art. 84 GG stellt sich hier die erschwerende Problematik, dass es nicht um den mittelbaren Vollzug von Unionsrecht, sondern dessen unmittelbaren Vollzug geht – ein Umsetzungsgesetz ist hier, da die Datenschutz-Grundverordnung das „Ob" selbst regelt nicht erforderlich. Insoweit findet jedoch Art. 84 GG jedenfalls deshalb Anwendung, da dem Bund die Gesetzgebungskompetenz zur Regelung des Datenschutzrechtes im nicht-öffentlichen Bereich als Annex zur Regelung des Rechtes der Wirtschaft nach Art. 74 Abs. 1 Nr. 11 i. V. m. Art. 72 Abs. 2 GG zusteht.

[334] *Seiler*, in: Epping/Hillgruber (Hrsg.), BeckOK GG, 27. Ed., 2015, Art. 73, Rn. 2.

[335] *Suerbaum*, in: Epping/Hillgruber (Hrsg.), BeckOK GG, 27. Ed., 2015, Art. 84, Rn. 31.

Nach der skizzierten verfassungsrechtlichen Kompetenzverteilung sollte das BDSG-neu anordnen, dass – soweit sich die Maßnahme gegen *öffentliche* Stellen des Bundes richtet – die BfDI und – soweit sich die Maßnahme gegen *nicht-öffentliche* Stellen richtet – jeweils die (örtlich) zuständige(n) Aufsichtsbehörde(n) der Länder für die Erlaubniserteilung nach Art. 62 Abs. 3 S. 1 Hs. 1 (ex Art. 56 Abs. 3 S. 1 Hs. 1) DSGVO zuständig ist. Die Länder wären dann nach der Datenschutz-Grundverordnung darauf verwiesen, ihren Aufsichtsbehörden die Erlaubniserteilung hinsichtlich Maßnahmen gegen ihre eigenen öffentlichen Stellen zuzuschreiben.

iii. Vorschlag zur Regelung des Verfahrens beim Bund und bei den Ländern

Jedenfalls wenn es sich bei der Erlaubniserteilung um einen Verwaltungsakt im Sinne des § 35 S. 1 VwVfG handelt, ist das Verwaltungsverfahrensgesetz des Bundes bzw. der Länder anzuwenden. Entscheidend ist hier erstens, ob die Behörden der Bundesrepublik überhaupt hoheitlich handeln dürfen und können, und zweitens, ob der Erlaubniserteilung eine Außenwirkung zukommt. Ersteres ist zu bejahen. Die Behörden des Bundes oder der Länder treffen eine Regelung alleine für das Territorium der Bundesrepublik bzw. ihrer eigenen Länder. Ihnen steht folglich als Ausfluss der Gebietshoheit des Bundes über sein Hoheitsgebiet das (völkerrechtlich) unbeschränkte Recht zu, hoheitlich zu handeln. Zweitens entfaltet eine Erlaubniserteilung auch zumindest relative Außenwirkung. Die Aufsichtsbehörden der anderen Mitgliedstaaten stehen als deren Teil einer dem Bund und den Ländern nicht (teil-)identischen Gebietskörperschaft gegenüber den nationalen Aufsichtsbehörden jedenfalls in einem Außenverhältnis. Eine besondere Regelung des Verfahrens ist mithin nicht zwingend erforderlich.

iv. Haftungsregelung

(1) Haftung nach der Datenschutz-Grundverordnung

Fehlerhafte Anwendungen der Datenschutz-Grundverordnung können Haftungsfolgen auslösen, für die entweder der Bund oder die Länder als Aufsicht führende Behörde ggf. einzustehen haben. Das gilt dann, wenn sie Mitglie-

dern oder Bediensteten unterstützende Aufsichtsbehörden Befugnisse übertragen. Der Mitgliedstaat der einladenden Aufsichtsbehörde ist in diesem Fall nach Maßgabe seines nationalen Rechts für daraus entstehende Schäden verantwortlich. So will es Art. 62 Abs. 4 (ex Art. 56 Abs. 3a) DSGVO.

Das Lastentragungsgesetz findet auf die in Art. 62 Abs. 4, 5 S. 2 (ex Art. 56 Abs. 3a, 3b S. 2) DSGVO geregelte Haftung keine Anwendung. § 1 Abs. 1 LastG gilt nur für die Verpflichtung des Bundes zu finanzwirksamen Leistungen wegen der Verletzung supranationaler oder völkerrechtlicher Verpflichtungen. Dies ist hier schon deshalb tatbestandlich nicht einschlägig, weil die der Haftungsregelung der Datenschutz-Grundverordnung (Art. 62 Abs. 4, 5 S. 1 [ex Art. 56 Abs. 3a, 3b S. 1] DSGVO) zugrunde liegende Situation sich auf die Verletzung nationalen Rechts bzw. von Rechtspositionen durch die Bediensteten einer ausländischen Aufsichtsbehörde bezieht. Dass gegebenenfalls eine Befugnis aus Art. 58 (ex Art. 53) DSGVO falsch angewendet wurde, ist dabei als fehlende Rechtfertigung nur mittelbar relevant.

Selbst wenn man die Verletzung der Befugnisse aus Art. 58 (ex Art. 53) DSGVO als Grundlage der Haftung betrachtet, ist § 1 Abs. 1 LastG nicht einschlägig. Denn der diesem zugrunde liegende Art. 104 Abs. 6 S. 1 GG wurde alleine für Fälle „finanzwirksamer Entscheidungen zwischenstaatlicher Einrichtungen“[336] geschaffen. Hier jedoch folgt die finanzielle Verpflichtung aus dem (nach Art. 62 Abs. 4, 5 S. 1 [ex Art. 56 Abs. 3a, 3b S. 1] DSGVO) anwendbaren mitgliedstaatlichen Haftungsregime. Die finanzielle Verpflichtung ergibt sich nicht im Einzelfall durch eine Entscheidung einer Einrichtung der Union.

Hinsichtlich der Übernahme der Haftung aus Art. 62 Abs. 5 S. 2 (ex Art. 56 Abs. 3b S. 2) DSGVO findet § 1 Abs. 1 LastG ebenfalls keine Anwendung. Denn hier steht nicht die Verletzung einer Verpflichtung in Rede, sondern der Mitgliedstaat übernimmt alleine den von einem anderen Mietgliedstaat verauslagten Schadensersatz.

Vielmehr ist der Haftung die Vorschrift des Art. 104 Abs. 5 S. 1 Hs. 2 GG zugrunde zu legen. Dieser geht dem allgemeinen Konnexitätsgrundsatz nach Art. 104a Abs. 1 GG vor. Der Haftung liegt die Ratio zugrunde, dass allein

[336] BT-Drs. 16/813, S. 19.

der handelnde Verwaltungsträger die Aufsichts- und Kontrollmöglichkeiten hat, um den Eintritt von Schäden zu verhindern.[337] Dann soll ihn auch die Haftung treffen. Art 104 Abs. 5 S. 1 Hs. 2 GG ist unmittelbare Anspruchsgrundlage; dass das ausgestaltende Gesetz noch nicht erlassen ist, schadet grundsätzlich nicht.[338] Dabei ist gleichgültig, ob die Verletzung des Grundsatzes der ordnungsmäßigen Verwaltung auf nationalem oder Unionsrecht beruht[339] – insoweit kann hier dahinstehen, welche Pflicht als Grundlage der Haftung des Bundes genau verletzt ist. Problematisch ist jedoch, dass sich die Haftung alleine aus Art. 104 Abs. 5 GG (ohne AusführungsG) nur auf schwerwiegende, d. h. nur vorsätzliche oder grob fahrlässige, Verstöße gegen die Grundsätze ordnungsmäßiger Verwaltung bezieht.[340] Hier jedoch kann eine Haftung z. B. aus § 839 Abs. 1 S. 1 BGB i. V. m. Art. 34 GG bereits bei einfacher Fahrlässigkeit entstehen. Insoweit verbleibt eine Lücke, in der der Bund seine Einstandspflicht aus der Datenschutz-Grundverordnung nicht an die Länder weiterreichen kann.

Um diese Lücke zu schließen, ist es empfehlenswert, von der Ausführungskompetenz aus Art. 104a Abs. 5 S. 2 GG Gebrauch zu machen und eine umfassende Weiterleitung der Haftung an das jeweils einladende Land vorzusehen. Hierunter sind dann alle Fälle der Haftung, nicht nur aus § 839 BGB, sondern z. B. auch aus allgemeiner Aufopferung oder enteignungsgleichen Eingriffen in das Eigentum, zu fassen. Zu beachten ist dann, dass das BDSG-neu jedenfalls deshalb zustimmungsbedürftig wird.

(2) Allgemeine Haftung, insbesondere bei Vertragsverletzungsverfahren

Eine spezifische Regelung zum Regress bei einer Verurteilung der Bundesrepublik und der Anordnung eines Zwangsgeldes bzw. Pauschbetrages (Art. 260 Abs. 2 UAbs. 2 AEUV) scheint nicht geboten. Hier findet grundsätzlich das Lastentragungsgesetz (§§ 1, 3 LastG) Anwendung. Ob der Bund im Rahmen seiner Gesetzgebungsbefugnis die Haftung an die BfDI weiterrei-

[337] *Kube*, in: Epping/Hillgruber (Hrsg.), BeckOK GG, 27. Ed., 2015, Art. 104a, Rn. 53.
[338] BVerfGE 116, 271 (317) = NVwZ 2007, 190 (195).
[339] BVerfGE 116, 271 (314 f.) = NVwZ 2007, 190 (194).
[340] *Kube* (Fn. 337), Art. 104a, Rn. 55 m. w. N.; BVerwGE 100, 56 (60) = NVwZ 1996, 595 (596); offen gelassen in BVerfGE 116, 271 (318) = NVwZ 2007, 190 (195).

chen könnte, scheint mehr als fraglich. Zwar käme hierdurch das Prinzip, dass die finanzielle Verantwortung der fachlichen Zuständigkeit folgt, konsequent zur Anwendung und könnte seine disziplinierende Wirkung entfalten. Gleichzeitig bemisst sich jedoch die Höhe beider Beträge insbesondere auch nach dem Bruttoinlandsprodukt des Mitgliedstaates[341] und ist damit an der Leistungsfähigkeit des gesamten Mitgliedstaates und nicht der jeweils zuständigen Behörde ausgelegt. Eine Weiterreichung der Haftung würde die Aufsichtsbehörde finanziell deutlich überfordern und ihre Handlungsfähigkeit faktisch aufheben. Auch eine teilweise Weiterleitung begegnet Bedenken sowohl mit Blick auf die Beeinträchtigung der Funktionsfähigkeit der Aufsicht als auch mit Blick auf die Wahrung der Unabhängigkeit. Sie ist deshalb, trotz des grundsätzlich geltenden Prinzips der Haftungs-Zuständigkeits-Kopplung, nicht zu empfehlen.

bb) Anwendung des Rechts der unterstützenden Aufsichtsbehörde, Art. 62 Abs. 3 S. 1 Hs. 2 (ex Art. 56 Abs. 3 S. 1 Hs. 2)

i. Kompetenz für die Regelung der Anwendung des Rechts des entsendenden Mitgliedstaates

Hinsichtlich der Anordnung einer Anwendung des Rechts des entsendenden Mitgliedstaates stellt sich bezüglich der Regelungskompetenz – im Gegensatz zu oben – die Frage nach dem „Ob“ *und* dem „Wie“.
Regelungen zu den Außenbeziehungen erfassen nur jene Sachverhalte, die für das Verhältnis der Bundesrepublik Deutschland zu anderen Staaten oder zwischenstaatlichen Einrichtungen, insbesondere für die Gestaltung der Außenpolitik, Bedeutung haben. Dies ist auch beim „Ob“ der Anwendung ausländischen Rechts nicht zu bejahen. Denn diese Inkorporation bzw. Transformation ausländischer Befugnisnormen bewegt sich im Ergebnis alleine auf der Ebene der Regelung der Befugnisse selbst.[342] Hierfür haben der Bund und die Länder die Kompetenz hinsichtlich ihrer eigenen öffentlichen Stellen. Hinsichtlich der nicht-öffentlichen Stellen folgt eine (konkurrierende) Befugnis

[341] *Ehricke*, in: Streinz (Hrsg.), EUV/AEUV, 2. Aufl., 2012, Art. 263 AEUV, Rn. 1.
[342] So auch *Seiler* (Fn. 334), Art. 73, Rn. 2.2, wonach die Transformationskompetenz sachbereichsabhängig den Art. 70 ff. GG folgt.

des Bundes aus Art. 74 Abs. 1 Nr. 11 i. V. m. Art. 72 Abs. 2 GG. Hinsichtlich des „Wie“ gilt das oben Gesagte zu den Verwaltungskompetenzen.

ii. Grenzen und Zweckmäßigkeit

Der Anwendung ausländischen Rechts als Eingriffsgrundlage für das Handeln ausländischer Aufsichtsbehörden in Deutschland stehen materiell-verfassungsrechtliche Hindernisse entgegen. So setzt Art. 2 Abs. 1 GG i. V. m. dem Rechtsstaats- und Demokratieprinzip der Überlassung von Normsetzungsbefugnissen an außerstaatliche Stellen Grenzen.[343] Unter den Begriff „außerstaatliche Stellen“ sind dabei auch andere Mitgliedstaaten der Union zu fassen, da diese dem Bürger gegenüber weder staatlich-demokratisch noch mitgliedschaftlich legitimiert sind. Wegen des dynamischen Bezugs auf ausländische Befugnisnormen fragt sich, ob der deutsche Gesetzgeber diese pauschal in seinen Willen aufnehmen kann.[344] Auf diese Gesetzgebung haben die normunterworfenen Bundesbürger keinen direkten Einfluss.[345] Auch dem Gebot der Publizität und der Normenklarheit ist nicht genügt.[346] Der Normunterworfene hat keine hinreichende Möglichkeit, sich selbst auf die ihn treffenden Duldungsverpflichtungen einzustellen. All diese Erwägungen dürfte auch die Integrationsoffenheit des Grundgesetzes nicht ausgleichen, die insbesondere gemäß Art. 20 Abs. 3 i. V. m. Art. 79 Abs. 1 GG am Demokratieprinzip Halt macht.
Eine derartige Öffnung der nationalen Rechtsordnung scheint auch verfassungspolitisch wenig sinnvoll. De lege ferenda ist im Vergleich eine Vollharmonisierung vorzugswürdig.
Sollte der Gesetzgeber trotz der geäußerten Bedenken von der Öffnungsklausel Gebrauch machen wollen, gilt für die Regelung der Zuständigkeit und des Verfahrens das oben Gesagte.

[343] BVerfGE 64, 208 (214 f.).
[344] Mutatis mutandis BVerfGE 44, 322 (348 f.).
[345] Mutatis mutandis BVerfGE 44, 322 (348 f.).
[346] Mutatis mutandis BVerfGE 44, 322 (349).

38. Art. 63 - 67 (ex Art. 57 - 63): Kohärenzverfahren

a. Kein Regelungsbedarf für das Kohärenzverfahren selbst

Das Kohärenzverfahren der Art. 63 bis 67 (ex Art. 57 bis 63) etabliert einen Mechanismus der vertikalen Koordinierung zwischen den nationalen Aufsichtsbehörden (und der Kommission) unter Einbezug des EDA (Art. 64, 65 [ex Art. 58, 58a] DSGVO). Es zielt darauf, zu einer einheitlichen Anwendung der Datenschutz-Grundverordnung in der gesamten Union in den Fällen beizutragen, in denen das Risiko unterschiedlicher aufsichtsbehördlicher Auslegung der Datenschutz-Grundverordnung besteht (Art. 63, EG 135 S. 1 [ex Art. 57, EG 105 S. 1] DSGVO). Aus den Artikeln ergibt sich kein unmittelbarer Umsetzungsbedarf. Das Kohärenzverfahren ist in der Datenschutz-Grundverordnung abschließend geregelt.

b. Regelungsbedarf für das nationale Begleitverfahren

Mitgliedstaaten, die mehrere unabhängige Aufsichtsbehörden installieren, legt Art. 51 Abs. 3 (ex Art. 46 Abs. 2) DSGVO die Pflicht auf, mit Hilfe eines Verfahrens sicherzustellen, dass diese die Regeln für das Kohärenzverfahren nach Art. 63 ff. (ex Art. 57 ff.) DSGVO einhalten. Entsprechend sollte nach dem Willen der Verordnung jeder Mitgliedstaat eine Aufsichtsbehörde bestimmen, die als „zentrale Anlaufstelle“ für eine wirksame Beteiligung der verschiedenen Aufsichtsbehörden am Kohärenzverfahren fungiert und eine rasche und reibungslose Zusammenarbeit mit anderen Aufsichtsbehörden, dem EDA und der Kommission gewährleistet (vgl. oben S. 112).
Eine Regelung ist dabei aber nur insoweit erforderlich, als das Kohärenzverfahren auch tatsächlich zur Anwendung kommt (aa). Im Außenverhältnis ist dabei die zentrale Anlaufstelle neben dem Vertreter im EDA erforderlich (bb). Für ihr Tätigwerden sind – ebenso wie im Rahmen des Zusammenarbeitsverfahrens (s. oben 36. a. bb) iv. (2), S. 211) und bei dem Vertreter im EDA (siehe S. 211) – grundsätzlich Regelungen für die Binnenkoordination erforderlich (cc).

aa) Teilweiser Anwendungsausschluss des Kohärenzverfahrens

Ebenso wie das Zusammenarbeitsverfahren (siehe S. 207) unterliegt auch das Kohärenzverfahren einem teilweisen Anwendungssauschluss. Art. 55 Abs. 2 und EG 128 (ex Art. 51 Abs. 2 und EG 98) DSGVO befreien – in einer dem Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO für den Bereich des Journalismus vergleichbaren Weise[347] – die Mitgliedstaaten für bestimmte Bereiche von dem Kohärenzverfahren, nämlich dort, wo sie von den Öffnungsklauseln für öffentliche Stellen in Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO Gebrauch machen (siehe oben S. 207). In diesen Fällen finden die Vorschriften über die federführende Behörde (Art. 56 [ex Art. 51a] DSGVO) und damit auch Art. 60 (ex Art. 54a) DSGVO und (insoweit) das Prinzip der zentralen Anlaufstelle keine Anwendung. Dies bedeutet für das Kohärenzverfahren, dass es in diesen Fällen auch nicht zu einem Beschluss des EDA nach Art. 65 Abs. 1 lit. a (ex Art. 58a Abs. 1 lit. a) DSGVO kommen kann. Denn die dort vorgesehene Streitbeilegung ist eine Fortsetzung des ausgeschlossenen Zusammenarbeitsverfahrens nach Art. 60 (ex Art. 54a) DSGVO.

bb) Im Außenverhältnis

Wichtigste Kontaktstelle für das nach außen gerichtete Handeln der deutschen Aufsichtsbehörden im Kohärenzverfahren ist der *gemeinsame Vertreter im EDA*. Dass neben diesem, wie es EG 119 (ex EG 93) DSGVO vorsieht, auch eine zentrale Anlaufstelle[348] erforderlich ist, versteht sich nicht von selbst. Denn grundsätzlich besteht der Kohärenzmechanismus gerade darin, über gewisse Sachfragen eine Verständigung im EDA herzustellen. Das verlangt einem Mitgliedstaat prima vista nicht mehr als einen gemeinsamen Vertreter ab, um aus unionaler Perspektive eine effektive Beteiligung zu gewährleisten. Gleichzeitig treten die (zuständigen) Aufsichtsbehörden im Kohärenzverfahren aber auch selbst in Kontakt mit dem EDA bzw. der EDA wendet sich an diese (vgl. Art. 64 Abs. 1, 2, 4, 5 lit. b, 7, 8, Art. 65 Abs. 2 S. 3, Abs. 5 S. 1, 6 S. 2 [ex Art. 58 Abs. 1, 2, 5, 6 lit. b, 8, 9, Art. 58a Abs. 2 S. 3, Abs. 6 S. 1, Abs. 7 S. 2] DSGVO). Um die jeweils einzubeziehenden bzw. zu adressie-

[347] Siehe dazu sowie zu dem Sonderfall „Religionsgemeinschaften“ unten S. 229.
[348] Siehe S. 136.

renden einzelnen Aufsichtsbehörden eines Mitgliedstaates zu bestimmen, ist jedoch – wie bereits im Rahmen des Zusammenarbeitsverfahrens – ein Rückgriff auf die Zuständigkeitsregelungen der DSGVO nicht zulässig. Denn „betroffene Aufsichtsbehörde“ meint auch hier nicht die jeweils nach nationalem Recht zuständige Aufsichtsbehörde, sondern bezieht sich alleine auf die Gesamtheit der Aufsichtsbehörden eines Mitgliedstaates.[349] In diesem Fall gewinnt die von EG 199 (ex EG 93) DSGVO vorgesehene *zentrale Anlaufstelle* an Bedeutung. Denn diese muss dann eine Scharnierfunktion zwischen den einzelnen mitgliedstaatlichen Aufsichtsbehörden und dem EDA übernehmen. Ihre Errichtung ist dann zwingend.
Gleichzeitig gilt hier wie im Verfahren der Zusammenarbeit, dass Kontakte in beiden Richtungen nicht ausschließlich vermittels der zentralen Anlaufstelle abgewickelt werden dürfen. Vielmehr folgt aus dem Ziel der Effektivitätssteigerung und dem Grundsatz der Einheitlichkeit des Staates nur, dass sich die einzelnen Aufsichtsbehörden ein Handeln ihrer zentralen Anlaufstelle zurechnen lassen müssen. Damit ist diese zwar stets möglicher Transmitter, nicht jedoch zwingende Zwischenstelle jeglicher Kommunikation. Andersherum muss sich der EDA nicht an die zentrale Anlaufstelle wenden, kann es aber jederzeit und ohne Begründung tun.

cc) Im Innenverhältnis

Für die binnenrechtliche Ausgestaltung der Abstimmung zwischen den nationalen Aufsichtsbehörden im Kohärenzverfahren lässt die Datenschutz-Grundverordnung den Mitgliedstaaten weitgehenden Spielraum. Die nationalstaatliche Regelung muss aber sicherstellen, dass sie dem Koordinierungsbe-

[349] Dabei ist zu beachten, dass – nach hier vertretener Auffassung – das Recht der einzelnen Aufsichtsbehörden, sich unmittelbar an den EDA zu wenden, nicht bereits aus dem Wortlaut von Art. 64 (ex Art. 58) DSGVO (wie: „übermittelt die zuständige Aufsichtsbehörde“, „Jede Aufsichtsbehörde“, „die betroffene Aufsichtsbehörde“) folgt. Denn damit ist eben nicht eine von mehreren innerstaatlichen Aufsichtsbehörden gemeint. Vielmehr folgen diese Formulierungen dem Idealtypus der Datenschutz-Grundverordnung, der davon ausgeht, dass in einem Mitgliedstaat nur eine Aufsichtsbehörde besteht.

dürfnis, das die Datenschutz-Grundverordnung vor Augen hat, hinreichend Rechnung trägt.[350]

i. Bei grenzüberschreitendem Sachverhalt

Bei grenzüberschreitenden Sachverhalten besteht Abstimmungsbedarf zwischen den einzelnen Aufsichtsbehörden eines Mitgliedstaates für sechs Grundfragen, die in weiten Teilen bereits aus dem Zusammenarbeitsverfahren bekannt sind. Der Regelungsbedarf im Begleitverfahren zum Kohärenzverfahren deckt sich in weiten Teilen mit denen im Begleitverfahren zum Zusammenarbeitsverfahren (s. oben S. 211). Jedoch finden sie eine Erweiterung um wesentliche Aspekte mit Blick auf die Tätigkeit des Vertreters im EDA; diese spielt im Zusammenarbeitsverfahren (noch) keine Rolle. Zu trennen ist dabei zwischen der Abstimmung hinsichtlich der Tätigkeit der zentralen Anlaufstelle (1) und der des gemeinsamen Vertreters im EDA (2).

(1) Abstimmung bzgl. der innerstaatlichen Zuständigkeit/Betroffenheit einzelner Aufsichtsbehörden

Wie auch im Verfahren zur Zusammenarbeit bedarf es der Identifizierung von betroffenen und federführenden Aufsichtsbehörden unter den deutschen Aufsichtsbehörden (s. oben S. 212). Relevant ist dies z. B. bei Art. 64 Abs. 1, Art. 65 Abs. 1 lit. a, c, Art. 66 Abs. 1 (ex Art. 58 Abs. 1, Art. 58a Abs. 1 lit. a, d, Art. 61 Abs. 1) DSGVO. Die Lage unterscheidet sich dabei nicht von der des Zusammenarbeitsverfahrens. Es bedarf ebenfalls materieller Regelungen der Zuständigkeit und eines Verfahrens, nach dem innerstaatlich die Zuständigkeitsordnung zu klären ist. Für beide Fragen ist es vorzugswürdig, dieselben Regelungen wie im Zusammenarbeitsverfahren anzuwenden.

[350] Entsprechend den beim Zusammenarbeitsverfahren skizzierten Fällen 1, 2 und 3 (s. oben S. 209 ff.) lässt sich hier zwischen dem Regelungsbedarf bei grenzüberschreitenden Sachverhalten (1) und rein innerstaatlichen Sachverhalten (2) unterscheiden.

(2) Abstimmung des Vorgehens einzelner oder mehrerer nationaler Aufsichtsbehörden hinsichtlich des Vorgehens im Europäischen Datenschutzausschuss

Auch hinsichtlich des Vorgehens des Vertreters im EDA liegen die Herausforderungen für eine Abstimmung zwischen den Aufsichtsbehörden ähnlich wie im Verfahren der Zusammenarbeit. Der Unterschied zum Zusammenarbeitsverfahren liegt in der Handlungsrichtung des Vorgehens der Aufsichtsbehörden: Im Rahmen des Kohärenzverfahrens ist alleine der EDA Adressat von Handlungen und Entscheidungen der Aufsichtsbehörden; einen unmittelbaren Kontakt zu den Aufsichtsbehörden der anderen Mitgliedstaaten sieht die Datenschutz-Grundverordnung hier nicht mehr vor.
Der Abstimmungsbedarf der nationalen Aufsichtsbehörden hinsichtlich des Vorgehens im EDA ist wegen der faktischen Bindungswirkung seiner Stellungnahmen und der rechtlichen Bindungswirkung seiner Beschlüsse besonders hoch (vgl. zum Kohärenzverfahren als solchem S. 112). So gibt es bestimmte Situationen, in denen der EDA in den Erlass einer Maßnahme der Aufsichtsbehörde einzubeziehen ist (Art. 64 Abs. 1 lit. a – f [ex Art. 58 Abs. 1 lit. c - f] DSGVO). Gleichzeitig haben alle Aufsichtsbehörden das Recht, den EDA bei Angelegenheiten mit allgemeiner Geltung mit dieser Sache zu befassen (Art. 64 Abs. 2 [ex Art. 58 Abs. 2] DSGVO). In diesen beiden Fällen entfalten die Entscheidungen des EDA faktische Bindungswirkung auf zukünftige gleich gelagerte Sachverhalte der Aufsichtsbehörden. Dies ergibt sich daraus, dass der EDA, wenn er „zu derselben Angelegenheit“ bereits eine Stellungnahme abgegeben hat, dann in Zukunft keine Stellungnahme zu einer Sache mehr abgibt (Art. 64 Abs. 3 S. 1 Hs. 2 [ex Art. 58 Abs. 3 S. 1 Hs. 2] DSGVO). Folgt eine Aufsichtsbehörde einer Stellungnahme nicht, wird der Streitbeilegungsmechanismus des Art. 65 (ex Art. 58a) DSGVO eingeleitet (Art. 65 Abs. 1 lit. c [ex Art. 58a Abs. 1 lit. d] DSGVO). In diesem Fall kann der EDA mit verbindlichem Beschluss entscheiden. Das Vorgehen einer einzelnen nationalen Aufsichtsbehörde kann folglich weit über diese hinauswirken. Aus diesem Grund scheint eine Einbeziehung der anderen Aufsichtsbehörden zumindest angezeigt.
Soweit der EDA bei Meinungsverschiedenheiten zwischen den Aufsichtsbehörden mehrerer Mitgliedstaaten im Kohärenzverfahren als Folge eines ge-

scheiterten Verfahrens der Zusammenarbeit entscheidet, erfolgt dies durch einen verbindlichen Beschluss (Art. 65 Abs. 1 lit. a, b [ex Art. 58a Abs. 1 lit. a, b] DSGVO). Die Bindungswirkung ist hier zwar etwas schwächer als in den oben genannten Situationen. Zu klären ist hinsichtlich desjenigen Falles mit grenzüberschreitendem Bezug, in dem innerstaatlich nur eine Aufsichtsbehörde der Länder zuständig ist, ob überhaupt ein Abstimmungsbedarf zwischen den einzelnen deutschen Aufsichtsbehörden besteht. Denn die anderen Aufsichtsbehörden sind dann nicht berührt. Es ist sachlich angemessen und rechtlich möglich, ihr das Recht einzuräumen, alleine über das Verhalten des Vertreters im EDA zu bestimmen. Sind mehrere Aufsichtsbehörden der Länder von einem Abstimmungssachverhalt innerstaatlich betroffen, ergibt sich das Bedürfnis nach einem Abstimmungsverfahren. Es stellt sich dann die Frage, ob nur die betroffenen oder alle nationalen Aufsichtsbehörden bei der Koordination zu beteiligen sind. Da auch hier eine faktische Bindungswirkung eintritt (der EDA wird in gleich gelagerten Fällen von seinen vorhergehenden Entscheidungen nicht ohne Grund abweichen), liegt es auch hier nahe, alle (potenziell betroffenen) nationalen Aufsichtsbehörden in die Abstimmung miteinzubeziehen.
In jedem Fall der Koordination sind Entscheidungsfindungs- und Beteiligungsregelungen erforderlich (vgl. auch Art. 51 Abs. 3 Hs. 2 [ex Art. 46 Abs. 2 Hs. 2] DSGVO[351]).

(3) Bestimmung und Verhalten des gemeinsamen Vertreters

Wie der Vertreter zu bestimmen ist und ob und ggf. welche Freiheiten der Vertreter im EDA genießt, ob ihm insbesondere (eine gewisse) Vertretungsmacht zusteht oder die Aufsichtsbehörde(n) ein Weisungsrecht innehaben, bedarf einer Klärung. Dies ist deshalb von besonderer Relevanz, da der Vertreter – je nach dem Modus der innerstaatlichen Abstimmung und Entscheidungsfindung – nicht mehr ist als ein Bote des Ergebnisses. Insbesondere als Folge der föderalen Zuständigkeitsverteilung darf dieser nicht durch ein freies

[351] Wobei sich Art. 51 Abs. 3 Hs. 1 (ex Art. 46 Abs. 2 Hs. 1) DSGVO seinem Wortlaut nach nur auf das Kohärenzverfahren nach Art. 63 (ex Art. 57) DSGVO bezieht. Dies ist jedoch zu kurz gesprungen. Denn insbesondere auch das Verfahren der Zusammenarbeit bedarf einer entsprechenden flankierenden innerstaatlichen Regelung.

Handeln und Abstimmungsverhalten den Willen der innerstaatlichen Aufsichtsbehörden verfälschen oder negieren. Die Lage ist vergleichbar mit der Situation des Vertreters der Bundesrepublik Deutschland im Rat der Europäischen Union und den Fragen seiner Bindung an den Willen der Bundesländer und der Bundesrepublik Deutschland. Es ist rechtspolitisch sachgerecht, sich an dafür gefundenen Lösungen zu orientieren.

(4) (Selbst-)Kontrolle der nationalen Aufsichtsbehörden

Auch im Kohärenzverfahren stellt sich die Frage, ob und ggf. wie die Erfüllung von Verpflichtungen der einzelnen Aufsichtsbehörden zu sichern ist.[352]
So ergeben sich Verpflichtungen z. B. bezüglich des Einholens einer Stellungnahme bei bestimmten Maßnahmen (Art. 64 Abs. 1 [ex Art. 58 Abs. 1] DSGVO), der Informationsübermittlung (Art. 64 Abs. 4 [ex Art. 58 Abs. 5] DSGVO), der Stillhalteverpflichtung (Art. 64 Abs. 6 [ex Art. 58 Abs. 7a] DSGVO), der Berücksichtigung einer Stellungnahme und des Berichts hierüber (Art. 64 Abs. 7 [Art. 58 Abs. 8] DSGVO). Ebenso der Stillhalteverpflichtung im Streitbeilegungsverfahren (Art. 65 Abs. 4 [ex Art. 58a Abs. 4] DSGVO) und der finalen Beschlussfassung der Aufsichtsbehörde (Art. 65 Abs. 6 [ex Art. 58a Abs. 7] DSGVO).
Hier ist, wie im Verfahren der Zusammenarbeit, daran zu denken, ob der zentralen Anlaufstelle auch eine gewisse Kontrollfunktion über die einzelnen Aufsichtsbehörden insoweit zukommt, als diese darauf achten muss, dass sich die Aufsichtsbehörden effektiv am Kohärenzverfahren beteiligen. Denn Fehler der einzelnen Aufsichtsbehörden fallen hier auf die Bundesrepublik als Ganze zurück.

(5) Haftung

Ebenso wie im Verfahren der Zusammenarbeit stellt sich auch im Kohärenzverfahren die Frage nach der Weiterleitung der Haftung der Bundesrepublik Deutschland, die diese im Außenverhältnis trifft. Jedoch ist im Rahmen des Kohärenzverfahrens alleine die Haftung aus Vertragsverletzungsverfahren

[352] Siehe S. 227.

(vgl. Art. 260 AEUV) problematisch; eine Haftungsnorm wie Art. 62 Abs. 4, 5 (ex Art. 56 Abs. 3a, 3b) DSGVO existiert hier nicht.

(6) Klagerecht für die Nichtigkeitsklage nach Art. 263 AEUV

Regelungsbedürftig ist die Wahrnehmung des Klagerechts zum EuGH insbesondere für die Nichtigkeitsklage (Art. 263 UAbs. 2 und 4 AEUV) gegen Stellungnahmen und Beschlüsse nach Art. 64, 65 (ex Art. 58, 58a) DSGVO.

α) Taugliche Klagegegenstände

Taugliche Klagegegenstände sind nach Art. 263 UAbs. 1 S. 2 AEUV Handlungen der Einrichtungen oder sonstigen Stellen der Union mit Rechtswirkung gegenüber Dritten, mithin verbindliche Rechtsakte[353]. Der Beschluss nach Art. 65 Abs. 1 (ex Art. 58a Abs. 1) DSGVO ist jedenfalls ein solcher verbindlicher Rechtsakt (vgl. auch Art. 288 UAbs. 1, 4 AEUV). Nicht gleichermaßen klar liegt es im Hinblick auf die Stellungnahme des EDA nach Art. 64 Abs. 1 (ex Art. 58 Abs. 1) DSGVO. Nach Art. 288 UAbs. 5 AEUV sind Stellungnahmen „nicht verbindlich". Gleichwohl kommt es weniger auf die Bezeichnung als vielmehr auf die tatsächlichen Wirkungen einer Handlung an.[354] Die Stellungnahme ist nicht nur eine einzelne Handlung eines mehrphasigen Beschlussvorgangs, sondern selbstständig als abschließende Maßnahme des Kohärenzverfahrens nach Art. 64 (ex Art. 58) DSGVO gedacht. Jedoch ist sie selbst nicht unmittelbar rechtsverbindlich; ihr kommt Verbindlichkeit nur mittelbar wegen der drohenden Fassung eines Beschlusses bei Abweichung zu (Art. 65 Abs. 1 lit. c [ex Art. 58a Abs. 1 lit. d] DSGVO). Ob dies für eine Anfechtbarkeit genügt, ist zweifelhaft. Insbesondere liegt kein Fall der Selbstbindung eines EU-Organs vor, da der Inhalt der Stellungnahmen auf die Tätigkeit der nationalen Aufsichtsbehörden gerichtet ist.

[353] *Ehricke* (Fn. 341), Art. 263 AEUV, Rn. 11.
[354] Vgl. *Ehricke* (Fn. 341), Art. 263 AEUV, Rn. 11.

β) Parteifähigkeit – Aufsichtsbehörden als juristische Personen nach UAbs. 4

Die einzelnen Aufsichtsbehörden sind *nicht* nach Art. 263 UAbs. 2 AEUV privilegiert klagebefugt. Dies ist nur der Mitgliedstaat an sich. Die Aufsichtsbehörden können jedoch – ohne gesetzliche Ermächtigung – nicht für diesen handeln.
Gleichzeitig sind die Aufsichtsbehörden auch keine juristischen Personen i. S. v. Art. 263 UAbs. 4 AEUV. Denn diese sind nicht rechtsfähig, sondern nach § 22 Abs. 5 S. 1 BDSG als oberste Bundesbehörde bzw. als oberste Landesbehörde (vgl. § 23 Abs. 3 LDSG Rh-Pf) Teil der bundes- bzw. landeseigenen Verwaltung. Gleichzeitig spricht der Umstand, dass die Aufsichtsbehörden nach Art. 65 Abs. 2 S. 3 (ex Art. 58a Abs. 2 S. 3) DSGVO jedenfalls mittelbarer Adressat des Beschlusses sind (der Beschluss wird an die federführende Aufsichtsbehörde und alle betroffenen Aufsichtsbehörden übermittelt und ist für diese verbindlich) dafür, ihnen insofern eine Teilrechtsfähigkeit jedenfalls nach dem Unionsrecht zuzuerkennen.

γ) An sie gerichtet (Var. 1) / unmittelbare und individuelle Betroffenheit (Var. 2) // Rechtsakte mit Verordnungscharakter und unmittelbare Betroffenheit (Var. 3)

Sollten der Bund und die Länder die Aufsichtsbehörden (wie die Datenschutz-Grundverordnung den EDA, Art. 68 Abs. 1 [ex Art. 64 Abs. 1a] DSGVO) mit Rechtsfähigkeit ausstatten bzw. sollte der EuGH diese wegen der ihnen zukommenden Unabhängigkeit trotzdem als juristische Personen i. S. v. Art. 263 UAbs. 4 AEUV anerkennen, stellt sich die Frage, ob und in welchen Fällen sie klagebefugt wären.

αα) Art. 263 UAbs. 4 Var. 1 AEUV

Klagebefugt sind nach Art. 263 UAbs. 4 Var. 1 AEUV in jedem Falle Adressaten verbindlicher Handlungen. Prima vista lassen sich hierunter jedenfalls im Falle des Art. 65 Abs. 1 lit. a (ex Art. 58a Abs. 1 lit. a) DSGVO die in einer Sache federführende, wohl auch alle in einer Sache betroffenen Aufsichtsbehörden fassen. Problemträchtig ist mit Blick auf Deutschland jedoch

wieder die Frage, ob die Datenschutz-Grundverordnung hier tatsächlich die einzelnen innerstaatlichen Aufsichtsbehörden in den Blick nimmt, oder nicht vielmehr die Gesamtheit der Aufsichtsbehörden eines Mitgliedstaates. Letztere Ansicht ist vorzugswürdig.[355] Folglich besteht keine unmittelbare Klagebefugnis nach Art. 263 UAbs. 4 Var. 1 AEUV.

ββ) Art. 263 UAbs. 4 Var. 2 AEUV

Gleichwohl können die Aufsichtsbehörden nach Art. 263 UAbs. 4 Var. 2 AEUV klagebefugt sein, wenn sie durch den Beschluss unmittelbar und individuell betroffen, mithin beschwert wären.[356] Dies ist wohl zu bejahen. Denn der gegen den Mitgliedstaat gerichtete Beschluss verpflichtet diesen zur Umsetzung und lässt ihm dabei keinen Ermessensspielraum.[357] Da die nach innerstaatlicher Zuständigkeitsordnung zur Umsetzung des Beschlusses berufenen Aufsichtsbehörden folglich ebenfalls an den Beschluss gebunden sind, sind sie in den genannten Fällen klagebefugt.
Gleiches dürfte auch in den Fällen gelten, in denen nach Art. 64 Abs. 1, Art. 65 Abs. 1 lit. c (ex Art. 58 Abs. 1, Art. 58a Abs. 1 lit. d) DSGVO über den Antrag bzw. das Verhalten einer (wenn auch innerstaatlichen) Aufsichtsbehörde entschieden wird.
Schwieriger sind die Fälle zu beurteilen, in denen *sonstige nicht betroffene Aufsichtsbehörden* gegen Beschlüsse des EDA vorgehen wollen, insbesondere um eine mittelbare Bindungswirkung in zukünftigen, sie betreffenden Fällen zu vermeiden. Die Bundesrepublik Deutschland könnte eine solche Klage anstrengen, da sie einer besonderen Klagebefugnis nicht bedarf. Die einzelnen Aufsichtsbehörden müssten in diesen Fällen jedoch auch unmittelbar und individuell betroffen sein. Die unmittelbare Betroffenheit ist dabei mit Blick auf die Vorwirkung zu bejahen. Diese trifft die Aufsichtsbehörden in ihrer zukünftigen Tätigkeit, ohne dass noch ein dazwischentretender weiterer Akt erforderlich ist.

---

[355] Siehe dazu im Einzelnen S. 212.
[356] *Ehricke* (Fn. 341), Art. 263 AEUV, Rn. 57 ff.
[357] Vgl. Mutatis mutandis die Fälle zur Anfechtung von Beschlüssen zur Rückforderung von rechtswidrig gewährten Beihilfen, *Ehricke* (Fn. 341), Art. 263 AEUV, Rn. 60.

Die individuelle Betroffenheit lässt sich mit der sog. „Plaumann-Formel“ wohl ebenfalls bejahen, da Entscheidungen die Aufsichtsbehörden „wegen bestimmter persönlicher Eigenschaften oder besonderer, [sie] aus dem Kreis aller übrigen Personen heraushebender Umstände berührt und [sie] daher in ähnlicher Weise individualisiert wie den Adressaten einer Entscheidung“[358]. Die eintretende Vorwirkung bindet die Aufsichtsbehörden nahezu so, als wären sie im konkreten Fall selbst Adressat des Beschlusses. Auch ist ihre besondere Rolle im Datenschutzrecht eine besondere persönliche Eigenschaft, die sie insbesondere aus dem Kreis aller dem Datenschutzrecht Unterworfenen heraushebt.
Wie der EuGH in all diesen Fragen die Frage nach der Klagebefugnis entscheiden wird, ist jedoch spekulativ. Es besteht deshalb dringender legislatorischer Regelungsbedarf, sollen die nationalen Aufsichtsbehörden die – ihre Unabhängigkeit wahrende – Möglichkeit haben, in all diesen Fällen selbst gegen Beschlüsse des EDA vorzugehen.

ii. Bei rein innerstaatlichen Sachverhalten – nationales Kohärenzverfahren

Für rein innerstaatliche Sachverhalte, bei denen also ein grenzüberschreitender Bezug fehlt, aber mehrere deutsche Aufsichtsbehörden berührt sind, bedarf es eines Koordinierungsmechanismus, der als Verlängerung des nationalen Verfahrens der Zusammenarbeit (s. S. 222) die Herstellung einer verbindlichen Beschlusslage für Streitfälle ermöglicht.
Auch wenn die Regeln des Kohärenzverfahrens hier nicht unmittelbar anwendbar sind, besteht die Verpflichtung zur effektiven Einhaltung der materiellen Vorgaben der Datenschutz-Grundverordnung auch in rein innerstaatlichen Sachverhalten.[359] Bei genauerem Hinsehen zeigt sich allerdings, dass

[358] EuGH, Rs. 25/62, Plaumann/Kommission, Slg. 1963, 211 (238); Rs. C-78/03 P, Kommission/Aktionsgemeinschaft Recht und Eigentum, Slg. 2005, I-10737 Rn. 33.
[359] Die Heranziehung von Art. 16 Abs. 2 S. 1 a. E. AEUVals Rechtsgrundlage setzt nicht voraus, dass in jedem Einzelfall, der von dem auf dieser Rechtsgrundlage ergangenen Rechtsakt erfasst wird, tatsächlich ein Zusammenhang mit dem freien Verkehr zwischen Mitgliedstaaten besteht; vgl. EuGH, Urt. v. 20.5.2003, Rs. C-465/00, C-138/01 und C-139/01, Österreichischer Rundfunk, Rn. 41 – noch zu Artikel 100a EG-Vertrag.

der Koordinierungsbedarf im Kohärenzverfahren deutlich schwächer ausgeprägt ist. Denn unabhängig von der innerstaatlichen Ausgestaltung der Aufsichtsstrukturen ist der EDA vor Erlass der in Art. 64 Abs. 1 (ex Art. 58 Abs. 1) DSGVO genannten Maßnahmen immer um eine Stellungnahme zu ersuchen. Ein Bedarf zur Abstimmung unter den Aufsichtsbehörden ergibt sich folglich nur bei Maßnahmen, die nach der Datenschutz-Grundverordnung im Verfahren der Zusammenarbeit abzustimmen sind und nur mittelbar – über Art. 65 Abs. 1 lit. a (ex Art. 58a Abs. 1 lit. a) DSGVO – zur Anwendung des Kohärenzverfahrens führen.

c. Ansätze für die Gewährleistung des Kohärenzverfahrens

Nähere Vorgaben, wie die zur Lösung zu etablierenden Verfahren ausgestaltet sein müssen, formuliert die Datenschutz-Grundverordnung nicht. Insoweit kommt dem Mitgliedstaat ein Handlungsspielraum zu. Einzig das Ziel, die Einhaltung der Regeln für das Kohärenzverfahren durch die Behörden sicherzustellen, ist dem Mitgliedstaat vorgegeben (Art. 51 Abs. 3 S. 2 [ex Art. 46 Abs. 2] DSGVO).

aa) Im Außenverhältnis: Vertreter im EDA und zentrale Anlaufstelle

Sub specie der Beziehungen im Außenverhältnis[360] bedarf es sowohl einer Regelung für den Vertreter im EDA als auch eine Regelung für die zentrale Anlaufstelle.

Die Ausgestaltung der Vertretung für die Tätigkeit in Kohärenzverfahren sollte dabei mit der *Vertretung im EDA* in sonstigen Bereichen (d. h. nach den oben bei Art. 51 Abs. 3 [ex Art. 46 Abs. 2] DSGVO skizzierten Modellen; siehe S. 141) parallel laufen. Es empfiehlt sich daher, für die Bestimmung des Vertreters keine abweichenden Regelungen für den Bereich der Vertretung im Kohärenzverfahren zu treffen. Gleichwohl schließt dies auch die Möglichkeit einer Doppelspitzenlösung (vgl. S. 144) mit ein. Hier wäre dann im Innenverhältnis zu klären, welcher Vertreter in welchem Fall für die Bundesrepublik Deutschland handelt.

[360] Siehe dazu bereits oben (S. 115).

Gleichzeitig braucht es eine *zentrale Anlaufstelle* i. S. v. EG 119 S. 2 (ex EG 93 S. 2) DSGVO für den Kontakt zwischen nationalen Aufsichtsbehörden und dem EDA. Für deren Einrichtung gilt das oben Gesagte (siehe S. 217). Insbesondere ist hier keine Trennung bzw. Errichtung einer Doppelspitzenlösung zulässig. Dies würde den Gedanken der nach außen hin einheitlichen Ansprechbarkeit der deutschen Aufsichtsbehörden zu stark schwächen und selbst bei einer gegenseitigen Zurechnung aller Handlungen eine „swift and smooth co-operation“ (EG 119 S. 2 [ex EG 93 S. 2] DSGVO) mit anderen Aufsichtsbehörden und dem EDA nicht hinreichend sicherstellen.

bb) Im Innenverhältnis

Für das Gelingen der Zusammenarbeit mehrerer nationaler Aufsichtsbehörden ist die Regelung der Abstimmung im Innenverhältnis entscheidend. Das gilt zum einen für die Abstimmung hinsichtlich der innerstaatlichen Zuständigkeit (i.) sowie zum anderen hinsichtlich des Abstimmungsverfahrens als solchen (ii.).

i. Abstimmung bzgl. innerstaatlichen Zuständigkeit/Betroffenheit einzelner Aufsichtsbehörden

(1) Materielle Regelung

Die Ansätze für die materiellen Zuständigkeitsregelungen unterscheiden sich nicht von denen für das Verfahren der Zusammenarbeit (dazu oben S. 219). Es sind keine weiteren Regelungen erforderlich.

(2) Verfahren der Zuständigkeitsbestimmung

Wie auch beim Verfahren der Zusammenarbeit bedarf es einer Klärung, welche Stelle Entscheidungen über die innerstaatliche Zuständigkeit von Aufsichtsbehörden trifft. Diese ergibt sich nicht unmittelbar aus dem Unionsrecht, sondern ist grundsätzlich alleine den nationalen Gesetzgeber überantwortet.
Auch hier bieten sich verschiedene Lösungswege an: Entweder trifft die zentrale Anlaufstelle verbindliche Entscheidungen bezüglich der Zuständigkeit einzelner Aufsichtsbehörden oder die Aufsichtsbehörden klären gemeinsam

Zuständigkeitsfragen. Da es für die Bestimmung der Zuständigkeit keinen Unterschied macht, ob hieraus eine Beteiligung im Zusammenarbeits- oder im Kohärenzverfahren folgt, sollte die Regelung für das Kohärenzverfahren der Regelung für das Verfahren der Zusammenarbeit folgen (dazu oben S. 221).

ii. Abstimmung des Vorgehens einzelner oder mehrerer nationaler Aufsichtsbehörden

Wie auch im Verfahren der Zusammenarbeit muss das Abstimmungsverfahren eine sachgerechte Koordination zwischen den deutschen Aufsichtsbehörden organisieren. Der Kreis der Fragen erweitert sich dabei im Kohärenzverfahren im Vergleich zum Zusammenarbeitsverfahren (dazu oben S. 222). wesentlich dadurch, dass nun das Verhalten des Vertreters im EDA neben dem Verhalten der zentralen Anlaufstelle einer Klärung bedarf.

(1) Beteiligung an der Programmierung des Vertreterhandelns

Hinsichtlich der Beteiligung der deutschen Aufsichtsbehörden an der Programmierung des Vertreterhandelns bietet es sich an, drei verschiedene Konstellationen zu unterscheiden:

- die Tätigkeit des Vertreters, soweit *keine Betroffenheit* (und damit auch Federführung) einer deutschen Aufsichtsbehörde besteht; unten ii). Dies ist regelmäßig dann der Fall, wenn der EDA über Anträge und Handeln usw. von Aufsichtsbehörden anderer Mitgliedstaaten entscheidet – sei es nach Art. 64 (ex Art. 58) DSGVO oder nach Art. 65 (ex Art. 58a) DSGVO. Hier sind Differenzierungen nach einer Betroffenheit der deutschen Aufsichtsbehörden nur bedingt, insbesondere nur nach ihrer sachlichen, nicht aber nach ihrer örtlichen Zuständigkeit möglich.
- die Tätigkeit des Vertreters, wenn *mehrere deutsche Aufsichtsbehörden betroffen* sind – sei es, weil der EDA nach Art. 64 Abs. 1 (ex Art. 58 Abs. 1), ggf. auch Art. 64 Abs. 1 lit. d [ex Art. 58 Abs. 1 lit. d]) DSGVO mit ihrer Sache befasst ist, sei es, weil der EDA wegen des Verfahrens der Zusammenarbeit auf den Plan gerufen ist (Art. 64 Abs. 2, Art. 65 Abs. 1 lit. a, b [ex Art. 58 Abs. 2, Art. 58a Abs. 1 lit. a, b] DSGVO). Dabei lässt sich insoweit weiter differenzieren, als es Situationen geben

kann, in denen von mehreren betroffenen deutschen Aufsichtsbehörden eine federführend ist und solche, in denen dies nicht der Fall ist, die Federführung also bei einer Aufsichtsbehörde eines anderen Mitgliedstaates liegt.

- der Fall, in dem *alleine eine deutsche Aufsichtsbehörde* betroffen und ggf. auch federführend ist.

α) Vorfrage: Betroffenheit bei Aufsicht über nicht-öffentlichen und öffentlichen Bereich

Als Vorfrage ist zu klären, ob und ggf. wann Bund und/oder Länder in den Kreis der potenziell entscheidungsberufenen Stellen einbezogen werden sollen.
Hier lassen sich wohl zwei Fälle unterscheiden: Handeln in Bezug auf oder mit Auswirkung auf die Aufsicht über (αα) öffentliche Stellen des Bundes und öffentliche Stellen der Länder und (ββ) nicht-öffentliche Stellen.

αα) Auswirkung auf die Aufsicht über öffentliche Stellen des Bundes und öffentliche Stellen der Länder

Soweit die Auswirkung einer Entscheidung des EDA nur die öffentlichen Stellen eines Landes oder des Bundes betreffen und das Kohärenzverfahren zur Anwendung kommt (siehe S. 242), also allen voran in Fällen des Art. 64, 65 Abs. 1 lit. c [ex Art. 58, 58a Abs. 1 lit. d] DSGVO), liegt es prima vista nahe, nur der entsprechenden Aufsichtsbehörde ein Mitspracherecht einzuräumen. Dies scheint eine verfassungsrechtliche Legitimation darin zu finden, dass in diesen Fällen die Länder bzw. der Bund die alleinige Gesetzgebungskompetenz und Kompetenz zu Regelung des Verwaltungsverfahrens haben. Doch muss auf der anderen Seite auch die faktische Ausstrahlung und Bindungswirkung von Entscheidungen und Stellungnahmen des EDA betrachtet werden. Diese greifen auch hier Platz. Denn es können jeweils in Bezug auf die Länder untereinander oder den Bund ähnliche aufsichtsrechtliche Fragen entstehen, die dann durch eine vorhergehende Entscheidung des EDA vorderterminiert sind. Dies spricht dafür, stets den Bund und alle Bundesländer an der Willensbildung zu beteiligen.

ββ) Auswirkung auf die Aufsicht über nicht-öffentlichen Stellen

Soweit (wie regelmäßig) die Aufsicht über nicht-öffentliche Stellen betroffen ist, liegt die Sache insoweit anders, als der Bund von einer Ausstrahlungswirkung auf seinen Aufsichtsvollzug nicht betroffen sein kann. Denn er ist vom Vollzug der Aufsicht über die nicht-öffentlichen Stellen gänzlich ausgeschlossen. Gleichwohl steht ihm hier die materielle Gesetzgebungsbefugnis (aus Art. 74 Abs. 1 Nr. 11 GG) zu. Insofern hat er zumindest eine sachliche Kompetenz auf seiner Seite. Dies spricht dafür, den Bund auch hier nicht von vorneherein vom Kreis der Mitwirkungsberechtigten auszuschließen.

β) Entscheidung, wenn keine deutsche Aufsichtsbehörde betroffen ist

Ist keine deutsche Aufsichtsbehörde betroffen, entscheidet der EDA beispielsweise über Standard-Datenschutzklauseln (Art. 64 Abs. 1 lit. d [ex Art. 58 Abs. 1 lit. d] DSGVO) auf die Initiative einer Aufsichtsbehörde eines anderen Mitgliedstaates hin, sind alle nationalen Aufsichtsbehörden grundsätzlich gleich stark bzw. schwach betroffen. Die Stellungnahme/Entscheidung betrifft sie zwar nicht unmittelbar selbst. Jedoch entfalten beide eine mittelbare Bindungswirkung. Die Datenschutz-Grundverordnung fordert eine weitestgehend einheitliche Anwendung des Datenschutzrechts. Entscheidungen im Bereich des Art. 64 Abs. 1 (ex Art. 58 Abs. 1) und Art. 65 Abs. 1 (ex Art. 58a Abs. 1) DSGVO tendieren dazu, eine Präzedenzwirkung auch für mittelbar betroffene ähnliche Sachverhalte zu entfalten. Dafür streitet bereits die Regelung des Art. 64 Abs. 3 S. 1 Hs. 2 (ex Art. 58 Abs. 3 S. 1 Hs. 2) DSGVO: Eine Stellungnahme wird nicht mehr abgegeben, „sofern [der EDA] nicht bereits eine Stellungnahme zu derselben Angelegenheit abgegeben hat“. Hiermit ist wohl nicht der einzelne Streitgegenstand selbst gemeint, sondern eine in der Sache gleich gelagerte Anfrage an den EDA. Der EDA kann damit in einer inhaltlich gleich gelagerten Sache nicht öfters befasst werden. Für den Fall des Abweichens von einer Stellungnahme erlässt er darüber hinaus einen verbindlichen Beschluss (Art. 65 Abs. 1 lit. c [ex Art. 58a Abs. 1 lit. d] DSGVO). Dies kann dann alle Aufsichtsbehörden treffen, ohne dass auf ihre Initiative hin die ursprüngliche Stellungnahme ergangen ist. Diese Bindungswirkung streitet dafür, jedenfalls alle potenziell von

einer Stellungnahme/Entscheidung des EDA betroffenen nationalen Aufsichtsbehörden an der Programmierung des Vertreters zu beteiligen.

γ) Entscheidung, wenn mehrere deutsche Aufsichtsbehörden betroffen sind

Sind von einer Entscheidung mehrere deutsche Aufsichtsbehörden betroffen, liegen die Dinge insofern etwas anders, als nach der nationalen Zuständigkeitsverteilung einzelne Aufsichtsbehörden zur Entscheidung über die Sache berufen sind. In dieser Situation ist zu überlegen, ob auch nur die betroffenen oder doch alle Landesbeauftragte für den Datenschutz und die Informationsfreiheit an einer Entscheidungsfindung und damit Programmierung des Vertreters miteinzubeziehen sind. Dabei kann noch einmal danach unterschieden werden, ob eine der betroffenen Aufsichtsbehörden federführend ist oder nicht.

αα) Mehrere Aufsichtsbehörden betroffen, keine federführend (insbesondere Art. 64 Abs. 1 [ex Art. 58 Abs. 1])

Der einfachere Fall scheint dabei derjenige, in dem mehrere Aufsichtsbehörden betroffen[361], von diesen jedoch keine federführend ist. Dies kann insbesondere in zwei Konstellationen relevant werden: einerseits, wenn es um eine Angelegenheit nach Art. 64 Abs. 1, Art. 65 Abs. 1 lit. c (ex Art. 58 Abs. 1, Art. 58a Abs. 1 lit. d) DSGVO geht, andererseits, wenn im Zusammenarbeitsverfahren ein Verarbeiter Niederlassungen (nur) in zwei Bundesländern hat, die Hauptniederlassung (und damit die Federführung) jedoch im europäischen Ausland liegt.
Eine Lösung kann dahin gehen, alleine unter den betroffenen Aufsichtsbehörden eine Abstimmung herbeizuführen (insoweit wäre dies bei der Aufsicht über öffentliche Stellen regelmäßig alleine die BfDI oder ein einzelner Landesbeauftragter für den Datenschutz und Informationsfreiheit). Für diesen

[361] Wobei hier primär eine örtlich-sachliche Betroffenheit i. S. d. Art. 4 Nr. 22 lit. a, b (ex Art. 4 Nr. 19a lit. a, b) DSGVO gemeint ist, nicht jedoch eine rein sachliche Betroffenheit bei einer Zuständigkeitsaufspaltung innerhalb eines Landes wie z. B. Bayern. Hier ist – wie auch auf nationaler Ebene im Verhältnis zum Unionsrecht – die Gesamtheit der bayerischen Aufsichtsbehörden i. d. S. betroffen.

Gedanken streitet, dass diese an sich in der Sache zuständig sind und es zumindest aus nationaler Perspektive keinen Grund gibt, deren Vollzugsentscheidungen von anderen Aufsichtsbehörden mitbestimmen zu lassen. Außerdem ließe sich so auch eine einfachere und damit schnellere Entscheidungsfindung erzielen (dies insbesondere, wenn die Aufsichtsbehörden nach dem Konsens-, nicht nach dem Mehrheitsprinzip entscheiden).
Andererseits könnte in allen Fällen – jedenfalls wenn die Aufsicht über nichtöffentliche Stellen betroffen ist – eine Entscheidung zwischen allen Landesbeauftragten für den Datenschutz und die Informationsfreiheit (und ggf. auch des BfDI) herbeigeführt werden. Das trüge der mittelbaren Bindungswirkung in angemessener Weise Rechnung, die von Stellungnahmen/Beschlüssen des EDA ausgeht (s. o.). Sollten nicht alle nationalen Aufsichtsbehörden in die Programmierung des Vertreters einbezogen werden, kann dies einen unerwünschten Wettlauf um die Befassung des EDA mit Fragen nach Art. 64 Abs. 1 (ex Art. 58 Abs. 1) DSGVO auslösen. Denn es ist zu erwarten, dass sich hier oftmals in allen Bundesländern gleich gelagerte Fragen ergeben. Werden nicht alle Aufsichtsbehörden, sondern nur die zuerst aktiv gewordene(n) an der Programmierung des Vertreters beteiligt, geht davon ein Anreiz aus, hier durch ein Vorpreschen den eigenen Einfluss auf die Entscheidungsfindung im EDA auszuweiten.
Ungeachtet ihrer unterschiedlichen Vor- und Nachteile sind beide Lösungen grundsätzlich sowohl mit dem nationalen Verfassungsrecht im Übrigen als auch mit der Datenschutz-Grundverordnung vereinbar.

ββ) Mehrere Aufsichtsbehörden betroffen, eine federführend

Eine besondere Situation tritt ein, wenn von mehreren betroffenen Aufsichtsbehörden eine federführend ist. Dies kann allerdings nur der Fall sein, wenn der EDA nach Art. 65 Abs. 1 lit. a (ex Art. 58a Abs. 1 lit. a) DSGVO – in Fortführung des Zusammenarbeitsverfahrens – oder nach lit. b hinsichtlich der Federführung zur Entscheidung berufen ist. In dieser Konstellation kann es sinnvoll sein, der (nach nationalem Recht) federführenden Aufsichtsbehörde das Recht zur exklusiven Programmierung des Vertreters (oder die Vertretung selbst) einzuräumen. Das deckt sich mit dem Ansatz der Datenschutz-

Grundverordnung, generell die federführende Aufsichtsbehörde mit einer Leitkompetenz auszustatten.

Gleichwohl verfängt diese Sicht nur auf den ersten Blick. Denn diese Leitfunktion will und kann die Datenschutz-Grundverordnung nur für das Verhältnis zwischen Aufsichtsbehörden verschiedener Mitgliedstaaten anordnen. Sie kann dies hingegen nicht mit Blick auf die innerstaatliche Zuständigkeitsordnung mehrerer Aufsichtsbehörden. Der Union fehlt die Kompetenz zur Regelung des Verfahrensrechts der Mitgliedstaaten; sie hat die Organisationshoheit der Mitgliedstaaten zu wahren.[362] Maßgeblich ist vielmehr die nationale Kompetenzordnung. Grundsätzlich gilt auch hier, dass alle nationalen Aufsichtsbehörden von einer mittelbaren Bindungswirkung betroffen sind. Gleichzeitig ist kein zwingender Grund ersichtlich, warum alleine der federführenden Aufsichtsbehörde die Entscheidung über das Vertreterhandeln vorzubehalten ist. Gleichwohl sind die Dinge in den Fällen des Art. 65 Abs. 1 lit. a, b (ex Art. 58a Abs. 1 lit. a, b) DSGVO insofern besonders, als eine Bindungswirkung ungleich schwächer ausfällt als in den Fällen des Art. 64 Abs. 1, Art. 65 Abs. 1 lit. c (ex Art. 58 Abs. 1, Art. 58a Abs. 1 lit. d) DSGVO. Denn im Verfahren der Zusammenarbeit betrifft die Entscheidung des EDA einen konkreten Fall. Im Zweifelsfall wird sich der EDA jedes neuen Falles, auch wenn er eine ähnliche Sachlage betrifft, selbst annehmen. Art. 65 (ex Art. 58a) DSGVO sieht hier keine dem Art. 64 Abs. 2 S. 1 Hs. 2 (ex Art. 58 Abs. 2 S. 1 Hs. 2) DSGVO entsprechende *res judicata*-Bestimmung vor. Gleichzeitig ist in Fällen des Zusammenarbeitsverfahrens eine zügige Entscheidung ungleich dringender als in Fällen des Art. 64 Abs. 1 (ex Art. 58 Abs. 1) DSGVO.

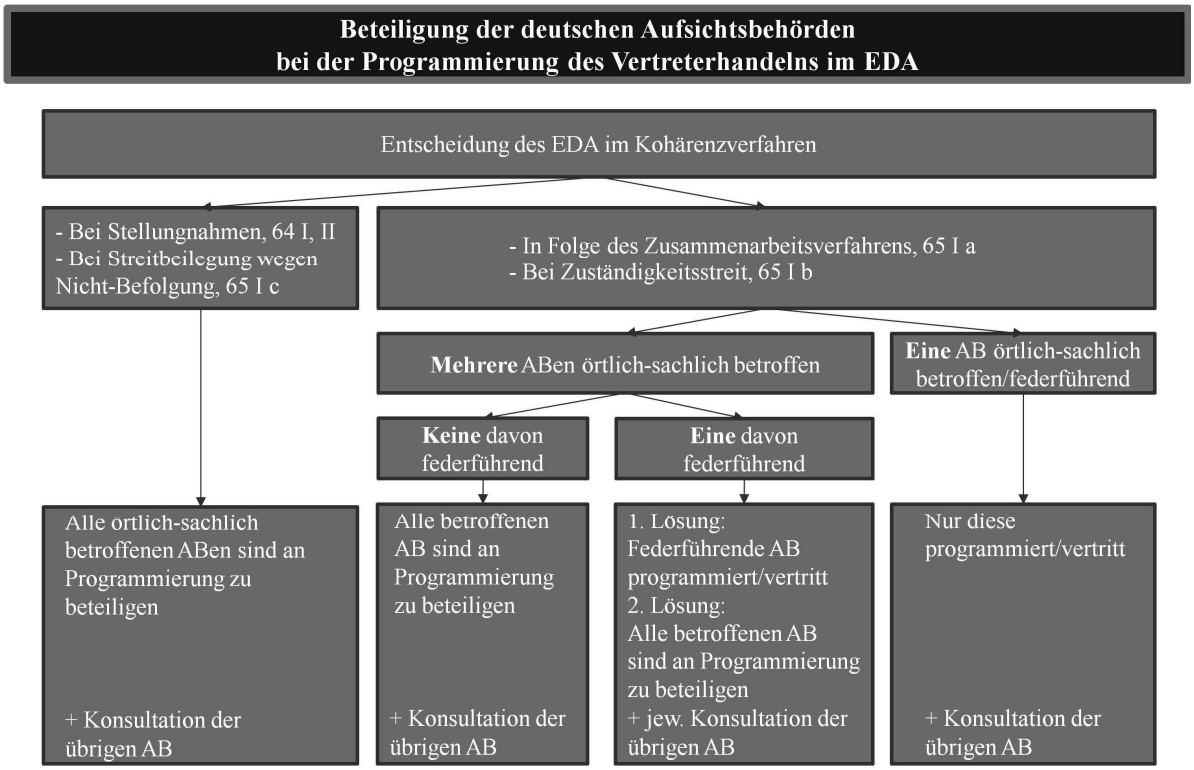
Diese Argumente streiten dafür, der federführenden Aufsichtsbehörde jedenfalls einen Vorzug in der Programmierung des Vertreterhandelns zu geben (oder sie selbst die Vertretung übernehmen zu lassen). Gleichzeitig schließt dies nicht aus, den anderen (betroffenen) Aufsichtsbehörden Gelegenheit zur Äußerung zu geben. Dabei folgt aus dem Gebot der Bundestreue auch eine Berücksichtigungspflicht hinsichtlich deren Meinung. Es ist deshalb angezeigt, jedenfalls eine Konsultation über das Vertreterhandeln durchzuführen.

---

[362] Vgl. *Wolff* (Fn. 149), S. 13 m. w. N.

δ) Entscheidung, wenn eine einzelne deutsche Aufsichtsbehörde betroffen/federführend ist

Soweit alleine *eine einzelne deutsche Aufsichtsbehörde betroffen oder federführend* ist, ergeben sich im Verhältnis zu dem zuvor Gesagten nur wenige Besonderheiten.
Hinsichtlich des Verfahrens nach Art. 64 Abs. 1, Art. 65 Abs. 1 lit. c (ex Art. 58 Abs. 1, Art. 58a Abs. 1 lit. d) DSGVO bestehen keine Unterschiede. Die Kategorien der Betroffenheit und Federführung passen hier nicht; vielmehr kann es alleine sein, dass die Initiative von einer nationalen Aufsichtsbehörde ausgeht. In diesem Fall ist es aus den oben genannten Gründen jedoch sachgerecht, alle (örtlich-sachlich) betroffenen Aufsichtsbehörden in die Programmierung miteinzubeziehen.
Im Fall der Entscheidung des EDA nach Art. 65 Abs. 1 lit. a, b (ex Art. 58a Abs. 1 lit. a, b) DSGVO streiten die oben genannten Argumente dafür, eine privilegierte Programmierung durch die betroffene/federführende Aufsichtsbehörde zuzulassen.



© Martini/Weinzierl

(2) Modus der Programmierung – Konsens- oder Mehrheitsprinzip

Die Länder müssen sich darauf verständigen, ob das Konsens- oder Mehrheitsprinzip (wenn letzteres, mit welchem Quorum) anzuwenden ist.

Das Konsensprinzip hat die souveräne Gleichheit der Länder auf ihrer Seite, die alleine im Mehrheitsprinzip – insbesondere in Anbetracht der mittelbaren Folgen von Entscheidungen des EDA – nicht überformt wird. Das Konsensprinzip wertet die Position des Bundes in den Bereichen der Aufsicht über nicht-öffentliche Stellen auf, in denen der Bund bisher keine aufsichtsrechtlichen Befugnisse genießt.

Gleichzeitig sprechen gewichtige Erwägungen für die Anwendung des Mehrheitsprinzips. Zuvorderst ist dies die Wahrung der Praktikabilität und Effektivität des Verfahrens. Entscheidungen müssen im europäischen Koordinierungsprozess ggf. in kürzester Zeit, jedenfalls im Zeitraum von ein bis zwei Monaten getroffen werden. Eine auf Konsens zielende Abstimmung läuft Gefahr, in diesem Zeitraum kein Ergebnis hervorzubringen. Die damit verbundene Überformung des Willens einzelner Bundesländer, die den verfas-

sungsrechtlichen Grundsatz eigenverantwortlicher Aufgabenerfüllung der Länder strapaziert, ist verfassungsrechtlich rechtfertigbar, sofern eine wirksame Wahrnehmung der Verpflichtungen, welche die Bundesrepublik auf der Grundlage des Art. 23 GG eingegangen ist, anderenfalls nicht wirksam erfüllbar ist.[363] Im Falle der Abstimmung der Länder zur Gewährleistung des unionsrechtlichen Kohärenzverfahrens ist das der Fall.

iii. Verhalten des gemeinsamen Vertreters – freie Vertretung oder Weisungsbindung

Jeder Mitgliedstaat der Europäischen Union muss klären, welche Befugnisse dem gemeinsamen Vertreter im Bereich des Kohärenzverfahrens zukommen sollen und auf welchem Weg die inhaltliche Programmierung erfolgen soll.[364] Das gilt insbesondere für die Frage, ob der Vertreter frei in seinem Handeln oder (im Innenverhältnis) an Weisungen oder eine gewisse Form der Programmierung gebunden sein soll.

Relevant wird die Frage der Bindung in allen Fällen, in denen nicht alleine *einer* Aufsichtsbehörde das Recht übertragen ist, die Vertretung wahrzunehmen und gleichzeitig auch die inhaltliche Position zu bestimmen. Je nach dem Einfluss der Aufsichtsbehörden auf die Position des Vertreters ist dabei ein verschieden hoher Grad der Bindung an den Willen der zur Abstimmung berufenen Aufsichtsbehörden angezeigt. Eine völlige Weisungsfreiheit – verbunden mit der freien Entscheidung über die Sache – würde die Wahrnehmung der jeweiligen Kompetenzen der Länder beeinträchtigen.

Aus dem Umstand alleine, dass die Datenschutz-Grundverordnung eine Vertretung im EDA vorsieht, ergibt sich noch nicht, dass der Vertreter im Innenverhältnis nicht gebunden sein dürfte. Dass dies zulässig ist, folgt vielmehr aus der Offenheit der Datenschutz-Grundverordnung für die verfassungsmä-

---

[363] Siehe dazu oben S. 152. Zur Verstetigung der Abstimmung sowie zur wechselseitigen Kontrolle der nationalen Aufsichtsbehörden (insbesondere mit Blick auf Art. 64 Abs. 6 [ex Art. 58 Abs. 7a] DSGVO) siehe S. 150 und S. 214.

[364] Hinsichtlich der Bestimmung des Vertreters im EDA im Rahmen des Kohärenzverfahrens kann grundsätzlich auf die obigen Ausführungen zur Bestimmung des Vertreters verwiesen werden (siehe S. 141).

ßigen, organisatorischen und administrativen Strukturen (EG 117 [ex EG 92] DSGVO) der Mitgliedstaaten.
Orientierungspunkte für eine sachgerechte Regelung der Bindung des gemeinsamen Vertreters an den Willen der Länder (und des Bundes) lassen sich §§ 3 bis 6 EUZBLG entnehmen. Hiernach richtet sich der Einfluss der Länder auf die Verhandlungsposition des Bundes nach dem Grad der Betroffenheit in eigenen (Rechts-)Positionen. Die Bindung an den Willen reicht dabei von einer bloßen Berücksichtigung des Länderwillens (§ 5 Abs. 1 EUZBLG) bis hin zu einer strikten Bindung (§ 5 Abs. 2 S. 5 EUZBLG). Gleichwohl ist dies nur teilweise eine taugliche Richtschnur, da dort die Frage, wer welchen Grad an Einfluss auf eine Position hat, mit der Frage der Bindung verknüpft ist. Für den Bereich der Koordinierung der Datenschutzaufsichtsbehörden kann es sinnvoller sein, generell eine Bindung an den in der Abstimmung zwischen den Ländern ermittelten Willen vorzusehen.

iv. (Selbst-)Kontrolle der nationalen Aufsichtsbehörden

Die Frage der Selbstkontrolle lässt sich wie im Begleitverfahren zum Verfahren der Zusammenarbeit beantworten (siehe S. 227). Die im Kohärenzverfahren hinzukommenden Fragen der Vertretung im EDA lösen keine zusätzlichen (Selbst-)Kontrollbedarfe aus.

v. Haftung

Die Weiterreichung der Haftung richtet sich hier allgemein nach dem LastG (s. S. 214). Der im Zusammenarbeitsverfahren problematische Fall einer Übertragung von Untersuchungsbefugnissen an Mitglieder oder Bedienstete unterstützende Aufsichtsbehörden des Art. 62 Abs. 4, 5 (ex Art. 56 Abs. 3a, 3b) DSGVO[365] besteht hier nicht. Eine gesetzliche Regelung ist deshalb nicht erforderlich.

[365] Dazu S. 236.

vi. Klagerecht für die Nichtigkeitsklage nach Art. 263 AEUV

Soll den nationalen Aufsichtsbehörden ein umfassendes Klagerecht hinsichtlich der Beschlüsse des EDA zustehen, besteht der einfachste Weg darin, ihnen die Entscheidung über das Gebrauchmachen der privilegierten Klagemöglichkeit der Bundesrepublik zu übertragen und sie (wohl entsprechend der Vertretungsregelung im EDA) mit der Vertretung vor dem EuGH zu betrauen.
Diesen Weg zeichnet § 7 EUZBLG jedenfalls teilweise vor. Der Bundesrat kann von der Bundesregierung das Vorgehen im Klagewege verlangen (§ 7 Abs. 1 S. 1 EUZBLG). Jedoch bleibt die Prozessvertretung bei der Bundesregierung; diese hat hierüber ein Einvernehmen mit dem Bundesrat herzustellen (§ 7 Abs. 3 EUZBLG).
Die Regelung für die Datenschutzaufsicht könnte einen Schritt weiter gehen. Entsprechend der allgemeinen Abstimmungs- und Beteiligungsregelungen hätten (primär[366]) die zu Entscheidungen berufenen Aufsichtsbehörden darüber zu befinden, ob Klage zu erheben ist. Zudem könnte der Gesetzgeber dem oder den jeweiligen mit der Vertretung im EDA betrauten Aufsichtsbehörden auch die Prozessführung übertragen. Das würde auch die Unabhängigkeit der Aufsichtsbehörden weitgehend sichern. Gleichzeitig verbinden sich mit einer solchen Lösung für den Bund nur sehr geringe Risiken, da die den Aufsichtsbehörden übertragenen Befugnisse nicht über den diese betreffenden Bereich der Beschlüsse des EDA hinausgehen.

cc) Bei rein innerstaatlichen Sachverhalten

Das Kohärenzverfahren auf nationaler Ebene muss auch dazu dienen, zwischen divergierenden Positionen bei der Anwendung der Datenschutz-Grundverordnung Einheitlichkeit herzustellen. Insoweit gilt das Gleiche wie in den Fällen, in denen eine innerstaatliche Abstimmung hergestellt werden muss, damit eine einheitliche deutsche Position in das Kohärenzverfahren nach der Datenschutz-Grundverordnung eingespeist werden kann. Insofern

[366] D. h. entsprechend § 7 Abs. 1 S. 2 EUZBLG unter Wahrung und Beachtung der Gesamtstaatlichen Verantwortlichkeit des Bundes.

sollte die hierfür getroffene Abstimmungsregelung für die Fälle des rein innerstaatlichen Kohärenzbedarfes übernommen werden.

39. Art. 68 Abs. 4 (ex Art. 64 Abs. 3): Vertreter im Europäischen Datenschutzausschuss

Art. 68 (ex Art. 64) DSGVO regelt die Einrichtung des EDA. Art. 68 bis 76 (ex Art. 64 bis 72) DSGVO regeln dessen Konstituierung, Verfahren, Befugnisse etc. umfassend und unmittelbar.
Einzig Art. 68 Abs. 4 (ex Art. 64 Abs. 3) DSGVO gibt den Mitgliedstaaten auf, wenn sie mehr als eine Aufsichtsbehörde eingerichtet haben, zu regeln, wer der nationale Vertreter beim EDA ist. Diese Vertretungsnotwendigkeit liegt parallel zum Regelungsbedarf beim Kohärenzmechanismus, wenn ein Mitgliedstaat mehr als eine Aufsichtsbehörde einrichtet. Die Regelungsverpflichtung wird jedoch primär von Art. 51 Abs. 1 Hs. 1 (ex Art. 46 Abs. 2 Hs. 1) DSGVO erfasst; siehe dazu S. 124 ff.

40. Zusammenfassung zu den Art. 51 ff. (ex Art. 46 ff.) unabhängige Datenschutzaufsichtsbehörden/Kohärenzverfahren

Die Datenschutz-Grundverordnung gibt den Mitgliedstaaten zahlreiche konkrete und unmittelbare Vorgaben für das System der aufsichtsrechtlichen Strukturen mit auf den Weg – nicht zuletzt auch zahlreiche Regelungsaufträge, denen diese nachkommen müssen. Das gilt insbesondere für diejenigen Staaten, die an Systemen mit mehreren Aufsichtsbehörden festhalten. Art. 51 Abs. 3 und Art. 68 Abs. 4 [ex Art. 46 Abs. 2 und Art. 64 Abs. 3] DSGVO) gestattet ihnen dies, legt ihnen dann aber besonderer Handlungspflichten auf, die ein einheitliches Auftreten nach außen verbürgen. Hiermit verbindet sich der Bedarf nach einer Abstimmung zwischen den nationalen Aufsichtsbehörden nach innen. Der deutsche Gesetzgeber muss eine wirksame behördliche koordinierte Datenschutzaufsicht innerhalb des durch die Datenschutz-Grundverordnung gezogenen Rahmens vorsehen. Dies stellt die Mitgliedstaaten im Hinblick auf den kurzen verbleibenden Zeitraum bis zum Inkrafttreten Datenschutz-Grundverordnung vor Herausforderungen.

a. Grundsätzliches

Eine besondere Regelungspflicht trifft den deutschen Gesetzgeber insbesondere im Hinblick auf das Auftreten im[367] und gegenüber[368] dem EDA im Kohärenzverfahren (Art. 63 ff. [ex Art. 57 ff.] DSGVO) sowie das Auftreten gegenüber anderen nationalen Aufsichtsbehörden im Bereich der Zusammenarbeit (Art. 60 ff. [ex Art. 54a ff.] DSGVO)[369]. Dagegen ist die Regelung eines einheitlichen Auftretens gegenüber der Kommission in Form einer speziellen Vorschrift nicht erforderlich.[370]
Die Art. 52 bis 59 (ex Art. 47 bis 54) DSGVO gestalten die Charakteristik der Aufsichtsbehörde[371] sowie materielle Vorgaben hinsichtlich der in der Aufsichtsbehörde tätigen Personen[372] sowie die aufsichtsbehördlichen Aufgaben[373] und Befugnisse[374] näher aus. Die Befugnisse der Aufsichtsbehörden regelt die DSGVO unmittelbar (wenn auch nicht abschließend, Art. 58 Abs. 6 [ex Art. 53 Abs. 4] DSGVO), so dass sich das BDSG-neu insoweit in Zurückhaltung üben kann.[375]

b. Auftreten im EDA

Ein kollektives Auftreten der jeweiligen nationalen Aufsichtsbehörden im EDA wird durch die Entsendung eines gemeinsamen Vertreters gewährleistet (vgl. Art. 51 Abs. 3[ex Art. 46 Abs. 2 DSGVO]; Art. 68 Abs. 4 [ex Art. 64 Abs. 3] DSGVO). Den nationalen Vertreter beim EDA muss der Mitglied-

---

[367] Vgl. S. 136 ff. sowie S. 265.
[368] Vgl. S. 241 ff.
[369] Vgl. S. 206 ff.
[370] Vgl. S. 120 f.
[371] Bedeutsam sind u. a. die in Art. 52 (ex Art. 47) DSGVO enthaltenen Vorgaben zur aufsichtsbehördlichen Unabhängigkeit. In Bezug auf die Unabhängigkeit der Aufsichtsbehörden sind insbesondere weiterhin die Vorgaben maßgeblich, die der EuGH zur Datenschutzrichtlinie entwickelt hat, vgl. S. 156 ff.
[372] Zur personellen Gestalt der Aufsichtsbehörde vgl. S. 123 f.
[373] Hierzu S. 178 ff.
[374] Hierzu S. 184 ff.
[375] Ausführlich S. 184 f.

staat bestimmen.[376] Eine koordinierte Rechtssetzung von Bund und Ländern kann im Rahmen eines Staatsvertrages erfolgen.[377]
Nach welchem Modus eine solche gesetzliche Regelung den Vertreter der deutschen Aufsichtsbehörden bestimmt, ist rechtlich nur schwach determiniert. Es kann sich empfehlen, die BfDI als ständige Vertreterin vorzusehen und ihr ein Mitglied einer Aufsichtsbehörde der Länder als Stellvertreter zur Seite zu stellen oder aber die Aufsichtsbehörden konsensual einen gemeinsamen Vertreter selbst wählen zu lassen.[378]
Der ständige Vertreter ist dann zwar vertretungsberechtigt, aber innerstaatlich nicht unbedingt für die jeweilige Angelegenheit sachlich zuständig. Er darf daher nicht alleine seinen eigenen Standpunkt vertreten, sondern ist an den Willen der anderen Aufsichtsbehörden gebunden. Es ist sachgerecht, den ständigen Vertreter an den Willen derjenigen übrigen Aufsichtsbehörden rückzubinden, deren innerstaatliche Zuständigkeit die Entscheidung in besonderer Weise berührt. Es empfiehlt sich, die Entscheidungskoordination durch eine gegenstandsbezogene, am Modell des Art. 23 GG orientierte Regelung vornehmen zu lassen.[379] Erwägenswert ist es darüber hinaus, ein organisatorisch verstetigtes Gremium zu schaffen, das als Plattform für den föderalen Dialog dient und eine Kooperation und Koordination der verschiedenen Aufsichtsbehörden ermöglicht.[380]

c. Auftreten gegenüber anderen nationalen Aufsichtsbehörden (im Bereich der Zusammenarbeit, Art. 60 ff. [ex Art. 54a ff.])

Das Zusammenarbeitsverfahren regelt die Datenschutz-Grundverordnung selbst. Der Mitgliedstaat muss nur ein entsprechendes Begleitverfahren vorsehen.[381] Dieses Begleitverfahren kann, je nach Sachverhalt, für unterschiedliche Konstellationen bedeutsam werden und eine Zusammenarbeit der Aufsichtsbehörden ermöglichen.[382] Die Aufsichtsbehörden eines anderen Mit-

[376] Siehe S. 131 ff.
[377] Zur Verbandskompetenz vgl. S. 136 ff.
[378] Zu den unterschiedlichen Modellen siehe S. 141 ff.
[379] Der inhaltlichen Entscheidungskoordination widmen sich die S. 146 ff.
[380] Sie hierzu als Referenzmodellen geeigneten Vergleichsgruppen ausführlich hierzu S. 150 ff.
[381] Siehe S. 206.
[382] Zu unterschiedlichen Fallkonstellationen vgl. S. 209 ff.

gliedstaats können an die deutschen Aufsichtsbehörden über eine deutsche zentrale Anlaufstelle (vgl. auch EG 119 [ex EG 93] DSGVO) herantreten, derer es damit gerade außerhalb des Kohärenzverfahrens bedarf. Nur mit ihrer Hilfe kann eine effektive und rasche Zusammenarbeit in grenzüberschreitenden Sachverhalten gelingen.[383] Im Innenverhältnis der deutschen Aufsichtsbehörden zueinander müssen sich diese auf eine gemeinsame Position einigen, die sie gegenüber der ausländischen Aufsichtsbehörde vertreten.

Immer dann, wenn die Datenschutz-Grundverordnung von der „betroffenen Aufsichtsbehörde“ spricht, rekurriert sie dabei nicht auf die nationale Zuständigkeitsverteilung, sondern meint die Gesamtheit der mitgliedstaatlichen Aufsichtsbehörden.[384]

Wie der Mitgliedstaat das Begleitverfahren ausgestaltet, gibt die Datenschutz-Grundverordnung (jenseits des Gebots wirksamer Erfüllung der mitgliedstaatlichen Verpflichtungen zur Datenschutzaufsicht und Zusammenarbeit) nicht vor. Dem Mitgliedstaat kommt mithin ein erheblicher Gestaltungsspielraum zu, innerhalb dessen er, geleitet von der Vorgabe einer effektiven Zusammenarbeit der Aufsichtsbehörden, regelnd tätig werden kann. Hinsichtlich der Errichtung der zentralen Anlaufstelle lassen sich grundsätzlich die Erwägungen betreffend der nationalen Vertretung beim EDA in analoger Weise fruchtbar machen.[385] Der gemeinsame Vertreter muss nicht zugleich personenidentisch mit der zentralen Anlaufstelle sein.

Komplizierter gestaltet sich eine geeignete Regelung für das Innenverhältnis der deutschen Aufsichtsbehörden. Rechtlich durch die Datenschutz-Grundverordnung nicht determiniert, aber rechtspolitisch sinnvoll ist eine Übertragung des Konzepts der Datenschutz-Grundverordnung von betroffenen und federführenden Aufsichtsbehörden auf die nationale Ebene.[386] Die innerstaatliche Zuständigkeitsbestimmung sollte im Streitfalle nicht alleine den Gerichten überlassen werden, sondern vielmehr entweder durch die zent-

[383] Vgl. S. 211 f.
[384] Vgl. S. 212 f.
[385] Vertieft hierzu S. 217 f.
[386] Siehe ausführlich auf S. 219 ff.

rale Anlaufstelle oder aber die Aufsichtsbehörden im Wege eines effizienten und zügigen Verfahrens gemeinsam getroffen werden.[387]
Für den Kreis der an der Abstimmung Beteiligten sind zwei unterschiedliche Konzepte denkbar, für die jeweils gute Gründe sprechen und die beide rechtlich zulässig sind: Entweder nehmen nur die betroffenen Aufsichtsbehörden an der Abstimmung teil oder aber alle Aufsichtsbehörden werden beteiligt.[388] Gleichzeitig sprechen gute Gründe dafür, einer innerdeutschen federführenden Aufsichtsbehörde eine herausgehobene Stellung zuzuweisen. Müssen sich mehrere Aufsichtsbehörden koordinieren und vertreten diese (zum Teil) inhaltlich unterschiedliche Positionen, kann eine Entscheidungsfindung grundsätzlich sowohl nach dem Konsens- als auch nach dem Mehrheitsprinzip erfolgen. Aus Gründen der Praktikabilität und Effektivität erscheint das Mehrheitsprinzip grundsätzlich vorzugswürdig.[389]

d. Auftreten im und gegenüber dem EDA (im Kohärenzverfahren)

Ebenso wie das Zusammenarbeitsverfahren regelt die Datenschutz-Grundverordnung auch das streitfallvermeidende und -regende Kohärenzverfahren unmittelbar und grundsätzlich abschließend.[390] Auch hier muss der Mitgliedstaat lediglich, sofern er mehrere Aufsichtsbehörden errichtet, ein Verfahren implementieren, das sicherstellt, dass die Regeln für das Kohärenzverfahren eingehalten werden.
Hinsichtlich des Regelungsbedarfs für das nationale Begleitverfahren ist zwischen dem Außen- und dem Innenverhältnis zu unterscheiden. Im Außenverhältnis muss der Mitgliedstaat einerseits ebenfalls eine Regelung für die Vertretung im EDA treffen sowie andererseits eine zentrale Anlaufstelle (vgl. auch EG 119 [ex EG 93] DSGVO) einrichten. Für beide bedarf es einer Binnenkoordination. Auch hier zeichnet die Datenschutz-Grundverordnung jedoch nicht vor, wie der Mitgliedstaat die innerstaatliche Abstimmung der nationalen Aufsichtsbehörden im Kohärenzverfahren organisieren muss.[391]

---

[387] Zu diesen beiden Möglichkeiten S. 221 f.
[388] Zum Für und Wider beider Konzepte vgl. S. 222 f.
[389] Ausführlicher hierzu sowie zum Rechtfertigungsbedürfnis für die Implementierung einer Mehrheitsentscheidung vgl. S. 226 f.
[390] Siehe S. 241.
[391] Ausführlich zum Innenverhältnis S. 243 ff.

Hinsichtlich der Vertretung im EDA liegt es nahe, grundsätzlich der allgemeinen Vertretungs- und Abstimmungsregelung zu folgen. Eine Ausnahme kann sich für Fälle empfehlen, in denen das Kohärenzverfahren als Fortführung des Verfahrens der Zusammenarbeit dient (Art. 65 Abs. 1 lit. a [ex Art. 58a Abs. 1 lit. a] DSGVO). Hier ist es ein denkbarer Weg, einer innerstaatlich federführenden Aufsichtsbehörde sowohl das Recht der (Unter-)Vertretung als auch die Bestimmung über den Inhalt der Vertretung zuzusprechen und die weiteren betroffenen oder sonstigen Aufsichtsbehörden nur im Rahmen einer Konsultation oder Anhörung zu beteiligen.
Hinsichtlich der Errichtung der zentralen Anlaufstelle liegt es ebenfalls nahe, der Regelung aus dem Begleitverfahren zum Zusammenarbeitsverfahren zu folgen. Anders als dort dient sie hier als Scharnier zwischen den mitgliedstaatlichen Aufsichtsbehörden und dem EDA. Der Zweck ihrer Einrichtung ist jedoch der gleiche wie im Rahmen des Zusammenarbeitsverfahrens.[392]
Ratsam ist es auch, den innerstaatlichen Aufsichtsbehörden weitgehend die Ausübung des privilegierten Klagerechts der Bundesrepublik aus Art. 263 Abs. 1 AEUV gegen Beschlüsse und Stellungnahmen des EDA zu übertragen. Dies stärkt einerseits die Unabhängigkeit der Aufsichtsbehörden und kann als Rechtfertigung einer Entscheidungskonzentration bei einer federführenden Aufsichtsbehörde dienen. Gleichzeitig erfüllt es wohl am besten die inhaltlichen Zielvorgaben des EuGH aus der Rs. Schrems[393].

e. Rein innerstaatliche Sachverhalte

Gute Gründe streiten dafür, ein dem Verfahren der Zusammenarbeit und Kohärenz entsprechendes innerstaatliches Abstimmungsverfahren auch in rein innerstaatlichen Sachverhalten ohne grenzüberschreitenden Bezug anzuwenden, bei denen mehrere nationale Aufsichtsbehörden berührt sind. Die entsprechenden Regelungen der Datenschutz-Grundverordnung selbst finden dann zwar keine unmittelbare Anwendung.[394] Allerdings erfordert sie mittelbar die Implementierung eines Zusammenarbeitsverfahrens auch für solche

[392] Zum Außenverhältnis betreffend den Regelungsbedarf für das nationale Begleitverfahren vgl. S. 242.
[393] EuGH, Rs. C-362/14, Urteil v. 6.10.2015 – „Schrems“.
[394] Vgl. S. 212 f.

Fallkonstellationen, da auch insoweit ein gesteigerter Abstimmungsbedarf besteht, den es zu kanalisieren gilt. Andernfalls wäre die effektive und einheitliche Durchsetzung des in der Datenschutz-Grundverordnung enthaltenen materiellen Datenschutzrechts gefährdet.[395]

41. Art. 80 Abs. 2 (ex Art. 76 Abs. 2): Beschwerde- und Klagerechte von Verbänden

a. Inhalt der Regelung

Art. 80 Abs. 2 (ex Art. 76 Abs. 2) DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, bestimmten Non-Profit-Organisationen ein Verbandsklagerecht einzuräumen. Diese können das Recht auf Beschwerde bei einer Aufsichtsbehörde (Art. 77 [ex Art. 73] DSGVO) und das Recht auf einen wirksamen gerichtlichen Rechtsbehelf gegen die Aufsichtsbehörde (Art. 78 [ex Art. 74] DSGVO) sowie gegen den Verantwortlichen oder den Auftragsverarbeiter (Art. 79 [ex Art. 75] DSGVO) ausüben, ohne dass es auf eine Mandatierung der betroffenen Person gemäß Art. 80 Abs. 1 (ex Art. 76 Abs. 1) DSGVO ankommt.
Nähere Konturierung erfährt die Öffnungsklausel des Art. 80 Abs. 2 (ex Art. 76 Abs. 2) DSGVO durch den EG 142 (ex EG 112) DSGVO. Dieser stellt insbesondere klar, dass der Mitgliedstaat nicht vorsehen darf, dass die genannten Entitäten auch Schadensersatz geltend machen können.

b. Einordnung in das System der Öffnungsklauseln

Bei Art. 80 Abs. 2 (ex Art. 76 Abs. 2) DSGVO handelt es sich um eine fakultative Öffnungsklausel. Dies ergibt sich bereits aus dem insoweit eindeutigen Wortlaut: „können vorsehen“ bzw. „may provide“.

c. Vergleich zur Datenschutzrichtlinie

Die Datenschutzrichtlinie sah kein Verbandsklagerecht vor. Sie verlangte den Mitgliedstaaten insbesondere nicht die Implementierung eines solchen ab.

[395] Ausführlich zum durch rein innerstaatliche Sachverhalte hervorgerufenen Regelungsbedarf S. 215 f.

Art. 28 Abs. 4 S. 1 DSRL gestattete es aber einem Verband, eine betroffene Person zu vertreten und sich mit einer Eingabe an jede Kontrollstelle zu wenden.

d. Bisherige Ausgestaltung im nationalen Recht

Macht der nationale Gesetzgeber von der ihm zukommenden Öffnungsklausel Gebrauch und implementiert mithin die genannten Rechte für die Entitäten, sieht er in dogmatischer Hinsicht altruistische Verbandsbeschwerde- bzw. Verbandsklagerechte vor.[396] Im Umweltrecht bspw. enthält § 2 UmwRG ein solches Verbandsklagerecht.

Ein derartiges Verbandsklagerecht sieht das BDSG selbst bislang nicht vor. Ob bzw. inwieweit datenschutzrechtliche Normen Verbraucherschutzgesetze i. S. d. § 2 Abs. 2 UKlaG darstellen, stößt de lege lata auf unterschiedliche Antworten.[397] So lehnte es etwa das OLG Frankfurt am Main ab, die §§ 3a, 4 BDSG als verbraucherschützende Normen zu charakterisieren. Zur Begründung berief es sich darauf, dass diese Normen alle natürlichen Personen – unabhängig von der Verbrauchereigenschaft – schützten. [398] Ob § 28 Abs. 4 BDSG ein Verbraucherschutzgesetz ist, ließ das OLG dagegen ausdrücklich offen.[399]

Gegenwärtig befindet sich aber der Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts im Gesetzgebungsverfahren.[400] Der Gesetzesentwurf der Bundesregierung will insbesondere datenschutzrechtliche Vorschriften[401]

---

396 Vgl. dazu für das deutsche Recht *Gola/Klug/Körffer* (Fn. 112), § 11, Rn. 26; *Martini*, Verwaltungsprozessrecht, 5. Aufl., 2011, S. 45.

397 Vgl. *Micklitz*, in: Krüger/Rauscher (Hrsg.), MüKoZPO, 4. Aufl., 2013, § 2 UKlaG, Rn. 40. Siehe auch *Gola/Wronka*, RDV 2015, 3, (8), unter Verweis auf die unterschiedlichen Judikate der Gerichte.

398 OLG Frankfurt am Main, Urt. v. 30.6.2005 – 6 U 168/04 –, juris, Rn. 25.

399 OLG Frankfurt am Main, Urt. v. 30.6.2005 – 6 U 168/04 –, juris, Rn. 25.

400 Der Gesetzesentwurf der Bundesregierung: BT-Drucks. 18/4631. Die Beschlussempfehlung und der Bericht des Ausschusses für Recht und Verbraucherschutz vom 2.12.2015: BT-Drucks. 18/6916.

401 Gemäß BT-Drucks. 18/4631, S. 21 sind dies „alle datenschutzrechtlichen Vorschriften […], die die Zulässigkeit der Erhebung, Verarbeitung oder Nutzung von Daten eines Verbrauchers regeln, wenn der Unternehmer die Daten zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- oder Nutzungs-

ausdrücklich in § 2 Abs. 2 UKlaG aufnehmen, um diese als verbraucherschützende Normen zu etablieren.[402] Während die Bundesregierung den Gesetzesentwurf für unionsrechtskonform hält,[403] ziehen manche dies unter dem Regime der Datenschutzrichtlinie in Zweifel.[404]

e. Zwischenfazit

Um die effektive Durchsetzung der Regelungen zu fördern, welche die Datenschutz-Grundverordnung vorsieht, kann es sinnvoll sein, von dem Regelungsspielraum des Art. 80 Abs. 2 (ex Art. 76 Abs. 2) DSGVO Gebrauch zu machen. Will der nationale Gesetzgeber seine Aktivität gegenwärtig auf die wesentlichen Maßnahmen beschränken, empfiehlt es sich hingegen, den durch Art. 80 (ex Art. 76) DSGVO eröffneten Regelungsspielraum aktuell noch nicht auszuschöpfen. Stattdessen kann zu einem späteren Zeitpunkt sorgfältig überlegt werden, ob und wenn ja, wie eine Nutzung des Regelungsspielraums erfolgen kann.

---

profilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken erhebt, verarbeitet oder nutzt."

[402] Vgl. BT-Drucks. 18/4631, S. 2: „Durch die Ergänzung des § 2 Absatz 2 UKlaG-E soll ausdrücklich geregelt werden, dass datenschutzrechtliche Vorschriften, welche die Zulässigkeit der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten eines Verbrauchers durch einen Unternehmer zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens von Auskunfteien, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken regeln, Verbraucherschutzgesetze im Sinne des § 2 Absatz 1 UKlaG sind."

[403] Vgl. BT-Drucks. 18/4631, S. 14: „Der Gesetzentwurf ist mit dem Recht der Europäischen Union und bestehenden Verpflichtungen der Bundesrepublik Deutschland aus völkerrechtlichen Verträgen vereinbar."

[404] Vgl. *Gerhard*, CR 2015, 338 (342 ff.).

42. Art. 83 Abs. 7 bis 9 (ex Art. 79 Abs. 3b bis Abs. 5): Allgemeine Bedingungen für die Verhängung von Geldbußen

a. Inhalt der Regelung

aa) Geeigneter Adressat von Geldbußen (Art. 83 Abs. 7 [ex Art. 793b] DSGVO

Im Interesse einer effektiven Durchsetzung des Datenschutzrechts der Union sieht Art. 83 (ex Art. 79) DSGVO die Verhängung von Geldbußen („administrative fines") vor. Sein Abs. 7 (ex Abs. 3b) hält eine Öffnungsklausel für die Mitgliedstaaten bereit. Sie gestattet die Verhängung von Geldbußen nicht nur gegenüber nicht-öffentlichen Stellen, sondern auch *gegenüber Behörden und öffentlichen Stellen*. Das kann (auch wenn diese ohnehin dem Gebot der Gesetzmäßigkeit der Verwaltung unterworfen sind) dazu beitragen, die Durchsetzung des in der Datenschutz-Grundverordnung enthaltenen materiellen Datenschutzrechts flächendeckend wirksam zu gewährleisten. Die Regelung will sicherstellen, dass auch die öffentlichen Stellen die Vorgaben der Datenschutz-Grundverordnung jenseits rechtlicher Gebote im praktischen Vollzugsalltag tatsächlich beachten.

Der dem nationalen Gesetzgeber zukommende Regelungsspielraum bezieht sich dabei sowohl auf das „Ob" als auf den Umfang („Wie") der Implementierung von Geldbußen (vgl. auch EG 150 [ex EG 120] DSGVO).

Eingang in den Gesetzgebungsprozess fand die Öffnungsklausel erst auf Vorschlag des Rates. Der vorherige Kommissionsentwurf und die legislative Entschließung des Parlaments sahen eine derartige Klausel hingegen nicht vor. Die Initiative des Rates beruhte auf den Bedenken einiger Mitgliedstaaten hinsichtlich der Verhängung von Bußgeldern gegen öffentliche Stellen.[405]

Die Datenschutz-Grundverordnung nennt als Adressaten einer Geldbuße ausdrücklich „öffentliche Behörden und öffentliche Einrichtungen". Es fragt sich, ob die Geldbuße nur gegen die staatliche Stelle selbst oder auch gegen den jeweiligen *Mitarbeiter* verhängt werden darf. Nach gegenwärtigem natio-

[405] Vgl. unter Bezugnahme auf die diesbezüglichen Mitteilungen der Ratspräsidentschaft *Nguyen*, RDV 2014, 26 (29).

nalem Recht kann eine Geldbuße grundsätzlich auch gegenüber der handelnden natürlichen Person ausgesprochen werden.[406] Angesichts des eindeutigen Wortlauts von Art. 83 Abs. 7 (ex Art. 79 Abs. 3b) DSGVO darf der nationale Gesetzgeber (beim Gebrauchmachen von der Öffnungsklausel) aber nur noch die staatliche Stelle als solche als Adressat einer Geldbuße vorsehen. Eine Haftung des einzelnen, den Datenschutzverstoß begehenden Mitarbeiters intendiert die Datenschutz-Grundverordnung auch bei Bußgeldern gegen nicht-öffentliche Stellen nicht. Dies macht z. B. Art. 83 Abs. 3 DSGVO deutlich. Er knüpft nur an (Mehrfach-)Verstöße von Verarbeitern und Auftragsverarbeitern, nicht aber an diesen unterstellte Personen an. Der nationale Gesetzgeber darf sie dann gleichfalls nicht implementieren. Diese Lücke kann der nationale Gesetzgeber alleine durch sonstige Sanktionen nach Art. 84 DSGVO schließen.

bb) Ergänzende Verfahrensgarantien als condicio sine qua non (Art. 83 Abs. 8 [ex Art. 79 Abs. 4] DSGVO)

Erlassen die mitgliedstaatlichen Behörden Geldbußen, müssen die Mitgliedstaaten angemessene Verfahrensgarantien für die Ausübung dieser Befugnis sicherstellen (Art. 83 Abs. 8 [ex Art. 79 Abs. 4] DSGVO). Das gilt insbesondere für die Gewährleistung von Rechtsschutz sowie die Einhaltung des Verhältnismäßigkeitsprinzips. Die Geldbuße kann – wie Art. 83 Abs. 7 (ex Art. 79 Abs. 3b) DSGVO mit der Wendung „unbeschadet der Abhilfebefugnisse“ andeutet – grundsätzlich auch selbstständig neben eine Abhilfebefugnis treten.

cc) Sonderregelung des Art. 83 Abs. 9 (ex Art. 79 Abs. 5) DSGVO

Art. 83 Abs. 9 (ex Art. 79 Abs. 5) DSGVO bietet Mitgliedstaaten, die administrativ verhängte Geldbußen nicht kennen, die Möglichkeit, die Geldbuße von Gerichten aussprechen zu lassen. Für Deutschland hat diese Regelung keine Bedeutung.

---

[406] Vgl. *Becker*, in: Plath (Hrsg.), BDSG, 2013, § 43, Rn. 6; *Ehmann*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 43, Rn. 22.

b. Einstufung in das System der Öffnungsklauseln

Die in Art. 83 Abs. 7 (ex Art. 79 Abs. 3b) DSGVO vorgesehene Öffnungsklausel ist fakultativer Natur. Das ergibt schon der eindeutige Normwortlaut: „kann […] festlegen" (bzw. in der englischen Fassung: „may lay down"). Gleiches gilt für Art. 83 Abs. 9 (ex Art. 79 Abs. 5) DSGVO. Art. 83 Abs. 9 gibt den Mitgliedstaaten demgegenüber einen Regelungsauftrag mit auf den Weg.

c. Vergleich zur Datenschutzrichtlinie

Die Datenschutzrichtlinie 95/46/EG thematisierte die Verhängung von Geldbußen nicht in der gleichen Klarheit wie die Datenschutz-Grundverordnung. Art. 24 DSRL spricht allgemein davon, dass die Mitgliedstaaten durch geeignete Maßnahmen die volle Anwendung der Richtlinie gewährleisten sollen. Hierunter kann auch die Verhängung einer Geldbuße fallen. EG 55 DSRL stellt schließlich fest, dass Sanktionen sowohl die Personen des Privatrechts als auch des öffentlichen Rechts treffen müssen.

d. Bisherige Ausgestaltung im nationalen Recht

Das BDSG regelt die Verhängung von Geldbußen gegenwärtig in § 43 BDSG. Auch zahlreiche Spezialgesetze, die bereichsspezifische Datenschutzvorschriften enthalten, kennen den Durchsetzungsmechanismus der Geldbuße. Ob § 43 BDSG auch bei Verstößen gegen datenschutzrechtliche Normen außerhalb des BDSG Anwendung findet, ist dabei umstritten.[407] Normadressat des § 43 BDSG sind neben nicht-öffentlichen auch öffentliche Stellen.[408] Das ergibt sich schon daraus, dass das Gesetz auch die Verpflichtungen der §§ 4d, 4e und 4f BDSG in die Bußgeldtatbestandskataloge aufgenommen hat. § 43 BDSG ist offen gefasst und erlaubt es mithin, in breitem Umfang Datenschutzverstöße mittels Geldbuße zu sanktionieren.
Die Verhängung von Geldbußen gegen öffentliche Stellen ist in der deutschen Rechtsordnung ein Fremdkörper. Dem Grundsatz der Polizeifestigkeit von

[407] Ausführlich hierzu und bejahend *Ehmann* (Fn. 406), § 43, Rn. 18 ff; dafür auch *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 43, Rn. 18; dagegen aber *Becker* (Fn. 406), § 43, Rn. 2.
[408] Vgl. *Gola/Klug/Körffer* (Fn. 407), § 43, Rn. 2.

Hoheitsträgern entspricht es, dass staatliche Stellen gegeneinander nicht ordnungsbehördlich vorgehen, sondern diese vielmehr selbst auf der Grundlage ihrer Gesetzesbindung für die Einhaltung der Normen sorgen. Entsprechend gesteht § 24 BDSG der BfDI bislang lediglich Kontrollrechte, aber keine Eingriffsbefugnisse zu. Die „störende" Behörde muss und kann selbst entscheiden, wie sie dem Datenschutz im Rahmen ihrer Aufgabenerfüllung und diesbezüglicher Rechtspflichten genügt (sog. Polizeifestigkeit von Hoheitsträgern).[409] Die auf eine präventive Abwehr von Gefahren gerichtete Kategorie der Polizeifestigkeit von Hoheitsträgern schließt eine nachträgliche Sanktionierung von Pflichtverletzungen durch die Verhängung von Bußgeldern aber nicht aus.

Auch die Datenschutzgesetze der Länder enthalten oftmals Normen, die eine Geldbuße zu verhängen gestatten. In Abhängigkeit von den jeweiligen Tatbeständen kommen grundsätzlich auch hier öffentliche Stellen bzw. deren Mitarbeiter als Normadressaten in Betracht.

Da Art. 83 DSGVO die Verhängung von Geldbußen (mit Ausnahme der beschriebenen Öffnungsklauseln) grundsätzlich abschließend regelt, verbleibt für § 43 BDSG in seiner bisherigen Form kein Raum mehr. Das gilt auch, obwohl der Katalog der Verstöße, den Art. 83 DSGVO formuliert, unvollständig ist. So fehlt etwa ein Bußgeldtatbestand für Verstöße gegen Art. 10 DGSVO sowie gegen Zertifizierungskriterien. Im Übrigen fehlen auch Regelungen zur Beihilfe und Anstiftung. Verstöße kann der Mitgliedstaat nur nach Art. 83 Abs. 7 und 8 DSGVO sowie nach Art. 84 Abs. 1 DSGVO in Gestalt anderer Sanktionsformen ahnden.

43. Art. 84 Abs. 1 (ex Art. 79b Abs. 1): Sanktionen

Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO legt den Mitgliedstaaten auf, Vorschriften zu Vorschriften über andere Sanktionen für Verstöße gegen die Datenschutz-Grundverordnung zu erlassen.[410]

---

[409] *Martini/Fritzsche*, NVwZ-Extra 2015/21, 1 (15 mit Fn. 170).

[410] Vgl. in diesem Zusammenhang auch die Überlegungen der Kommission in KOM(2010) 609 endgültig vom 4.11.2010, S. 10.

a. Einstufung in das System der Öffnungsklauseln

Bereits die Wortwahl der Norm macht deutlich, dass es sich bei Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO nicht um eine fakultative Öffnungsklausel handelt. Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO enthält vielmehr eine obligatorische Öffnungsklausel. Hintergrund für den zwingenden Charakter der Öffnungsklausel ist die Zielsetzung, eine effektive Durchsetzung des unionalen Datenschutzrechts zu gewährleisten. Dies deutet auch der zweite Satz des ersten Absatzes der Vorschrift an: „Diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein."

b. Inhalt der Öffnungsklausel

aa) „Sanktionen"

Was die Verordnung unter „Sanktionen" (im Englischen: „penalties") versteht, definiert sie nicht näher. Abstrakt kommen unterschiedliche Arten von Sanktionen, insbesondere strafrechtliche, aber auch ordnungsrechtliche Maßnahmen in Betracht.[411] Zulässig ist etwa die strafrechtliche Ahndung vorsätzlich gegen Entgelt begangener Verstöße gegen die Datenschutz-Grundverordnung, die widerrechtliche Erstellung eines Persönlichkeitsprofils oder die illegale Speicherung von Daten auf Vorrat, um den Zugriff Dritter zu ermöglichen.

Abzugrenzen sind Sanktionen von den ordnungsrechtlichen Maßnahmen der Aufsichtsbehörden, die die Datenschutz-Grundverordnung an anderer Stelle vorsieht (vgl. die Gegenüberstellung in EG 148 S. 1 [ex EG 118b S. 1] DSGVO). Solche Maßnahmen unterfallen nicht dem Sanktionsbegriff des Art. 84 (ex Art. 79b) DSGVO.

Die Datenschutz-Grundverordnung verwendet dabei eine uneinheitliche bzw. verwirrende Terminologie, die dem Normanwender Rätsel hinsichtlich des Verhältnisses von Art. 83 und 84 aufgibt: In ihren Erwägungsgründen macht sie deutlich, dass Sanktionen der Oberbegriff sind, der auch Geldbußen ein-

[411] Auch in der bisherigen wissenschaftlichen Diskussion zeichnet sich insoweit noch keine ganz klare Linie zum Verständnis der Vorschriften ab Vgl. *Härting* (Fn. 145) (462): „privatrechtliche Sanktionen"; *Hornung/Städtler*, CR 2012, 638 (642): „Einführung verhältnismäßig hoher Streitwerte".

schließt (EG 148 S. 1 DSGVO: „Sanktionen einschließlich Geldbußen“; ähnlich S. 4). Der Regelungsauftrag des Art. 84 (ex Art. 79b) DSGVO, den die Verordnung mit „Sanktionen“ überschreibt, schließt aber – entgegen der dadurch insinuierten Vermutung – Geldbußen nicht ein. Vielmehr scheint Art. 83 (ex Art. 79) DSGVO Umfang und Ausmaß von Geldbußen abschließend regeln zu wollen.

bb) Sanktionsbegriff der Datenschutzrichtlinie

Die Datenschutzrichtlinie regelte die mitgliedstaatliche Festschreibung von Sanktionen in Art. 24. Ähnlich wie die Datenschutz-Grundverordnung, sprach sie lediglich unspezifiziert von „Sanktionen“, ohne den Begriff weiter zu erläutern. Dementsprechend verstand man den Terminus als hinreichend flexibel, um unterschiedliche Sanktionsarten, wie strafrechtliche, verwaltungsrechtliche oder etwa zivilrechtliche, hierunter zu subsumieren.[412]

cc) Analyse der Erwägungsgründe

EG 148 S. 1 (ex EG 118a S. 1) DSGVO („Sanktionen einschließlich Geldbußen“) lässt sich einerseits als Klarstellung deuten, dass Sanktionen Geldbußen beinhalten. Andererseits lässt er sich aber auch so verstehen, dass Geldbußen grundsätzlich nicht dem Sanktionsbegriff unterfallen, hier aber eingeschlossen sind. Der Blick auf die englische Textfassung legt letzteres Verständnis nahe, da dort die Begriffe deutlicher gegenübergestellt werden („penalties and administrative fines“).
Eine Ausdifferenzierung erfährt der Sanktionsbegriff in EG 149 S. 3 (ex EG 119 S. 3) DSGVO. Dieser unterscheidet zwischen strafrechtlichen („criminal sanctions“) und verwaltungsrechtlichen Sanktionen („administrative sanctions“). Der erste Satz des Erwägungsgrundes scheint explizit auf Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO abzuzielen. Das hat zur Folge, dass der in Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO verwendeten Sanktionsbegriff jedenfalls strafrechtliche Sanktionen beinhaltet. Aufgrund der inneren Syste-

[412] So wohl *Brühann*, in: Grabitz/Hilf (Hrsg.), EU-Recht, 13. EL, Art. 24 Datenschutzrichtlinie, Rn. 5.

matik des Erwägungsgrundes scheint dies prima vista nicht für verwaltungsrechtliche Sanktionen zu gelten.
Wie der Begriff der verwaltungsrechtlichen Sanktionen zu verstehen ist, ist nicht ganz eindeutig. Aus EG 150 S. 1 (ex EG 120 S. 1) DSGVO lässt sich jedoch entnehmen, dass der Terminus nicht gleichbedeutend mit dem der Geldbuße ist, sondern vielmehr einen Oberbegriff darstellt, der die Geldbuße als einen Teilausschnitt aus einem umfassenderen Spektrum verwaltungsrechtlicher Sanktionen mitumfasst.
EG 152 (ex EG 120a) DSGVO legt nahe, dass unter „Sanktionen" im Sinne des Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO wohl auch solche verwaltungsrechtlicher Art zu verstehen sind. Aus der Zusammenschau von EG 150 S. 1 und 152 (ex EG 120 S. 1 und 120a) DSGVO ergibt sich jedoch, dass dies nicht für die Geldbuße als spezielle Form der verwaltungsrechtlichen Sanktion gilt.

dd) Gesetzessystematik; insbesondere Verhältnis zu Art. 83 (ex Art. 79)

Das Kapitel „Rechtsbehelfe, Haftung und Sanktionen" der Datenschutz-Grundverordnung stellt Art. 83 (ex Art. 79) DSGVO („Allgemeine Bedingungen für die Verhängung von Geldbußen") und Art. 84 (ex Art. 79b) DSGVO („Sanktionen") nicht ganz unverbunden nebeneinander: Laut Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO „legen [die Mitgliedstaaten] die Vorschriften über *andere Sanktionen* […] fest"[413].[414] Mit dieser Wendung nimmt die Vorschrift auf die vorangehende Vorschrift des Art. 83 (ex Art. 79) DSGVO Bezug und klammert damit die Verhängung von Geldbußen aus dem Sanktionsbegriff des Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO aus. Damit verbindet sich zugleich eine *Sperrwirkung*, die es dem mitgliedstaatlichen Gesetzgeber verbietet, Geldbußen zu implementieren. Er kann lediglich auf Grundlage von Art. 83 Abs. 7 (ex Art. 79 Abs. 3b) DSGVO Geldbußen vorsehen, die Behörden und öffentliche Stellen adressieren. Auf Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO darf er hingegen grundsätzlich nicht zurückgrei-

[413] Hervorhebung durch die Verfasser.
[414] Der Wortlaut der Trilog-Fassung (Art. 79b Abs. 1 DSGVO) enthielt die Vokabel „andere" noch nicht. Erst die abschließende Fassung sieht diese Klarstellung vor.

fen, etwa um (zusätzliche) Tatbestände zu schaffen, welche die Verhängung einer Geldbuße gegenüber Privatrechtssubjekten erlauben.[415]
Für das Sanktionsregime der Datenschutz-Grundverordnung insgesamt bedeutet dies, dass Geldbußen zwar grundsätzlich – entsprechend der systematischen Stellung des Art. 83 (ex Art. 79) DSGVO in Kapitel VIII – Sanktionen sind, aber nicht dem Anwendungsbereich des Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO unterfallen. Auf diese Weise gerät Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO zu einer Art Auffangtatbestand („insbesondere für Verstöße, die keiner Geldbuße gemäß Artikel 83 (ex Artikel 79) unterliegen"). Er will insbesondere diejenigen Fälle einer Ahndung zugänglich machen, in denen nicht bereits eine Geldbuße verhängt ist. Damit eröffnet die Datenschutz-Grundverordnung auch die Möglichkeit für ein gestuftes Sanktionsregime, das in Abhängigkeit vom konkreten Verstoß eine Kaskade von Sanktionen vorsieht: Verwarnung, Geldbuße, Sanktion (vgl. EG 148 S. 1-3 i. V. m. Art. 84 Abs. 1 DSGVO [ex EG 118b S. 1-3 i. V. m. Art. 79b Abs. 1 DSGVO]). Die auf Grundlage von Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO möglicherweise implementierten strafrechtlichen Sanktionen bilden mit Blick auf die Belastung des Sanktionsadressaten die Spitze des verordnungsrechtlichen Sanktionsregimes.

ee) Fazit

Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO zeigt sich – gerade auch im Zusammenspiel mit EG 152 (ex EG 120a) DSGVO – offen für verschiedene Sanktionsarten. Mit Blick auf die Erwägungsgründe bzw. aufgrund ihres Schweigens umfasst die Vorschrift jedoch wohl nur strafrechtliche[416] und verwaltungsrechtliche Sanktionen (unter Ausschluss der in Art. 83 [ex Art. 79] DSGVO geregelten Geldbußen) – keine zivilrechtlichen Sanktionen. Dies gilt umso mehr, als nach dem Willen des Unionsgesetzgebers auch die Einziehung der durch Verstöße gegen die Verordnung erzielten Gewinne

[415] Zu den Bereichen, in denen eine Öffnungsklausel den nationalen Gesetzgebern einen Regelungsspielraum belässt, sogleich auf S. 282 f.
[416] Siehe auch *Ashkar*, DuD 2015, 796 (799).

durch strafrechtliche Sanktionen abgedeckt werden soll (EG 149 S. 2 [ex EG 119 S. 2] DSGVO).

Gleichwohl ist der in der Vorschrift enthaltene Sanktionsbegriff nicht alleine auf strafrechtliche Sanktionen verengt. Der mitgliedstaatliche Gesetzgeber kann also auf Grundlage von Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO folglich auch andere verwaltungsrechtliche Sanktionen erlassen.

Die Bußgeldtatbestände des § 43 BDSG kann der Bund daher nicht mehr aufrechterhalten. Denkbar ist eine Sanktionierung mit eigenen Bußgeldtatbeständen allenfalls dort, wo die Mitgliedstaaten von ihrem eigenen Regelungsspielraum Gebrauch machen, den die Datenschutz-Grundverordnung ihnen einräumt.

Für den Bereich *strafrechtlicher Sanktionen*, welche die Mitgliedstaaten auf der Grundlage der Verordnung vorsehen, gestattet die Datenschutz-Grundverordnung dies in ihren Erwägungsgründen ausdrücklich (EG 149 S. 1 [ex EG 119 S. 1] DSGVO: „auch für Verstöße gegen auf der Grundlage und in den Grenzen dieser Verordnung erlassene nationale Vorschriften“). Die bewusste Begrenzung auf Strafen legt einen Gegenschluss nahe: Den Mitgliedstaaten fehlt dann ein Regelungsspielraum. Allerdings kann das eine Sanktionslücke erzeugen: Die Mitgliedstaaten dürfen Rechtspflichten begründen, die aber im Falle eines Verstoßes mangels Sanktionsbefugnis weitgehend folgenlos bleiben. So weit will die Datenschutz-Grundverordnung auch nicht gehen. In EG 152 (ex EG 120a) DSGVO macht sie deutlich, dass die Mitgliedstaaten auch dort eine verwaltungsrechtliche Sanktion vorsehen dürfen und sollten, soweit die Verordnung die Sanktionen nicht harmonisiert hat. Eine Harmonisierung hat die Datenschutz-Grundverordnung nur insoweit vorgenommen, als sie den Mitgliedstaaten nicht eigene inhaltliche Regelungsspielräume zugesteht. Die Geldbuße ist ein Unterfall der verwaltungsrechtlichen Sanktion im Sinne der Verordnung. Das streitet dafür, dass die Mitgliedstaaten auch in den Bereichen Bußgeldtatbestände schaffen dürfen, in denen sie von mitgliedstaatlichen Regelungsspielräumen Gebrauch machen, welche ein Sanktionsbedürfnis auslösen, das nicht bereits Art. 83 (ex Art. 79) DSGVO erfasst (vgl. auch EG 152 i. V. m. EG 150 S. 1 DSGVO).

c. Inhalt und Reichweite der Öffnungsklausel

aa) Mitgliedstaatliche Gestaltungsfreiheit hinsichtlich des „Wie“

Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO eröffnet den Mitgliedstaaten grundsätzlich einen weiten Spielraum hinsichtlich der Ausgestaltung und des Umfangs ihrer Sanktionsmaßnahmen („Wie“). Insbesondere obliegt es dem mitgliedstaatlichen Gesetzgeber zu entscheiden, welche Art von Sanktionen – strafrechtliche oder verwaltungsrechtliche (unter Ausschluss der Geldbuße) – er vorsieht (siehe auch EG 152 [ex EG 120a] S. 2 DSGVO). Das gilt allerdings nicht für das „Ob“ der Sanktionierung: Die Mitgliedstaaten müssen Verstöße gegen die Verordnung in geeigneter Weise sanktionieren – und damit im Grundsatz jeglichen Verstoß gegen Vorschriften der Verordnung. Anderenfalls besteht die Gefahr, dass die Regelungen der Verordnung zu einem „Papiertiger“ degenerieren, gegen dessen Regeln Verantwortliche ahndungslos verstoßen können.
Die den nationalen Gesetzgeber leitende Zielvorgabe ist vor allem die effektive Durchsetzung des unionalen Datenschutzrechts. Es genügt daher nicht, dass die Tatbestände überhaupt bestehen. Die Sanktionen müssen auch wirksam, verhältnismäßig und abschreckend sein (Art. 84 Abs. 1 S. 2 [ex Art. 79b Abs. 1 S. 2] DSGVO). Insbesondere darf der Mitgliedstaat es nicht dabei bewenden lassen, Sanktionstatbestände zu erlassen. Er muss auch die zur Durchsetzung erforderlichen Maßnahmen treffen, wobei Letzteres den praktischen Verwaltungsvollzug adressiert und damit nicht notwendig normativen Regelungsbedarf auslöst.

bb) Allgemeine Konkretisierungsbefugnis

Ergänzend kann der nationale Gesetzeber das verordnungsrechtliche Sanktionsregime insgesamt konkretisieren, soweit die Verordnung das nicht abschließend in harmonisierender Weise getan hat, sondern Regelungslücken offen lässt. Denn Art. 83 und 84 (ex Art. 79 und Art. 79b) DSGVO enthalten Regelungen, die an einigen Stellen nicht hinreichend detailliert in die Tiefe reichen, um ein hinreichendes Sanktionsregime auszugestalten. So mangelt es beispielsweise an einer verordnungsrechtlichen Norm zur Verjährung. Es ist rechtspolitisch sachgerecht, wenn der nationale Gesetzgeber die Regelungslücke schließt. Allerdings ist er dazu nicht ohne Weiteres befugt. Er ist insoweit

auf eine Öffnungsklausel angewiesen. Für Sanktionen jenseits von Geldbußen hält Art. 84 Abs. 1 diese selbst vor.[417] Für den Bereich der Geldbußen verbleibt dem Gesetzgeber lediglich der Regelungsauftrag des Art. 83 Abs. 7 und Abs. 8 DSGVO. Für Geldbußen gegen Behörden und öffentliche Stellen verleiht Art. 83 Abs. 7 DSGVO den Mitgliedstaaten eine Regelungsbefugnis; sie schließt auch die Regelung von Verjährungsfristen ein. Für andere Adressaten von Geldbußen verbleibt allenfalls die Befugnis zur Regelung von „angemessenen Verfahrensgarantien… einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren". Verjährungsregeln sind grundsätzlich Teil des materiellen Sanktionsrechts, nicht des Verfahrensrechts; allerdings wirken sie sich unmittelbar verfahrensrechtlich aus. Es bedarf angesichts des Doppelcharakters von Verjährungsregeln einer genaueren Klärung, ob Art. 83 Abs. 8 DSGVO diesen mitgliedstaatlichen Regelungsspielraum noch einschließt. Anderenfalls ist die Union zur Schließung der Regelungslücke aufgerufen. Art. 70 Abs. 1 lit. k DSGVO weist dem Ausschuss die Aufgabe zu, Leitlinien für die Aufsichtsbehörden für die Festsetzung von Geldbußen gemäß Art. 83 DSGVO zu entwerfen. Leitlinien implizieren keine Regelungssubstrate, die einer normativen Entscheidung des EU-Gesetzgebers bedürfen. Verjährungsregeln definieren die Verfolgbarkeit begangenen Unrechts und bedürfen daher einer normativen Verankerung jenseits von Leitlinien.

d. Vergleich zur Datenschutzrichtlinie

Die Datenschutzrichtlinie verlangte in Art. 24 von den Mitgliedstaaten, Sanktionen im nationalen Recht vorzusehen, um die Einhaltung des Datenschutzrechts sicherzustellen. Zu der Frage, welche Datenschutzverstöße von den Mitgliedstaaten zu sanktionieren sind und welcher Sanktionsformen sie sich bedienen können, enthielt die Richtlinie keine Aussage.[418]

---

[417] Eine äußere Grenze, die der Gesetzgeber zu beachten hat, wenn er konkretisierende Detailregelungen erlässt, ergibt sich aus Art. 84 Abs. 1 S. 2 (ex Art. 79b Abs. 1 S. 2) DSGVO, wonach die „Sanktionen […] wirksam, verhältnismäßig und abschreckend sein [müssen]".
[418] Vgl. *Ehmann* (Fn. 406), § 43, Rn. 4 ff.

e. Bisherige Ausgestaltung im nationalen Recht

Strafrechtliche Sanktionen als Durchsetzungsinstrument für das materielle Datenschutzrecht sind dem nationalen Recht nicht fremd. Das nationale Recht sieht sie gegenwärtig sowohl im BDSG (§ 44 BDSG) als auch im bereichsspezifischen Fachrecht vor. Derartige Strafvorschriften mit Bezug zum Datenschutzrecht sind insbesondere: § 148 TKG; § 19 TPG; § 25 GenDG; § 63b SGB II; § 307b SGB V; § 85a SGB X; § 42 AZRG. Aber auch das StGB hält entsprechende Normen bereit: z. B. §§ 202a ff.[419]; 238 und 353b.
Zudem kennen auch die Landesdatenschutzgesetze Straftatbestände, die datenschutzrechtliche Verstöße sanktionieren wollen.[420] Der Mitgliedstaat muss überdies prüfen, welche neuen Tatbestände der Datenschutz-Grundverordnung das bisherige Recht nicht sanktioniert und damit dem Gebot des Art. 84 (ex Art. 79b) DSGVO noch nicht gerecht wird. Denn die Datenschutz-Grundverordnung verlangt dem Mitgliedstaat eine lückenlose Sanktionskette ab. Gerade im Hinblick auf das der Verordnung zugrunde liegende abgestufte Sanktionsregime darf der nationale Gesetzgeber jedoch nur bei solchen Verstößen strafrechtliche Sanktionen vorsehen, bei denen dies nicht unverhältnismäßig erscheint. Denn strafrechtliche Sanktionen bilden das schärfste Schwert, welches das staatliche Handlungsinstrumentarium bereithält. Neben strafrechtlichen Sanktionen kommen auch Betätigungssperren, Sperrzeiten und andere Maßnahmen in Betracht.

44. Art. 85 (ex Art. 80): Verarbeitung und Freiheit der Meinungsäußerung und Informationsfreiheit

Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO enthält eine Öffnungsklausel hinsichtlich der Verarbeitung personenbezogener Daten u. a. zu journalistischen Zwecken. Sie zielt darauf ab, die Konfliktlage zwischen der Meinungs- und Informationsfreiheit sowie dem Recht auf informationelle Selbstbestimmung in Einklang zu bringen. Es handelt sich um eine Sonderregelung zum Schutz

[419] Zum Verhältnis dieser Normen zu § 44 BDSG siehe *Gola/Klug/Körffer* (Fn. 303), § 44, Rn. 2; *Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl., 2015, § 44, Rn. 2.
[420] Eine synoptische Darstellung findet sich etwa bei *Gola/Klug/Körffer* (Fn. 303), § 44, Rn. 9.

der Kommunikationsfreiheit.[421] Sie bringt eine wichtige unionsrechtliche Grundrechtswertung aus: Dem Recht auf freie Meinungsäußerung ist in einer demokratischen Gesellschaft hinreichend Rechnung zu tragen (vgl. EG 153 S. 7 [ex EG 121 S. 6] DSGVO). Zu diesem Zweck will der Unionsgesetzgeber Begriffen wie Journalismus eine weite Auslegung unterlegen.
Prima facie enthält auch Art. 85 Abs. 1 (ex Art. 80 Abs. 1) DSGVO eine entsprechende Öffnungsklausel. Bei genauerem Hinsehen zeigt sich jedoch, dass die Norm alleine einen Anpassungsauftrag für das mitgliedstaatliche Recht enthält, der inhaltlich das Niveau des einzuhaltenden Persönlichkeitsschutzes ohne Abweichungsmöglichkeit vorgibt.

a. Art. 85 Abs. 1 (ex Art. 80 Abs. 1)

aa) Keine echte Öffnungsklausel, sondern Anpassungsauftrag

Art. 85 Abs. 1 (ex Art. 80 Abs. 1) DSGVO entpuppt sich als Querschnittsklausel und Anpassungsauftrag. Zwar scheint der Wortlaut der Norm ein Verständnis als Öffnungsklausel nahe zu legen. Der Wortlaut der Norm insinuiert, dass Art. 85 Abs. 1 DSGVO es den Mitgliedstaaten anheimstellt, in allen Einzelfällen die Abwägung zwischen dem Datenschutz und der Meinungs- sowie Informationsfreiheit vorzunehmen („die Mitgliedstaaten bringen durch Rechtsvorschriften das Recht auf den Schutz personenbezogener Daten gemäß dieser Verordnung mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit […] in Einklang“. Die Aufgabe und Gestaltungsfreiheit, den Konflikt zwischen dem Recht auf informationelle Selbstbestimmung sowie der Meinungs- und Informationsfreiheit aufzulösen, liegt bei diesem Verständnis in den Händen der Mitgliedstaaten – und gewährt ihnen erhebliche regulatorische Gestaltungsfreiheit. Wie sie die kollidierenden Güter in ihrem Verhältnis zueinander gewichten, weist die DSGVO dann der Kompetenz der Mitgliedstaaten zu. Kollidiert der Persönlichkeitsschutz mit dem Rechtsgut der Meinungsfreiheit, dürfen die Mitgliedstaaten grundsätzlich auch von den Regelungen zum Schutz personenbezogener Daten abweichen, welche die Datenschutz-Grundverordnung vorsieht. Bedeutung hat dies vor allem im Hinblick auf die Verarbeitung allgemein zugänglicher Daten (§ 28

[421] Vgl. *Härting*, ITRB 2016, 36 (39).

Abs. 1 Satz 1 Nr. 3 BDSG, § 29 Abs. 1 Satz 1 Nr. 2 BDSG, § 30a Abs. 1 Satz 1 Nr. 2 BDSG[422]). Sie sind Ausdruck der Konfliktlage zwischen Persönlichkeitsschutz und Kommunikationsfreiheit. Zwar tritt unterdessen Art. 6 DSGVO grundsätzlich an die Stelle dieser Verarbeitungsgrundlagen. Er lässt den Mitgliedstaaten insbesondere für nicht-öffentliche Stellen kaum nationalstaatlichen Regelungsspielraum. Das ergibt sich im Umkehrschluss aus Art. 6 Abs. 2 und 3 (ex Art. 6 Abs. 2a und 3) DSGVO. Art. 85 Abs. 1 (ex Art. 80 Abs. 1) DSGVO lässt sich – jedenfalls bei weiter Deutung – speziell für den Konflikt zwischen der grundrechtlich geschützten Informationsfreiheit und dem Persönlichkeitsschutz aber als spezialgesetzliche Öffnungsklausel im Verhältnis zu Art. 6 DSGVO verstehen.

Gleichwohl machen die innere Systematik der Vorschrift, der Regelungszweck der DSGVO sowie der EG 153 DSGVO deutlich:[423] Alleine Art. 85 Abs. 2 DSGVO lässt mitgliedstaatliche Ausnahmen von Regelungen der Verordnung für spezifische, insbesondere journalistische Zwecke zu — für alle anderen Verarbeitungszwecke und in allen anderen Bereichen enthält Art. 85 Abs. 1 DSGVO keine Öffnungsklausel. Dafür streitet nicht nur der Umkehrschluss aus Art. 85 Abs. 1 DSGVO, sondern dies entspricht auch dem Regelungszweck der DSGVO. Ließe Abs. 1 umfassende eigene Regelungen der Mitgliedstaaten im Bereich der Abwägung zwischen dem Datenschutz und der Meinungs- sowie Informationsfreiheit zu, wäre das fein ausziselliert Regelungssystem des Art. 6 Abs. 1 – 3 DSGVO obsolet. Denn es ließe sich leicht unterwandern. Die DSGVO legt das Schutzniveau für personenbezogene Daten selbst abschließend fest. Art. 85 Abs. 1 DSGVO gibt den Mitgliedstaaten lediglich auf, ihre bestehenden „Vorschriften über die freie Meinungsäußerung und die Informationsfreiheit“ an diese Vorgaben anzupassen.[424] So

[422] Zur Abgrenzung zwischen § 28 und § 30a BDSG siehe bspw. *Ehmann*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 30a, Rdnr. 33 ff.; *Munz*, in: Taeger/Gabel (Hrsg.), BDSG, 2. Aufl., 2013, § 30a BDSG, Rdnr. 5 ff.

[423] Dazu und zum Folgenden auch *Martini*, VerwArch. 107 (2016), 307 (350).

[424] So ist auch die Gesetzgebungsgeschichte zu deuten: In der Fassung der Kommission war der heutige Abs. 1 noch nicht enthalten, sondern alleine die heutigen Abs. 2 und 3. Das Parlament änderte dies grundlegend dahin gehend, dass Abweichungen oder Ausnahmen von der DSGVO nicht alleine für bestimmte Verarbeitungszwecke, sondern „wann immer dies notwendig ist“ zulässig sein sollen (wobei als Maßstab für die Abwägung die GrCh festgesetzt wurde). Der Rat (und so beibehalten im Trilog) führten dann die heute gültige Fassung der Abs. 1 und 2 ein.

bringt es auch EG 153 S. 1 DSGVO zum Ausdruck. Entsprechend bezieht auch EG 153 S. 2 DSGVO die Zulässigkeit von „Abweichungen und Ausnahmen von bestimmten Vorschriften dieser Verordnung“ alleine auf die besonderen Verarbeitungszwecke nach Abs. 2. Nicht zuletzt spricht auch die Systematik der Vorschrift für dieses Verständnis. Es wäre nicht recht erklärlich, warum Art. 85 Abs. 3 DSGVO den Mitgliedstaaten eine Meldepflicht nur für Ausnahmen nach Abs. 2, nicht aber für (die inhaltlich weiter greifenden) Regelungen nach Abs. 1 auferlegt.

bb) Inhalt des Anpassungsauftrages

Art. 85 Abs. 1 (ex Art. 80 Abs. 1) DSGVO gibt den Mitgliedstaaten einen unionsrechtlichen Anpassungsauftrag mit auf den Weg: Er eröffnet ihnen – außerhalb des Abs. 2 – jedoch keine regulatorische Gestaltungsfreiheit. Wie die kollidierenden Güter im Verhältnis zueinander zu gewichten sind, legt die DSGVO grundsätzlich selbst fest, so etwa für das Recht auf Vergessenwerden des Art. 17 DSGVO. Im Art. 17 Abs. 3 lit. a Datenschutz nimmt die DSGVO selbst auf den Konflikt zwischen dem informationellen Selbstbestimmungsrecht sowie der Informationsfreiheit Bezug: Das Recht auf Löschung besteht nicht, soweit die Verarbeitung zur Ausübung der Informationsfreiheit erforderlich ist. Dies schließt grundsätzlich auch eine Konkretisierung aus. Diese wären zwar wünschenswert, um die Vollzugfähigkeit der Norm in der diffizilen Konfliktlage grundrechtlicher Positionen zu steigern. Gleichzeitig würde eine entsprechende Konkretisierung durch die Mitgliedstaaten das Harmonisierungsziel der Verordnung konterkarieren. Art. 85 Abs. 1 DSGVO lässt sich damit auch nicht als spezialgesetzliche Konkretisierungsermächtigung des Art. 17 Abs. 3 lit. a DSGVO verstehen, die den Mitgliedstaaten Regelungsmacht zugesteht. Er zielt alleine auf eine Anpassung des bestehenden mitgliedstaatlichen Rechts an die Vorgaben der Verordnung. Gleichzeitig weist er damit auch über die Verordnung hinaus. Denn in ihrem Anwendungsbereich greifen nach Art. 51 Abs. 1 S. 1 Hs. 2 GrCh die Grundrechte der GrCh.

Ausnahmen und Abweichungen waren nunmehr nach Abs. 2 (ausdrücklich) nur mehr für bestimmte Verarbeitungszwecke zulässig. Dies ist als Abkehr von der weiten, vom Parlament vorgeschlagenen Öffnungsklausel zu verstehen.

Der Grundrechtsschutz in diesem Bereich wird damit unionalisiert – die Unionsgrundrechte überspielen die nationalen Grundrechte.[425] Ein Rekurs auf nationale Grundrechtsabwägungen scheidet (weitestgehend) aus. Der Datenschutz und der Meinungs- sowie Informationsfreiheit müssen also so in Einklang gebracht werden, wie dies nach den Vorgaben der GrCh – und damit nach Ansicht des EuGH – zu erfolgen hat.
Ausnahmen gelten allenfalls da, wo den Mitgliedstaaten ein Regelungsspielraum im Rahmen einer expliziten Öffnungsklausel verbleibt. Doch auch dort werden sie wohl grds. in „Durchführung" des Unionsrechts, hier der DSGVO, tätig.[426] Der EuGH scheint dies jedenfalls so zu sehen.[427] Gleichwohl können die Mitgliedstaaten in diesem Bereich auf eine „margin of appreciation" zurückgreifen, die ihnen eigenen Abwägungsspielraum belässt.[428]
Das BVerfG stellt dem wohl einen etwas weiteren Anwendungsspielraum der nationalen Grundrechte. Wo der deutsche Gesetzgeber bei der Umsetzung von Unionsrecht Gestaltungsfreiheit hat, das heißt durch das Unionsrecht nicht determiniert ist, finden nach seiner Wahrnehmung die Grundrechte des Grundgesetzes Anwendung.[429]

cc) Vergleich zur Vorgängerregelung in der Datenschutzrichtlinie 95/46/EG

Eine allgemeine Regelung, die mit Art. 85 Abs. 1 (ex Art. 80 Abs. 1) DSGVO vergleichbar ist, findet sich in der Datenschutzrichtlinie nicht. Art. 9 DSRL gestattet es den Mitgliedstaaten, punktuell Ausnahmen von der DSRL vorzusehen, um im Bereich der Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, die

[425] Vgl. zum Verhältnis zwischen Unionsgrundrechten und nationalen Grundrechten im Bereich des Datenschutzrechts: *Sobotta*, in: Grabitz/Hilf (Hrsg.), EU-Recht, 57. Erg.-Lfg., 2015, Art. 16 AEUV, Rn. 14 f.
[426] Vgl. *Borowsky*, in: Meyer (Hrsg.), GrCh, Online-Ausg, 2014, Art. 51, Rn. 27.
[427] Vgl. EuGH zu den (weitreichenden) Handlungsspielräumen nach der DSRL: „Von diesen Möglichkeiten muss aber in der in Richtlinie 95/46/EG vorgesehenen Art und Weise und im Einklang mit ihrem Ziel Gebrauch gemacht werden, ein Gleichgewicht zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre zu wahren.", EuGH, Urteil vom 6. 11. 2003 - C-101/01 – Lindqvist, Rn. 97.
[428] So u. a in EuGH, Urt. v. 14.10.2004 - C-36/02– Omega, Rn. 31
[429] BVerfGE 125, 260 (306 f.).

Meinungsfreiheit mit dem informationellen Selbstbestimmungsrecht in Einklang zu bringen. Diese Ermächtigung entspricht aber eher dem Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO als dem Art. 85 Abs. 1 (ex Art. 80 Abs. 1) DSGVO.
Auch der DSRL liegt das Verständnis zugrunde, den Konflikt zwischen dem Datenschutz und der Meinungs- sowie Informationsfreiheit im Grundsatz selbst aufzulösen. Denn im Umkehrschluss zu Art. 9 DSRL dürfen die Mitgliedstaaten bei anderen Verarbeitungszwecken ebenfalls nicht von den unionsrechtlichen Regelungen abweichen. EG 17 DSRL hält entsprechend fest, dass alleine in dem von Art. 9 DSRL erfassten Bereich „die Grundsätze dieser Richtlinie […] eingeschränkt Anwendung“ finden. Damit traf die Mitgliedstaaten in Bereichen, die Art. 9 nicht erfasst, nach Art. 288 Abs. 3 AEUV, Art. 4 Abs. 3 EUV die Pflicht, bestehendes Recht an die Wertungen der DSRL anzupassen. Das entsprach dem grundsätzlichen Vollharmonisierungsanspruch der DSRL.[430]

dd) Bisherige Ausgestaltung im nationalen Recht und Bereinigungsbedarf

Das nationale Recht enthält keine allgemeine übergreifende Abwägungsklausel, die in ihrer Diktion als Generalklausel ausdrücklich dem Gebot des Art. 85 (ex Art. 80) DSGVO entspricht. Das heißt aber nicht, dass die deutsche Rechtsordnung den Anforderungen des Art. 85 (ex Art. 80) DSGVO nicht genügt.

i. Verfassungsrechtliche Ebene

Die Abwägung zwischen dem Persönlichkeitsschutz sowie der Meinungs- und Informationsfreiheit ist ein fester Bestandteil aller Ebenen der deutschen Rechtsordnung – beginnend vom Verfassungsrecht bis hin zu den einzelnen Verästelungen des einfachen Rechts. Entsprechend dem Abstraktionsgrad der Kollisionslage enthalten sowohl Art. 5 GG – mit dem Hinweis auf die Schranken der allgemeinen Gesetze – als auch Art. 2 Abs. 1 GG – mit seinem Hinweis auf die Schranke der verfassungsmäßigen Ordnung – abstrakte Ab-

[430] EuGH (Dritte Kammer), Urt. v. 24. 11. 2011 − C-468, 469/10 –, EuZW 2012, 37, Rn. 25 ff.

wägungsregeln, die den Konflikt der kollidierenden Rechtsgüter einer Lösung zuzuführen trachten. Auch für sie gilt: Die kollidierenden Rechtsgüter dürfen nicht einseitig auf Kosten des jeweils anderen zur Entfaltung gebracht werden. Beschränkungen des jeweils einen unterliegen dem Gebot der Verhältnismäßigkeit und praktischer Konkordanz, also dem Gebot, die kollidierenden Rechtsgüter schonend gegeneinander auszugleichen und zur optimalen Entfaltung zu bringen (ähnlich auf der Ebene der unionsrechtlichen Grundrechte: Art. 52 GrCh).

ii. Einfachgesetzliche Ebene

Einfachgesetzlich bestehen jeweils spezielle Normierungen, die dem Bedürfnis einer Anpassung kommunikationsrechtlicher Regelungen an die Bedürfnisse des Persönlichkeitsschutzes normativen Ausdruck verleihen. Im Zivilrecht fangen die allgemeinen Tatbestände des § 823 Abs. 1 und des § 1004 Abs. 1 S. 1 BGB Interessen und Positionen jeweils generalklauselartig auf. Spezifischere Bestimmungen sind zum Teil regelungstechnisch auch schwer vorstellbar und keineswegs durch die Vorgaben der DSGVO („durch Rechtsvorschrift“) erzwungen. Öffentlich-rechtliche Vorschriften suchen den Anspruch auf Zugang zu amtlichen Informationen an zahlreichen Stellen in Einklang mit dem Persönlichkeitsschutz in Einklang zu bringen, so etwa § 5 IFG Bund, § 5 Abs. 1 BWLIFG; § 6 Abs. 1 BlnIFG; § 5 Abs. 1 S. 1 Nr. 1 BbgAIG; § 5 Abs. 1 BremIFG; § 4 Abs. 1 S. 1 HmbTG; § 7 IFG M-V; § 9 Abs. 1 IFG NRW; § 16 Abs. 1 S. 1 Nr. 2 Rh-PfLTranspG; § 1 S. 1 SaarlIFG i. V. m. § 5 Abs. 1 IFG; § 5 Abs. 1 IZG LSA; § 10 S. 1 Nr. 1 IZG-SH; § 9 Abs. 1 ThürIFG. Sie sind Ausfluss des Anpassungsbedürfnisses, das sich aus dem Zusammentreffen kollidierender Rechtspositionen ergibt. Fortgeltende oder in Ausführung der DSGVO erlassene einfachgesetzliche Regelungen sind daraufhin zu prüfen, ob sie dem unionsrechtlichen Anpassungsgebot (in den Grenzen der den nationalen Grundrechten eingeräumten Spielraums) gerecht werden.

iii. Schlussfolgerungen

Die Vorgaben des Art. 85 (ex Art. 80) DSGVO lösen keinen akuten Bereinigungsbedarf im nationalen Recht aus. Soweit ein Spielraum für eigene Rege-

lungen und Abwägungsentscheidungen verbleibt, bewältigt das nationale Recht die Kollisionslage bereits im Rahmen seiner bestehenden Grundrechtserwägungen in Übereinstimmung mit dem Unionsrecht.

b. Art. 85 Abs. 2 (ex Art. 80 Abs. 2)

aa) Inhalt der Öffnungsklausel

Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO bricht den Regelungsauftrag des Art. 85 Abs. 1 (ex Art. 80 Abs. 1) DSGVO auf einer konkreteren Ebene auf diejenigen Gruppen herunter, bei denen typischerweise eine Kollisionslage ihrer meinungsbildenden Tätigkeit mit dem Recht auf informationelle Selbstbestimmung besteht. Er privilegiert die Verarbeitung personenbezogener Daten zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken.

Die Verordnung verlangt von den Mitgliedstaaten, dass sie im Hinblick auf die genannten Verarbeitungen Ausnahmen von den Vorgaben der Kapitel II – VII der Datenschutz-Grundverordnung vorsehen, soweit dies zum Ausgleich des Rechts auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit erforderlich ist (EG 153 S. 4 [ex EG 121 S. 4] DSGVO verwendet auch den Begriff „notwendig“). EG 153 S. 3 (ex EG 121 S. 3) DSGVO fordert solche Ausnahmen insbesondere für den audiovisuellen Bereich sowie in Nachrichten- und Pressearchiven. Dabei dürfen die Mitgliedstaaten insbesondere Ausnahmen von den allgemeinen Grundsätzen, den Rechten der betroffenen Personen, den Regeln über Auftragsverarbeitung und Verantwortlichkeit, die Übermittlung von Daten an Drittländer oder an internationale Organisationen, die unabhängigen Aufsichtsbehörden, die Zusammenarbeit und die Kohärenz vorsehen.

Für den Fall, dass die Mitgliedstaaten von ihrer Regelungsbefugnis in unterschiedlicher Weise Gebrauch machen, kommt das Recht des Mitgliedstaates zur Anwendung, welchem der Verantwortliche unterliegt (EG 153 S. 5 [ex EG 121 S. 5] DSGVO).

bb) Einordnung in das System der Öffnungsklauseln

Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO eröffnet den Mitgliedstaaten keinen Spielraum hinsichtlich des grundsätzlichen „Ob“, sondern nur hinsicht-

lich des konkreten „Wie“. Es handelt sich um eine obligatorische Öffnungsklausel. Die Umsetzungspflicht besteht allerdings nur unter der Voraussetzung, dass die Befreiung von den datenschutzrechtlichen Regelungen erforderlich ist, um den Schutz personenbezogener Daten mit der Meinungsäußerungs- sowie Informationsfreiheit in Einklang zu bringen. Damit bleibt den Mitgliedstaaten ein (ungeschrieben) weiter Einschätzungsspielraum. Gleichwohl deutet die Datenschutz-Grundverordnung bereits selbst an, dass die Mitgliedstaaten jedenfalls im Sinne eines Untermaßverbotes zum Schutz u. a. des Journalismus tätig werden müssen (so auch EG 153 S. 2, 4 [ex EG 121 S. 2, 4] DSGVO, der davon spricht, dass Ausnahmen gelten „sollten“ bzw. die Mitgliedstaaten tätig werden „sollten“).

cc) Vergleich zur Vorgängerregelung in der Datenschutzrichtlinie

Die DSRL enthielt eine ähnliche Vorgabe wie Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO: Ausnahmen von der Richtlinie waren nach ihrem Art. 9 vorzusehen, sofern die Verarbeitung zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt. Datenverarbeitung zu wissenschaftlichen Zwecken erfasst die Richtlinie demgegenüber nicht. Daneben beschränkt sich die Richtlinie hinsichtlich der Ausnahmeverpflichtungen auf die Kapitel IV (Information der betroffenen Person) und VI (Ausnahmen und Einschränkungen). Die Datenschutz-Grundverordnung nimmt hingegen eine größere Zahl an Regelungsbereichen aus.
Wie die Datenschutz-Grundverordnung knüpft auch die RL die Öffnungsklausel an eine Bedingung: Es muss die *Notwendigkeit* bestehen, das Recht auf Privatsphäre mit den Vorschriften zur Meinungsäußerungsfreiheit in Einklang zu bringen. Auch hier geht die Datenschutz-Grundverordnung weiter als die Richtlinie 95/46/EG, denn das Recht auf Privatsphäre ist in seinem Anwendungsbereich enger zu fassen als der generalisierte Schutz personenbezogener Daten. Daneben bezieht die Verordnung auch die Informationsfreiheit mit ein.

dd) Bisherige Ausgestaltung im nationalen Recht

Die Regelung des Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO hat Anknüpfungspunkte im nationalen Recht. So nimmt § 41 BDSG mit seinem Medien-

privileg Unternehmen sowie Hilfsunternehmen *der Presse* aus dem Anwendungsbereich des BDSG grundsätzlich heraus.[431] Die Regelung ist Ausdruck der verfassungsrechtlichen garantierten freien Presse.[432] Das BDSG gibt den Ländern lediglich einen Regelungsauftrag mit auf den Weg, einen Minimaltatbestand[433] an Haftungsregeln vorzusehen. Beispielhaft für solch eine Umsetzung steht § 12 Abs. 1 - 2 RhPfLMG. Gegenüber der Regelung in der Datenschutz-Grundverordnung stellt sich die bisherige nationale Umsetzung jedoch als strenger dar: Während die Verordnung es genügen lässt, dass die Verarbeitung die genannten Zwecke als eines von mehreren Zielen verfolgt, muss nach dem deutschen Recht die Datenverarbeitung *ausschließlich* zu eigenen journalistisch-redaktionellen oder literarischen Zwecken erfolgen.[434]
Die Länder[435] haben in ihren Mediengesetzen für ihre Landesrundfunkanstalten unterschiedliche Regelungen getroffen. So klammert § 42 Abs. 1 NDR-StV weitestgehend die Regelungen des HmbDSG für den NDR aus, sofern auch hier Daten zu journalistisch-redaktionellen Zwecken verarbeitet werden. § 31 Abs. 1 BlnDSG verweist für den Sender Freies Berlin auf § 41 Abs. 2 und 3 BDSG. § 12 Abs. 2 RhPfLMG will für Rundfunkveranstalter sowie ihre Hilfsunternehmen nur die Bestimmungen des BDSG im Hinblick auf den Datenschutz durch Technik und Organisation anwenden. Dieser legislative Flickenteppich ist Ausfluss der fehlenden Gesetzgebungskompetenz des Bundes für die Rundfunkanstalten der Länder.
Für die Deutsche Welle enthält § 41 BDSG in seinen Abs. 2 bis 4 Sonderregelungen, die das Medienprivileg verbürgen. Zudem bestellt die Deutsche Welle gemäß § 42 Abs. 1 S. 1 BDSG einen Beauftragten für den Datenschutz, der an die Stelle der oder des BfDI tritt; seine Bestellung und die Amtszeit

---

[431] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 41, Rn. 2. Alternativ ist auch die Rede von einem „publizistischem Vorbehalt", vgl. *Dörr/Schiedermair*, Rundfunk und Datenschutz, 2002, S. 26. Zur Kollision des Medienprivilegs mit Informationsansprüchen des Zivilrechts *Bruns*, Informationsansprüche gegen Medien, 1997, S. 39.
[432] Vgl. *Dörr/Schiedermair* (Fn. 431), S. 26.
[433] Es handelt sich um einen Mindeststandard, *Tinnefeld*, Grundlagen des Datenschutzes, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, S. 188 (193).
[434] Vgl. dazu *Spindler/Nink*, in: Spindler/Schuster (Hrsg.), Recht der elektronischen Medien, 3. Aufl., 2015, § 41 BDSG, Rn 3.
[435] Vor der Gesetzesänderung hat das BDSG auch den Rundfunk als Adressat des Medienprivilegs angesehen, vgl. *Fechner* (Fn. 207), S. 172.

regelt Abs. 1 S. 2; Abs. 1 S. 3 bestimmt die Unvereinbarkeiten. § 42 Abs. 2 BDSG beschreibt die Aufgaben des Datenschutzbeauftragten und seine Unabhängigkeit. Weiter sieht § 42 Abs. 4 S. 1 BDSG eine zweijährliche allgemeine sowie S. 2 eine besondere Berichtspflicht vor. Schließlich wird der Deutschen Welle das Recht übertragen, Regelungen entsprechend der §§ 23-26 BDSG selbst zu treffen (Abs. 5 S. 1). Die Regelungen im BDSG beruhen darauf, dass es sich um eine Rundfunkanstalt des Bundesrechts handelt, sodass den Ländern ausnahmsweise keine Kompetenz zukommt.[436] Unter den Voraussetzungen des § 41 Abs. 2 und 3 BDSG besteht ein Recht auf Speicherung von Gegendarstellungen sowie ein Auskunftsrecht.[437] Damit sind die bisherigen Regelungsansätze im Grundsatz kompatibel mit den Vorgaben der Datenschutz-Grundverordnung.

45. Art. 86 (ex Art. 80a): Zugang zu öffentlichen Dokumenten

a. Inhalt der Öffnungsklausel und Einordnung in das Regelungssystem der DSGVO

Art. 86 (ex Art. 80a) DSGVO erlaubt es den Mitgliedstaaten, die Weitergabe von Daten auf der Grundlage ihrer nationalen Vorschriften zuzulassen oder zu beschränken, um das Recht auf öffentlichen Zugang zu amtlichen Dokumenten mit dem Recht auf informationelle Selbstbestimmung in Einklang zu bringen. Gegenständlich bezieht sich diese nationale Freigabemöglichkeit allerdings nur auf „personenbezogene Daten in amtlichen Dokumenten, die sich im Besitz einer öffentlichen Behörde oder einer öffentlichen Einrichtung oder einer privaten Einrichtung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe befinden“. Die Vorschrift dient damit letztlich dem Ausgleich des öffentlichen Informationsinteresses an amtlichen Informationen mit dem Schutz personenbezogener Daten. Welche Einheiten unter den Begriff der Behörden oder sonstigen öffentlichen Stellen fallen, konturiert EG 154 S. 4 (ex EG 121a S. 4) DSGVO: Gemeint sind damit diejenigen Stellen, welche das Recht des jeweiligen Mitgliedstaates über den Zugang der

[436] Vgl. *Gola/Klug/Körffer* (Fn. 431), § 41, Rn. 13.
[437] *Schaffland/Wiltfang*, Bundesdatenschutzgesetz, 2012, § 41, Rn. 8.

Öffentlichkeit zu Dokumenten erfasst. Den Mitgliedstaaten kommt also insoweit ein Gestaltungsspielraum zu.
EG 154 (ex EG 121a) DSGVO stellt auch klar, dass die Richtlinie 2003/98/EG über die Weiterverwendung von Informationen des öffentlichen Sektors (sog. PSI-RL) die Regelungen der Datenschutzgrundverordnung unberührt lässt. Im Falle einer Kollision zwischen beiden Normgehalten setzt sich die Datenschutz-Grundverordnung durch.
Der ursprüngliche Kommissionsentwurf sah eine dem Art. 86 (ex Art. 80a) DSGVO entsprechende Regelung zunächst nicht vor. Sie fand erst durch die legislative Entschließung des Parlaments Eingang in den Gesetzgebungsprozess der Datenschutzgrundverordnung.

b. Einordnung in das System der Öffnungsklauseln

Art. 86 (ex Art. 80a) DSGVO enthält eine *fakultative* Öffnungsklausel, die den nationalen Gesetzgeber nicht zum Tätigwerden zwingt, sondern es vielmehr ihm selbst überlässt, ob er eine entsprechende gesetzliche Regelung vorsieht. Dies ergibt bereits der explizite Wortlaut der Norm: „können […] gemäß […] dem Recht des Mitgliedstaats […] offengelegt werden“. Die Mitgliedstaaten sollen selbst darüber entscheiden können, wie sie den Konflikt zwischen dem Informationsinteresse der Öffentlichkeit und dem Schutz personenbezogener Daten entschärfen, insbesondere in welchem Umfang sie welchem der beiden schutzwürdigen Positionen den Vorrang einräumen. Insoweit dispensiert die Datenschutz-Grundverordnung von ihren datenschutzrechtlichen Vorgaben und ihrem Schutzniveau.

c. Bisherige Ausgestaltung im nationalen Recht

Das nationale Recht hält bereits gegenwärtig zahlreiche Regelungen bereit, die den Zugriff auf amtliche Informationen gestatten und umgekehrt für den Fall einer Beeinträchtigung personenbezogener Daten beschränken.

aa) Informationsfreiheitsgesetze

Die prominentesten Beispiele einer Kollisionsregelung zwischen der Informationsfreiheit und dem Schutz personenbezogener Daten bilden Sondervorschriften des Informationsfreiheitsgesetze des Bundes und sowie die Informa-

tionsfreiheitsgesetze der Länder, namentlich § 5 IFG; § 6 Abs. 1 BlnIFG; § 5 Abs. 1 Nr. 1 BbgAIG; § 5 Abs. 1 BremIFG; § 4 Abs. 1 S. 1 HmbTG; § 7 IFG M-V; § 9 IFG NRW; § 12 Rh-PfLIFG; § 1 S. 1 SaarlIFG i. V. m. § 5 Abs. 1 IFG; § 5 Abs. 1 IZG LSA; § 10 Abs. 1 Nr. 1 IZG SH; § 9 Abs. 1 ThürIFG.[438]

bb) Sonderregelungen des Informationsrechts

Auch zahlreiche Spezialgesetze eröffnen Bürgern den Zugang zu amtlichen Informationen nur nach Maßgabe einer Abwägung mit den betroffenen schutzwürdigen Interessen Einzelner, etwa das Umweltinformationsgesetz (§ 9 Abs. 1 S. 1 Nr. 1 UIG) oder das Verbraucherinformationsgesetz (§ 3 S. 1 Nr. 2 lit. a, S. 2 VIG). So regelt es auch § 12 Abs. 2 GeoZG i. V. m. § 9 Abs. 1 S. 1 Nr. 1 UIG für Geodaten.[439] Diese Bestimmung beruht auf Art. 13 Abs. 1 S. 2 lit. f INSPIRE-RL. Art. 13 Abs. 3 INSPIRE-RL bestimmt für das Verhältnis der INSPIRE-RL zur DSRL (und damit mittelbar zu dessen Nachfolgerin der Datenschutz-Grundverordnung), dass die datenschutzrechtlichen Anforderungen des speziellen Datenschutzrechts einzuhalten sind.
Das IFG ist darauf bedacht, einen Ausgleich zwischen dem Informationsinteresse anfragender Bürger und dem Schutz personenbezogener Daten von betroffenen Personen herzustellen. Dementsprechend ist der Informationszugang gemäß § 5 IFG nur dann eröffnet, wenn der Betroffene in die Weitergabe seiner personenbezogenen Daten eingewilligt hat oder das Informationsinteresse des Anfragenden das Recht des Betroffenen auf Geheimhaltung seiner personenbezogenen Daten überwiegt. Ähnliche Wertungen enthalten alle anderen Vorschriften des Informationsfreiheitsrechts. Der Gesetzgeber hat von der Regelungsmöglichkeit des Art. 86 (ex Art. 80a) DSGVO mithin bereits Gebrauch gemacht. Eine Regelungsnotwendigkeit besteht nicht.

46. Art. 87 (ex Art. 80b): Verarbeitung der nationalen Kennziffer

Mitgliedstaaten können nationale Identifikationsnummern nach dieser Vorschrift nutzen. Soweit in Deutschland eine derartige Nummer im Rahmen

[438] Dazu bspw. *Martini* (Fn. 215), S. 114.
[439] Siehe bspw. *Martini*, NVwZ-Extra 3/2016, 1 (2).

spezialrechtlicher Regelungen vorgehalten werden soll, wäre dies „unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Personen“ möglich.

47. Art. 88 (ex Art. 82): Arbeitnehmerdatenschutz

Art. 88 (ex Art. 82) DSGVO eröffnet den Mitgliedstaaten letztlich die Möglichkeit, den Arbeitnehmerdatenschutz eigenständig zu regeln. Eine nähere Konditionierung erfolgt hier nicht. EG 155 (ex EG 124) DSGVO stellt zudem klar, dass insoweit auch die Reichweite der Einwilligung im Beschäftigungskontext geregelt werden kann. Die Schranke der Menschenwürde, der Grundrechtsinteressen der Betroffenen und der Transparenz in Art. 88 Abs. 2 (ex Art. 82 Abs. 2) DSGVO ergibt sich ohnehin aus nationalen verfassungsrechtlichen Vorgaben, so dass insoweit keine zusätzliche unionsrechtliche Konditionierung erfolgt. Deutschland ist insoweit also letztlich frei, an der bislang rudimentären Regelung des Arbeitnehmerdatenschutzes in § 32 BDSG festzuhalten oder den in der vergangenen Legislaturperiode unternommenen Versuch eines eigenständigen ausdifferenzierten Arbeitnehmerdatenschutzes wieder aufzugreifen.

48. Art. 89 (ex Art. 83): Statistik/Forschung

Art. 89 Abs. 2 und 3 (ex Art. 83 Abs. 2 und 3) DSGVO erlaubt es den Mitgliedstaaten, zugunsten der privilegierten Verarbeitungszwecke im Bereich Statistik und Forschung Ausnahmen von einzelnen Betroffenenrechten der Art. 15, 16, 18, 21 (ex Art. 15, 16, 17a und 19) DSGVO im Bereich der Forschung und zusätzlich der Art. 19 und 20 (ex Art. 17b und 18) im Bereich der Statistik gesetzlich zu regeln. Allerdings sind die Anforderungen an derartige Ausnahmen sehr hoch: So muss die Wahrnehmung der Betroffenenrechte die Verwirklichung der jeweiligen privilegierten Zwecke „unmöglich machen oder ernsthaft beeinträchtigen“. Zudem müssen die gewählten Ausnahmen sodann „für die Erfüllung dieser Zwecke notwendig“ sein.

49. Art. 90 Abs. 1 (ex Art. 84 Abs. 1): Kompetenzen der Datenschutzaufsichtsbehörden gegenüber Berufsgeheimnisträgern

Mitgliedstaaten dürfen national spezielle Regelungen bezüglich der Kompetenzen der Datenschutzaufsichtsbehörden gegenüber Berufsgeheimnisträgern erlassen. Die Vorschrift trägt dem Konflikt zwischen dem Schutz personenbezogener Daten und der Geheimhaltungspflicht Rechnung, denen berufliche Geheimnisträger nach dem Recht der Mitgliedstaaten (vgl. z. B. § 203 StGB) unterliegen. Die Union nimmt Rücksicht auf die Schutzbedürfnisse, welche das nationale Recht bei der Ausgestaltung berufsrechtlicher Geheimnispflichten, etwa der Ärzte, Notare und Rechtsanwälte, verankert, und gibt den Mitgliedstaaten daher eine vergleichsweise weitgehende Regelungsbefugnis an die Hand. Sie ist allerdings thematisch eng begrenzt: Sie erstreckt sich ausschließlich auf die Befugnisse der Aufsichtsbehörden beim Zugang zu Geschäftsräumen und personenbezogenen Daten, die zur Aufgabenerfüllung notwendig sind (Art. 58 Abs. 1 lit. e und f DSGVO). Art. 90 DSGVO hat Ähnlichkeit mit der Kollisionsregelung des Art. 85 Abs. 1 DSGVO, welche den Konflikt zwischen Informationsfreiheit und dem Persönlichkeitsschutz zum Gegenstand hat. Anders als diese Norm gesteht Art. 90 DSGVO den nationalen Gesetzgebern aber bewusst die Abweichung von Schutzstandards zu, welche sich aus der Datenschutz-Grundverordnung ergeben. Art. 90 Abs. 1 DSGVO etabliert damit eine echte, fakultative Öffnungsklausel. Die Regelungsfreiheit der Mitgliedstaaten findet ihre Grenze jedoch in dem Prinzip der Verhältnismäßigkeit: Den Schutz personenbezogener Daten dürfen sie im Interesse beruflicher bzw. diesen äquivalenter Geheimhaltungspflichten nur zurückstellen, soweit sich dies als erforderlich und angemessen erweist, um die kollidierenden Prinzipien zum schonenden Ausgleich zu bringen. Entsprechend erstreckt sich – wie Abs. 1 S. 2 zur Sicherheit klarstellend betont – die Regelungsfreiheit nur auf solche Verarbeitungsbereiche personenbezogener Daten, für welche die Geheimhaltungspflicht tatsächlich grundsätzlich besteht. Um eine ungebührliche Ausdehnung mitgliedstaatlicher Regelungsbefugnisse unter Berufung auf Art. 90 Abs. 1 DSGVO zulasten des Persönlichkeitsschutzes zu vermeiden und jedenfalls kontrollieren zu können, ordnet Art. 90 Abs. 2 DSGVO eine Notifikationspflicht der Mitgliedstaaten an: Sie müssen bis zum 25.5.2018 die Kommission über diejenigen Vor-

schriften in Kenntnis setzen, welche sie auf der Grundlage des Art. 90 Abs. 1 DSGVO erlassen oder ändern.

50. Art. 91 (ex Art. 85): Besonderes Datenschutzrecht der Kirchen

Das besondere Datenschutzrecht der Kirchen in Deutschland kann zwar grundsätzlich erhalten bleiben; die Kirchen müssen es aber in Einklang mit der Datenschutz-Grundverordnung bringen, Art. 91 Abs. 1 (ex Art. 85 Abs. 1) DSGVO. Sie müssen eine – gegebenenfalls gesonderte – den Anforderungen des Kapitels VI entsprechende unabhängige Aufsichtsbehörde schaffen, Art. 91 Abs. 2 (ex Art. 85 Abs. 2) DSGVO.

V. Änderungsbedarf im BDSG

Die Datenschutz-Grundverordnung hält zwar zahlreiche Öffnungsklauseln vor, die den Mitgliedstaaten Handlungsspielräume für eigenständige, abweichende, ergänzende oder einschränkende Regelungen eröffnen. Das gilt namentlich für die Datenverarbeitung zur Verfolgung eines öffentlichen Interesses, also nach bisheriger deutscher Lesart v. a. die Datenverarbeitung durch öffentliche Stellen.
Gleichwohl ist die Verordnung grundsätzlich auf eine Vollharmonisierung angelegt. Das gilt insbesondere in den Fällen, in denen Datenverarbeitungen keine öffentlichen Interessen verfolgen, also v. a. bei der Datenverarbeitung durch nicht-öffentliche Stellen. Jegliche möglicherweise – gerade noch – zulässige Nutzung von Öffnungsklauseln läuft Gefahr, das Ziel einer unionsweit einheitlichen Regelung zu gefährden, und verkompliziert das ohnehin schon komplexe Datenschutzrecht durch ein Nebeneinander von europäischer Rechtsverordnung und mitgliedstaatlicher Regelung. Der Gesetzgeber ist daher gut beraten, in jedem Einzelfall kritisch zu prüfen, ob eine sichere oder gegebenenfalls sogar mit Restrisiken verbundene Nutzung von Handlungsspielräumen auf nationaler Ebene tatsächlich erfolgen sollte. Das gilt auch für eine womöglich zulässige wiederholende Normierung[440] des Wortlauts der Datenschutz-Grundverordnung. Ein Verweis auf die Verordnung – kombiniert mit ggf. ergänzenden nationalen Vorschriften – kann im Einzelfall sinnvoller sein. Die rechtliche Analyse der Reichweite mitgliedstaatlicher Handlungsspielräume ist daher keineswegs als rechtspolitische Empfehlung ihrer Nutzung zu verstehen.

§§ 1 - 11: Allgemeine und gemeinsame Bestimmungen

§ 1: Zweck und Anwendungsbereich des Gesetzes

In seinem § 1 formuliert das BDSG zentrale Grundaussagen zu seiner Zweckbestimmung des Gesetzes (Abs. 1), seinem räumlichen (Abs. 5) und personellen Anwendungsbereich (Abs. 2) und bestimmt das Verhältnis zu

[440] Zum Wiederholungsverbot siehe S. 6.

anderen Gesetzen (Abs. 3, 4). Damit korrespondieren Art. 1 Abs. 1, 2, Art. 3 Abs. 1, 2 DSGVO als sedes materiae.

a. Abs. 1: Zweck des Gesetzes

Das BDSG zielt auf den Schutz des Einzelnen vor der Beeinträchtigung seines Persönlichkeitsrechts beim Umgang mit seinen personenbezogenen Daten. Obgleich der Begriff »Datenschutz« der Zentralbegriff des Rechtsgebietes ist, ist er irreführend: Der Schutzanspruch des BDSG ist nicht der Schutz der Daten. Schutzsubjekt ist der Einzelne, der bei der Verarbeitung personenbezogener Daten vielfältigen Gefahren ausgesetzt ist.[441] Ziel ist die grundsätzliche Absicherung der individuellen Entscheidungsfreiheit über die Preisgabe von personenbezogenen Daten.[442] Der Schutz personenbezogener Daten ist als Konkretisierung des informationellen Selbstbestimmungsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG anzusehen.[443] Entsprechend reicht der Schutzanspruch des BDSG über den Datenschutz hinaus.
Auch wenn die Zweckbestimmung aus Art. 1 Abs. 1 DSRL und Art. 1 Abs. 1, 2 DSGVO umfassender anmutet als diejenige des nationalen Rechts[444] (insbesondere weil die europarechtlichen Normen auf Grundrechte und Grundfreiheiten Bezug nehmen) folgen beide gleichen Zielsetzungen. Für § 1 Abs. 1 BDSG als zielbestimmende Einleitung eines BDSG-Nachfolgegesetzes besteht insoweit kein Anpassungsbedarf. Unbedingt notwendig ist der Passus umgekehrt aber auch nicht.
Er kann auch vor dem Hintergrund des unionsrechtlichen Wiederholungsverbots[445] Bestand haben. Denn die Datenschutz-Grundverordnung steht Konkretisierungen des Regelungsgehaltes im nationalen Recht nicht entgegen, soweit sie im Zusammenhang mit einem den Mitgliedstaaten eröffneten Regelungsspielraum stehen. Zielsetzung des BDSG-neu ist es, diejenigen Regelungen des allgemeinen Datenschutzrechts zu bündeln, in denen Deutschland von seinem nationalen Regelungsspielraum Gebrauch macht. Gleichwohl

---

[441] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 1, Rn. 1.
[442] *Gola/Klug/Körffer* (Fn. 441), § 1, Rn. 7-9.
[443] *Plath*, in: ders. (Hrsg.), BDSG, 2013, § 1, Rn. 9.
[444] *Gola/Klug/Körffer* (Fn. 441), § 1, Rn. 2; zum weiten Schutzkonzept der DSRL *Brühann*, in: Grabitz/Hilf (Hrsg.), EU-Recht, 40. EL, 2009, Art. 1 Datenschutzrichtlinie, Rn. 5.
[445] Siehe dazu S. 6.

empfiehlt es sich aus Klarstellungsgründen, an dieser Stelle auf die unmittelbare Geltung der Verordnung hinzuweisen, damit dem Rechtsunterworfenen nicht die Urheberschaft des Unionsgesetzgebers verborgen bleibt.

b. Abs. 2: Normadressaten

§ 1 Abs. 2 BDSG führt die Unterscheidung zwischen datenverarbeitenden öffentlichen und nicht-öffentlichen Stellen ein, welche das BDSG durchzieht. Eine vergleichbare Differenzierung findet sich in der Datenschutz-Grundverordnung in dieser Klarheit nicht.[446] Tatsächlich räumt sie aber den Mitgliedstaaten im Hinblick auf öffentliche Stellen einen deutlich weiteren Regelungsspielraum ein als im Hinblick auf nicht-öffentliche Stellen. Die überkommene Differenzierung des nationalen Rechts kann daher auch unter dem Regelungsregime der Datenschutz-Grundverordnung zulässig und sinnvoll sein.

c. Abs. 3: Subsidiarität

§ 1 Abs. 3 BDSG schreibt die Spezialität anderer bundesrechtlicher Vorschriften fest, soweit diese in Bezug auf personenbezogene Daten und deren Veröffentlichung Regelungen treffen. An dieser nationalen Regelungssystematik darf der Gesetzgeber als Teil seines nationalen Regelungsspielraums festhalten.
Um Missverständnisse zu vermeiden, ist aber in diesem Regelungskontext ein Hinweis darauf sinnvoll, dass das BDSG nur zur Anwendung gelangt, soweit nicht die Datenschutz-Grundverordnung unmittelbar geltendes Recht setzt.

d. Abs. 4: Verhältnis zum VwVfG

§ 1 Abs. 4 regelt das Verhältnis des BDSG zum VwVfG. Das rechtssystematische Stufenverhältnis, das sie ausdrückt, bleibt durch die Datenschutz-Grundverordnung unangetastet.

---

[446] Siehe aber immerhin bspw. Art. 27 Abs. 2 lit. a, Art. 37 Abs. 3, Art. 41 Abs. 6, Art. 83 Abs. 7. Faktisch zielt Art. 6 Abs. 1 UAbs.1 lit. e, Abs. 2 u. 3 weitgehend auf die Datenverarbeitung zur Erfüllung öffentlicher Aufgaben ab.

e. Abs. 5: Ausnahme vom Anwendungsbereich

Gemäß § 1 Abs. 5 S. 1 BDSG findet deutsches Datenschutzrecht keine Anwendung, wenn die Verarbeitung in Deutschland durch eine Stelle erfolgt, die in einem anderen Mitgliedstaat der Union belegen ist, es sei denn, die Verarbeitung erfolgt durch eine Niederlassung im Inland.

f. Abs. 5 S. 1 a. E.

Der Wortlaut des Abs. 5 S. 1 a. E. macht die Anwendbarkeit des BDSG davon abhängig, ob die inländische Niederlassung eines Unternehmens, das in einem anderen Mitgliedstaat belegen ist[447], die Verarbeitung vornimmt. Damit verschließt sich das nationale Recht der feingliedrigen Unterscheidung in Art. 4 lit. a DSRL. Er stellt auf den Kontext ab („im Rahmen der Tätigkeit einer [inländischen] Niederlassung[448]“). Dies greift der EuGH im Urteil Google Spain und Google auf: Es geht nicht darum, ob die Niederlassung selbst die Daten verarbeitet, sondern nur ob dies im Rahmen ihrer Tätigkeit geschieht.[449] Diese Maßgeblichkeit des Marktortprinzips findet sich nun auch explizit in Art. 3 Abs. 1 DSGVO. Eine kontextuale Datenverarbeitung liegt dann vor, wenn die Arbeit der Niederlassung untrennbar mit der eigentlichen Datenverarbeitung zusammenhängt.[450]
Dieses Prinzip findet sich so nicht ohne Weiteres in § 1 Abs. 5 S. 1. Er bedarf daher einer Modifizierung.

g. Abs. 5 S. 2

Abs. 5 S. 2 stellt darauf ab, ob die Datenverarbeitung durch einen Verantwortlichen mit Sitz in einem Drittstaat außerhalb der Union im Inland erfolgt. Demgegenüber verlangt Art. 3 Abs. 2 DSGVO präzisierend, dass die Verarbeitung dazu dient, betroffenen Personen, die sich in der EU aufhalten, Waren bzw. Dienstleistungen anzubieten (lit. a) oder diese Personen und ihr Verhalten zu beobachten (lit. b). Wie EG 21 DSGVO darlegt, soll lit. b vor allem Gefahren des Profilings erfassen.

---

[447] Primär stellt die Vorschrift auf das Sitzlandprinzip ab; dazu *Wieczorek*, DuD, 644 (645).
[448] Eine Niederlassung setzt nach EG 19 DSGVO die „effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus“.
[449] EuGH, Rs. 131/12, Google Spain und Google, Slg. 2014, 1, Rn. 52-55.
[450] Vgl. dazu *Kühling*, EuZW 2014, 527 (528 f.).

h. Abs. 5 S. 3

Die Pflicht zur Benennung eines Vertreters in der Union ergibt sich unmittelbar aus Art. 27 Abs. 1 (ex Art. 25 Abs. 1) i. V. m. Art. 3 Abs. 2 DSGVO. Einer ergänzenden Regelung im nationalen Recht bedarf es nicht. Vor allem belässt Art. 27 DSGVO den Mitgliedstaaten keinen eigenen Regelungsspielraum.

i. Abs. 5 S. 5

Die Norm betrifft nur die Befugnisse der Aufsichtsbehörden. Diese regelt die Datenschutz-Grundverordnung unmittelbar in ihren Art. 55 ff. (ex Art. 51 ff).

§ 1 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	Art. 1 Abs. 1, 2	(Ggf. um einen Hinweis auf die DSGVO ergänzt) beibehalten	
Abs. 2		Beibehalten möglich	Auch ohne explizite Differenzierung in der DSGVO geht der Unionsgesetzgeber von zwei unterschiedlichen Normadressaten aus. Dies zeigt sich daran, dass die DSGVO im Bereich der Datenverarbeitung durch öffentliche Stellen weiter reichende Öffnungsklauseln vorsieht, während dies im privaten Bereich nicht der Fall ist (dazu sogleich § 2).[451] Im Bereich seines eigenen, ihm verbliebenen Regelungsspielraum darf der nationale Gesetzgeber an der Differenzierung zwischen öffentlichen und nicht-öffentlichen Stellen festhalten.
Abs. 3		Beibehalten und um einen Hinweis auf die unmittelbare Geltung der	Eine Ergänzung der Subsidiaritätsklausel um einen Hinweis auf die DSGVO führt dem Rechtsanwender vor Augen, dass diese unmittelbar anwendbar ist und nur im Falle von

[451] Zum unterschiedlichen Harmonisierungsgrad, *BfDI*, in: Deutscher Bundestag, Ausschuss Digitale Agenda, Ausschussdrucksache 18(29)93, S. 4.

		DSGVO ergänzen. („Soweit andere Rechtsvorschriften des Bundes oder die Datenschutz-grundverord-nung…“)	Öffnungsklauseln oder Konkretisierungen unbestimmter Rechtsbegriffe (u. ä.) Raum für das nationale Recht bestehen bleibt.
Abs. 4	-	Beibehalten	Kein Änderungsbedarf durch die Einwirkung der DSGVO. Das Stufenverhältnis zwischen DSGVO und VwVfG bleibt unverändert.
Abs. 5 S. 1	Art. 3 Abs. 1, EG 22 (ex EG 19)	Modifizieren Vorschlag: „Soweit die DSGVO dem Recht der Mit-gliedstaaten Kon-kretisierungs- oder Durchführungs-spielräume belässt, ist das BDSG anwendbar, wenn der Verantwortli-che diese im Rah-men der Tätigkeit einer inländischen Niederlassung durchführt.“	Der Wortlaut von Abs. 5 S. 1 a. E. macht die Anwendbarkeit des BDSG davon abhängig, ob die inländische Niederlassung eines Unter-nehmens, das in einem anderen Mitgliedstaat belegen ist[452], die Verarbeitung vornimmt. Damit verschließt sich das nationale Recht der feingliedrigen Unterscheidung in Art. 4 lit. a DSRL. Er stellt auf den Kontext ab („im Rahmen der Tätigkeit einer [inländischen] Niederlassung[453]“). Dies greift der EuGH im Urteil Google Spain und Google auf: Es geht nicht darum, ob die Niederlassung selbst die Daten verarbeitet, sondern nur ob dies im Rahmen ihrer Tätigkeit geschieht.[454] Diese Maßgeblichkeit des Marktortprinzips findet sich nun auch explizit in Art. 3 Abs. 1 DSG-VO. Eine kontextuale Datenverarbeitung liegt dann vor, wenn die Arbeit der Niederlassung untrennbar mit der eigentlichen Datenverar-beitung zusammenhängt.[455] Dieses Prinzip findet sich so nicht ohne Wei-teres in Abs. 5 S. 1. Er bedarf daher einer Modifizierung.

[452] Primär stellt die Vorschrift auf das Sitzlandprinzip ab; dazu *Wieczorek* (Fn. 447), 645.
[453] Eine Niederlassung setzt nach EG 19 DSGVO die „effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung voraus“.
[454] EuGH, Rs. 131/12, Google Spain und Google, Slg. 2014, 1, Rn. 52-55.
[455] Vgl. dazu *Kühling* (Fn. 450) (528 f.).

Abs. 5 S. 2	Art. 3 Abs. 2, EG 23 f. (ex EG 20 f.)	Modifizieren Vorschlag: „Das BDSG findet ergänzend zur DSGVO Anwendung, wenn die in Art. 3 Abs. 2 DSGVO beschriebene Verarbeitung Personen innerhalb der Bundesrepublik Deutschland betrifft.“	Umsetzung des Marktortprinzips, das in Art. 3 Abs. 2 DSGVO angelegt ist.
Abs. 5 S. 3, 4		Streichen	Nunmehr unmittelbar in Art. 27 Abs. 1 (ex Art. 25 Abs. 1) i. V. m. Art. 3 Abs. 2 DSGVO geregelt.
Abs. 5 S. 5		Streichen	Nunmehr unmittelbar in i Art. 55 ff. (ex Art. 51 ff.) geregelt.

§ 2: Öffentliche und nicht-öffentliche Stellen

§ 2 BDSG definiert, was das Gesetz unter öffentlichen und nicht-öffentlichen Stellen im Einzelnen versteht. Die Definitionen sind deswegen von zentraler Bedeutung, weil das deutsche Datenschutzrecht – anders als die Datenschutz-Grundverordnung und zuvor die RL 95/46/EG – das normative Anforderungsprofil an öffentliche und nicht-öffentliche Stellen stark ausdifferenziert, also kategorial zwischen zwei Adressatengruppen unterscheidet.
Art. 4 Nr. 7 (ex Art. 4 Nr. 5) DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, den Verantwortlichen in den Fällen näher zu bestimmen, in denen sie Zweck und Mittel der Verarbeitung festlegen können.[456] Damit sind eine Kategorisierung der Verantwortlichen und die Aufrechterhaltung der Unterscheidung zwischen öffentlichen und nicht-öffentlichen Stellen grundsätzlich möglich. Nicht zuletzt knüpfen bspw. Art. 27 Abs. 2 lit. a, Art. 37 Abs. 3, Art. 41 Abs. 6, Art. 83 Abs. 7 DSGVO an den Begriff der öffentlichen Stelle an. Faktisch zielt Art. 6 Abs. 1 UAbs. 1 lit. e, Abs. 2 u. 3 DSGVO auch weitgehend auf die Datenverarbeitung zur Erfüllung öffentlicher Aufgaben ab. § 2

[456] Siehe dazu S. 25.

BDSG, der die entsprechenden Stellen als öffentliche oder nicht-öffentliche Stellen definiert, kann somit aufrechterhalten werden.

§ 2 BDSG	Korrespondierende Norm in der DSG-VO	Gesetzgeberische Handlungsoption	Begründung
§ 2	Art. 4 Nr. 7 (ex Art. 4 Nr. 5)	Aufrechterhalten möglich	Die Trennung der Normadressaten in öffentliche und nicht-öffentliche Stellen lässt Art. 4 Nr. 7 (ex Art. 4 Nr. 5) DSGVO zu. Damit ist auch die entsprechende Definition in § 2 BDSG möglich.

§ 3: Weitere Begriffsbestimmungen

§ 3 BDSG definiert zentrale Bestimmungen des BDSG, die teilweise mit den entsprechenden Definitionen in der Datenschutz-Grundverordnung vergleichbar sind, teilweise aber auch ausführlicher oder knapper sind oder dort gänzlich fehlen. Insoweit ist zu differenzieren:
Die Definition der personenbezogenen Daten in § 3 Abs. 2 BDSG entspricht Art. 4 Nr. 1 DSGVO, der allerdings etwas umfassender ist. Insoweit ist jedenfalls keine allgemeine, abweichende Definition im BDSG von einer Öffnungsklausel gedeckt und auch nicht tunlich. Die Definition ist also zu streichen.
Dasselbe gilt für die parallele Definition von „pseudonymisieren“ in § 3 Abs. 6a BDSG in Relation zu Art. 4 Nr. 5 (ex Art. 4 Nr. 3b) DSGVO, „Verantwortliche Stelle“ in § 3 Abs. 7 BDSG in Relation zu Art. 4 Nr. 7 (ex Art. 4 Nr. 5) DSGVO sowie „Empfänger“ und „Dritter“ in § 3 Abs. 7 BDSG in Relation zu Art. 4 Nr. 9 (ex Art. 4 Nr. 7) und Art. 4 Nr. 10 (ex Art. 4 Nr. 7a) DSGVO. Den Begriff des „Anonymisierens“ definiert die Datenschutz-Grundverordnung nicht in Art. 4 näher, klärt ihn aber in EG 26 (ex EG 23) DSGVO. Denn dort heißt es, dass es sich dabei um Informationen handelt, „die sich nicht auf eine bestimmte oder bestimmbare natürliche Person beziehen, oder Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann“. Eine abweichende Definition in § 3 Abs. 6 BDSG ist vor diesem Hintergrund aus denselben Gründen zu streichen. „Besondere Arten personenbezogener Daten“,

die in § 3 Abs. 9 BDSG eine Begriffsbestimmung erfahren, definiert die Datenschutz-Grundverordnung nicht in Art. 4 nicht näher, sondern umreißt den Begriff in Art. 9 Abs. 1 DSGVO. Art. 9 DSGVO weist zwar weitreichende Öffnungsklauseln auf. Diese beziehen sich aber nicht auf die Definition der besonderen Kategorien personenbezogener Daten, so dass auch hier eine mitgliedstaatliche Definition unzulässig und jedenfalls untunlich ist. Auch § 3 Abs. 9 BDSG ist daher zu streichen.

Die (nicht) automatisierte Verarbeitung nach § 3 Abs. 2 BDSG hat in der Datenschutz-Grundverordnung kein Äquivalent, findet dort aber an zahlreichen Stellen Verwendung, ohne dass in diesen Kontexten jeweils umfassend eine Öffnungsklausel greift. Das gilt beispielsweise im Zusammenhang mit der Pflicht zur Datenschutz-Folgenabschätzung nach Art. 35 Abs. 3 lit. a (ex Art. 33 Abs. 2 lit. a DSGVO), der auf den Begriff der automatisierten Verarbeitung rekurriert und insoweit nicht vollständig der Öffnungsklausel des Art. 33 Abs. 10 (ex Art. 33 Abs. 5) DSGVO unterliegt. Daher werden die Kommission und der EuGH den Begriff unionsrechtsautonom zu klären haben. Eine eigenständige nationale Definition ist insofern jedenfalls untunlich und wäre allenfalls im Bereich der Öffnungsklauseln denkbar. Der Absatz sollte daher gestrichen werden.

Komplizierter ist die Bewertung in Bezug auf die fein ausdifferenzierende Konkretisierung der Schritte des Datenumgangs in § 3 Abs. 3 bis 5 BDSG. Sie korrespondiert mit der knapperen Definition in Art. 4 Nr. 2 (ex Art. 4 Nr. 3) DSGVO. Insoweit hat der deutsche Gesetzgeber im allgemeinen wie im bereichsspezifischen Datenschutzrecht – abweichend von der in der RL 95/46/EG vorgesehenen umfassenden Definition des Verarbeitungsbegriffs – einen engeren Verarbeitungsbegriff mit den fünf Teilaspekten des Speicherns, Veränderns, Übermittelns, Sperrens und Löschens normiert, der ergänzt wird durch die Schritte des Erhebens und des Nutzens.[457] Teilweise definieren auch die bereichsspezifischen Normen die Begriffe noch einmal (siehe etwa § 67 Abs. 6 SGB X), sehr häufig greifen sie (wie etwa im Bundesmeldegesetz) auf diese Begrifflichkeit des BDSG zurück.

Das streitet – mit Blick auf jene bereichsspezifischen Normen, die aufgrund der Öffnungsklauseln auch im weiten Umfang bestehen bleiben können (wie

[457] Siehe dazu im Überblick *Kühling/Seidel/Sivridis* (Fn. 44) Rn. 232 ff.

etwa das BMG) – dafür, die Begriffe weiterhin als Teil des allgemeinen Datenschutzrechts im BDSG zu definieren. Das gilt zusätzlich dann, wenn im BDSG – unter Rückgriff auf Art. 6 Abs. 2 u. 3 i. V. m. Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO auch einzelne Normen aufrechterhalten bleiben, die auf die Terminologie der verschiedenen Teilaspekte des Datenumgangs rekurrieren (wie etwa die §§ 12 ff. BDSG) und daher in ihrer Anwendung durch entsprechende Definitionen erleichtert würden. Soweit diese Normen von den Öffnungsklauseln Gebrauch machen (wie wiederum die §§ 12 ff. BDSG), dürfen auch Differenzierungen für verschiedene Formen des Datenumgangs konkreter formuliert werden, was sodann auch die Möglichkeit und Zulässigkeit einer diesbezüglichen Definition impliziert. Allerdings wird dann der unglückliche Zustand, der schon unter der Geltung der RL 95/46/EG irritierend war, dass ein Verarbeiten i. w. S. richtlinienrechtlich verwendet wurde und i. e. S. nationalrechtlich, perpetuiert. Insoweit erscheint es zweckmäßiger, auf derartige Sonder-Begriffsdefinitionen zu verzichten und im Rahmen der Gesetzgebung klarzustellen, dass entsprechende Teilschritte weiterhin grundsätzlich im Sinne der bisherigen BDSG-Definitionen verstanden werden können und dabei zugleich überall dort, wo der Begriff des Verarbeitens i. e. S. des BDSG verwendet wird, im Falle einer etwaigen Aufrechterhaltung dieser Bestimmung (etwa § 14 Abs. 3 S. 1 BDSG) die entsprechenden fünf Teilaspekte explizit anzuführen. Daher empfiehlt sich eine Streichung der Abs. 3 bis 5 des § 3 BDSG.

Die Streichung der Definition mobiler personenbezogener Daten steht und fällt mit der Streichung der damit korrespondierenden Vorschrift des § 6c BDSG.[458]

Ob die Definition des Beschäftigten in § 3 Abs. 11 BDSG aufrechterhalten bleiben kann, die sich auf den Beschäftigtendatenschutz nach § 32 BDSG bezieht[459], ist unklar. Zwar greift hier die weitreichende Öffnungsklausel des Art. 88 (ex Art. 82) DSGVO, die auch eine Konturierung des Beschäftigtenbegriffs zulassen dürfte, soweit dieser nicht unionsautonom durch die Unionsorgane zu bestimmen ist. Der Begriff des Beschäftigten unterliegt aber nicht selbst einer Öffnungsklausel. Insofern verbleiben Restrisiken.

[458] Siehe dazu unten § 6c.

[459] *Eßer*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 3 BDSG, Rn. 88.

Der Kommission sind nach Art. 88 Abs. 3 i. V. m. Art. 99 Abs. 2 (ex Art. 82 Abs. 2a i. V. m. Art. 91 Abs. 2) DSGVO ohnehin die Rechtsvorschriften mitzuteilen, die auf der Basis dieser Öffnungsklausel erlassen werden, so dass in diesem Rahmen die Frage geklärt werden könnte. In jedem Fall spricht wenig dafür, eine eigenständige Definitionsnorm nur für § 32 BDSG aufrechtzuerhalten, so dass die Norm auch gestrichen werden könnte und als Leitvorgabe für die Anwendung des § 32 BDSG ohnehin weitergelten würde.

§ 3 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	Art. 4 Nr. 1	Streichen	Keine Öffnungsklausel/Definition in DSGVO; abweichende Definition unzulässig und irreführend.
Abs. 2	-	Streichen	Dito
Abs. 3 – 5	Art. 4 Nr. 2 (ex Art. 4 Nr. 3)	Streichen empfohlen; Aufrechterhaltung für den Bereich der Öffnungsklauseln zulässig	Da die Begriffsbildung im BDSG von der in der DSGVO abweicht, sollte keine Sonderterminologie im BDSG aufrechterhalten werden, auch wenn das für den Bereich der Öffnungsklauseln zulässig sein mag.
Abs. 6	EG 26 (ex EG 23)	Streichen	Keine Öffnungsklausel/Definition in DSGVO; abweichende Definition unzulässig und irreführend.
Abs. 6a	Art. 4 Nr. 5 (ex Art. 4 Nr. 3b DSGVO)	Streichen	Dito
Abs. 7	Art. 4 Nr. 7 (ex Art. 4 Nr. 5)	Streichen	Dito
Abs. 8	Art. 4 Nr. 9, 10 (ex Art. 4 Nr. 7, 7a)	Streichen	Dito
Abs. 9	Art. 9 Abs. 1	Streichen	Dito
Abs. 10	-	Teilt Schicksal des § 6c	
Abs. 11	-/Öffnungsklausel in Art. 88 (ex Art. 82) für Datenverarbeitung im Beschäftigungskontext	Aufrechterhalten mit Risiken möglich; Streichung und allenfalls Integration in	Ob die Öffnungsklausel des Art. 88 (ex Art. 82) DSGVO auch die Definition des Beschäftigten selbst erfasst oder dieser Begriff als Eingrenzung der Reichweite der Öffnungsklausel

		§ 32 BDSG empfehlenswert	ratione personae nicht unionsautonom bestimmt werden muss, ist fraglich.

§ 3a: Datenvermeidung und Datensparsamkeit

Die Prinzipien des § 3a BDSG zielen darauf, soweit möglich Daten überhaupt nicht (Datenvermeidung) oder nur in sehr geringer Zahl (Datensparsamkeit) zu erheben.[460] Dies trägt dem verfassungsrechtlichen Grundanliegen des Persönlichkeitsschutzes Rechnung, dem Einzelnen eine nach Möglichkeit unbeobachtete Entfaltung zu gestatten, die nicht von einem opaken „Gefühl des Überwachtwerdens“ überlagert wird.

§ 3a S. 1 BDSG ist aufgrund des Wiederholungsverbotes zu streichen; Art. 5 Abs. 1 lit. c DSGVO enthält beide Prinzipien bereits. Der Begriff „Datenminimierung“ impliziert als Minus die grundsätzliche Datenvermeidung.

§ 3a S. 2 BDSG beschreibt regelbeispielhaft zwei zentrale Maßnahmen, die der Umsetzung der Prinzipien nach S. 1 dienen: Anonymisierung und Pseudonymisierung – soweit der Verwendungszweck dies ermöglicht und sie nicht einen im Vergleich zum angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordern. Auch wenn sich die Datenschutz-Grundverordnung lediglich in EG 26 S. 5, 6 zu anonymisierten Daten äußert und diese vom Anwendungsbereich der Verordnung ausnimmt, gestaltet sie die Anforderungen an die Datenminimierung doch unmittelbar und grundsätzlich abschließend aus; so etwa neben Art. 5 Abs. 1 lit. c in Art. 25 Abs. 1 DSGVO und Art. 32 Abs. 1 Hs. 2 lit a[461].

[460] *Eßer*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 3a BDSG, Rn. 1.
[461] *Martini*, in: Paal/Pauly (Hrsg.), DSGVO, 2016, Art. 32, Rn. 31 f.

§ 3a BDSG	Korrespondierende Norm in der DSG-VO	Gesetzgeberische Handlungsoption	Begründung
S. 1, 2	Art. 5 Abs. 1 lit. c	Streichen	Die DSGVO regelt den Grundsatz der Datenminimierung. Der Grundsatz als solcher ist zwar noch konkretisierungsbedürftig. Diese Aufgabe übernehmen aber spezifische Bestimmungen der Verordnung. Eine zusätzliche Normierung im nationalen Gesetz verstieße gegen das Wiederholungsverbot. Das gilt auch für die Konkretisierung in § 3a S. 2 BDSG.

§ 4: Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung

a. Abs. 1: Verbot mit Erlaubnisvorbehalt

§ 4 Abs. 1 BDSG normiert das datenschutzrechtliche Verbot mit Erlaubnisvorbehalt: Jedweder Umgang mit personenbezogenen Daten ist grundsätzlich verboten, solange er nicht ausdrücklich erlaubt wird. Dieser Ansatz fand sich bereits in Art. 7 DSRL. Er ist nun in Art. 6 Abs. 1 DSGVO verankert. § 4 Abs. 1 BDSG stellt die Datenerhebung, -verarbeitung und -nutzung unter den Vorbehalt, dass das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Soweit § 4 Abs. 1 BDSG für die Zulässigkeit auf das BDSG oder andere Rechtsvorschriften verweist, können diese Bestimmungen aufrechterhalten bleiben, soweit die DSGVO den Mitgliedstaaten Regelungsspielraum belässt. Die Aufrechterhaltung kann sinnvoll sein, um die Systematik des BDSG in sich stimmig zu erhalten und Klarheit für den Normadressaten dahin gehend zu schaffen, dass das Verbot mit Erlaubnisvorbehalt auch dort gilt, wo Öffnungsklauseln bestehen und das BDSG-neu oder die bereichsspezifischen Gesetze Zulässigkeitstatbestände normieren. Gleichwohl wäre die Regelung eine bloße Wiederholung zur Grundnorm des Art. 6 Abs. 1 DSGVO. Ob diese in einer solchen Allgemeinheit und an einer derart zentralen Schaltstelle zulässig ist, ist nicht gesichert. Das Anliegen der Datenschutz-Grundverordnung – wie jeder Verordnung – ist es nämlich, selbst als die maßgebliche Regelung wahrgenommen zu wer-

den. Eine Aufrechterhaltung ist deswegen grundsätzlich systemwidrig und abzulehnen.
Jedenfalls hinsichtlich des Verweises auf die Einwilligung des Betroffenen ist eine Streichung geboten. Die Rechtmäßigkeit der Verarbeitung durch Einwilligung des Betroffenen sieht Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO ebenfalls vor. Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO enthält insoweit keine Öffnungsklausel, weswegen § 4 Abs. 1 Hs. 2 Var. 3 BDSG insofern eine Wiederholung des Wortlauts der Verordnung darstellen würde. Da indes eine Reihe von Öffnungsklauseln in Bezug auf allgemeine und bereichsspezifisch normierte Zulässigkeitstatbestände greifen, kann es aus Gründen der systematischen Klarstellung wünschenswert sein, den Regelungsadressaten das Verhältnis der verschiedenen Legitimationstatbestände klar vor Augen zu führen, indem die Legitimationstatbestände zusammengefasst werden. Doch kommt diese Aufgabe primär Art. 6 Abs. 1 DSGVO selbst zu. Soll dies im nationalen Recht noch einmal Ausdruck finden, wäre dann allerdings eine Formulierung notwendig, die an die Verordnung in der Weise anknüpft, dass eine Verarbeitung nur rechtmäßig ist, wenn eine der Bedingungen der Datenschutz-Grundverordnung und insbesondere des Art. 6 erfüllt sind, insbesondere wenn das BDSG-neu oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat. Ob dies allerdings eine größere Klarheit schafft, kann wiederum bezweifelt werden, da auch noch deutlich werden müsste, dass die Einwilligungsanforderungen grundsätzlich aus der Datenschutz-Grundverordnung folgen.

b. Abs. 2: Direkterhebungsgrundsatz

§ 4 Abs. 2 BDSG normiert den Grundsatz der Direkterhebung: Daten dürfen nur beim Betroffenen direkt erhoben werden. Der Grundsatz soll dem Betroffenen den Umgang mit den Daten transparent machen und ihm die Möglichkeit eröffnen, über die Preisgabe personenbezogener Daten selbst zu entscheiden.[462] Verfassungsrechtlich zwingend ist die jetzige umfassende Regelung für den öffentlichen und nicht-öffentlichen Bereich jedoch keineswegs.
Die Datenschutz-Grundverordnung kennt den Grundsatz der Direkterhebung nicht. § 4 Abs. 2 BDSG aufrechtzuerhalten, ist auch deshalb problematisch,

[462] *Kühling/Seidel/Sivridis* (Fn. 44), Rn. 291 f.

weil diese Bestimmung sich gleichermaßen an öffentliche wie nicht-öffentliche Stellen richtet und damit Grundrechtspositionen nicht nur des Betroffenen, sondern auch der verantwortlichen Stelle berühren kann. Die Einschränkung der Grundrechte der nicht-öffentlichen Stellen sieht die Datenschutz-Grundverordnung so aber nicht vor. Vielmehr zeigt Art. 14 (ex Art. 14a) DSGVO, dass sie davon ausgeht, dass Daten nicht beim Betroffenen erhoben werden müssen. Daher wäre es besser, den Direkterhebungsgrundsatz ggf. direkt bei den entsprechenden Regelungen zu integrieren, welche den Mitgliedstaaten Regelungsspielraum einräumen, etwa bei den Regelungen der §§ 12 ff. BDSG, die sich nur an öffentliche Stellen richten. So sieht Art. 6 Abs. 3 S. 3 DSGVO etwa vor, dass die mitgliedstaatlichen Rechtsgrundlagen für Fälle des Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO auch allgemeine Bedingungen für die Rechtmäßigkeit der Datenverarbeitung durch den Verantwortlichen regeln können, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung. Damit ließe sich für öffentliche Stellen als Normadressaten auch ein Direkterhebungsgrundsatz in die entsprechenden Normen integrieren, sofern der Gesetzgeber dies als rechtspolitisch geboten bzw. vorzugswürdig ansieht.

c. Abs. 3: Hinweispflichten an den Betroffenen

§ 4 Abs. 3 BDSG regelt Hinweispflichten an den Betroffenen, sofern die Daten beim Betroffenen erhoben werden. Die Datenschutz-Grundverordnung sieht diese Hinweispflichten umfangreich in Art. 13 (ex Art. 14) DSGVO vor. Von diesen Betroffenenrechten dürfen die Mitgliedstaaten alleine im Rahmen der Öffnungsklausel des Art. 23 DSGVO abweichen. Eine Aufrechterhaltung des § 4 Abs. 3 BDSG wäre daher grundsätzlich eine Normwiederholung. Diese wäre alleine dann zulässig, wenn sie erforderlich ist, um Abweichungen im Rahmen der Öffnungsklausel des Art. 23 DSGVO[463] verständlich zu machen. Daher ist entsprechend der Empfehlungen zur Nutzung der Öffnungsklausel des Art. 23 (ex Art. 21) DSGVO eine Streichung angezeigt.

[463] Vgl. dazu S. 68.

§ 4 BDSG	Korrespondierende Norm in der DSG-VO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1 Hs. 2 Var. 1, 2	Art. 6 Abs. 1	Streichung indiziert; u. U modifizieren.	Grds. Wiederholung der nun von Art. 6 Abs. 1 DSGVO vorgenommenen Regelung; Aufrechterhaltung evtl. zweckmäßig, um Systematik des BDSG-neu klarzumachen.
Abs. 1 Hs. 2 Var. 3	Art. 6 Abs. 1 UAbs. 1 lit. a	Streichung	Die Verarbeitung aufgrund Einwilligung des Betroffenen ist in Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO geregelt und sieht keine Öffnungsklausel vor.
Abs. 2	-	Streichung für nicht-öffentliche Normadressaten; Beibehalten für öffentliche Stellen möglich, aber nicht nötig	Der Direkterhebungsgrundsatz findet sich nicht in der DSGVO. Aufgrund betroffener Grundrechtspositionen nicht-öffentlicher Stellen und mangelnder Öffnungsklauseln ist die Aufrechterhaltung der Norm, die sich gleichermaßen an öffentliche wie nicht-öffentliche Stellen richtet, nicht möglich.
Abs. 3	Art. 13 (ex Art. 14); Art. 23 (ex Art. 21) (Öffnungsklausel)	Grds. Streichung; nur Normierung von Abweichungen iRd Öffnungsklausel notwendig	Die Hinweispflichten an den Betroffenen sind in Art. 13 (ex Art. 14) DSGVO umfassend geregelt. Zwar erlaubt die Öffnungsklausel des Art. 23 DSGVO Abweichungen von dieser Norm; nur diese müssten geregelt werden, wobei keine Gründe für dessen (pauschale, nicht bereichsspezifische) Nutzung ersichtlich sind.

§ 4a: Einwilligung

Die in § 4a BDSG vorgesehenen Bestimmungen für die Einwilligung ergeben sich unmittelbar aus der DSGVO: Die Einwilligung selbst ist in Art. 4 Nr. 11 DSGVO definiert und in Art. 7 DSGVO geregelt. Regelungsmöglichkeiten verbleiben den Mitgliedstaaten in zwei Fällen. Art. 8 DSGVO sieht eine Öffnungsklausel für den Spezialbereich der Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft vor, die bislang kein Pendant im BDSG kennt. Außerdem besteht die Möglichkeit des Ausschlusses der Ein-

willigung bei der Verarbeitung besonderer Kategorien personenbezogener Daten in Art. 9 Abs. 2 lit. a DSGVO. Soweit § 4a BDSG keine von der Datenschutz-Grundverordnung abweichenden, von einer Öffnungsklausel gedeckte, Regelungen trifft, ist die Vorschrift zu streichen[464].

§ 4a BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1 und 2	Art. 4 Nr. 11 (ex Art. 4 Nr. 8), Art. 7	Streichen	Regelung in DSGVO grds. ohne Öffnungsklausel.
Abs. 3	Art. 9 Abs. 2 lit. a	Streichen	Art. 9 Abs. 2 lit. a DSGVO sieht ebenfalls das Erfordernis einer ausdrücklichen Regelung vor. Er deckt als Öffnungsklausel für den Ausschluss einer Einwilligung bei der Verarbeitung besonderer Kategorien personenbezogener Daten wohl als Minus auch die Verschärfung der formalen Anforderungen an deren Zustandekommen. Dies wäre ein zulässiger Regelungsgegenstand des § 4a BDSG. Gegenwärtig geht § 4a BDSG jedoch über Art. 9 Abs. 1 lit. a DSGVO nicht hinaus.

§ 4b: Übermittlung personenbezogener Daten ins Ausland

§ 4b BDSG regelt die Übermittlung personenbezogener Daten ins Ausland. Für die Übermittlung in Drittländer finden sich entsprechende Regelungen in der Datenschutz-Grundverordnung in den Art. 44 ff. (ex Art. 40 ff) DSGVO. Dort sind die Bestimmungen für die Übermittlung in Drittländer abschließend geregelt. Öffnungsklauseln finden sich nur in Art. 49 (ex Art. 44) DSGVO. Soweit die Regelungen des § 4b BDSG die Übermittlung personenbezogener Daten in Drittländer betreffen, müssen sie gestrichen werden. Das gilt insbesondere für § 4b Abs. 2 und 3 BDSG.

[464] Siehe dazu oben ausführlich im Rahmen der Analyse des Art. 9 DSGVO S. 49.

Soweit die Übermittlung i. S. d. § 4b Abs. 1 BDSG stattfindet, also innerhalb des datenschutzrechtlichen Binnenraums der EU und des EWR, können diese grundsätzlich aufrechterhalten bleiben. Dies gilt jedenfalls insoweit, als die Normen, auf die § 4b Abs. 1 BDSG verweist, aufrechterhalten werden. § 4b Abs. 4 BDSG, der auf § 16 Abs. 1 Nr. 2 BDSG verweist, kann ebenso wie § 16 Abs. 1 Nr. 2 BDSG selbst daher grundsätzlich aufrechterhalten werden.
Es stellt sich aber in Bezug auf § 4b Abs. 1 Nr. 1 und 3 und Abs. 4 BDSG die Frage, ob es noch einer besonderen Regelung für die Übermittlung an Stellen innerhalb der EU bedarf, da die Datenschutz-Grundverordnung selbst – wie schon die RL 95/46/EG[465] – nicht zwischen Fällen mit und ohne Grenzübertritt innerhalb der EU materiell-rechtlich unterscheidet. Hinzu kommt, dass die Verordnung nunmehr mit unmittelbarer Wirkung greift und damit der Anwendungsbereich sachlich entsprechend geklärt ist. So regelt etwa Art. 2 Abs. 3 (ex Art. 2 Abs. 2a) DSGVO die Anwendung der Verordnung auf die Verarbeitung personenbezogener Daten durch Unionsorgane. Unklar ist dies allerdings, soweit der nationale Gesetzgeber von Öffnungsklauseln Gebrauch macht. Hier kann im Einzelfall entweder deklaratorisch oder konstitutiv die Feststellung der Anwendung auch auf Fälle mit grenzüberschreitendem EU-Bezug sinnvoll bzw. notwendig sein. Das gilt insbesondere für die §§ 15, 16 BDSG (im Fall ihrer Beibehaltung), die zudem mit ihrer Differenzierung zwischen öffentlichen und nicht-öffentlichen Stellen als Entitäten, an die Daten übermittelt werden, gerade einen spezifisch deutschen Regelungsgehalt generieren und dabei öffentliche Stellen des Bundes adressieren (§ 12 Abs. 1 BDSG) und gerade solche öffentliche Stellen im EU-Ausland oder der Europäischen Union selbst nicht erfassen. Daher dürfte es erforderlich sein, diesen Regelungsgehalt aufrechtzuerhalten. Dabei ist eine sprachliche Anpassung an die Datenschutz-Grundverordnung erforderlich, indem etwa von den Organen der Europäischen Union gesprochen wird.
Der Regelungsgehalt des § 4b Abs. 1 Nr. 2 BDSG (also die Übermittlung innerhalb des EWR) muss unabhängig davon grundsätzlich aufrechterhalten bleiben, da die Datenschutz-Grundverordnung die Frage nicht regelt. Voraus-

[465] Siehe *Thomale*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 4b BDSG, Rn. 6, der treffend ausführt: „Nach der Konzeption der Richtlinie gelten deshalb die Staaten der Europäischen Union datenschutzrechtlich untereinander als Inland."

setzung ist allerdings, dass die EWR-Staaten den Inhalt der Datenschutz-Grundverordnung übernehmen, wie zuvor den Inhalt der RL 95/46/EG[466].
Die Benennung des Verantwortlichen für solche Übermittlungen i. S. d. § 4b Abs. 5 BDSG ist gem. Art. 4 Nr. 7 (ex Art. 4 Nr. 5) DSGVO möglich.
§ 4b Abs. 6 BDSG regelt eine Hinweispflicht der übermittelnden Stelle an die Empfängerstelle auf den Zweck, zu dessen Erfüllung die personenbezogenen Daten übermittelt werden. Eine ähnliche Vorschrift findet sich in der Datenschutz-Grundverordnung nicht. Die Regelung des Art. 14 (ex Art. 14a) DSGVO adressiert die Pflichten des Verarbeiters gegenüber Betroffenen und nicht gegenüber Dritten, denen die Daten übermittelt werden, und ist also nicht einschlägig. Auch ohne explizit korrespondierende Norm gibt Art. 6 Abs. 3 DSGVO den Mitgliedstaaten einen weiten Spielraum hinsichtlich der Gestaltung der Rechtsgrundlagen i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO, insbesondere auch zur Spezifizierung und Präzisierung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten[467].

§ 4b BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 Nr. 1 und 3	Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e i. V. m. Abs. 2, 3 (ex Abs. 2a, 3)	Modifikation nötig, soweit Bestimmungen des BDSG gestrichen werden, auf die die Norm verweist.	Werden Normen, auf die Abs. 1 verweist, gestrichen, muss die Norm entsprechend angepasst werden.
Abs. 1 Nr. 2	-	Ggf. beibehalten	Keine Regelung in DSGVO. Beibehaltung abhängig von Vereinbarung mit EWR-Staaten zur Übernahme des Inhalts der DSGVO.
Abs. 2 S. 1, S. 2	Art. 44, 45 (ex Art. 40, 41)	Streichen	Die Übermittlung in Drittstaaten bei angemessenem Schutzniveau ist in Art. 44, 45 (ex Art. 40, 41) DSGVO geregelt. Die Normen sehen keine Öffnungsklausel für eine Regelung durch die Mitgliedstaaten vor.

[466] Dazu mit näheren Hinweisen *Schantz*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 4b BDSG, Rn. 3.
[467] Vgl. ausführlich S. 34.

Abs. 2 S. 3	-	Streichen	Die Bestimmungen für Übermittlungen in Drittländer sind in den Art. 44 ff. (ex Art. 40 ff.) DSGVO abschließend geregelt. Es findet sich keine Öffnungsklausel für diese Norm.
Abs. 3	Art. 45 (ex Art. 41)	Streichen	Der Angemessenheitsbeschluss kann gem. Art. 45 Abs. 1 (ex Art. 41 Abs. 1) DSGVO nur durch die Kommission erfolgen. Die Norm sieht keine Öffnungsklausel für eine Regelung durch die Mitgliedstaaten vor.
Abs. 4	-	Beibehalten	Kann aufrechterhalten werden, da Verweis auf § 16 Abs. 1 Nr. 2 BDSG, der ebenfalls aufrechterhalten werden kann.
Abs. 5	Art. 4 Nr. 7 (ex Art. 4 Nr. 5)	Beibehalten	Die Benennung eines Verantwortlichen ist gem. Art. 4 Nr. 7 (ex Art. 4 Nr. 5 DSGVO) möglich.
Abs. 6	-	Beibehalten	Art. 6 Abs. 2, 3 (ex Art. 6 Abs. 2a, 3) DSGVO eröffnet den Mitgliedstaaten weitreichenden Spielraum, spezifische Bestimmungen zu schaffen bzw. beizubehalten, die Maßnahmen bestimmen, um eine rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten.

§ 4c: Ausnahmen

Von dem Grundsatz des § 4b BDSG, dass eine Übermittlung nur in Drittländer mit angemessenem Datenschutzniveau zulässig ist, lässt Ausnahmen § 4c BDSG zu. Er ist nahezu identisch mit Art. 49 Abs. 1 (ex Art. 44 Abs. 1) DSGVO. Öffnungsklauseln finden sich dort lediglich in Art. 49 Abs. 1 UAbs. 1 lit. d (ex Art. 44 Abs. 1 lit. d) (i. V. m. Abs. 5 DSGVO), die identisch ist mit § 4c Abs. 1 S. 1 Nr. 4 Alt. 1 BDSG – sowie in Art. 49 Abs. 1 UAbs. 1 lit. g (ex Art. 44 Abs. 1 lit. g) DSGVO, der identisch ist mit § 4c Abs. 1 S. 1 Nr. 6 BDSG. Die Öffnung des Art. 49 Abs. 1 UAbs. 1 lit. g (ex Art. 44 Abs. 1 lit. g) DSGVO bezieht sich allerdings ausschließlich auf die normative Regelung des Registers, aus dem die Übermittlung erfolgen soll, und lässt keine Öffnung hinsichtlich des Erlaubnistatbestandes für Übermittlungen in ein Drittland an sich zu. Damit können die Mitgliedstaaten allgemeine Regelungen zu Registern vorsehen; eine Aufrechterhaltung des § 4c Abs. 1 S. 1 Nr. 6 BDSG ist hingegen nicht zulässig.

Art. 49 Abs. 1 UAbs. 1 lit. d (ex Art. 44 Abs. 1 lit. d) (i. V. m. Abs. 4 [ex Abs. 5]) DSGVO bestimmt, dass das öffentliche Interesse, das eine Übermittlung notwendig macht, in dem Recht des Mitgliedstaates, dem der Verantwortliche unterliegt, anerkannt sein muss. Die Formulierung „wichtige Gründe eines öffentlichen Interesses / important reasons of public interest" zeigt, dass die Anforderungen an eine Datenübermittlung höher sind als in Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1 DSGVO, in denen für die Zulässigkeit einer Datenverarbeitung eine Wahrnehmung einer Aufgabe im öffentlichen Interesse ausreicht. In Art. 26 Abs. 1 lit. d Var. 1 DSRL sowie in § 4c Abs. 1 S. 1 Nr. 4 Alt. 1 BDSG findet sich eine ähnliche Formulierung, welche auf die Wahrung von wichtigen öffentlichen Interessen[468] hinweist. Die Unterscheidung im Wortlaut „eines wichtigen Grundes im öffentlichen Interesse" einerseits und „zur Wahrung wichtiger öffentlicher Interessen" andererseits dürfte rein sprachlicher Natur sein. Denn sowohl EG 58 DSRL als auch EG 112 (ex EG 87) DSGVO nennen als Beispiele für das Vorliegen eines wichtigen öffentlichen Interesses i. S. d. DSRL bzw. eines wichtigen Grundes, der im öffentlichen Interesse liegt i. S. d. DSGVO, den Datenaustausch zwischen Steuer- oder Zollverwaltungen oder zwischen Diensten, die für soziale Sicherheit zuständig sind. Darüber hinaus erwähnt EG 112 (ex EG 87) DSGVO ferner den Datenaustausch zwischen Wettbewerbsbehörden, Finanzaufsichtsbehörden und Diensten, die für Angelegenheiten der öffentlichen Gesundheit zuständig sind, als solche Gründe.

Art. 49 Abs. 4 (ex Art. 44 Abs. 5) DSGVO verlangt, dass das öffentliche Interesse i. S. d. Art. 49 Abs. 1 UAbs. 1 lit. d (ex Art. 44 Abs. 1 lit. d) DSGVO vom Unionsrecht oder dem mitgliedstaatlichen Recht *anerkannt* sein muss, d. h. das öffentliche Interesse muss nicht in einer Sammelnorm zur Aktivierung der Öffnungsklausel festgelegt sein. Eine konkrete Benennung der öffentlichen Interessen, aufgrund derer eine Übermittlung in Drittstaaten möglich ist, wäre insofern möglich und würde Rechtssicherheit für die Normadressaten schaffen. Im Übrigen erstreckt sich die Öffnungsklausel nur auf die Konkretisierung des *öffentlichen Interesses*. Sie lässt keinen Spielraum, um die Vorgaben des Art. 49 Abs. 1 UAbs. 1 lit. d (ex Art. 44 Abs. 1 lit. d)

[468] Vgl. Art. 26 Abs. 1 lit. d Var. 1 RL 95/46/EG: „the transfer is necessary (…) on important public interest grounds (…)".

DSGVO selbst zu modifizieren oder zu konkretisieren. Da 49 Abs. 1 UAbs. 1 lit. d (ex Art. 44 Abs. 1 lit. d) DSGVO identisch mit § 4c Abs. 1 S. 1 Nr. 4 Alt. 1 BDSG ist, und die Aufrechterhaltung wohl keinen Verstoß gegen das Wiederholungsverbot darstellt (da hier ja eine Öffnungsklausel vorliegt), wäre eine Aufrechterhaltung zwar möglich. Sie ist jedoch nicht erforderlich, um das bestehende Datenschutzniveau zu erhalten. Eine Streichung ist daher empfehlenswert. Damit könnte die Norm auch insgesamt gestrichen werden.

§ 4c BDSG	**Korrespondierende Norm in der DSG-VO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 S. 1 Nr. 1–3; Nr. 4 Alt. 2; Nr. 5	Art. 49 Abs. 1 UAbs. 1 lit. a-c; lit. e-f (ex Art. 44 Abs. 1 lit. a-c; lit. e-f)	Streichen	Die Normen sind identisch. Eine Aufrechterhaltung ist durch keine Öffnungsklausel gedeckt und auch nicht nötig, um das bestehende Datenschutzniveau zu erhalten.
Abs. 1 S. 1 Nr. 4 Alt. 1	Art. 49 Abs. 1 UAbs. 1 lit. d (ex Art. 44 Abs. 1 lit. d), Abs. 4 (ex Abs. 5)	Streichen möglich; Beibehalten in bestehender Form oder Modifikation ebenfalls möglich	Die Normen sind identisch. Eine Aufrechterhaltung ist nicht nötig, um das bestehende Datenschutzniveau zu erhalten. Eine konkrete Benennung der öffentlichen Interessen ist möglich, aber nicht nötig.
Abs. 1 S. 1 Nr. 6	Art. 49 Abs. 1 UAbs. 1 lit. g (ex Art. 44 Abs. 1 lit. g)	Streichen	Die Normen sind identisch. Eine Aufrechterhaltung ist von der Öffnungsklausel nicht umfasst und ist nicht nötig, um das bestehende Datenschutzniveau zu erhalten.
Abs. 1 S. 2	-	Streichen	Wegen der Streichung von Abs. 1 S. 1 auch Streichung von Abs. 1 S. 2.
Abs. 2	Art. 46, 47 (ex Art. 42, 43)	Streichen	Die Bestimmungen über die Übermittlung aufgrund von geeigneten Garantien bzw. verbindlicher unternehmensinterner Vorschriften sind abschließend in Art. 46 bzw. 47 (ex Art. 42 bzw. Art. 43) DSGVO geregelt und enthalten keine Öffnungsklauseln für Mitgliedstaaten.
Abs. 3	-	Streichen	Aufgrund der Streichung von § 4c Abs. 2 BDSG, muss § 4c Abs. 3

			BDSG, der auf § 4 Abs. 2 S. 1 BDSG verweist, gestrichen werden.

§ 4d: Meldepflicht

§ 4d BDSG begründet für automatisierte Verarbeitungen öffentlicher und nicht-öffentlicher Stellen eine Meldepflicht. Sie setzt insbesondere die Regelungen des Art. 20 Abs. 1 RL 95/46/EG um. Von dem Regelungskonzept der Meldepflicht rückt die Datenschutz-Grundverordnung ab. Sie sieht vielmehr nunmehr in Art. 35 (ex Art. 33) DSGVO eine Datenschutz-Folgenabschätzung für bestimmte Fälle vor,[469] sowie eine Pflicht zur vorherigen Konsultation alleine in besonders gelagerten Fällen (Art. 36 DSGVO). Diese Regelungen ersetzen auch die Vorabkontrolle in § 4d Abs. 5 BDSG; die Regelungen des § 4d BDSG sind nunmehr obsolet.[470] Den Terminus „Meldung" gebraucht die Datenschutz-Grundverordnung nunmehr alleine in Art. 33 DSGVO, der die Pflicht des Verantwortlichen zur Information der Aufsichtsbehörde im Falle einer Verletzung des Schutzes personenbezogener Daten regelt.

§ 4d BDSG	**Korrespondierende Norm in der DSG-VO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	Art. 35 (ex Art. 33), Art. 36 Abs. 1 (ex Art. 34 Abs. 2)	Streichen; stattdessen ggf. Regelung zum Gebrauchmachen von der Öffnungsklausel des Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO	Abs. 1 regelt lediglich die Meldepflicht für Verfahren automatisierter Verarbeitungen; gemäß EG 89 (ex EG 70) soll dieses mit bürokratischem Aufwand verbundene Verfahren abgeschafft werden. Laut EG 90 (ex EG 70a) sollten in Fällen erhöhter Risiken für die Rechte Betroffener vielmehr Folgenabschätzungen durchgeführt werden.

[469] Von ihr kann der nationale Gesetzgeber unter bestimmten Voraussetzungen absehen, soweit er von seiner Regelungsbefugnis zur Wahrnehmung öffentlicher Aufgaben bzw. zur Erfüllung einer rechtlichen Verpflichtung nach Art. 6 UAbs. 1 lit. c oder e DSGVO Gebrauch macht – Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO. Dazu S. 89.
[470] *Martini*, in: Paal/Pauly (Hrsg.), DSGVO, 2016, Art. 35, Rn. 74 ff.

Abs. 2	Art. 35, Art. 36 Abs. 1 (ex Art. 33, Art. 34 Abs. 2)	Streichen	Dito
Abs. 3	Art. 35, Art. 36 Abs. 1 (ex Art. 33, Art. 34 Abs. 2)	Streichen	Dito
Abs. 4	Art. 35, Art. 36 Abs. 1 (ex Art. 33, Art. 34 Abs. 2)	Streichen	Dito
Abs. 5	Art. 35, Art. 36 Abs. 5 (ex Art. 34 Abs. 7a)	Grds. streichen; ggf. als Konsultations- und Genehmigungspflicht nach Art. 36 Abs. 5 fortführen	Die Vorabkontrolle ist in ihrer kategorischen Art nicht mit dem risikobasierten Ansatz des Art. 36 Abs. 1 DSGVO vereinbar, und wird grds. vollständig durch Art. 35 DSGVO ersetzt. Möglich ist ein Gebrauchmachen von der (fakultativen) Öffnungsklausel des Art. 36 Abs. 5 DSGVO und damit die Etablierung einer Konsultations- und Genehmigungspflicht auf die dort genannten Themen. Hiermit verbindet sich aber eine Ausweitung der Bürokratiekosten.
Abs. 6	Art. 35, Art. 36 Abs. 5 (ex Art. 34 Abs. 7a)	Streichen	Macht der Mitgliedstaat von Art. 36 Abs. 5 DSGVO Gebrauch, ist die Aufsichtsbehörde zuständig für die Konsultation und Genehmigung. Eine Abweichung hiervon ist nicht möglich. Nach § 4d Abs. 5 BDSG und Abs. 6 S. 1 DSGVO ist der Datenschutzbeauftragte für die Vorabkontrolle zuständig. Diese entfällt durch Art. 35 DSGVO: Für die Datenschutz-Folgenabschätzung ist nunmehr der Verantwortliche – also die Unternehmensleitung – zuständig.

§ 4e: Inhalt der Meldepflicht

§ 4e BDSG	Korrespondierende Norm in der DSG-VO	Gesetzgeberische Handlungsoption	Begründung
S. 1	Art. 35, Art. 36 Abs. 1 (ex Art. 33, Art. 34 Abs. 2)	Streichen	Siehe Begründung zu § 4d Abs. 1 – 4.
S. 2	Art. 35, Art. 36 Abs. 1 (ex Art. 33, Art. 34 Abs. 2)	Streichen	Siehe Begründung zu § 4d Abs. 1 – 4.

§ 4f: Beauftragter für den Datenschutz

§ 4f enthält differenzierte Regelungen zur Institution des Datenschutzbeauftragten. Ihm kommt nach der Wahrnehmung Vieler eine Schlüsselrolle bei der „Erfolgsgeschichte" des Datenschutzes in Deutschland zu.[471] Dieses Konzept ist eine Ausprägung der datenschutzrechtlichen *Selbstkontrolle* der datenverarbeitenden Stelle.

Abs. 1 BDSG bestimmt, welche datenverarbeitenden Stellen einen Datenschutzbeauftragten implementieren müssen: alle öffentlichen Stellen sowie nicht-öffentliche Stellen ab einer bestimmten Größe oder abhängig von der Art der Datenverarbeitung, in jedem dieser Fälle schriftlich und spätestens innerhalb eines Monats. Die weiteren Absätze legen die praxisrelevanten Qualifikationsanforderungen an den Datenschutzbeauftragten (Abs. 2), seine Stellung und Unabhängigkeit, mithin den Status (Abs. 3) sowie Verschwiegenheitspflicht und Geheimnisschutz (Abs. 4, 4a) fest. Abs. 5 S. 2 macht den Datenschutzbeauftragten zum „Anwalt der Betroffenen": Mit dem Recht Betroffener zur Anrufung des Datenschutzbeauftragten geht dessen Pflicht einher, das Anliegen zu prüfen und erforderlichenfalls Maßnahmen zu ergreifen.[472] Die Aufgaben des Datenschutzbeauftragten regelt der Gesetzgeber –

[471] *Moos*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 4f BDSG, Rn. 3.
[472] *Gola/Klug/Körffer* (Fn. 104), § 6a, Rn. 57.

abgesehen von § 4f Abs. 5 S. 2 – in einer gesonderten Vorschrift (§ 4g). Über Abs. 3 S. 7 und Abs. 5 S. 1 ist umgekehrt auch die verantwortliche Stelle verpflichtet, den Datenschutzbeauftragten zu unterstützen, indem sie ihm Fortbildungen ermöglicht und die für seine Aufgabenwahrnehmung erforderlichen Mittel bereitstellt.

Mit dem Konzept des betrieblichen Beauftragten für den Datenschutz hat Deutschland grundsätzlich gute Erfahrungen gesammelt. Den meisten anderen EU-Ländern ist es bisher fremd. Eben dieses Konzept greift die Datenschutz-Grundverordnung in ihren Art. 37 ff. (ex Art. 35 ff.) auf und zont es auf die Unionsebene hoch.

Art. 37 (ex Art. 35) regelt die Pflicht zur Bestellung eines Datenschutzbeauftragten; im Gegensatz zu § 4f Abs. 1 BDSG enthält die Datenschutz-Grundverordnung keinen Hinweis darauf, dass dies *schriftlich* zu erfolgen hat, jedenfalls sind aber die Kontaktdaten des Datenschutzbeauftragten zu veröffentlichen. Art. 38 (ex Art. 36) gestaltet die Stellung des Datenschutzbeauftragten näher aus und legt der verarbeitenden Stelle die Pflicht auf, diesen zu unterstützen. Wie im BDSG (§ 4g) regelt auch die Datenschutz-Grundverordnung die Aufgaben des Datenschutzbeauftragten in einer gesonderten Vorschrift (Art. 39 [ex Art. 37]).

Die Regelungen des deutschen Rechts können zur Ausfüllung des verbleibenden nationalen Regelungsspielraums womöglich – in modifizierter Form – beibehalten werden.[473] Unionsrechtlicher Hintergrund ist die Öffnungsklausel des Art. 37 Abs. 4 Hs. 2 (ex Art. 35 Abs. 4 Hs. 2) DSGVO.[474] Denkbar erscheint es prima facie, die nationalen Regelungen zum Datenschutzbeauftragten für den rechtsanwendenden Bürger in den Kontext einer Vollregelung zu stellen, welche die Vorschriften als in sich geschlossenes und konsistentes Regime verständlich macht. Allerdings erstreckt sich die Öffnungsklausel des Unionsrechts grundsätzlich nur auf den Anwendungsbereich der Verpflichtung, einen Datenschutzbeauftragten zu bestellen, nicht aber auf die Stellung und Aufgaben des Datenschutzbeauftragten (Art. 38 und 39 [ex Art. 36 und 37] DSGVO).[475] Kein Konflikt der bisherigen Regelungen zum Unionsrecht

[473] In diese Richtung auch *Voßhoff/Hermerschmidt*, PinG 2016, 56 (58).
[474] Dazu S. 95.
[475] Dazu auch S. 99

besteht grundsätzlich dann, wenn eine nationale Vorschrift in ihrer Anwendung nicht in einen Widerspruch zu den Vorgaben der unionsrechtlichen Vorgabe der Verordnung tritt, weil sie diese – ohne das Regelungsziel der Verordnung zu verletzen – nur ergänzt.[476]

§ 4f BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1 S. 1 u. 2	Art. 37 (ex Art. 35); Art. 2 Abs. 1	Modifizieren, Vorschlag: Ergänzung um den Passus „soweit nicht bereits eine Pflicht zur Benennung eines Datenschutzbeauftragten nach Art. 37 Abs. 1 (ex Art. 35 Abs. 1) Datenschutzgrundverordnung besteht…“	Art. 37 Abs. 4 Hs. 2 (ex Art. 35 Abs. 4 Hs. 2) DSGVO lässt den Mitgliedstaaten bei der Implementierung von Datenschutzbeauftragten als Kontrollstellen einen Ergänzungsspielraum. Teilweise ist § 4f Abs. 1 BDSG enger, teilweise weiter als Art. 37 Abs. 1 (ex Art. 35 Abs. 1) DSGVO: § 4f Abs. 1 S. 1 BDSG erfasst bspw. nur die automatisierte Datenverarbeitung. Art. 2 Abs. 1 DSGVO aber zusätzlich auch die nicht-automatisierte Verarbeitung personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen. Als Ergänzung zu den Regelungen des Art. 37 (ex Art. 35) DSGVO darf die Regelung des Abs. 1 S. 1 und 2 aufgrund der Öffnungsklausel des Unionsrechts in modifizierter Form erhalten bleiben.
Abs. 1 S. 3	Art. 37 (ex Art. 35)	Dito	Dito
Abs. 1 S. 4	Art. 37 (ex Art. 35)	Streichen	In dem Pflichtbereich des Art. 37 Abs. 1 (ex Art. 35 Abs. 1) DSGVO ist die Ausnahmere-

[476] Ebenso auch *Roßnagel*, in: Deutscher Bundestag, Ausschuss Digitale Agenda, Ausschussdrucksache 18(24)94, S. 5 f: „Soweit kein Widerspruch vorliegt, sondern nur eine Präzisierung unbestimmter Rechtsbegriffe, eine Konkretisierung ausfüllungsbedürftiger Vorgaben oder die Ergänzung von unvollständigen Regelungen oder die Schließung von Regelungslücken, ohne das Regelungsziel der Verordnung zu verletzten, kann die mitgliedstaatliche Regelung weiter anwendbar bleiben, auch wenn ihr Wortlaut sich von der Regelung in der Verordnung unterscheidet.“

			gelung des § 4f Abs. 1 S. 4 BDSG (bei lediglich neun permanent mit der Datenverarbeitung befassten Personen in nicht-öffentlichen Stellen) mit der in der DSGVO geregelten Pflicht zur Benennung eines Datenschutzbeauftragten *unabhängig von der Zahl der mit der Verarbeitung beschäftigten Personen* nicht vereinbar. Jenseits dieses Pflichtbereichs kann die Vorschrift aber (soweit rechtspolitisch erwünscht) aufrechterhalten bleiben.
Abs. 1 S. 5	Art. 37 Abs. 1 lit. a, Abs. 3 (ex Art. 35 Abs. 1 lit. a, Abs. 3)	Modifizieren	Art. 37 Abs. 3 (ex Art. 35 Abs. 3) DSGVO regelt bereits präzise die Möglichkeit, für mehrere Stellen oder Behörden einen *gemeinsamen* Datenschutzbeauftragten zu bestellen und erweitert diese Option. Zur Klarstellung kann es sinnvoll sein, diese Möglichkeit auch für den Bereich ausdrücklich zu erwähnen, in dem Deutschland von seiner Regelungsmacht des Art. 37 Abs. 4 (ex Art. 35 Abs. 4) DSGVO Gebrauch macht.
Abs. 1 S. 6	Art. 37 (ex Art. 35)	Modifizieren	Die Norm kann aufgrund der Öffnungsklausel des Art. 37 Abs. 4 Hs. 2 (ex Art. 35 Abs. 4 Hs. 2) DSGVO bestehen bleiben, soweit sie weitere nicht-öffentliche Stellen zur Bestellung eines Datenschutzbeauftragten verpflichtet. Im Hinblick auf Art. 2 Abs. 1 DSGVO ist eine Ausweitung auf nicht-automatisierte Verarbeitungen personenbezogener Daten, die in einer Datei gespeichert sind oder gespeichert werden sollen, erwägenswert, um ein einheitliches Schutzniveau zu gewährleisten.
Abs. 2	Art. 37 Abs. 5 (ex Art. 35 Abs. 5)	Streichen; beibehalten u. U. möglich	Die deutsche Norm präzisiert die – allgemein gehaltenen – Anforderungen des Art. 37 Abs. 5 (ex Art. 35 Abs. 5) DSGVO an die *Qualifikation* des Datenschutzbeauftragten und kann so Rechtsunsicherheit vorbeugen. Den Mitgliedstaaten steht hinsichtlich des Spielraums, den ihnen die Öffnungsklausel des Art. 37 Abs. 4 (ex Art. 35 Abs. 4) DSGVO sub specie des „Ob“ einräumt, womöglich in begrenztem Umfang die Befugnis zu, die inhaltlichen Anforderungen an die Personen, also das „Wie“, zu präzisieren. Das Unions-

			recht nimmt seinen Anwendungsvorrang bei diesem Verständnis insoweit zurück. Die besseren Gründe sprechen aber wohl für die gegenteilige Sichtweise.
Abs. 3 S. 1 (Stellung)	Art. 38 Abs. 3 S. 3 (ex Art. 36 Abs. 3 S. 3)	Streichen; beibehalten u. U. möglich	Die Vorschrift kann allenfalls als Ergänzung und Konkretisierung des Art. 38 Abs. 3 S. 3 (ex Art. 36 Abs. 3 S. 3) DSGVO mit Blick auf die Öffnungsklausel des Art. 37 Abs. 4 (ex Art. 35 Abs. 4) DSGVO im Interesse einer in sich konsistenten und verständlichen Regelung bestehen bleiben.
Abs. 3 S. 2 (Weisungsfreiheit)	Art. 38 Abs. 3 S. 1 (ex Art. 36 Abs. 3 S. 1)	Streichen oder modifizieren: Bezugnahme auf Art. 38 (ex Art. 36) DSGVO	Die Norm begründet die Weisungsfreiheit des Datenschutzbeauftragten („ist … weisungsfrei“). Art. 38 Abs. 3 S. 1 (ex Art. 36 Abs. 3 S. 1) DSGVO ist etwas weiter als das bisherige deutsche Recht formuliert und regelt die Rechtsstellung grundsätzlich unmittelbar. Eine nationale Regelung ist allenfalls unter Rückgriff auf eine Regelungsfreiheit für das „Wie“ zulässig, die sich womöglich mittelbar aus der Freiheit des „Ob“ (Art. 37 Abs. 4 S. 1 DSGVO) ergibt. Die nationale Regelungsbefugnis des Art. 38 Abs. 5 DSGVO (Geheimhaltung und Vertraulichkeit) ist mittelbar berührt. Auf sie zu rekurrieren, hieße jedoch den unionsrechtlichen Regelungsanspruch des Art. 38 Abs. 3 S. 1 DSGVO nationalstaatlich zu unterwandern.
Abs. 3 S. 3 (Benachteiligungsverbot)	Art. 38 Abs. 3 S. 2 (ex Art. 36 Abs. 3 S. 2)	Streichen; beibehalten u. U. möglich	§ 4f Abs. 3 S. 2 BDSG deckt sich inhaltlich mit dem Regelungsinhalt des Art. 38 Abs. 3 S. 2 (ex Art. 36 Abs. 3 S. 2) DSGVO („nicht abberufen oder benachteiligt“). Das macht die deutsche Regelung noch nicht zwingend entbehrlich oder im Hinblick auf das Wiederholungsverbot unzulässig, wie EG 8 (ex EG 6a) deutlich macht. Sie stellt insbesondere die nationalen Regelungen zum Datenschutzbeauftragten für den rechtsanwendenden Bürger in einen Regelungskontext, der die Regelungen in sich als geschlossenes Regime verständlich macht, und kann als solche u. U. beibehalten werden.

Abs. 3 S. 4 – 6	Art. 38 Abs. 3 S. 2 (ex Art. 36 Abs. 3 S. 2)	Streichen; beibehalten u. U. möglich	Art. 38 (ex Art. 36) DSGVO regelt in Abs. 3 S. 2, dass der Datenschutzbeauftragte „*wegen* der Erfüllung seiner Aufgaben nicht abberufen“ werden darf. Der Datenschutzbeauftragte genießt keinen absoluten Kündigungsschutz. Eine Kündigung aus anderen Gründen als der „Erfüllung seiner Aufgaben“ schließt die DSGVO nicht aus. Das deutsche Recht stellt in § 4f Abs. 3 S. 4 bis 6 BDSG die grundsätzliche Kündigungsfreiheit des Datenschutzbeauftragten sicher. Es ist denkbar, die Regelung im deutschen Recht als Baustein einer in sich geschlossenen Vollregelung zum Datenschutzbeauftragten aufrechtzuerhalten, die von der Öffnungsklausel Gebrauch macht. Bei sehr weitem Verständnis lässt sich die Vorschrift als Teil der mitgliedstaatlichen Regelungsbefugnis zur Sicherung der Geheimhaltung und Vertraulichkeit in Art. 38 Abs. 5 DSGVO verstehen.
Abs. 3 S. 7	Art. 38 Abs. 2 (ex Art. 36 Abs. 2)	Streichen; beibehalten u. U. möglich	Der Regelungsgehalt des Abs. 3 S. 7 ist mit demjenigen des Art. 38 Abs. 2 (ex Art. 36 Abs. 2) DSGVO identisch. Allenfalls als Teil einer in sich konsistenten Vollregelung darf der nationale Gesetzgeber diese Vorschrift in seinem Rechtsregime wiederholen.
Abs. 4 (Verschwiegenheit)	Art. 38 Abs. 5 (ex Art. 36 Abs. 4)	Beibehalten möglich	Art. 38 Abs. 5 (ex Art. 36 Abs. 4) DSGVO räumt den Mitgliedstaaten das Recht ein, die Anforderungen an die Wahrung der Geheimhaltung und Vertraulichkeit zu präzisieren. Davon macht § 4f Abs. 4 BDSG Gebrauch.
Abs. 4a (Zeugnisverweigerungsrecht)	-	Beibehalten möglich	Dito
Abs. 5	Art. 38 Abs. 2 (ex Art. 36 Abs. 2)	Beibehalten / Streichen (je nach engem oder weitem Verständnis des Wiederholungsverbots)	§ 4f Abs. 5 S. 1 BDSG deckt sich weitgehend mit dem Regelungsgehalt des Art. 38 Abs. 2 (ex Art. 36 Abs. 2) DSGVO. Ob die Vorschrift des nationalen Rechts zwingend obsolet wird, darüber lässt sich trefflich streiten. Es ist vorstellbar, sie als Teil eines in sich konsistenten Regelungsmodells für den Datenschutzbeauftragten aufrechterhalten zu

			dürfen, ohne einen Verstoß gegen das Wiederholungsverbot auszulösen.

§ 4g: Aufgaben des Beauftragten für den Datenschutz

§ 4g regelt die Aufgaben des Datenschutzbeauftragten. § 4g Abs. 1 S. 4 BDSG zählt sie beispielhaft, nicht abschließend („insbesondere“) auf. Dazu zählt das Hinwirken auf die Einhaltung der Vorschriften zum Datenschutz, die Konsultation der Aufsichtsbehörde mit der entsprechenden Beratung, die Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen sowie die Schulung der mit der Datenverarbeitung betrauten Mitarbeiter. Eine Ergänzung findet Abs. 1 in Abs. 2 S. 2, der dem Datenschutzbeauftragten auferlegt, das sog. Öffentliche Verfahrensverzeichnis jedermann verfügbar zu machen. Zusätzlich regelt § 4g auch Pflichten der verantwortlichen Stelle: Abs. 2 S. 1 betrifft die Verpflichtung zur Erstellung des sog. *internen* Verfahrensverzeichnisses, Abs. 2a die Aufgabenerfüllung bei Nichtvorhandensein eines Datenschutzbeauftragten.
Abs. 3 formuliert eine Sondervorschrift für bestimmte Typen öffentlicher Stellen im Bereich Gefahrenabwehr und Strafverfolgung. Ausweislich des EG 19 (ex EG 16) DSGVO gilt für diesen Bereich im Besonderen die entsprechende neue Richtlinie (EU) 2016/680; daneben verbleibt den Mitgliedstaaten ein großer Regelungsspielraum.
Die Datenschutz-Grundverordnung etabliert in Art. 39 (ex Art. 37) DSGVO weitreichende Regelungen zu den Aufgaben des Datenschutzbeauftragten. Sie machen die Parallelvorschriften im BDSG grundsätzlich obsolet. Die Aufrechterhaltung der nationalen Vorschriften ist allenfalls als Teil eines für Rechtsklarheit sorgenden ganzheitlichen Regelungskonzepts mit dem unionsrechtlichen Wiederholungsverbot vereinbar.

§ 4g BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 S. 1 und 2 (Hinwirkungs-	Art. 39, insb. Abs. 1 lit. b, Art. 38 Abs. 4 (ex	Streichen	Der Inhalt der Regelung ist bereits von der unmittelbar geltenden Vorschrift des Art. 39 Abs. 1 lit. b (ex Art. 37 Abs. 1 lit. b) DSGVO erfasst. Sie kann allenfalls als Teil einer in

pflicht)	Art. 37, insb. Abs. 1 lit. b, Art. 36 Abs. 2a (neu))		sich konsistenten Vollregelung erhalten bleiben (dazu auch bei § 4f).
Abs. 1 S. 3	Art. 39, Art, 38 Abs. 2 (ex Art. 37, Art. 36 Abs. 2)	Beibehalten u. U. möglich	Nach Art. 39 Abs. 1 lit. d DSGVO hat der Datenschutzbeauftragte mit der Aufsichtsbehörde zusammenzuarbeiten. Hierin liegt wohl auch das Recht begründet, sich in Zweifelsfällen an die Aufsichtsbehörde zu wenden. § 4g Abs. 1 S. 3 BDSG ist die Spiegelnorm zu § 38 Abs. 1 S. 2 BDSG, die den Aufsichtsbehörden die Aufgabe der Beratung und Unterstützung von Datenschutzbeauftragten auferlegt. Art. 57 (ex Art. 52) DSGVO enthält diese Aufgabenzuweisung an die Aufsichtsbehörden nicht in dieser Klarheit. Am ehesten ist die Beratungspflicht noch unter Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab) DSGVO zu rubrizieren. In diesem Rahmen können die Mitgliedstaaten die Beratung der Datenschutzbeauftragten als zusätzliche Befugnis nach Art. 58 Abs. 6 DSGVO festlegen.
Abs. 1 S. 4	Art. 39, Art. 38 Abs. 1(ex Art. 37, Art. 36 Abs. 2a (neu))	Streichen; beibehalten u. U. möglich	Die konkrete Aufgabenbeschreibung in S. 4 kann womöglich von einem Konkretisierungsspielraum Gebrauch machen, den Art. 39 Abs. 1 (ex Art. 37 Abs. 1) i. V. m. Art. 37 Abs. 4 DSGVO den Mitgliedstaaten – bei sehr weitem Verständnis – für einen ihnen u. U. verbleibenden Regelungsbereich einräumt („zumindest folgende Aufgaben“). Die besseren Gründe sprechen aber dagegen.
Abs. 2 (sog. Verfahrensverzeichnis)	Art. 30 (ex Art. 28), vgl. auch EG 82 (ex EG 65)	Streichen	§ 4g Abs. 2 BDSG nimmt auf die Dokumentationspflichten der Meldepflicht Bezug, die nach dem neuen Rechtsregime entfallen werden. Art. 30 (ex Art. 28) DSGVO legt dem Verarbeiter zwar die Verpflichtung auf, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. Die Pflicht, dieses Dritten zur Verfügung zu stellen, beschränkt die DSGVO in ihrem Art. 30 Abs. 4 (ex Art. 28 Abs. 3) DSGVO aber auf die Aufsichtsbehörde. Eine

			Ausweitung dieser Pflicht ist mit der DSGVO nur dann in Einklang zu bringen, wenn der Datenschutzbeauftragte auch als „Aufsichtsbehörde“ in diesem Sinne einzustufen ist oder man sie als Pflicht unmittelbar aus Art. 38 Abs. 1 u. 2 DSGVO herausliest. In beiden Fällen ist die Pflicht unmittelbar unionsrechtlich ohne mitgliedstaatlichen Regelungsspielraum geregelt.
Abs. 2a		Beibehalten u. U. möglich	Die DSGVO sieht als Kategorie begleitender Überwachung ordnungsgemäßen betrieblichen Datenschutzes als solche nur den Datenschutzbeauftragten vor. In Art. 47 Abs. 2 lit. h (ex Art. 43 Abs. 2 lit. h) DSGVO deutet sich u. U. zumindest eine Offenheit für andere Formen einer Beauftragung mit der Überwachung der Einhaltung verbindlicher unternehmensinterner Datenschutzvorschriften an. Art. 37 Abs. 4 (ex Art. 35 Abs. 4) DSGVO gesteht den Mitgliedstaaten aber das Recht zu, den Umfang selbst zu bestimmen, in dem sie Unternehmen die Bestellung von unternehmenseigenen Beauftragten für den Datenschutz festschreiben wollen. Die DSGVO versteht den Datenschutzbeauftragten zwar als formelles Amt mit korrespondierender Ernennung, geht dabei von einem funktionsbezogenen Aufgabenverständnis aus. Das streitet dafür, dass die Mitgliedstaaten ihren nicht-öffentlichen Stellen statt eines Datenschutzbeauftragten womöglich auch andere Formen einer unternehmensinternen Überprüfung der Einhaltung von Datenschutzbestimmungen auferlegen können.
Abs. 3	EG 19 (ex EG 16) sowie die neue RL (EU) 2016/80	Mit den Vorgaben der neuen Richtlinie für den Datenschutz bei Gefahrenabwehr- und Strafverfol-	Die Vorschrift enthält eine Sonderregelung für gewisse Typen öffentlicher Stellen (Polizei, Staatsanwaltschaften, BND, Verfassungsschutz), denen im Sinne einer effektiven Gefahrenabwehr geringere datenschutzrechtliche und bürokratische Pflichten auferlegt werden sollen. Die Veröffentlichungspflicht (§ 4g Abs. 2 S. 2: „macht die Angaben … jedermann … verfügbar“) könnte laufende

		gungsbehörden abgleichen	Ermittlungen gefährden oder seinerseits Persönlichkeitsrechte verletzen und damit die Intention des Datenschutzes konterkarieren. EG 19 (ex EG 16) stellt daher klar, dass den Mitgliedstaaten auf diesem Gebiet ein Regelungsspielraum verbleibt. Somit gilt: Grundsätzlich enthält die DSGVO keine Regelungen für die Tätigkeiten dieser Behörden/ Stellen. Stattdessen gilt die neue RL (EU) 2016/80. Die Mitgliedstaaten können diesen Bereich eigenständig ausgestalten (vgl. EG 19 S. 3-5 [ex EG 16 S. 3-5]). Die DSGVO gilt aber dort, wo diesen Behörden andere Aufgaben auferlegt werden und die Datenverarbeitungsvorgänge in den Bereich der VO fallen.

§ 5: Datengeheimnis

Das Datengeheimnis verbietet denjenigen Personen, die dem Datenverarbeiter oder dem Auftragsdatenverarbeiter unterstellt sind, personenbezogene Daten unbefugt zu verarbeiten. Die Vorschrift dehnt die datenschutzrechtlichen Pflichten auf die dem Verantwortlichen unterstellten Personen aus; vielfach ergibt sich diese Pflicht schon aus vertraglichen Verhältnissen zwischen diesen Personengruppen oder aus anderen gesetzlichen Vorschriften.[477]
Das neue Unionsrecht hält dem Datengeheimnis ähnelnde Regelungen vor, die kraft ihres Anwendungsvorrangs das bisherige nationale Recht verdrängen. Das allgemeine Verbot, Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen, ergibt sich aus Art. 6 Abs. 1 DSGVO. Die den Verantwortlichen und den Auftragsverarbeiter unterstellten Personen binden Art. 28 Abs. 3 lit. a und Art. 29 DSGVO an dessen Weisung (eine vertragliche Gewährleistungspflicht zur Sicherung der Vertraulichkeit begründet Art. 28 Abs. 3 lit. b DSGVO[478]; vgl. auch Art. 32 Abs. 4 DSGVO). Eine Ausnahme von dieser Regel enthält die Datenschutz-Grundverordnung, wenn die unterstellten Personen einer Verarbeitungspflicht unterworfen sind. Dies folgt aus den (unech-

[477] *Herbst*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 5 BDSG, Rn. 1.
[478] *Martini*, in: Paal/Pauly (Hrsg.), DSGVO, 2016, Art. 28, Rn. 43.

ten) Öffnungsklauseln des Art. 29 (ex Art. 27)[479] und des Art. 32 Abs. 4 (ex Art. 30 Abs. 2b) DSGVO[480], wonach die Verarbeitungspflicht auch aus dem mitgliedstaatlichen Recht stammen kann. Dann gilt aber auch nach § 5 S. 1 BDSG das Datengeheimnis nicht, da die Personen in solchen Fällen gerade zur Verarbeitung befugt sind.

§ 5 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
S. 1	Art. 28 Abs. 3 UAbs. 1 S. 2 lit. b (ex Art. 26 Abs. 2 lit. b), 29 (ex Art. 27), 32 Abs. 4 (ex Art. 30 Abs. 2b) i. V. m. Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO	Streichen	§ 5 S. 1 BDSG legt eine dem Art. 32 Abs. 4 (ex Art. 30 Abs. 2b) und Art. 29 (ex Art. 27) DSGVO entsprechende Verpflichtung fest: Art. 29 (ex Art. 27) DSGVO erlaubt denjenigen Personen, die den Verantwortlichen oder den Auftragsdatenverarbeitern unterstellt sind, eine Verarbeitung personenbezogener Daten nur auf Weisung des Verantwortlichen. Spiegelbildlich drückt sich darin ein Verbot aus, nicht unbefugt Daten zu verarbeiten.481
S. 2	Art. 28 Abs. 3 UAbs. 1 S. 2 lit. b (ex Art. 26 Abs. 2 lit. b) i. V. m. Art. 6 Abs. 1 UAbs. 1	Streichen	§ 5 S. 2 ist weitgehend deklaratorisch.482 Denn die Verpflichtung auf das Datengeheimnis bzw. das Verbot unbefugter Datenverarbeitung ergibt sich schon aus S. 1. S. 2 bekräftigt die formelle Absicherung der Verpflichtungen, die sich aus dem Datengeheimnis ergeben. Die Regelung deckt sich weitgehend mit den unionsrechtlichen Vorgaben, namentlich der Pflicht des Auftragsda-

[479] Dazu S. 85.
[480] Dazu S. 88.
[481] *Martini*, in: Paal/Pauly (Hrsg.), DSGVO, 2016, Art. 29, Rn. 20; a. A. wohl *Herbst* (Fn. 477), § 5 BDSG, Rn. 35.
[482] Siehe dazu *Plath*, in: ders. (Hrsg.), BDSG, 2013, § 5, Rn. 11.

	lit. c bzw. e DSGVO		tenverarbeiters, die konkreten mit der Verarbeitung betrauten Personen auf die Verschwiegenheit zu verpflichten (Art. 28 Abs. 3 UAbs. 1 S. 2 lit. b [ex Art. 26 Abs. 2 lit. b] DSGVO) sowie der Sicherstellungspflicht des Art. 32 Abs. 4 (ex Art. 30 Abs. 2b) DSGVO. Der Regelung des § 5 S. 2 BDSG bedarf es insofern nicht zwingend. Vor allem ist keine Öffnungsklausel ersichtlich, auf deren Grundlage eine solche Pflicht des Verantwortlichen und Auftragsverarbeiters erlassen werden könnte.
S. 3	Art. 28 Abs. 3 UAbs. 1 S. 2 lit. b (ex Art. 26 Abs. 2 lit. b) i. V. m. Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO	Streichen	Die Fortgeltung des Datengeheimnisses folgt an sich bereits – ratione materiae – aus Art. 6 Abs. 1 DSGVO bzw. aus dem Wegfall der die Tätigkeit legitimierenden Weisung (vgl. auch 29, Art. 32 Abs. 4) sowie mittelbar der Nachsorgepflicht eines Auftragsverarbeiters (Art. 28 Abs. 3 lit. g). Ob S. 3 aus Klarstellungsgründen fortbestehen kann, ist mehr als zweifelhaft. Zwar können die Gefahren für die Persönlichkeitsrechte Betroffener auch nach Beendigung eines Beschäftigungsverhältnisses fortbestehen, wenn der jeweilige Mitarbeiter weiterhin Zugriff auf die Daten hat. Eine Konkretisierung des unionsrechtlichen Normgehalts wäre insofern durchaus sinnvoll. Gleichwohl besteht hierfür keine Öffnungsklausel.

§ 6: Rechte des Betroffenen

§ 6 BDSG steht im Zusammenhang mit den Betroffenenrechten gemäß den §§ 19 – 21[483] und §§ 33 – 35 BDSG[484]. Da die Datenschutz-Grundverordnung hinsichtlich des Regelungsgehalts des § 6 BDSG keinen Raum für eine mitgliedstaatliche Regelung lässt, ist die Streichung der Norm angezeigt.

[483] Dazu S. 401.
[484] Dazu S. 451.

§ 6 BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1 (Unabdingbarkeit)	-/Art. 12 ff.	Streichen	Regelung nicht erforderlich. Die DSGVO sieht keine Abbedingung der Betroffenenrechte durch Einwilligung vor. Eine Einwilligung ist nur für die Legitimation der Datenverarbeitung in Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO vorgesehen, nicht aber in Bezug auf die Betroffenenrechte (auch nicht in Art. 23 DSGVO). Im Gegenschluss ist eine solche freiwillige Abdingbarkeit daher nicht möglich. Ihr Ausschluss muss daher nicht eigens geregelt werden.
Abs. 2 (Verbunddateien)		Streichen	Umfassende Regelung in der DSGVO ohne Öffnungsklausel. Die Sätze 4 und 5 fallen in den Anwendungsbereich der Datenschutzrichtlinie (EU) 2016/80.
Abs. 3 (Zweckbindung)	-	Wohl streichen	Zwar findet sich in der DSGVO keine diesbezügliche explizite Regelung. Aber der Regelungsgehalt ergibt sich aus Art. 6 DSGVO, der für jede Verarbeitung einen Legitimationsgrund verlangt. Die Verarbeitung von Daten zur Erfüllung der Pflichten des Verarbeiters im Rahmen der Betroffenenrechte ist eine Verarbeitung i. S. d. Art. 6 Abs. 1 DSGVO, so dass ein entsprechender Grund vorliegen muss, der aber gerade nur in der Erfüllung der Pflichten im Zusammenhang mit den Betroffenenrechten gegeben ist. Andernfalls läge eine Zweckänderung nach Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) DSGVO vor, die dort unter angemessene Restriktionen gestellt wird. Daher ist wohl eine Streichung der Bestimmung indiziert.

§ 6a: Automatisierte Einzelentscheidung

§ 6a BDSG setzt automatisierten Einzelentscheidungen Grenzen. Die Norm verbietet diese – sofern hiermit für den Betroffenen eine rechtliche Folge oder eine erhebliche Beeinträchtigung einhergeht – grundsätzlich.

Den Regelungsgehalt des § 6a BDSG übernimmt nunmehr weitgehend Art. 22 (ex Art. 20) DSGVO. Das muss nicht unbedingt heißen, dass der Regelungsgehalt des § 6a BDSG in seiner Gänze einer Streichung anheimfällt. Zwar untersagt das Unionsrecht im Interesse der Normenklarheit und des Schutzes des unionsrechtlichen Anwendungsvorrangs den Mitgliedstaaten für Verordnungen grundsätzlich gleichlautende Regelungen im nationalen Recht. In Übereinstimmung mit der Rechtsprechung des EuGH gestattet die DSGVO den Mitgliedstaaten aber, Bestandteile der Verordnung in ihre jeweiligen nationalen Rechtsvorschriften aufzunehmen – dies unter drei Voraussetzungen: Die Wiederholung muss erforderlich sein, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen. Wiederholungen sind auch nur im Zusammenhang mit Öffnungsklauseln zulässig, welche Präzisierungen oder Einschränkungen der DSGVO durch das Recht der Mitgliedstaaten zulassen.

a. Abs. 1 S. 1: Verbotscharakter

Entscheidungen, welche für den Betroffenen rechtliche Folgen begründen oder ihn erheblich beeinträchtigen, dürfen nach der normativen Wertung des § 6a Abs. 1 S. 1 BDSG nicht lediglich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt sein.

Der Wortlaut des Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO scheint dem Betroffenen demgegenüber prima facie lediglich einen Anspruch zu gewähren, nicht ausschließlich einer automatisierten Einzelentscheidung ausgesetzt zu sein („Die betroffene Person hat das Recht“). Auch seine systematische Stellung als Teil des Kapitels III „Rechte der betroffenen Person“ weist ihn als subjektives Recht des Einzelnen aus. Eine Ausgestaltung als Anspruch macht seine Durchsetzung immer vom Willen der berechtigten Betroffenen abhängig, auch tatsächlich – ggf. prozessual – gegen die Verarbeitung vorzugehen. Bestimmte Geschäftsmodelle könnten dann darauf vertrauen, dass Betroffene gerade vor der Anspruchsgeltendmachung zurückschrecken. Dem durch die Datenschutz-Grundverordnung intendierten effektiven Schutz personenbezogener Daten und der Entscheidungsfreiheit Betroffener über die Preisgabe jener Daten entspricht es aber am ehesten, in Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO ein Verbot zu sehen, wie es § 6a Abs. 1 S. 1 BDSG

bereits formuliert. Insoweit lässt sich § 6a Abs. 1 S. 1 BDSG als Präzisierung des Verbotscharakters verstehen.
Ob eine Beibehaltung des § 6a Abs. 1 S. 1 BDSG in seiner bisherigen Form nach dieser Lesart gegen das Wiederholungsverbot verstieße, ist unklar. Die isolierte Betrachtung der mitgliedstaatlichen Vorschrift legt eine Unvereinbarkeit mit der Datenschutz-Grundverordnung nahe, da die Norm inhaltlich nur Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO wiedergibt. Es besteht die Gefahr, dass die unmittelbare Anwendung der Verordnungsnorm verborgen bliebe.[485] Der EuGH erlaubt inhaltsgleiche Wiederholungen im nationalen Recht grundsätzlich nur, wenn ein vielschichtiges Regelungsgeflecht[486] im Mehrebenensystem besteht.[487] Eine Normwiederholung kann insbesondere im Interesse der Rechtsklarheit geboten sein – vor allem um den Regelungszusammenhang mit den Ausnahmebestimmungen klarzustellen, welche die Öffnungsklausel des Art. 22 Abs. 2 lit. b (ex Art. 20 Abs. 1a lit. b) DSGVO eröffnet. Eine solche wiederholende Neufassung des § 6a Abs. 1 S. 1 BDSG könnte etwa lauten: „Es ist verboten, im Wege ausschließlich automatisierter Verarbeitung – einschließlich Profiling – Entscheidungen zu treffen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen.“ Um sich nicht dem Verdikt des Verstoßes gegen das Normwiederholungsverbot durch § 6a Abs. 1 S. 1 BDSG auszusetzen, ist dann jedenfalls ein Hinweis auf Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO sinnvoll. Abgesehen von der Zielsetzung, das Regelungssystem verständlicher zu machen (EG 8 [ex EG 6a] DSGVO), besteht aber neben Art. 22 DSGVO kein Bedarf für eine eigene, wenn auch neu gefasste Bestimmung im BDSG.

b. Abs. 1 S. 2: Einbeziehung auch formeller menschlicher Entscheidungen

§ 6a Abs. 1 S. 2 BDSG stellt deklaratorisch fest, dass eine automatisierte Einzelentscheidung auch dann anzunehmen ist, wenn eine natürliche Person

---

[485] EuGH, Rs. 34/73, Variola, Slg. 1973, 981, Rn. 11; Rs. 94/77, Zerbone, Slg. 1978, 99, Rn. 22/27.
[486] *Nettesheim*, in: Grabitz/Hilf (Hrsg.), EU-Recht, 48. EL, Art. 288 AEUV, Rn. 101.
[487] EuGH, Rs. 272/83, Kommission/Italien, Slg. 1985, 1057, Rn. 26 f.

eine Entscheidung trifft, die ihm keinen inhaltlichen Bewertungsspielraum einräumt. Es handelt sich um die Erweiterung des grundsätzlichen Verbotes um solche von Menschen getroffenen Entscheidungen, denen keine inhaltliche Bewertung und darauf gestützte Entscheidung vorausgegangen ist.
Eine ähnlich gelagerte Klarstellung lässt sich Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO nicht entnehmen. Der Sinn und Zweck der Norm zielt aber darauf, die Gefahren einer nicht überprüfbaren automatisierten Verarbeitung zu begrenzen, insbesondere wenn diese Verarbeitung der Bildung von Persönlichkeitsprofilen dient. Der Einzelne soll nach der normativen Wertung nicht zum Objekt eines Entscheidungsautomatismus verkümmern. Denn dies könnte schwerwiegende Folgen für den Persönlichkeitsschutz zeitigen.[488] Diese Gefahr besteht auch dann, wenn eine natürliche Person lediglich formal eine automatisierte Datenverarbeitung bestätigt, ohne selbst eine inhaltliche Entscheidung zu treffen. Wenn ausschließlich eine *ohne jegliche* menschliche Entscheidungsgewalt stattfindende Entscheidung das Tatbestandsmerkmal des Art. 22 (ex Art. 20) DSGVO erfüllen würde, so schränkte dies den persönlichkeitsschützenden Anwendungsbereich des Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO nachhaltig ein. Bei teleologischer Auslegung schließt der Tatbestand des Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO auch rein formale Entscheidungen natürlicher Personen ein. Damit entsprechen sich Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO und § 6a Abs. 1 S. 2 BDSG.
Bei dieser Lesart dient § 6a Abs. 1 S. 2 BDSG nur der Klarstellung dessen, was Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO durch beredtes Schweigen festschreibt: Die formale Entscheidung eines Menschen ist auch als automatische Einzelentscheidung anzusehen. Diese Klarstellung kann sich damit womöglich auf Art. 4 Abs. 3 EUV i. V. m. Art. 291 Abs. 1 AEUV, namentlich auf die Pflicht berufen, geeignete innerstaatliche Maßnahmen zu erlassen, um die uneingeschränkte Anwendbarkeit zu gewährleisten.

c. Abs. 2 Nr. 1: Ausnahme für Vertragsverhältnisse

§ 6a Abs. 2 Nr. 1 BDSG regelt eine Ausnahme von dem grundsätzlichen Verbot des Abs. 1 für vertragliche Beziehungen. Wird durch die (automatisiert

[488] *Scheja/Haag* (Fn. 95), Teil 5 - Datenschutzrecht, Rn. 225.

getroffene) Entscheidung dem Begehren des Betroffenen stattgegeben und geschieht dies innerhalb eines Vertragsverhältnisses, ist diese zulässig. Diesem Ausnahmetatbestand entspricht Art. 22 Abs. 2 lit. a DSGVO, der aber grundsätzlich weiter gefasst ist, weil er nicht nur solche Entscheidungen, die dem Begehren des Betroffenen entsprechen, von dem Verbot ausnimmt. Für Vertragsverhältnisse trifft Art. 22 Abs. 2 lit. a DSGVO eine abschließende Regelung dar. Die Öffnungsklausel des lit. b steht insoweit nicht zur Verfügung. Neben Art. 22 Abs. 2 lit. a DSGVO besteht für § 6a Abs. 2 Nr. 1 im Ergebnis weder Regelungsbedürfnis noch -spielraum.

d. Abs. 2 Nr. 2: Ausnahme bei Wahrung der berechtigten Interessen

§ 6a Abs. 2 Nr. 2 BDSG befreit von dem Verbot automatisierter Einzelentscheidungen, wenn die berechtigten Individualinteressen durch geeignete Maßnahmen gewahrt sind und der Verantwortliche dem Betroffenen „die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitteilt sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mitteilt und erläutert."[489] Zwar wiederholt § 6a Abs. 2 Nr. 2 BDSG lediglich, was die DSGVO als „suitable safeguards" deklariert. Eine Konkretisierung enthält aber § 6a Abs. 2 Nr. 2 aE BDSG, der die Öffnungsklausel des Art. 22 Abs. 2 lit. b (ex Art. 20 Abs. 1a lit. b) DSGVO schon hinreichend ausfüllt, so dass kein Anpassungsbedarf und auch kein Verstoß gegen das Normwiederholungsverbot besteht. Die Regelung des § 6a Abs. 2 Nr. 2 BDSG macht von dem Umsetzungsspielraum des Art. 15 Abs. 2 lit. b DSRL in zulässiger Weise Gebrauch; sie ist neben Art. 22 Abs. 2 lit. b DSGVO aber nicht mehr (zwingend) erforderlich.

[489] Vgl. zum darin zu sehenden dreistufigen Verfahren aus Information über die automatisierte Einzelentscheidung, Mitteilung und Erläuterung der wesentlichen Entscheidungsgründe auf Anfrage des Betroffenen und schließlich die Möglichkeit, den eigenen Standpunkt deutlich zu machen, um ggf. eine Revision der Entscheidung zu erreichen, so *Gola/Klug/Körffer* (Fn. 104), § 6a, Rn. 14, 14a.

§ 6a BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1 S. 1	Art. 22 Abs. 1 (ex Art. 20 Abs. 1)	Streichen (oder modifizieren) Formulierungsvorschlag: „Es ist verboten, im Wege ausschließlich automatisierter Verarbeitung – einschließlich Profiling – Entscheidungen zu treffen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen.“	Auch wenn Art. 22 Abs. 1 (ex Art. 20 Abs. 1) DSGVO sich vom Wortlaut wie eine Anspruchsnorm Betroffener liest, enthält er das grundsätzliche, von einer Geltendmachung des Einzelnen unabhängige Verbot automatisierter Einzelentscheidungen. § 6a Abs. 1 S. 1 BDSG kann grds. gestrichen werden. Gleichwohl lässt sich eine den Verbotscharakter hervorhebende Klarstellung mit dem unionsrechtlichen Wiederholungsverbot als Teil einer in sich konsistenten Regelung, die von der Öffnungsklausel des Art. 22 Abs. 2 lit. b DSGVO Gebrauch macht, womöglich in Einklang bringen (vgl. auch EG 8 [ex EG 6a]). Die neue Fassung des nationalen Rechts bringt den Regelungsgehalt des (in seiner Diktion nicht ganz präzisen) Unionsrechts klarer zum Ausdruck. Dabei ist ein Verweis auf Art. 22 Abs. 1 DSGVO angezeigt, um den unionsrechtlichen Ursprung der Norm aufzuzeigen.
Abs. 1 S. 2	Art. 22 Abs. 1 (ex Art. 20 Abs. 1)	Streichen (beibehalten zur Präzisierung des Art. 22 Abs. 1 wohl möglich)	§ 6a Abs. 1 S. 1 BDSG stellt klar, dass auch rein formale Entscheidungen von Menschen als autonome Einzelentscheidung anzusehen sind. Bei Gebrauchmachen von der Öffnungsklausel des Art. 22 DSGVO als Konkretisierung nach EG 8 (ex EG 6a) zulässig.
Abs. 2 Nr. 1	Art. 22 Abs. 2 lit. a (ex Art. 20 Abs. 1a lit. a)	Streichen bzw. Verweis auf DSGVO	Der Ausnahmetatbestand ist nur erfüllt, wenn die Entscheidung dem Begehren des Betroffenen entspricht. Art. 22 Abs. 2 lit. a (ex Art. 20 Abs. 1a lit. a) DSGVO gilt hingegen nicht nur im Falle einer Stattgabe, sondern auch bei für den Betroffenen nachteiligen Entscheidungen. Das Merkmal der Erforderlichkeit dient hier als Korrektiv.

Abs. 2 Nr. 2	Art. 22 Abs. 2 lit. b (ex Art. 20 Abs. 1a lit. b)	Beibehalten möglich	Abs. 2 Nr. 2 kann unter der Öffnungsklausel des Art. 22 Abs. 2 lit. b DSGVO grds. aufrechterhalten werden, falls der Gesetzgeber von ihr Gebrauch macht.
Abs. 3	Art. 15 Abs. 1 lit. h, EG 63	Streichen; u. U. beibehalten	Die DSGVO regelt Betroffenenrechte grundsätzlich umfänglich, insbesondere unmittelbar. Insbesondere legt sie dem Verantwortlichen auf, bei automatisierter Entscheidungsfindung „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person“ zu erteilen (Art. 15 Abs. 1 lt. h DSGVO). Art. 23 gestattet den Mitgliedstaaten Ausnahmen. Soweit die Bundesrepublik von dieser Möglichkeit Gebrauch macht, kann das Auskunftsrecht als Teil einer konsistenten, in sich verständlichen Regelung als Konkretisierung nach EG 8 (ex EG 6a) aufrechterhalten bleiben.

§ 6b: Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

Die vergleichsweise junge Vorschrift des § 6b BDSG[490] trägt dem besonderen Schutzbedürfnis eines besonderen Aspekts des Allgemeinen Persönlichkeitsrechts Rechnung, nämlich dem Recht am eigenen Bild in öffentlich zugänglichen Räumen. Sie ergänzt damit die allgemeinen Verarbeitungstatbestände, die für allgemeine Videoüberwachungsmaßnahmen vor allem in privaten Räumen gelten, insbesondere § 28 Abs. 1 S. 1 Nr. 2 BDSG.[491] § 6b BDSG sucht das Recht am eigenen Bild mit dem Bedürfnis nach einem angemessenen Schutz der öffentlichen Sicherheit sowie berechtigten Interessen von Eigentümern und weiteren Schutzbedürftigen in Einklang zu bringen. Es

[490] Die Vorschrift fand im Jahr 2001 Eingang in das BDSG. Vgl. BR-Drucks. 461/00.

[491] Für den Bereich von Beschäftigtenverhältnissen ist die Sondernorm des § 32 Abs. 1 BDSG zu beachten. Unionsrechtlich ist insoweit Art. 85 Abs. 2 (ex Art. 82 Abs. 2) DSGVO berührt. Er verpflichtet die Mitgliedstaaten, geeignete Maßnahmen zur Wahrung der Betroffenenrechte auch und gerade im Hinblick auf Überwachungssysteme am Arbeitsplatz zu treffen.

vermischen sich in der Vorschrift insofern öffentliche und private Interessen als Rechtfertigungsgrundlagen.
Diese Differenzierung strahlt insbesondere auf den Regelungsspielraum aus, der den Mitgliedstaaten nach Inkrafttreten der Datenschutz-Grundverordnung verbleibt. Im Hinblick auf private Interessen ist dieser sehr eng, im Hinblick auf den Schutz öffentlicher Interessen vergleichsweise weit (Art. 6 Abs. 2 [ex Art. 6 Abs. 2a] und 3 DSGVO). Entsprechend ereilt die Verarbeitungstatbestände des § 6b Abs. 1 S. 1 Nr. 1 BDSG auf der einen Seite und der Nrn. 2 und 3 auf der anderen Seite ein unterschiedliches unionsrechtliches Schicksal. Nr. 1 kann beibehalten werden, für den Regelungstatbestand der Nrn. 2 und 3 hingegen fehlt der Bundesrepublik Deutschland mit Inkrafttreten der Datenschutz-Grundverordnung die Regelungskompetenz.
Für die systematische Überwachung öffentlich zugänglicher Bereiche durch Videoüberwachung ordnet die Datenschutz-Grundverordnung eine Datenschutz-Folgenabschätzung an (Art. 35 Abs. 3 lit. c, EG 91 S. 3 [ex Art. 33 Abs. 2 lit. c, EG 71 S. 3] DSGVO). Ihre Erforderlichkeit ergibt sich unmittelbar aus der Verordnung. Einer ergänzenden Regelung im nationalen Recht bedarf es insoweit nicht.

§ 6b BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 Nr. 1 (Aufgaben öffentlicher Stellen)	Art. 35 Abs. 3 lit. c (ex Art. 33 Abs. 2 lit. c), Art. 5 Abs. 1 lit. b, Art. 6 Abs. 1 UAbs. 1 lit. e (vgl. auch Art. 35 Abs. 3 lit. c, EG 91 S. 3 [ex Art. 33 Abs. 2 lit. c, EG 71 S. 3])	Beibehalten möglich	§ 6b BDSG unterwirft die Videoüberwachung öffentlich zugänglicher Räume mit speziellen Zulässigkeitsanforderungen. Die DSGVO enthält keine spezielle Regelung für die Videoüberwachung. Ihre Rechtmäßigkeit unterliegt unionsrechtlich dem Regime der Art. 5 und 6 DSGVO. Erforderlich ist insbesondere eine Verarbeitungsgrundlage. § 6b Abs. 1 Nr. 1 lässt sich auf Art. 6 Abs. 1 UAbs. 1 lit. e, Abs. 2 (ex Abs. 2a), Abs. 3 DSGVO stützen. Die Vorschrift des § 6b BDSG beinhaltet „spezifische Anforderungen für die Verarbeitung […], um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten“ (im Sinne des Art. 6 Abs. 2 [ex Abs. 2a] DSGVO). Diese

			Verarbeitungsgrundlage ist auf eine im öffentlichen Interesse liegende Aufgabenerfüllung im Sinne des Art. 6 Abs. 3 S. 2 DSGVO beschränkt. § 6b Abs. 1 Nr. 1 erfüllt diese Voraussetzungen. Die Vorschrift kann daher bestehen bleiben.
Abs. 1 Nr. 2 u. 3 (Hausrecht; berechtigte Interessen für konkrete Zwecke)		Streichen bzw. ersetzen durch Verweis auf DSGVO, etwa: „zur Wahrnehmung berechtigter Interessen nach Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO“ bzw. „soweit dies zur Wahrnehmung …. erfolgt“.	Verarbeitungsgrundlage für die Videoüberwachung zur Wahrung des Hausrechts ist Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Anders als für Art. 6 Abs. 1 UAbs. 1 lit. c und e sieht die DSGVO für lit. f *keine Öffnungsklausel* vor. Aus diesem Regelungssystem folgt im Umkehrschluss, dass alle Fälle jenseits der lit. c und e die Rechtfertigungsgrundlage ausschließlich im Unionsrecht zu finden sind. Der nationale Gesetzgeber darf keine eigene Verarbeitungsgrundlage schaffen, im Interesse der Konsistenz und Verständlichkeit spezifischer Verarbeitungsgrundlagen (vgl. oben die Regelung zu Nr. 1) aber auf die unionsrechtliche Verarbeitungserlaubnis verweisen, ohne gegen das Wiederholungsverbot zu verstoßen. Anderenfalls könnte die Regelung den Umkehrschluss indizieren, dass für die dort genannten Fälle keinerlei Verarbeitungsgrundlage besteht. Klarstellende Regelungen, um eine in sich konsistente Regelung unter Verweis auf das EU-Recht herzustellen, sind ist den Mitgliedstaaten aber auch durch das Wiederholungsverbot nicht verwehrt.
Abs. 2 (Erkennbarkeit, Transparenz)	Art. 5 Abs. 1 lit. a	Beibehalten möglich für Verarbeitungen nach der Öffnungsklausel des Art. 6 Abs. 1 UAbs. 1 lit. c und e.	Die Vorschrift konkretisiert und erweitert das Transparenzgebot des Art. 5 Abs. 1 lit. a i. V. m. Art. 6 Abs. 2 (ex Abs. 2a) DSGVO. Die Verordnung normiert die Transparenz und Erkennbarkeit bzgl. der Datenverarbeitung (Art. 4 Nr. 2 DSGVO), damit auch bzgl. der Daten*erhebung*. Das nationale Recht ist somit grds. wiederholend. Für die Verarbeitungsgrundlage des § 6b *Nr. 1* besteht jedoch ausdrücklich eine Öffnungsklausel und eine damit korrespondierende Regelungsaufgabe.

			Auf die *Nrn. 2 und 3* erstreckt sich diese Regelung der Sache nach nicht, da die Nationalstaaten insoweit keine eigene Regelungsbefugnis haben. Das Transparenzerfordernis ergibt sich inhaltlich unmittelbar aus der unionsrechtlichen Regelung des Art. 5 Abs. 1 lit. a DSGVO.
Abs. 3 S. 1 (Zweckbindung, Abwägung)	Art. 5 Abs. 1 lit. a, b, c, Art. 6 Abs. 3, 4 (ex Abs. 3a)	Beibehalten möglich für Verarbeitungen nach der Öffnungsklausel des Art. 6 Abs. 1 UAbs. 1 lit. c und e.	Soweit die Verarbeitung unter eine Öffnungsklausel nach Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO fällt, entspricht S. 1 inhaltlich der Vorgabe des Art. 6 Abs. 3 S. 2 DSGVO. Sie geht in Ausschöpfung des mitgliedstaatlichen Regelungsspielraums darüber insoweit hinaus, als sie fordert, dass keine Anhaltspunkte dafür bestehen dürfen, dass schutzwürdige Interessen der Betroffenen überwiegen. Das entspricht einer sachgerechten Abwägung der konfligierenden Interessen und damit auch dem Gebot der Verhältnismäßigkeit, das Art. 6 Abs. 3 S. 4 DSGVO als Voraussetzung für die Öffnungsklausel formuliert.
Abs. 3 S. 2	Art. 6 Abs. 1 UAbs. 1 lit. d und e sowie Abs. 3a i. V. m. Art. 23 Abs. 1 lit. c und d	Beibehalten möglich	Die Norm macht von der Öffnungsklausel in Art. 6 Abs. 4 (ex Art. 6 Abs. 3a (neu)) DSGVO Gebrauch. Die DSGVO gestattet eine Durchbrechung der Zweckbindung, wenn diese sich in einer demokratischen Gesellschaft als notwendige und verhältnismäßige Maßnahme zum Schutz der öffentlichen Sicherheit oder zur Verfolgung von Straftaten erweist.
Abs. 4 (Benachrichtigungspflicht)	Art. 12 ff., insb. Art. 13	Streichen bzw. auf die jeweils einschlägige Benachrichtigungspflicht des Unionsrechts verweisen	Die Betroffenenrechte regelt die DSGVO unmittelbar. Art. 23 (ex Art. 21) eröffnet den Mitgliedstaaten zwar die Möglichkeit, Ausnahmen zuzulassen. Solche erweisen sich aber nicht als angezeigt. Die Benachrichtigungspflicht des § 6b Abs. 4 hatte inhaltlich ihren guten Sinn. Sie besteht als Teil der unionsrechtlichen Regelungen der Betroffenenrechte weiter. Regelungstechnisch ist es sinnvoll, auf die Norm des Unionsrechts zu verweisen.

Abs. 5	Art. 17 Abs. 1 lit. a, Art. 5 Abs. 1 lit. e, EG 66 (ex EG 54), EG 39 S. 8-10	Streichen oder modifizieren	Die Löschungspflicht ergibt sich unmittelbar aus Art. 17 Abs. 1 lit. a DSGVO. Die Mitgliedstaaten können kraft Art. 23 (ex Art. 21) DSGVO die Betroffenenrechte beschränken. Davon Gebrauch zu machen, ist aber nicht empfehlenswert.
-	Art. 35 Abs. 3 lit. c (ex Art. 33 Abs. 2 lit. c) DSGVO	Klarstellende Regelung möglich, soweit rechtspolitisch erwünscht	Für die systematische weiträumige Überwachung öffentlich zugänglicher Bereiche sieht die DSGVO in Art. 35 Abs. 3 lit. c (ex Art. 33 Abs. 2 lit. c) DSGVO grundsätzlich zwingend eine Datenschutz-Folgenabschätzung vor. Eine Ausnahme gestattet Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO für auf Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO gründende Verarbeitungen, dass bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass der Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte. Ob eine Datenschutz-Folgenabschätzung durchzuführen ist, liegt dann im Ermessen der Mitgliedstaaten. Von diesem Spielraum Gebrauch zu machen, kann sinnvoll sein.

§ 6c: Mobile personenbezogene Speicher- und Verarbeitungsmedien

Die Regelung des § 6c BDSG trifft Sonderregelungen für mobile Speichermedien, wie etwa Mobilfunk-SIM-Karten (vgl. die zeitgleich in das BDSG aufgenommene korrespondierende Begriffsbestimmung in § 3 Abs. 10 BDSG). Die Norm soll Transparenz bei Verarbeitungsprozessen auf diesen Medien sicherstellen.[492] Reine Speichermedien, z. B. Magnetkarten, sind nicht erfasst, sehr wohl aber die elektronische Gesundheitskarte.[493]
Mit dem Begriff „mobile personenbezogene Speicher- und Verarbeitungsmedien“ wollte der Gesetzgeber den Anwendungsbereich für zukünftige techni-

[492] *Hornung*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 6c BDSG, Rn. 8.
[493] *Hornung* (Fn. 492), § 6c BDSG, Rn. 3.

sche Entwicklungen offen halten.[494] Regelungsbedarf sah der Gesetzgeber insofern, als solche mobilen Medien nicht nur Datenträger sind, sondern hierauf Daten auch *verarbeitet* werden, ohne dass diese Verarbeitungen von dem Betroffenen unmittelbar nachvollziehbar sind.[495]

Die Norm enthält *keine datenschutzrechtliche Ermächtigung* für das Auslesen von Daten aus dem Medium oder zur Vornahme von Datenverarbeitungen auf diesem; sie regelt auch nicht die technische Ausgestaltung. Ihr ist es vielmehr um Informationspflichten bestellt, die das Transparenzgebot untermauern.[496] Zielsetzung und Wortlaut („muss den Betroffenen […] unterrichten") legen nahe, dass § 6c zudem einen echten, durchsetzungsfähigen Anspruch auf Unterrichtung begründet.[497]

§ 6 Abs. 1 regelt die Unterrichtungspflicht als solche (verpflichtete Stelle, Umfang der Unterrichtung). Diese kann zwar inhaltlich identisch mit der Hinweispflicht aus § 4a Abs. 1 S.2 sein; sie kann jedoch, wenn es sich um ein zur automatisierten Verarbeitung lediglich vorausgerüstetes Medium handelt, auch schon weit vor der Pflicht aus § 4a eingreifen: § 6c begründet insoweit eine vorgezogene Informationspflicht.[498]

§ 6c Abs. 2 betrifft Maßnahmen zur effektiven Wahrnehmung des Auskunftsrechts, namentlich das unentgeltliche Bereitstellen der erforderlichen Geräte und Einrichtungen. Abs. 3 verpflichtet zur Erkennbarkeit von Kommunikationsvorgängen auf dem Medium.

Die Norm hat kein Äquivalent in der Datenschutz-Grundverordnung, sie beruht auch nicht auf der DSRL. Informationspflichten regelt nunmehr die Datenschutz-Grundverordnung unmittelbar und umfassend in Art. 13 (ex Art. 14) und 14 (ex 14a) (i. V. m. EG 60-62 [ex EG 48-50] DSGVO). Sie lässt zwar in Art. 23 (ex Art. 21) DSGVO den Mitgliedstaaten Raum für Be-

---

[494] *Hornung* (Fn. 492), § 6c BDSG, Rn. 14. Dies insbesondere deshalb, weil die Verbreitung von Chipkarten im Alltag stetig weiter zunimmt – Beispiele sind der Zahlungsverkehr, Mobilfunk, Kundenkarten, Betriebsausweise – und aufgrund des Einsatzes in verschiedenen Lebensbereichen ein erhebliches Risiko der Profilbildung enthält; vgl. auch § 6a BDSG und Art. 22 (ex Art. 20) DSGVO.

[495] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 6c, Rn. 2, s.a. Rn. 1, der die Norm dem „modernen Datenschutz" zurechnet.

[496] *Scholz*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 6c, Rn. 20.

[497] *Hornung* (Fn. 492), § 6c BDSG, Rn. 9. Dies gilt für alle drei Absätze des § 6c.

[498] *Hornung* (Fn. 492), § 6c BDSG, Rn. 2.

schränkungen. Eine solche Beschränkung regelt § 6c BDSG jedoch nicht, so dass für eine nationale Regelung auf der Grundlage einer Öffnungsklausel kein Raum mehr besteht.

§ 6c BDSG	Korrespondierende Norm in der DSG-VO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1	Vgl. EG 60-62 (ex EG 48-50), Art. 13 f.	Streichen	Die DSGVO enthält keine vergleichbare Regelung und auch keine entsprechende Öffnungsklausel, sodass kein Regelungsspielraum mehr besteht (denkbar ist es allerdings, die Regelung des § 6c als »Vorfeldregelung des Datenschutzes« nicht von dem Normierungsanspruch der DSGVO erfasst und insoweit den mitgliedstaatlichen Regelungsspielraum nicht berührt zu sehen). Aufgrund der unmittelbaren Regelung von Informationspflichten in der DSGVO besteht kein Regelungsbedarf. Nach Art. 23 DSGVO sind lediglich Abweichungen hiervon zulässig, die § 6c BDSG jedoch nicht vorsieht.
Abs. 2		Streichen	Dito
Abs. 3		Streichen	Dito

§ 7: Schadensersatz

Ausgefeilte Datenschutzgesetzgebung degeneriert zum Papiertiger, wenn sich an die Verpflichtungen im Falle ihres Verstoßes keine Haftungsfolgen knüpfen. So sah es bereits das nationale Recht nach §§ 7 f. BDSG vor. § 7 S. 1 eröffnet natürlichen Personen daher einen eigenen deliktischen Anspruch zum Ausgleich materieller Schäden bei vermutetem Verschulden, ohne die allgemeinen Ansprüche zu verdrängen. S. 2 eröffnet eine Exkulpationsmöglichkeit für den Fall nachgewiesenermaßen fehlenden Verschuldens. § 7 gilt dabei – im Gegensatz zu § 8 – sowohl für öffentliche als auch nicht-öffentlich Stellen.

Die §§ 7, 8 verfolgen die allgemeinen Schadensersatzziele Ausgleich, Sanktion und Prävention.[499]

§ 7 BDSG entfaltete in der Praxis bislang geringe Relevanz.[500] Das gründet sich zum einen auf die Nachweishürden, namentlich die Schwierigkeit des Anspruchsberechtigten, den Ursachenzusammenhang zwischen Datenschutzverstoß und Schaden zu belegen. Zum anderen reduziert die Beschränkung der Norm auf materielle Schäden ihre praktische Wirksamkeit. Auf den in § 7 ausgestalteten deliktischen Anspruch finden die allgemeinen Regelungen des BGB Anwendung (Gesamtschuld, Verjährung, Verzicht).[501]

Auch die Datenschutz-Grundverordnung normiert in Art. 82 ff. (ex Art. 77 ff.) Haftungsfolgen für den Fall eines Verstoßes gegen Datenschutzrecht. Die Mitgliedstaaten sind daher hinsichtlich der Ausgestaltung des Haftungsregimes nicht vollkommen frei. Anderenfalls könnten sie durch die Ausfüllung der Haftungstatbestände die Wirksamkeit der datenschutzrechtlichen Primärnormen, welche die Datenschutz-Grundverordnung als zwingendes Recht vorsieht, aushöhlen. Auch soweit die Mitgliedstaaten von dem Spielraum der Öffnungsklauseln Gebrauch machen, welche die Datenschutz-Grundverordnung vorhält, sind sie nach der Wertung des EG 146 (ex EG 118) DSGVO in der Ausgestaltung des Haftungsregimes nicht ganz frei. Die inhaltlichen Vorgaben des unionsrechtlichen Haftungsregimes formuliert Art. 82 (ex Art. 77) DSGVO.

Nimmt man die Überschrift des Art. 82 (ex Art. 77) DSGVO beim Wort, etabliert er zwei Formen von Ersatzansprüchen: eine Haftung *und* ein Recht auf Schadenersatz. Ein solches Verständnis würde dem Sinngehalt der inhaltlichen Ausgestaltung, welche die Norm in ihren Absätzen erfährt, aber wohl nicht gerecht. Wahrscheinlich sind beide Anspruchsformen inhaltlich identisch. Abs. 1 legt die Grundlagen für den Schadensersatzanspruch des Be-

[499] *Quaas*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 7 BDSG, Rn. 2 sowie *Quaas*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 8 BDSG, Rn. 1.

[500] *Quaas* (Fn. 499), § 7 BDSG, Überblick vor Rn. 1, Rn. 3.

[501] *Quaas* (Fn. 499), § 7 BDSG, Rn. 70. Im Gegensatz zu § 8 BDSG – dort Abs. 4-6 – bedurfte es für den allgemeineren Anspruch in § 7 BDSG keines Verweises, vgl. *Gola/Piltz*, RDV 2015, 279 (281).

troffenen. Abs. 2 füllt den Haftungsmaßstab aus und schränkt ihn für die unterschiedlichen Anspruchsschuldner in unterschiedlichem Maße ein.

§ 7 BDSG verspricht Schadensersatz grundsätzlich bei Verstößen gegen (andere) nationale Datenschutzvorschriften. Art. 82 (ex Art. 77) DSGVO knüpft demgegenüber an einen Verstoß gegen die Datenschutz-Grundverordnung als Haftungstatbestand an. Dies stimmt damit überein, dass die Datenschutz-Grundverordnung von einem Gleichlauf der Pflichtenstellung und des Haftungsregimes ausgeht, um die wirksame Durchsetzung der datenschutzrechtlichen Grundvorstellungen der Union zu verbürgen. EG 146 S. 4 DSGVO deutet mit der Wendung „unbeschadet von Schadensersatzforderungen aufgrund von Verstößen gegen andere Vorschriften des Unionsrechts oder des Rechts der Mitgliedstaaten“ prima facie auch an, dass den Mitgliedstaaten dieser Spielraum verbleibt. Dürfen die Mitgliedstaaten von Öffnungsklauseln Gebrauch machen, obliegt es ihnen grundsätzlich auch, korrespondierende Haftungstatbestände zu erlassen.[502]

Dem erteilt allerdings EG 146 S. 5 DSGVO wohl eine Absage. Die Verpflichtung zum Schadensersatz soll danach auch für Verarbeitungen greifen, die nicht mit „Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang“ stehen. Das widerspricht zwar auf den ersten Blick ein Stück weit der Logik der Öffnungsklauseln, ist aber womöglich der erklärte Wille der Verordnung. Denkbar ist aber auch, dass die Union mit der Wendung „Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung“ ausschließlich Regelungsaufträge der DSGVO adressiert, nicht aber echte Öffnungsklauseln, die den Mitgliedstaaten – insbesondere in Respekt vor deren originären Kompetenzen bei Verarbeitungsprozessen öffentlicher Stellen – eigene Gestaltungsspielräume zugestehen. Immerhin unterscheidet die Verordnung insbesondere an anderer Stelle, nämlich dort, wo sie ihr Verhältnis zu mitgliedstaatlichen Recht und das Recht zu wiederholenden Regelungen allgemein behandelt, ausdrücklich zwischen „Präzisierungen“ und

[502] Diese Befugnis ergibt sich jedoch nicht aus Art. 84 (ex Art. 79b) DSGVO. Denn dieser nimmt auf Sanktionen Bezug und meint damit etwas anderes als den Schadensausgleich, den Art. 82 (ex Art. 77) DSGVO im Auge hat. Einschlägig sind vielmehr die jeweiligen allgemeinen Öffnungsklauseln, insbesondere für den Datenschutz bei Verarbeitungen öffentlicher Stellen.

„Einschränkungen“ der Vorschriften, welche die DSGVO enthält (EG 8 DSGVO). Mit „Einschränkungen“ meint sie wohl „echte Öffnungsklauseln“, wie z. B. Art. 23 und Art. 85 Abs. 2 DSGVO, die den Mitgliedstaaten ausdrücklich Abweichungen von Grundsätzen der Union zugestehen.[503]
Bei dieser Lesart schränkt EG 146 S. 5 DSGVO den nationalen Regelungsspielraum ein, indem er die Mitgliedstaaten auch im Bereich ihrer Präzisierungsregeln „in die Haftung nimmt“. Er lässt sich als Definition dessen lesen, was Art. 82 Abs. 1 DSGVO als „Verstoß gegen diese Verordnung“ versteht. Denkbar ist es aber auch, ihn für den Bereich von Präzisierungen als Regelungsauftrag an die Mitgliedstaaten zu lesen: Sie müssen Tatbestände schaffen, welche an den Verstoß gegen mitgliedstaatliche *Präzisierungsregeln* auch einen Haftungstatbestand knüpfen. Dem wird das BDSG dann dadurch gerecht, wenn es einen Schadensersatzanspruch für solche Fälle begründet, für die es datenschutzrechtliche Pflichten etabliert. Hält der Gesetzgeber den § 7 BDSG mit dieser Prämisse aufrecht, sollte er in die Vorschrift jedoch eine Formulierung aufnehmen, welche im Wege eines Verweises die enge Verzahnung mit Art. 82 DSGVO und die Nachrangigkeit bzw. den Ergänzungscharakter der BDSG-Norm deutlich macht. Für denjenigen Bereich, in dem die Mitgliedstaaten von eigenen Öffnungsklauseln Gebrauch machen, genießen sie – hält man an der Unterscheidung zwischen „Präzisierung“ und „Einschränkung“ fest – grundsätzlich ein größeres Maß an Regelungsfreiheit; auch hier dürfen die Mitgliedstaaten die grundsätzlichen Vorgaben der DSGVO aber nicht unterwandern.
Hinsichtlich des die Haftung auslösenden Tatbestands, namentlich der Frage, ob nur eine (Daten-)Verarbeitung, oder aber jedwede mit der Verordnung nicht zu vereinbarende *Handlung* zum Schadensersatz verpflichten soll, bestand zwischen Rat und Parlament Uneinigkeit.[504] Art. 82 Abs. 1 DSGVO legt eine umfassende Haftungsverpflichtung nahe, Abs. 2 benennt hingegen

[503] Ob sich die Differenzierung aber sauber durchdeklinieren lässt, ist nicht gesichert. Deutlich wird das etwa am Beispiel des Art. 6 Abs. 2 und 3 DSGVO. Bei ihnen handelt es sich in der Terminologie des EG 19 S. 5 um eine „spezifischere Bestimmung“ (…), „um die Anwendung der Vorschriften dieser Verordnung anzupassen.“ In dieser Lesart handelt es sich um eine „Präzisierung“. Eine Anpassung im Sinne des EG 19 S. 5 ist von einer Abweichung bzw. Einschränkung der Verordnung aber auch nur ein kleiner Schritt.
[504] Vgl. dazu auch *Gola/Piltz* (Fn. 501), 284.

nur die „Verarbeitung“ als Haftungstatbestand. Dafür, dass nur rechtswidrige *Verarbeitungen* und nicht andere Handlungen eine Ersatzpflicht auslösen, spricht sich auch EG 146 S. 1 DSGVO deutlich aus. Insoweit besteht ein inhaltlicher Gleichlauf mit § 7 BDSG, der auch nur die unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erfasst. Im Interesse der Vereinheitlichung sollte sich dieser jedoch an die Terminologie der Datenschutz-Grundverordnung anpassen und fortan nur noch von „Verarbeitung“ sprechen.

Art. 82 Abs. 1 DSGVO erfasst nach dem klaren Wortlaut materielle und immaterielle Schäden. § 7 BDSG knüpft bislang seinen Ersatzanspruch allgemein an einen „Schaden“ an.[505] Ob es sich dabei auch um einen *immateriellen* Schaden handeln kann, lässt die Vorschrift – anders als § 8 Abs. 2 BDSG – offen. § 8 Abs. 2 BDSG deutet mit seiner Beschränkung von Ersatzansprüchen auf „schwere Verletzungen des Persönlichkeitsschutzes“ im Umkehrschluss an, dass § 7 im Grundsatz ausschließlich auf den Ersatz materieller Schäden abzielt.

Die Neufassung des § 7 S. 1 BDSG sollte klarstellen, dass nach Inkrafttreten der Datenschutz-Grundverordnung – entsprechend dem Gebot des Art. 82 Abs. 1 DSGVO („materieller oder immaterieller Schaden“) – auch immaterielle Schäden einen Schadensersatzanspruch auslösen. Die Mitgliedstaaten sind hierzu wohl sogar verpflichtet, ohne einen eigenen Regelungsspielraum zu genießen (vgl. EG 146 S. 5 [ex EG 118 S. 4] DSGVO). Denn vollständig i. S d. EG 146 S. 5 DSGVO kann nur ein Ersatz auch für immaterielle Schäden sein. Die DSGVO verwendete in der Trilog-Fassung anstelle des Begriffs „immateriell“ noch die Wendung „moralisch“. Dieser Begriff ist dem deutschen Haftungsrecht bisher fremd. Ein Rückgriff auf die synonyme Wendung „immateriell“, so wie sie sich in der im Amtsblatt veröffentlichten Fassung der DSGVO nunmehr findet, ermöglicht der deutschen Rechtsordnung einen Rückgriff auf die differenzierte Rechtsprechung zum Schmerzensgeldrecht.

[505] Ein materieller Schaden kann z. B. in der Verweigerung eines Kredites oder dem Fehlschlagen einer Reisebuchung liegen; s. dazu auch *Gola/Piltz* (Fn. 501), 280.

§ 7 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
S. 1	Art. 82, EG 146 (ex Art. 77, EG 118)	Beibehalten – ergänzt um die Wendung: „eine verantwortliche Stelle *oder ein Auftragsverarbeiter*“ sowie „… ist sie oder ihr Träger dem Betroffenen *unbeschadet der Vorschriften des Art. 82 DSGVO…*“ sowie „materiellen *oder immateriellen* Schaden“	Art. 82 (ex Art. 77) DSGVO knüpft als Haftungstatbestand an einen Verstoß gegen die DSGVO an. § 7 BDSG erweitert den Tatbestand und ermöglicht Schadensersatz auch bei Verstößen gegen andere – nationale – Datenschutzvorschriften, die nach EG 146 S. 5 DSGVO nicht bereits von Art. 82 DSGVO erfasst werden. Art. 82 enthält zwar keine Öffnungsklausel. Vielmehr ist es (je nach Verständnis des EG 146 S. 5) eine dem Effektivitätsgebot folgende Aufgabe der Mitgliedstaaten, Verstöße in den Bereichen, in denen sie Regelungsaufträgen nachkommen, oder von Öffnungsklauseln Gebrauch machen, durch Haftungsnormen zu flankieren. Anders als das bisherige deutsche Recht macht die DSGVO auch den Auftragsverarbeiter zum Schadensersatzpflichtigen (Art. 82 Abs. 1 [ex Art. 77 Abs. 1]). Dies muss sich auch im deutschen Recht abbilden. Aufgrund des Art. 82 Abs. 1 (ex Art. 77 Abs. 1) DSGVO („materieller oder immaterieller Schaden“) muss eine Ersatzpflicht auch für immaterielle Schäden Eingang in das BDSG-neu finden.
S. 2 (keine Ersatzpflicht bei Einhaltung der gebotenen Sorgfalt)	Art. 82 Abs. 3 (ex Art. 77 Abs. 3)	Modifizieren in Anlehnung an Art. 82 Abs. 3 DSGVO	Die bisherige deutsche Regelung des § 7 S. 2 BDSG bleibt hinter der Regelung in Art. 82 Abs. 3 (ex Art. 77 Abs. 3) DSGVO zurück. Denn diese gewährt dem Verantwortlichen eine Haftungsbefreiung nur, wenn er nachweist, dass er in *keinerlei* Hinsicht für den schadensauslösenden Umstand verantwortlich ist. Die Begrifflichkeiten – Verschulden und gebotene Sorgfalt einerseits und Verantwortlichkeit andererseits – sind nicht völlig deckungsgleich. Erwägenswert ist deshalb eine Übernahme der Terminologie der DSGVO.

Bisher nicht geregelt	Art. 82 Abs. 2 S. 2 (ex Art. 77 Abs. 2 S. 2) i. V. m. Art. 28 (ex Art. 26) (Haftungsbefreiung des Auftragsverarbeiters)	Klarstellung im nationalen Recht empfehlenswert. Evtl. empfiehlt sich auch ein Hinweis auf Art. 26 (ex Art. 24) DSGVO an.	Die DSGVO konkretisiert bzw. beschränkt die Haftung des Auftragsverarbeiters. Die Vorschrift des Art. 82 Abs. 2 S. 2 (ex Art. 77 Abs. 2 S. 2) ist aufgrund des Harmonisierungsanspruchs der DSGVO wohl so zu verstehen, dass auch das nationale Recht den Auftragsverarbeiter in den Fällen des Art. 82 Abs. 2 S. 2 DSGVO selbst dann nicht mit einer Haftung belegen darf, wenn der Mitgliedstaat von seiner Öffnungsklausel Gebrauch macht. Sonst würden die Regelungen über die Verantwortlichkeit des Auftragsdatenverarbeiters (im Zusammenspiel mit § 7 S. 1 BDSG neu) verschärft, welche die DSGVO grundsätzlich als abschließend versteht.
Bisher nicht geregelt	Art. 82 Abs. 4-5 (ex Art. 77 Abs. 4-5) (Haftung mehrerer; Gesamtschuldner)	Klarstellung erwägenswert.	Die DSGVO regelt die Haftung mehrerer Personen und das Ausgleichsverhältnis zwischen ihnen grundsätzlich abschließend und hinreichend konkret, so dass kein nationaler Regelungs- oder Konkretisierungsspielraum mehr verbleibt. Eine Sonderregelung im BDSG (für den Bereich der Haftung für Verletzungen nationalen, auf der Grundlage von Öffnungsklauseln erlassenen Rechts) ist grundsätzlich nicht notwendig (zumal hilfsweise auf die Haftungsgrundsätze der §§ 421, 426 bzw. § 840 BGB [je nach Beziehung untereinander] zurückgegriffen werden könnte). Aus Klarstellungsgründen kann mit Blick auf EG 146 S. 5 DSGVO ein Hinweis auf die einschlägigen Regelungen der DSGVO (für den Bereich der Haftung für Rechtsverletzungen in Bereichen, in denen die Bundesrepublik von Regelungsspielräumen Gebrauch gemacht hat) sinnvoll sein.

§ 8: Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen

Im Gegensatz zur Grundvorschrift des § 7 implementiert bislang § 8 eine verschuldens*unabhängige* Haftung öffentlicher Stellen, welche allerdings auf Rechtsverstöße bei automatisierten Verfahren beschränkt ist. Damit begründet

§ 8 eine Form der Gefährdungshaftung, welche dem besonderen Gefährdungspotenzial der automatisierten Datenverarbeitung[506] Rechnung zu tragen sucht. Denn durch die Automatisierung steigt das Risiko einer Beeinträchtigung des Rechts auf informationelle Selbstbestimmung, da sich die Datenmengen dann leichter zu neuen Informationen verknüpfen lassen und dem Betroffenen während des Verarbeitungsvorgangs die Einwirkungs- und Kontrollmöglichkeit regelmäßig fehlt.[507] Nicht erfasst ist rechtswidriges Verhalten bei manueller Datenverarbeitung. Hier kann je nach Konstellation § 7 Anwendung finden. Die Unterscheidung des BDSG in öffentliche und nicht-öffentliche Stellen[508] findet sich so auch im datenschutzrechtlichen Haftungsrecht des § 7 f. In der Praxis hat § 8 ebenso wie § 7 bislang geringe Relevanz erlangt.[509]

Die verschuldensunabhängige Haftung öffentlicher Stellen, welche § 8 Abs. 1 BDSG auslöst, erstreckt sich auch auf immaterielle Schäden (Abs. 2). Die Ansprüche nach diesen beiden Absätzen belegt Abs. 3 mit einer Anspruchsobergrenze. Die weiteren Absätze 4 bis 6 enthalten eine Regelung zur Haftung mehrerer (Abs. 4) sowie Verweise auf die Vorschriften des BGB für Mitverschulden (Abs. 5) und Verjährung (Abs. 6).

Die Datenschutz-Grundverordnung unterscheidet in ihrem Haftungsregime des Art. 82 (ex Art. 77) nicht zwischen öffentlichen und nicht-öffentlichen Stellen. § 8 Abs. 1 BDSG nimmt aber (wie § 7 BDSG) als Teil eines BDSG-neu auf diejenigen Vorschriften Bezug, die *nach nationalem Recht* auf der Grundlage von Öffnungsklauseln für den öffentlichen Bereich (insbesondere Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO) neben der DSGVO weiter bestehen dürfen.

Das insinuiert auch einen erheblichen Regelungsspielraum der Mitgliedstaaten für die Ausgestaltung des Haftungsrechts. Gleichwohl ist der nationale Gesetzgeber in der Bestimmung des Haftungsumfangs und der Begründung des Haftungstatbestandes auch in diesen Fällen *nicht* gänzlich frei. Das ergibt sich aus EG 146 S. 5 (ex EG 118 S. 4) DSGVO. Dort stellt die Union klar,

[506] Vgl. § 3 Abs. 2, § 6a BDSG.
[507] *Quaas* (Fn. 499), § 8 BDSG, Rn. 2.
[508] Vgl. § 1 Abs. 2, § 2 und § 12 Abs. 1 BDSG.
[509] *Quaas* (Fn. 499), § 8 BDSG, Überblick vor Rn. 1.

dass zu den haftungsauslösenden Tatbeständen i. S. d. Art. 82 Abs. 1 auch eine Verarbeitung zählt, „die nicht mit (…) Rechtsvorschriften der Mitgliedstaaten zur Präzisierung von Bestimmungen der vorliegenden Verordnung im Einklang steht“. Die Union will mit dieser Einschränkung sicherstellen, dass mit seinem Pflichtenregime – auch dort, wo die Mitgliedstaaten Regelungsaufträgen der Verordnung nachkommen, um den Inhalt der Verordnung zu konkretisieren, ein vollständiges Haftungsregime als Spiegelbild korrespondiert. Wo die Mitgliedstaaten durch echte Öffnungsklauseln zur Einschränkung des Regelungsinhalts der DSGVO legitimiert sind (siehe die sprachliche Differenzierung in EG 8 DSGVO), genießen sie in ihrem nationalstaatlichen Haftungsregime aber eine größere Freiheit.[510]

Mit der Formulierung „unabhängig von einem Verschulden“ geht § 8 Abs. 1 BDSG über den Schutzstandard der Datenschutz-Grundverordnung hinaus. Das ist durchaus im Interesse des angestrebten *effektiven* Datenschutzes (vgl. z. B. Art. 52 Abs. 4 [ex Art. 47 Abs. 5] DSGVO). Ihn beizubehalten, kann aber umgekehrt dem mit der Verordnung intendierten Gedanken der Vollharmonisierung im Interesse eines einheitlichen Datenschutzniveaus der Union zuwiderlaufen. EG 146 S. 5 DSGVO lässt sich womöglich aber so lesen, dass er sich als Mindestforderung eines Haftungsregimes versteht, welches die darüber hinausgehenden mitgliedstaatlichen Sanktionen jedenfalls in dem Bereich ermöglicht, in dem die Mitgliedstaaten von ihrem Spielraum der materiell-rechtlichen Öffnungsklauseln (z. B. Art. 6 Abs. 1 UAbs. 1 lit. c oder e DSGVO) Gebrauch machen. Bei diesem Verständnis können die Regelungen des § 8 (in modifizierter Form, insbesondere unter Hinweis auf die Schadensersatzpflicht auch des Auftragsverarbeiters, die § 8 BDSG bislang nicht etabliert) überwiegend aufrechterhalten werden. Dies gilt insbesondere dort, wo das Schutzniveau des BDSG über das der Datenschutz-Grundverordnung hinausgeht, aber ebenso auch für die Regelungen zu Mitverschulden und Verjährung. § 7 BDSG und dessen allgemeiner Haftungstatbestand entbehren bislang entsprechender Verweisungen (§ 8 Abs. 4 bis 6), weil dort ohnehin die deliktischen Haftungsregeln zur Anwendung kommen. Nach Eintritt der Verjährung kann sich der Betroffene ergänzend – auch ohne spezielle Regelung in der Datenschutz-Grundverordnung oder im BDSG-neu – auf § 852

[510] Dazu auch S. 352.

BGB berufen und einen bereicherungsrechtlichen Herausgabeanspruch gegen den Verantwortlichen geltend machen.

§ 8 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 (verschuldensunabhängige Haftung öffentlicher Stellen)	Art. 82, EG 146 S. 3 und 4 (ex Art. 77, EG 118 S. 3 und 4)	Modifiziert (insbesondere unter Hinweis auf die Schadensersatzpflicht des Auftragsverarbeiters und die Unbeschadetheit von Art. 82 DSGVO) für den Bereich beibehalten, in dem die Bundesrepublik von materiellrechtlichen Öffnungsklauseln Gebrauch macht.	§ 8 Abs. 1 BDSG geht über den Schutzstandard der DSGVO hinaus. Das ist auch im Lichte der EG 146 S. 1 und 4 (ex EG 118 S. 1 und 4) wohl zumindest dort möglich, wo die Mitgliedstaaten von ihrem durch Öffnungsklauseln ermöglichten Regelungsspielraum Gebrauch machen. Die besseren Gründe sprechen dafür, dass eine Aufrechterhaltung der Norm unionsrechtlich zulässig ist. Die DSGVO betont indes, dass nicht nur der Verantwortliche, sondern auch der Auftragsverarbeiter schadensersatzpflichtig ist (Art. 82 Abs. 1 [ex Art. 77 Abs. 1]). Dies sollte auch § 8 BDSG-neu klarstellen.
Abs. 2	Art. 82 (ex Art. 77)	Modifizieren: „*schweren*“ streichen	Die DSGVO sieht für Fälle eines „immateriellen Schadens“ ausdrücklich eine Verpflichtung zum Schadensersatz vor. § 8 Abs. 2 BDSG steht insoweit bereits mit dem Unionsrecht in Einklang. Er begrenzt diesen Anspruch aber auf Fälle einer „*schweren* Verletzung des Persönlichkeitsrechts“. Die Vorschrift ist damit enger als Art. 82 Abs. 1 (ex Art. 77 Abs. 1) DSGVO. Das macht eine Modifizierung erforderlich.

Abs. 3 (Anspruchs-obergrenze)	-	Modifizieren – Beschränkung der Obergrenze auf Fälle der verschuldens*unabhängigen* Haftung	Die DSGVO regelt keine Obergrenze für den Schadensersatzanspruch und enthält auch keine entsprechende Öffnungsklausel. Das limitiert den mitgliedstaatlichen Regelungsspielraum. § 8 BDSG entfaltet zwar nur in dem Haftungskontext Wirkung, in dem der Mitgliedstaat von seinem eigenen Regelungsspielraum Gebrauch macht. Der Mitgliedstaat ist dann allerdings nicht grundsätzlich frei in der Festlegung des Haftungsmaßstabs, sondern unionsrechtlich determiniert. Art. 82 Abs. 4 (ex Art. 77 Abs. 4) und EG 146 (ex EG 118) zeigen, dass die DSGVO einen *vollständigen* (und wirksamen) Schadensersatz sicherzustellen sucht. Eine Obergrenze für einen Schadensersatzanspruch ist nach systematischer Auslegung der VO nur dort zulässig, wo das BDSG ein über die DSGVO hinausgehendes Schutzniveau enthält: Für den Bereich verschuldensunabhängiger Haftung öffentlicher Stellen ist die Obergrenze weiterhin zulässig, weil Art. 82 Abs. 3 (ex Art. 77 Abs. 3) auch öffentliche Stellen bei fehlender Verantwortlichkeit von der Haftung befreit – im Übrigen aber nicht.
Abs. 4	Art. 82 Abs. 4-5 (ex Art. 77 Abs. 4-5)	Beibehalten zur Klarstellung / Konkretisierung wohl möglich	Die Norm konkretisiert und ergänzt Art. 82 Abs. 4-5 (ex Art. 77 Abs. 4-5) DSGVO. Kein Verstoß gegen das Wiederholungsverbot (soweit die Haftung an Regelungsbereiche der Mitgliedstaaten anknüpft) da die DSGVO hierzu keine Aussage trifft.
Abs. 5 (Mitverschulden des Betroffenen)	-	Beibehalten zur Klarstellung möglich bzw. modifizieren	Die Norm hat kein Äquivalent in der DSGVO. Sie kann als lückenfüllende Ausgestaltungsregelung in dem Maße bestehen bleiben, als sie die verschuldensunabhängige Haftung öffentlicher Stellen betrifft. Der Gedanke des Mitverschuldens stellt einen allgemeinen Rechtsgrundsatz des Unionsrechts dar. Als Teil des nicht in der DSGVO geregelten Haftungsfolgenrechts unterfällt er weiterhin dem mitgliedstaatlichen Recht.

Abs. 6 (Verjährung)	-	Beibehalten möglich	Die DSGVO äußert sich nicht zur Verjährung von Schadenersatzansprüchen. Das kann einen nationalstaatlichen residualen Spielraum eröffnen. Verjährungsregelungen schränken jedoch die praktische Wirksamkeit unionsrechtlicher Haftungstatbestände ein, höhlen sie im Extremfall sogar aus. Wie bei allen Anspruchsgewährleistungen ist – auch im Hinblick auf den unionsrechtlichen Gedanken der Rechtssicherheit – aber davon auszugehen, dass der Normgeber ihre Durchsetzung nicht ad infinitum gewährleisten wollte. Es verbleibt insoweit eine Regelungslücke, die der Mitgliedstaat ausfüllen darf, soweit er dadurch die praktische Wirksamkeit der Regelungen in Art. 82 (ex Art. 77) DSGVO nicht unterläuft und auf eigenen Regelungsspielräumen zur Regelung der Zulässigkeit einer Verarbeitung aufsetzt. Die Verjährung für unerlaubte Handlungen, auf die § 8 Abs. 6 verweist, unterliegt einer Dreijahresfrist (§ 195 BGB). Diese Frist ist kurz und deshalb unionsrechtlich nicht ganz unbedenklich. Sie entspricht aber zugleich dem Zeitraum, in dem Ansprüche typischerweise nicht mehr durchsetzbar sind. Diese Länge der Verjährungsfrist ist im Interesse der Rechtssicherheit im Rechtsverkehr daher auch unionsrechtlich rechtfertigbar. Zudem beginnt die Frist ohnedies frühestens mit dem Ende des Jahres, in dem der Betroffene Kenntnis der den Anspruch begründenden Umstände und der Person des Schuldners erlangt oder ohne grobe Fahrlässigkeit erlangen müsste (§ 199 Abs. 1 Nr. 2 BGB), zu laufen.

§ 9: Technische und organisatorische Maßnahmen

Die in § 9 BDSG geregelte Datensicherheit verpflichtet Auftrags- und Datenverarbeiter, geeignete und zur Rechtskonformität erforderliche, technische und organisatorische Maßnahmen zu treffen. Damit eröffnet der Gesetzgeber

der verantwortlichen Stelle einen breiten Handlungsspielraum, soweit sich die getroffenen Maßnahmen als zur Datensicherheit erforderlich erweisen.
§ 9 S. 2 BDSG verlangt gleichwohl nur das, was im Rahmen der Verhältnismäßigkeit angemessen ist, um dem Schutzzweck gerecht zu werden. Parallele Bestimmungen enthält die DSGVO in Art. 24 Abs. 1 (ex Art. 22 Abs. 1), Art. 25 Abs. 1, Art. 28 Abs. 1 (ex Art. 26 Abs. 1) und Art. 32 Abs. 1 (ex Art. 30 Abs. 1). Ihnen ist es ebenfalls darum bestellt, die Anforderungen der Verordnung, insbesondere an die Datensicherheit, einzuhalten; ihre Regelungstiefe übersteigt aber die noch recht abstrakte Vorschrift des § 9 BDSG, so dass dieser vollständig der Harmonisierung durch das Unionsrecht zum Opfer fällt, auch wenn sich aus der Anlage des BDSG für die Praxis relevante Konkretisierungen ergeben. Ihr Inhalt kann als Grundlage genehmigter Verhaltensregeln (Art. 40 DSGVO) oder eines Zertifizierungsverfahrens (Art. 42 DSGVO) weiterhin eine sinnvolle Funktion erfüllen (siehe auch die Privilegierung des Art. 24 Abs. 3, Art. 25 Abs. 3 und Art. 32 Abs. 3). Soweit der nationale Gesetzgeber von den Öffnungsklauseln des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO Gebrauch macht, kann er die in der Anlage enthaltenen Bestimmungen grundsätzlich auch als Präzisierung i. S. d. Art. 6 Abs.2 DSGVO aufrechterhalten.

§ 9 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
S. 1	Art. 24 Abs. 1 (ex Art. 22 Abs. 1); Art. 25 Abs. 1; Art. 28 Abs. 1 (ex Art. 26 Abs. 1); Art. 32 Abs. 1 (ex Art. 30 Abs. 1).	Streichen	Art. 24 Abs. 1 und Art. 25 Abs. 1 DSGVO verpflichten den Verantwortlichen und – über die Auswahl des Auftragsdatenverarbeiters gemäß Art. 28 Abs. 1 (ex Art. 26 Abs. 1) – auch mittelbar den Auftragsdatenverarbeiter dazu, bei der Verarbeitung geeignete „technische und organisatorische Maßnahmen“ zu treffen, so dass die Verarbeitung nicht gegen die Verordnung verstößt. Inhaltlich entspricht dies der Vorgabe

			des § 9 S. 1 BDSG, dem es ebenso um die Datensicherheit bestellt ist[511]. Soweit diese nationale Bestimmung überobligatorische Maßnahmen, also solche, die über die normierten Anforderungen hinausgehen, verlangt,[512] entspricht die Norm Art. 32 Abs. 1 (ex Art. 30 Abs. 1) DSGVO. Inhaltlich besteht neben dem Unionsrecht insoweit kein Regelungsbedarf. Es besteht auch kein Regelungsspielraum. Die DSGVO gesteht den Mitgliedstaaten im Hinblick auf die Verantwortung des Verantwortlichen (Art. 24 Abs. 1, 25 Abs. 1) keine Öffnungsklausel zu. Im Hinblick auf den Auftragsverarbeiter verhält sich das zwar anders (vgl. dazu die Ausführungen zu § 11 BDSG). Der damit eröffnete Spielraum rechtfertigt aber keine Aufrechterhaltung des § 9 S. 1 BDSG.
S. 2	Art. 24 Abs. 1 (ex Art. 22 Abs. 1), Art. 25 Abs. 1, 2 (ex Art. 23 Abs. 1, 2); v. a. Art. 32 Abs. 1 (ex Art. 30 Abs. 1)	Streichen	§ 9 S. 2 BDSG konkretisiert die Anforderungen an die Verhältnismäßigkeit etwaiger technischer oder organisatorischer Maßnahmen. Der Regelungsgehalt der Norm läuft parallel zu Art. 24 Abs. 1 (ex Art. 22 Abs. 1), Art. 25 Abs. 1, 2 (ex Art. 23 Abs. 1, 2) und Art. 32 Abs. 1 (ex Art. 30 Abs. 1) DSGVO, so dass es keiner Aufrechterhaltung der Norm bedarf.

§ 9a: Datenschutzaudit

Das von einem sinnvollen Regelungsgedanken getragene Konzept des Datenschutzaudits entfaltete mangels gesetzlicher Ausgestaltung im Sinne des § 9a S. 2 bereits unter dem BDSG kein Leben.[513] Nach Inkrafttreten der DSGVO,

[511] Siehe dazu *Plath*, in: ders. (Hrsg.), BDSG, 2013, § 9, Rn. 1; Rn. 1.
[512] Dazu *Plath* (Fn. 511), § 9, Rn. 9.
[513] Siehe *Hornung*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 9a BDSG, Rn. 1 f., 15 ff.

insbesondere der Regelungen zu Art. 42 f. DSGVO, ist für § 9a BDSG kein Raum mehr. Denn jene enthalten bereits detaillierte Anforderungen an die Vergabe und die Verfahren für Datenschutzsiegel und -prüfzeichen. Die DSGVO hält zwar eine Öffnungsklausel vor, die eine Förderungspflicht (Art. 42 Abs. 1 S. 1) sowie einen Regelungsauftrag im Hinblick auf die Akkreditierung der Zertifizierungsstellen (Art. 43 Abs. 1 S. 2 DSGVO) umfasst. Zu ihrer Ausfüllung dürfen die Mitgliedstaaten Regelungen treffen. § 9a BDSG kann aber vor diesem Hintergrund allenfalls als Erfüllung der Förderpflicht des Art. 42 Abs. 1 DSGVO im deutschen Recht weiterhin Bestand haben.

§ 9a BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
S. 1	i. w. S. Art. 42, 43 DSGVO	Streichen	Ratio legis des § 9a S. 1 BDSG war die Schaffung eines Datenschutzaudit-Siegels;[514] dies regeln nunmehr Art. 42, 43 DSGVO.
S. 2		Streichen	Bislang fehlte ohnehin die nähere Ausgestaltung durch Gesetz. Umfassendere und nichtkonkretisierungsbedürftige Bestimmungen enthalten die Art. 42, 43 DSGVO, die nur in Bezug auf die Akkreditierungsstelle konkretisierungsbedürftig sind (dazu siehe unten die Ausführungen zu § 38a BDSG).

§ 10: Einrichtung automatisierter Abrufverfahren

In § 10 BDSG trägt der Gesetzgeber der Erkenntnis Rechnung, dass die Einrichtung eines automatisierten Abrufverfahrens schon vor der eigentlichen Datenübermittlung ein erhöhtes Gefährdungspotenzial für die personenbezogenen Daten Betroffener aufweist. Aus diesem Grund hält § 10 BDSG verfahrensbezogene und organisatorische Anforderungen bereit, insbesondere die Dokumentationspflicht (Abs. 2) und die Beteiligung der Aufsicht bzw. der

[514] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 9, Rn. 2.

Sicherheitsbehörden (Abs. 3 S. 1, 2). Ausgenommen vom Anwendungsbereich der Norm sind allgemein zugängliche Abrufverfahren, etwa bei frei zugänglichen Onlinepräsenzen (Abs. 5).
Prima facie scheint § 10 BDSG ein von der DSGVO gänzlich unbeackertes Feld zu bestellen, namentlich den Datenschutz bei der Einrichtung automatisierter Abrufverfahren noch vor der Datenweitergabe. Gleichwohl fügt sich diese Maßnahme in eine natürliche Handlungseinheit mit der davor regelmäßig stattfindenden Datenverarbeitung ein, so dass § 10 BDSG jedenfalls für den Bereich nicht-öffentlicher Stellen zu streichen ist. Für den Bereich öffentlicher Stellen ist eine Beibehaltung im Hinblick auf den Regelungsspielraum des nationalen Gesetzgebers erwägenswert, den Art. 6 Abs. 1 UAbs. 1 lit. c und e i V. m. Abs. 2 und 3 einräumt. Für § 10 BDSG lassen sie aber nur Raum, soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer im öffentlichen Interesse liegenden oder in Ausübung öffentlicher Gewalt nachfolgenden Verarbeitung erforderlich ist. Art. 6 Abs. 3 S. 3 DSGVO gestattet den Mitgliedstaaten insbesondere besondere Regeln zu Verarbeitungsvorgängen und –verfahren.

§ 10 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
§ 10 insgesamt	Art. 4 Nr. 2 (Verarbeiten u. a. auch „die Weitergabe durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung“), Art. 6 Abs. 1 UAbs. 1	Streichen bzw. in modifizierter Form für öffentliche Stellen aufrechterhalten	§ 10 BDSG begründet besondere Anforderungen an die Bereitstellung von Daten im Rahmen von automatisierten Abrufverfahren. Von ihnen geht nach der Wertung des nationalen Gesetzgebers ein erhöhtes Risiko für die Persönlichkeitsrechte Betroffener aus[515]. Die Bestimmung setzt auf der Vorstufe einer Verarbeitung, namentlich der Übermittlung der Daten, an. So wird auch § 3 Abs. 4 S. 2 Nr. 3 BDSG ausgelegt: Eröffnet eine Stelle lediglich eine Zugriffsmöglichkeit, erfüllt dies noch nicht den Tatbestand des Übermittelns. Wann ein datenschutzrechtliches Rechtfertigungsbedürfnis entsteht, regelt Art. 6 Abs. 1

[515] *Plath*, in: ders. (Hrsg.), BDSG, 2013, § 10, Rn. 2.

	lit. c und c i. V. m. Art. 6 Abs. 2 und 3 S. 3 DSGVO		DSGVO. Er knüpft an die *Verarbeitung* im Sinne des Art. 4 Nr. 2 DSGVO an. Dieser stuft grundsätzlich auch die Bereitstellung als Verarbeitung ein.[516] Auch die Vorfeldmaßnahme der Einrichtung automatisierter Abrufverfahren ist daher als Verarbeitung im Sinne der DSGVO einzustufen. In welchem Umfang *nicht-öffentliche* Stellen personenbezogene Daten verarbeiten dürfen, behält sich die Union in Art. 6 DSGVO grundsätzlich zur alleinigen Entscheidung vor. Art. 23 (ex Art. 21) DSGVO vermittelt ebenso keine Regelungsbefugnis. Er gestattet vielmehr die Absenkung der Schutzrechte Betroffener, bietet aber keine Verarbeitungsgrundlage. Art. 6 Abs. 3 S. 3 DSGVO i. .V. m. Art. 6 Abs. 1 UAbs. 1 lit. c und e i V. m. gestattet den Mitgliedstaaten für den Bereich öffentlicher Stellen besondere Regeln zu Verarbeitungsvorgängen und –verfahren.

§ 11: Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

Wie schon die DSRL und § 11 BDSG regelt auch die Datenschutz-Grundverordnung das Instrument der Auftragsverarbeitung als effizienter Gestaltungsform arbeitsteiliger Datenverarbeitung. Sie ermöglicht (praeter

[516] Dies allerdings nicht pauschal, sondern nur, wenn sie Bestandteil einer Vermittlung ist („Weitergabe durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung"). Das deutet auf den ersten Blick darauf hin, dass im Bereitstellen nur dann eine Verarbeitung zu sehen ist, wenn die Daten tatsächlich weitergegeben werden. Das würde aber zu kurz greifen. Vielmehr sieht Art. 4 Nr. 2 (ex Art. 4 Nr. 3) DSGVO in der Bereitstellung selbst bereits eine Form der Weitergabe (so auch für § 3 Abs. 4 S. 2 Nr. 3 BDSG, *Eßer* (Fn. 459), § 3 BDSG, Rn. 57, der Bereitstellen und Übermitteln gleichsetzt). Den Begriff der Verarbeitung konzipiert Art. 4 Nr. 2 (ex Art. 4 Nr. 3) auch bewusst weit. Insbesondere reicht jede „Vorgangsreihe im Zusammenhang mit personenbezogenen Daten" aus. Das bestätigt auch Art. 25 Abs. 1 (ex Art. 23 Abs. 1) DSGVO. Indem er verlangt, dass schon im Vorfeld der eigentlichen Verarbeitung, wenn also die Mittel der Verarbeitung festgelegt werden, sichernde Maßnahmen vorzunehmen, bringt er zum Ausdruck, dass die DSGVO auch auf diese Phase Anwendung findet. Des Weiteren fallen tatsächliche Verarbeitungsvorgänge und die Errichtung eines automatisierten Abrufverfahrens häufig zusammen, stellen aber zumindest einen einheitlichen Lebenssachverhalt dar, der sich nur schwerlich trennen lässt.

propter) rechtlich die Einbeziehung von Auftragnehmern in die eigene Datenverarbeitung, als seien sie Teil des eigenen Betriebs.[517] Art. 28 (ex Art. 26) und 29 (ex 27) DSGVO formen die wesentlichen Aspekte des Verhältnisses zwischen Verantwortlichem und Auftragsverarbeiter nunmehr selbst aus. Insbesondere Vorgaben für die Auswahl, das notwendige vertragliche Grundverhältnis und die Weisungsbindung folgen direkt aus der Datenschutz-Grundverordnung. Gleichzeitig enthalten Art. 28 (ex Art. 26) und 29 (ex 27) DSGVO an mehreren Stellen (echte wie unechte)[518] Öffnungsklauseln. Die Datenschutz-Grundverordnung ermöglicht den Mitgliedstaaten insbesondere, ein eigenes Rechtsinstrument (statt eines Vertrages) für die Gestaltung der Auftragsbeziehungen zwischen dem Verantwortlichen und dem Auftragsverarbeiter vorzusehen. Mittelbar eröffnet die Datenschutz-Grundverordnung auch Handlungsspielräume für die Pflichten, die den Auftragsverarbeiter treffen – etwa im Hinblick auf die Weisungsbindung (Art. 28 Abs. 3 UAbs. 1 S. 2 lit. a [ex Art. 26 Abs. 2 lit. a] DSGVO) und die Löschung (Art. 28 Abs. 3 UAbs. 1 S. 2 lit. g [ex Art. 26 Abs. 2 lit. g] DSGVO) – bzw. verweist auf solche Handlungsoptionen.

Vergleicht man die Regelung des BDSG mit derjenigen der Datenschutz-Grundverordnung, so fällt auf, dass § 11 Abs. 2 BDSG im Hinblick auf die Ausgestaltung des Auftragsverhältnisses vielfach deutlich detailliertere Vorgaben trifft, während die Datenschutz-Grundverordnung pauschal auf die zwischen dem Verantwortlichen und dem Auftragsverarbeiter geltenden Anforderungen verweist. Mit der Wendung „insbesondere“ in Art. 28 Abs. 3 UAbs. 1 S. 2 [ex Art. 26 Abs. 2 S. 1] gibt die Datenschutz-Grundverordnung zu erkennen, dass sie ihre Regelungen nicht als abschließend konzipiert hat, sondern für weitere Konkretisierungen offen ist. Primär denkt die Verordnung an eine Konkretisierung durch ergänzendes EU-Recht, v. a. soweit genehmigte Verhaltensregeln und zertifizierte Verfahren dies ausformen (Abs. 5 [ex Abs. 2aa]) bzw. Standardvertragsklauseln der Kommission bzw. der Aufsichtsbehörden eine Typisierung vornehmen (Abs. 6 [ex Abs. 2ab]). Eine *inhaltliche* Konkretisierung datenschutzrechtlicher Verarbeitungsvorgaben

[517] Dazu etwa *Martini/Fritzsche* (Fn. 409), 5 f. m. w. N.
[518] Zu der Terminologie S. 11.

durch nationale Vorschriften ist hingegen mangels Öffnungsklausel nicht zulässig.
Um im Interesse der Rechtsklarheit für den Anwender einen einheitlichen Regelungskontext herzustellen, ist es dem nationalen Gesetzgeber aber gestattet, die Regelungen teilweise mit in sein nationales Recht aufzunehmen, ohne gegen das Wiederholungsverbot zu verstoßen, soweit ihm noch ein eigener Regelungsspielraum verbleibt.[519]

§ 11 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 S. 1 Klarstellung der Verantwortlichkeit des Auftraggebers	Art. 28 Abs. 10 (ex Art. 26 Abs. 4)	Streichen (beibehalten [und ergänzen um eine dem Art. 28 Abs. 10 (ex Art. 26 Abs. 4) DSGVO entsprechende Regelung] nur in den Grenzen des Wiederholungsverbots zulässig)	Die DSGVO geht – wie auch § 11 Abs. 1 S. 1 BDSG – von der Verantwortlichkeit des Auftraggebers aus. Das folgt jedenfalls im Umkehrschluss aus Art. 28 Abs. 10 (ex Art. 26 Abs. 4) DSGVO. Art. 82 Abs. 1 und 2 (ex Art. 77 Abs. 1 und 2) DSGVO unterwerfen den Auftragsverarbeiter zwar auch einem Schadensersatzanspruch sowie einem beschränkten Haftungsanspruch. Dies macht den Auftragsverarbeiter aber – wie sich aus der Gegenüberstellung der Begriffe in den Vorschriften ergibt – noch nicht zum für die Verarbeitung Verantwortlichen. Konstruktiv ist denkbar, dass das deutsche Recht im Hinblick auf Art. 28 Abs. 10 DSGVO klarstellt, dass der Auftragsverarbeiter, der unter Verstoß gegen die DSGVO die Zwecke und Mittel der Datenverarbeitung bestimmt, in Bezug auf diese Verarbeitung als für die Verarbeitung Verantwortlicher gilt. Das ergibt sich aber aus der DSGVO selbst. Ein Zusammenhang mit einer Öffnungsklausel, der eine Normwiederholung rechtfertigt, ist nicht erkennbar.

[519] Dazu auch S. 6.

Abs. 1 S. 2 (Verweis auf die Betroffenenrechte und Schadensersatzansprüche)	Art. 28 Abs. 10 (ex Art. 26 Abs. 4), Art. 82 Abs. 3 und 4 (ex Art. 77 Abs. 3 und 4)	Streichen	Das deutsche Recht weist die Verantwortung für die Betroffenenrechte dem Auftraggeber, nicht aber dem Auftragsverarbeiter zu. Auch die DSGVO beschränkt die Betroffenenrechte in ihren Artikeln 16 ff. auf den für die Verarbeitung Verantwortlichen. Sie legt dem Auftragsverarbeiter aber eine Unterstützungspflicht gegenüber dem Verantwortlichen auf (Art. 28 Abs. 3 UAbs. 1 lit. e). Für eine eigene nationale Regelung besteht weder Bedarf noch (mangels Konnex zu einer einschlägigen Öffnungsklausel, etwa Art. 23, 28 Abs. 3 S. 1) Regelungsspielraum.
Abs. 2 S. 1 (Auswahlverantwortung)	Art. 28 Abs. 1, Abs. 3 UAbs. 1 S. 2 lit. c i. V. m. Art. 32 (ex Art. 26 Abs. 2 lit. c i. V. m. Art. 30)	Streichen	Die Auswahlverantwortung des Verantwortlichen drückt Art. 28 Abs. 1 DSGVO (ohne diesen Begriff zu verwenden) aus. Art. 28 Abs. 3 UAbs. 1 S. 1 (ex Art. 26 Abs. 2 S. 1) lässt für nationalstaatliche Präzisierungen und Ergänzungen keinen Raum. Soweit man in der Vorschrift einen solchen Spielraum erkennen mag, erstreckt er sich jedenfalls nur auf das „Wie“ einer Auftragsgestaltung, nicht aber auf das „Ob“ der Auswahl.
Abs. 2 S. 2 (Vertragsinhalt)	Art. 28 Abs. 3, 9 (ex Art. 26 Abs. 2, Abs. 3)	Streichen	Die inhaltlichen Anforderungen an das Verhältnis zum Auftragsverarbeiter zeichnet bereits die DSGVO vor, ohne den Mitgliedstaaten einen inhaltlichen Regelungsspielraum zuzugestehen. Zwar regelt die DSGVO den Vertragsinhalt nicht abschließend („insbesondere“). Sie gesteht jedoch nicht den Mitgliedstaaten das Recht zu, diesen Inhalt näher zu konkretisieren. Die DSGVO räumt den Mitgliedsstaaten lediglich den Spielraum zur Wahl einer anderen Handlungsform ein („Rechtsinstrument nach dem … Recht der Mitgliedstaaten“), den das BDSG jedoch gerade nicht nutzt („Auftrag“).
Abs. 2 S. 3 (Erteilung des Auftrags durch die Fachaufsichtsbehör-	Art. 28 Abs. 3 UAbs. 1 S. 1 (ex Art. 26 Abs. 2 S. 1)	Bei Bedarf modifiziert aufrechterhalten	Die Erteilung eines Auftrages durch die Fachaufsichtsbehörde bei öffentlichen Stellen macht prima facie von dem Regelungsspielraum Gebrauch, den Art. 28 Abs. 3 S. 1 (ex Art. 26 Abs. 2) DSGVO mit der Wendung „oder eines anderen Rechtsinstruments nach

de)			dem Recht der Union oder der Mitgliedstaaten“ eröffnet. Bei genauerem Hinsehen trifft § 12 Abs. 2 S. 3 BDSG aber nur eine spezielle Zuständigkeitsregelung, mit der kein sich besonderes Handlungsinstrument verbindet. In modifizierter Form aufrechterhalten bleiben kann die Vorschrift nur dann, wenn sich mit der Auftragserteilung bei öffentlichen Stellen auch ein besonderes mitgliedstaatliches Handlungsinstrument, z. B. ein einseitig verpflichtendes öffentlich-rechtliches Rechtsgeschäft, verbindet. Ein Regelungsbedarf ist dafür aber nicht erkennbar.
Abs. 2 S. 4 (Prüfung- und Überwachungspflicht)	Art. 28 Abs. 1, Abs. 3 UAbs. 1 S. 2 lit. h, UAbs. 2, Art. 32 Abs. 1 (ex Art. 26 Abs. 1, Abs. 2 lit. h, Art. 30 Abs. 1)	Streichen	Die Norm bildet spiegelbildlich die Formulierung in Art. 28 Abs. 1 (ex Art. 26 Abs. 1) und Art. 28 Abs. 3 UAbs. 1 S. 2 lit. h, UAbs. 2 (ex Art. 26 Abs. 2 lit. h) DSGVO ab, indem sie dem Auftraggeber gewisse Kontrollpflichten auch in zeitlicher Hinsicht („vor Beginn der Datenverarbeitung und sodann regelmäßig“) auferlegt. Die Regelungen der DSGVO sind als abschließend konzipiert, ohne den Mitgliedsstaaten inhaltlichen Regelungsspielraum zu belassen.
Abs. 2 S. 5 (Dokumentationspflicht)	Art. 28 Abs. 1, Art. 30 Abs. 1 lit. g (ex Art. 26 Abs. 1, Art. 28 Abs. 1 lit. h)	Streichen	Die Vorschrift trägt ergänzend zur Erhöhung von Transparenz und Nachvollziehbarkeit der Verantwortlichkeit bei. Allerdings lässt die DSGVO den Mitgliedstaaten keinen hinreichenden eigenen inhaltlichen Regelungsspielraum.
Abs. 3 S. 1 (Weisungsbindung)	Art. 29 (ex Art. 27)	Streichen / u. U. beibehalten	Art. 29 (ex Art. 27) DSGVO verlangt dem Verantwortlichen sowie dem Auftragsverarbeiter unterstellten Personen Weisungsgebundenheit ab. Im Interesse einer konsistenten und in sich verständlichen Regelung darf § 11 Abs. 3 BDSG diese Regelung für das deutsche Recht u. U. wiederholen, falls die Bundesrepublik von dem in Art. 29 i. V. m. Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO eröffne-

			ten Handlungsspielraum Gebrauch macht.
Abs. 3 S. 2 (Hinweispflicht)	Art. 28 Abs. 3 UAbs. 2	Streichen	Die DSGVO sieht ebenso eine Pflicht des Auftragnehmers zum Hinweis bei rechtswidrigen Weisungen ausdrücklich vor. Daneben besteht weder Regelungsspielraum noch -bedarf.
Abs. 4 (Verweis auf die gegenüber dem Auftragsverarbeiter anwendbaren Normen)	-	Streichen / Modifizieren	Welchem Regelungsregime der Auftragsverarbeiter unterworfen ist, regelt die DSGVO grundsätzlich abschließend. Der Verweis auf die anwendbaren Normen kann allenfalls modifiziert in der Form aufrechterhalten bleiben, die Normen *der DSGVO* in Bezug zu nehmen, welche auf den Auftragsverarbeiter Anwendung finden (vgl. z. B. Art. 33 Abs. 2 [ex Art. 31 Abs. 2] DSGVO). Sinnvoll ist das jedoch nicht.
Abs. 5 („Fernwartung“)	-	Streichen	§ 11 Abs. 5 BDSG bezieht sich insbesondere auf solche Konstellationen, in denen durch Wartungs- und Prüfungsvorgänge ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.[520] Solche Konstellationen nehmen in der praktischen Bedeutung des Rechtsalltags stetig zu. Den Mitgliedstaaten steht es aber nicht frei, den Begriff des Auftragsverarbeiters zu definieren, seinen Inhalt auszudehnen oder den Pflichtenkatalog von Datenverarbeitern zu erweitern. Eine Öffnungsklausel hält die DSGVO insoweit nicht vor.

[520] *Petri*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 38a, Rn. 98 ff.

§§ 12 – 18: Rechtsgrundlagen der Datenverarbeitung durch öffentliche Stellen

§ 12: Anwendungsbereich

§ 12 BDSG legt die Normadressaten für die Bestimmungen der §§ 12 – 26 BDSG fest. Diese gelten nach § 12 Abs. 1 BDSG für öffentliche Stellen des Bundes (mit Ausnahme der am Wettbewerb teilnehmenden öffentlich-rechtlichen Unternehmen).
Die Unterscheidung von öffentlichen und nicht-öffentlichen Stellen ist in der Datenschutz-Grundverordnung nicht angelegt. Allerdings ermöglicht Art. 4 Nr. 7 (ex Art. 4 Nr. 5) DSGVO den Mitgliedstaaten, einen Verantwortlichen zu bestimmen oder spezifische Kriterien festzulegen, mittels derer der Verantwortliche bestimmt werden soll. Damit ist auch eine Kategorisierung der Verantwortlichen in öffentliche und nicht-öffentliche Stellen möglich.[521] § 12 BDSG kann damit aufrechterhalten werden.

§ 12 BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
§ 12	Art. 4 Nr. 7 (ex Art. 4 Nr. 5 DSGVO)	Beibehalten	Konkretisierung des Verantwortlichen zulässig; „Einstiegsnorm“ für die §§ 13 – 16 BDSG – vgl. insoweit die weiteren diesbezüglichen Ausführungen

§§ 13 – 16: Trennung der Verarbeitungsschritte

Die §§ 13 – 16 BDSG regeln unterschiedliche Zulässigkeitstatbestände für verschiedene Verarbeitungsschritte. So regelt § 13 BDSG das Erheben von personenbezogenen Daten durch öffentliche Stellen, § 14 BDSG demgegenüber das Speichern, Verändern und Nutzen. Die §§ 15, 16 BDSG regeln die Zulässigkeitsanforderungen an die Datenübermittlung.

[521] Vgl. ausführlich S. 25.

Die DSGVO definiert in Art. 4 Nr. 2 (ex Art. 4 Nr. 3) (wie schon die RL 95/46/EG) nur einen allgemeinen Verarbeitungsbegriff, der jedoch all diese Handlungen der in Deutschland ausdifferenzierten Schritte des Erhebens, der verschiedenen Verarbeitungsschritte im Sinne des deutschen Datenschutzrechts und der Nutzung umfasst. Zudem ist der in Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO i. V. m. Art. 6 Abs. 2, 3 (ex Art. 6 Abs. 2a, 3) DSGVO eingeräumte Spielraum für die Mitgliedstaaten weit zu verstehen.[522] Somit sind auch eine Trennung der Verarbeitungsvorgänge und damit korrespondierende unterschiedliche Regelungen im Rahmen der von den Öffnungsklauseln gegebenen Spielräume möglich. Denkbar wäre jedoch auch eine Zusammenfassung der Verarbeitungsschritte in eine einheitliche Vorschrift im BDSG-neu. Das gilt insbesondere, wenn allgemein im deutschen Datenschutzrecht die Ausdifferenzierung in die Kategorien des Erhebens, Verarbeitens und Nutzens eingeebnet werden soll.

§ 13: Datenerhebung

§ 13 Abs. 1 BDSG lässt eine Erhebung personenbezogener Daten durch öffentliche Stellen dann zu, wenn deren Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Damit entspricht die Norm in großen Teilen der Vorgabe des Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1 DSGVO – mit dem Unterschied, dass § 13 Abs. 1 BDSG explizit nur auf öffentliche Stellen anwendbar ist und nur für das Erheben von Daten gilt. § 13 BDSG kommt damit dem Erfordernis nach, dass Art. 6 Abs. 3 S. 1 DSGVO eine Rechtsgrundlage für die Aktivierung der Verarbeitungen nach Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO erforderlich ist. Ob insoweit überhaupt eine Konkretisierung erforderlich ist und wenn ja, wie weit diese Konkretisierungsnotwendigkeit reicht und § 13 BDSG sie sodann erfüllt, harrt einer Klärung.

[522] Vgl. ausführlich S. 33 und S. 34.

a. Abs. 1: Erheben personenbezogener Daten durch öffentliche Stellen

Bei einer Betrachtung des § 13 Abs. 1 BDSG stellt sich die Frage, ob die Norm die Voraussetzungen des Art. 6 Abs. 2 (ex Abs. 2a) i. V. m. Abs. 3 DSGVO erfüllt. Klärungsbedürftig ist insofern der Umfang der nötigen Spezifikation bzw. Präzisierung der nationalen Norm. Die Formulierungen in Art. 6 Abs. 2 (ex Abs. 2a) DSGVO („spezifischere Bestimmungen (…) beibehalten oder einführen“ / „maintain or introduce *more specific* provisions“ sowie „spezifische Anforderungen [...] präziser bestimmen“ / „determining *more precisely specific* requirements“) deuten jedenfalls daraufhin, dass die Normen ein „Mehr“ an Regelungsgehalt gegenüber den Normen der Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO beinhalten müssen. Das führt zunächst zu der Annahme, dass eine Regelung, die lediglich die Vorgaben aus Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO wiederholt, nicht ausreichend sein kann. Gleichzeitig ist der Wortlaut der Öffnungsklausel aber relativierend gehalten, spricht er doch lediglich von „spezifischeren Regelungen“[523] und einer „präziseren Bestimmung spezifischer Voraussetzungen“[524]. Daraus lässt sich also noch keine Aussage über die nötige Reichweite der Spezifizierung und Präzisierung ableiten. EG 45 S. 2 (ex EG 36 S. 2) DSGVO stellt hierzu klar, dass kein spezifisches Gesetz für jeden individuellen Verarbeitungsvorgang nötig ist. Es soll demnach auch ausreichen, wenn ein Gesetz Basis für mehrere Verarbeitungsvorgänge i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO ist. Das spricht dafür, dass die Normen für eine Mehrzahl von Fällen abstrakt gehalten werden kann.
Hinzu kommt, dass der Wortlaut des Art. 6 Abs. 3 DSGVO, demzufolge die rechtliche Grundlage für solche Verarbeitungen spezifischere Regelungen enthalten *kann*, wie etwa *generelle* Bedingungen über die Rechtmäßigkeit der Datenverarbeitung durch den Verantwortlichen oder die Art der Daten, die verarbeitet werden dürfen, den Mitgliedstaaten Handlungsbefugnisse bloß eröffnet, sie aber nicht zur Handlung zwingt. Damit wäre überhaupt keine Konkretisierung erforderlich.

[523] „more specific provisions”.
[524] „determining more precisely specific requirements“.

Daraus ist zu schließen, dass die Mitgliedstaaten nach Art. 6 Abs. 2 (ex Abs. 2a) DSGVO wohl jedenfalls keine bereichsspezifischen Regelungen erlassen können, die rein den Wortlaut der Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO wiedergeben. Sollten diese Regelungen die genaueren Umstände aber präzisieren, sind die Anforderungen aus Art. 6 Abs. 2 (ex Abs. 2a) DSGVO erfüllt. Das „Mehr" an Präzision in den nationalen Normen muss demnach nicht sehr groß sein. Aus dem Zusammenspiel von Art. 6 Abs. 2 (ex Abs. 2a) und Abs. 3 DSGVO lässt sich herauslesen, dass eine allgemeine, letztlich wiederholende Bestimmung zu Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO in einem allgemeinen datenschutzrechtlichen Teil zulässig wäre und nur im Falle einer bereichsspezifischen Regelung aus der Konkretisierungsoption des Art. 6 Abs. 3 DSGVO eine (sehr moderate) Konkretisierungspflicht des Art. 6 Abs. 2 (ex Abs. 2a) DSGVO erwächst.
Danach erfüllt § 13 Abs. 1 BDSG die Voraussetzungen der Art. 6 Abs. 3 DSGVO, da die Norm im Zusammenspiel mit den §§ 14 und 15 BDSG bereits eine Ausdifferenzierung hinsichtlich der verantwortlichen Stellen (nur öffentliche Stellen) und der Verarbeitungsschritte (hier nur Erhebung, abweichende Regelungen für die Verarbeitung und Übermittlung) vorsieht. Damit erfolgt eine hinreichende Ausdifferenzierung des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO. § 13 Abs. 1 BDSG kann daher zulässigerweise aufrechterhalten werden. Da auch ein entsprechendes Erhebungsbedürfnis allgemein für öffentliche Stellen greift, das die Datenschutz-Grundverordnung so nicht selbst regelt, ist eine entsprechende Regelung im nationalen Recht auch geboten, um entsprechende Erhebungen weiterhin zu ermöglichen.

b. Abs. 1a: Hinweispflichten bei der Erhebung bei nicht-öffentlichen Stellen

§ 13 Abs. 1a BDSG sieht Informationspflichten der öffentlichen Stelle vor, wenn die personenbezogenen Daten nicht beim Betroffenen, sondern bei einer nicht-öffentlichen Stelle erhoben werden. Eine ähnliche Vorschrift findet sich in der Datenschutz-Grundverordnung nicht. Die Regelung des Art. 14 (ex Art. 14a) DSGVO adressiert die Pflichten des Verarbeiters gegenüber Betroffenen und nicht gegenüber Dritten, bei denen die Daten erhoben werden; sie ist somit nicht einschlägig. Auch ohne explizit korrespondierende Norm gibt Art. 6 Abs. 3 DSGVO den Mitgliedstaaten einen weiten Spielraum hin-

sichtlich der Gestaltung der Rechtsgrundlagen i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO, insbesondere auch zur Spezifizierung und Präzisierung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten.[525] Solche zusätzlichen Bestimmungen können damit zulässigerweise aufrechterhalten werden. Dies gilt insbesondere vor dem Hintergrund, dass die Datenschutz-Grundverordnung – wie schon die RL 95/46/EG – keinen expliziten Grundsatz der Direkterhebung kennt.

c. Abs. 2: Erhebung besonderer Arten personenbezogener Daten durch öffentliche Stellen

§ 13 Abs. 2 BDSG regelt Fälle, in denen die Erhebung besonderer Arten personenbezogener Daten durch öffentliche Stellen ausnahmsweise zulässig ist. Die Zulässigkeit der Verarbeitung besonderer Arten personenbezogener Daten ist in der Datenschutz-Grundverordnung in Art. 9 DSGVO geregelt. Die Verarbeitung i. S. d. Datenschutz-Grundverordnung umfasst gem. Art. 4 Nr. 2 (ex Art. 4 Nr. 3) DSGVO auch das Erheben.
Dabei stimmt der Begriff der besonderen Arten personenbezogener Daten aus § 13 Abs. 2 i. V. m. § 3 Abs. 9 BDSG mit dem Begriff der besonderen Kategorien personenbezogener Daten aus Art. 9 DSGVO weitgehend überein, wobei Art. 9 Abs. 1 DSGVO noch weiter greift, indem auch genetische und biometrische Daten erfasst werden.

d. Abs. 2 Nr. 1 Alt. 1

§ 13 Abs. 2 Nr. 1 Alt. 1 BDSG regelt, dass die Erhebung besonderer Arten personenbezogener Daten zulässig ist, wenn eine Rechtsvorschrift dies vorsieht. Damit entspricht § 13 Abs. 2 Nr. 1 Alt. 1 BDSG dem Verbot mit Erlaubnisvorbehalt und ist grundsätzlich vereinbar mit Art. 9 Abs. 1 DSGVO, der ein grundsätzliches Verbot der Verarbeitung dieser Daten vorsieht, die nur in den abschließend geregelten Fällen des Art. 9 Abs. 2 DSGVO erlaubt ist. Dazu muss die nationale Vorschrift aber die Voraussetzungen des Katalogs in Art. 9 Abs. 2 DSGVO erfüllen, d. h. z. B., dass eine entsprechende Erlaubnisregel im Sinne des Art. 9 Abs. 2 lit. g DSGVO „angemessene und

[525] Vgl. ausführlich S. 34.

spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht“. Eine solche Konkretisierung sieht § 13 Abs. 2 Nr. 1 Alt. 1 BDSG nicht vor, so dass die Norm so nicht aufrechterhalten bleiben kann. Die Bestimmung ist als Verweis bzw. „Schaltnorm“ auf andere Rechtsvorschriften und insbesondere einschlägige Erlaubnistatbestände in bereichsspezifischen Gesetzen aber auch überflüssig, da sich die entsprechenden Anforderungen ohnehin aus der spezifischen Norm ergeben müssen und Art. 9 Abs. 2 DSGVO insofern schon die Öffnungsklausel darstellt, die nicht noch einmal im nationalen Recht formuliert werden muss.

e. Abs. 2 Nr. 1 Alt. 2

§ 13 Abs. 2 Nr. 1 Alt. 2 BDSG regelt die Zulässigkeit der Erhebung besonderer Arten personenbezogener Daten, wenn eine Rechtsvorschrift dies aus Gründen eines wichtigen öffentlichen Interesses zwingend erfordert. Art. 9 Abs. 2 lit. g DSGVO sieht ebenfalls die Zulässigkeit dieser Daten auf Grundlage des Unionsrechts oder Rechts eines Mitgliedstaates vor, verlangt allerdings weiterreichend, dass die allgemeinen Anforderungen des Verhältnismäßigkeitsgrundsatzes und des Wesensgehalts zu wahren sind und die mitgliedstaatliche Grundlage außerdem angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der Betroffenen vorsehen muss. Die Anforderung des Verhältnismäßigkeitsgrundsatzes und des Wesensgehalts spiegeln lediglich Vorgaben des Grundgesetzes und der Grundrechtecharta wider, die ohnehin zu wahren sind.[526] Es stellt sich jedoch die Frage, ob § 13 Abs. 2 Nr. 1 Alt. 2 BDSG den Anforderungen des Art. 9 Abs. 2 lit. g DSGVO hinsichtlich geeigneter und spezifischer Maßnahmen genügen kann. Der Hinweis auf den spezifischen Charakter der Maßnahme spricht dabei eher für eine eigenständige Absicherung. Eine allgemein gehaltene Norm wie § 13 Abs. 2 Nr. 1 Alt. 2 BDSG, die keine weiteren Anforderungen zur Wahrung der Grundrechte oder Interessen der betroffenen Person vorsieht, wird deswegen wohl nicht aufrechterhalten bleiben können.
Allerdings verlangt bereits jetzt EG 34 S. 2 RL 95/46/EG von den Mitgliedstaaten, im Fall der Aktivierung der Ausnahme vom Verarbeitungsverbot für

[526] Vgl. hierzu S. 53 f.

sensible Daten entsprechende Maßnahmen („geeignete besondere Garantien zu Schutz der Grundrechte und der Privatsphäre von Personen“) vorzusehen, ohne dass sich dies im Gesetzeswortlaut niedergeschlagen hätte. Die Kommentarliteratur sieht das, soweit erkennbar, offensichtlich als nicht weiter problematisch an[527] und versteht die Garantiepflichten als durch den Gesetzgeber im Rahmen der Normschaffung zu erfüllendes Prüfprogramm[528]. Unabhängig davon lässt sich argumentierten, dass § 13 Abs. 2 Nr. 1 Alt. 2 BDSG verschärfend verlangt, dass das Erheben „zwingend“ erforderlich ist und impliziert damit einen besonders verschärften Maßstab[529]. Dann lassen sich die „angemessenen und spezifischen Maßnahmen“ als Teil eines verschärfenden Maßstabs zur Wahrung der Grundrechte deuten. Auch wenn insoweit Restzweifel verbleiben, entstehen diese nicht erst anlässlich der Datenschutz-Grundverordnung, sondern bestanden wenn dann auch schon gegenwärtig mit Blick auf die Vorgaben der RL 95/46/EG.

f. Abs. 2 Nr. 2

§ 13 Abs. 2 Nr. 2 BDSG lässt die Erhebung besonderer Arten personenbezogener Daten zu, soweit der Betroffene eingewilligt hat und entspricht im Wesentlichen Art. 9 Abs. 2 lit. a DSGVO. Allerdings setzt § 13 Abs. 2 Nr. 2 BDSG eine Einwilligung nach § 4 Abs. 3a BDSG voraus. Geht man davon aus, dass die Öffnungsklausel angesichts der weit gehenden mitgliedstaatlichen Gestaltungsbefugnis als Minus auch das Aufstellen zusätzlicher Anforderungen an die Einwilligung abdeckt[530], und dass § 4 Abs. 3a BDSG weiterreichende Anforderungen aufstellt als Art. 4 Nr. 11 (ex Art. 4 Nr. 8) DSGVO[531], kann § 13 Abs. 2 Nr. 2 BDSG zulässigerweise aufrechterhalten werden. Die Sonderregelung kann jedoch auch gestrichen werden, was ausschließlich einer rechtspolitischen Bewertung unterliegt.

---

[527] Siehe etwa *Stender-Vorwachs*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 13 BDSG, Rn. 23 ff.
[528] So explizit *Eßer*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 13 BDSG, Rn. 22 für § 13 Abs. 2 Nr. 1 Alt. 1.
[529] *Eßer* (Fn. 528), § 13 BDSG, Rn. 22 m. w. N.
[530] Vgl. hierzu S. 49.
[531] Vgl. hierzu S. 49.

g. Abs. 2 Nr. 3

§ 13 Abs. 2 Nr. 3 BDSG kann gestrichen werden. Er entspricht Art. 9 Abs. 2 lit. c DSGVO. Dieser enthält keine Öffnungsklausel für die Mitgliedstaaten. Im Übrigen muss durch die Übereinstimmung die Norm auch nicht beibehalten werden, um das bestehende Datenschutzniveau zu erhalten.

h. Abs. 2 Nr. 4

§ 13 Abs. 2 Nr. 4 BDSG kann gestrichen werden, da dieser Art. 9 Abs. 2 lit. e DSGVO entspricht und dort keine Öffnungsklausel für die Mitgliedstaaten enthalten ist. Im Übrigen muss durch die Übereinstimmung die Norm auch nicht beibehalten werden, um das bestehende Datenschutzniveau zu erhalten.

i. Abs. 2 Nr. 5, Nr. 6, Nr. 9

§ 13 Abs. 2 Nr. 5 BDSG betrifft die Zulässigkeit der Datenerhebung zur Abwehr einer erheblichen Gefahr für die öffentlichen Sicherheit, § 13 Abs. 2 Nr. 6 BDSG die Zulässigkeit der Datenerhebung zur Abwehr erheblicher Nachteile für das Gemeinwohl bzw. zur Wahrung desselben und § 13 Abs. 2 Nr. 9 BDSG regelt die Zulässigkeit der Erhebung besonderer Arten personenbezogener Daten aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Bundes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Maßnahmen. Diese drei Nummern betreffen damit Gründe eines wichtigen öffentlichen Interesses i. S. d. Art. 9 Abs. 2 lit. g DSGVO[532]. Auch hier stellt sich jedoch die Frage, wie sich das Erfordernis geeigneter und spezifischer Maßnahmen zur Wahrung der Grundrechte und Interessen Betroffener an die mitgliedstaatliche Rechtsgrundlage i. S. d. Art. 9 Abs. 2 lit. g DSGVO auswirkt. Insoweit kann auf die Ausführungen zu § 13 Abs. 2 Nr. 1 Alt. 1 BDSG verwiesen werden. Demnach können diese Normen in ihrer bestehenden Form wohl auch ohne Modifikationen aufrechterhalten werden.

[532] Zu den Anforderungen an das wichtige öffentliche Interesse vgl. S. 53.

j. Abs. 2 Nr. 7

§ 13 Abs. 2 Nr. 7 BDSG bestimmt die Zulässigkeit der Erhebung besonderer Arten personenbezogener Daten u. a. zum Zweck der Gesundheitsvorsorge und medizinischen Diagnostik, sofern die Verarbeitung durch ärztliches Personal oder sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, erfolgt. Die Voraussetzungen des § 13 Abs. 2 Nr. 7 BDSG decken sich somit mit den Voraussetzungen des Art. 9 Abs. 2 lit. h i. V. m. Art. 9 Abs. 3 (ex Art. 9 Abs. 4) DSGVO. § 13 Abs. 2 Nr. 7 BDSG kann demnach aufrechterhalten werden.

k. Abs. 2 Nr. 8

§ 13 Abs. 2 Nr. 8 BDSG regelt die Zulässigkeit der Erhebung besonderer Arten personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung. Dieser Fall ist in Art. 9 Abs. 2 lit. j (ex Art. 9 Abs. 2 lit. i) DSGVO geregelt. Auch Art. 9 Abs. 2 lit. j (ex Art. 9 Abs. 2 lit. i) DSGVO verlangt jedoch neben der Wahrung des Verhältnismäßigkeitsgrundsatzes und des Wesensgehalts des Rechts auf Datenschutz, dass das mitgliedstaatliche Recht „angemessene und spezifische Maßnahmen“ vorsehen muss, um jene Rechte zu schützen. Insoweit kann auf die Ausführungen zu § 13 Abs. 2 Nr. 1 Alt. 1 BDSG verwiesen werden. Damit gilt auch hier, dass § 13 Abs. 2 Nr. 8 BDSG in seiner bestehenden Form wohl auch ohne Modifikationen aufrechterhalten werden kann.

§ 13 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1 DSGVO	Beibehalten	§ 13 Abs. 1 BDSG stimmt mit Anforderungen aus Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1 DSGVO überein. Art. 6 Abs. 2 (ex Abs. 2a), Abs. 3 DSGVO fordert Präzisierung und Spezifizierung der mitgliedstaatlichen Norm, die durch Ausdifferenzierung der verantwortlichen Stelle und Verarbeitungsgründe erfüllt.
Abs. 1 a	-	Beibehalten	Art. 6 Abs. 2 (ex Abs. 2a), Abs. 3 DSGVO eröffnet den Mitgliedstaaten weitreichenden

			Spielraum zur Schaffung oder Aufrechterhaltung spezifischer Bestimmungen, die Maßnahmen bestimmen, um eine rechtmäßige und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten.
Abs. 2 Nr. 1 Alt. 1	- /(Art. 9 Abs. 2 lit. g)	Streichen	Verweis auf andere Rechtsvorschriften wg. Eventueller Erlaubnistatbeständen in bereichsspezifischen Gesetzen nicht nötig und derart unkonditioniert auch nicht von Öffnungsklauseln gedeckt.
Abs. 2 Nr. 1 Alt. 2	Art. 9 Abs. 2 lit. g	Beibehalten wohl auch ohne Modifikation in Form einer Erweiterung um angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen des Betroffenen	Anforderungen des spezifischen Charakters der Maßnahme unklar hinsichtlich einer Umsetzungsnotwendigkeit im Gesetz selbst.
Abs. 2 Nr. 2	Art. 9 Abs. 2 lit. a	Beibehalten oder Streichen	Art. 9 Abs. 2 lit. a DSGVO deckt das Aufstellen zusätzlicher Anforderungen an die Einwilligung ab.
Abs. 2 Nr. 3	Art. 9 Abs. 2 lit. c	Streichen	Keine Öffnungsklausel; keine Notwendigkeit zur Aufrechterhaltung, da entsprechende Regelung in DSGVO.
Abs. 2 Nr. 4	Art. 9 Abs. 2 lit. e	Streichen	Keine Öffnungsklausel; keine Notwendigkeit und Legitimation zur Aufrechterhaltung, da entsprechende Regelung in DSGVO.
Abs. 2 Nr. 5	Art. 9 Abs. 2 lit. g	Beibehalten wohl auch ohne Modifikation in Form einer Erweiterung um angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen des Betroffenen	Anforderungen des spezifischen Charakters der Maßnahme unklar hinsichtlich einer Umsetzungsnotwendigkeit im Gesetz selbst.
Abs. 2 Nr. 6	Art. 9 Abs. 2 lit. g	Dito	Dito

Abs. 2 Nr. 7	Art. 9 Abs. 2 lit. h i. V. m. Art. 9 Abs. 3 (ex Art. 9 Abs. 4)	Beibehalten; Streichen zulässig aber untunlich	Die Norm erfüllt die Voraussetzungen der Öffnungsklausel.
Abs. 2 Nr. 8	Art. 9 Abs. 2 lit. j (ex Art. 9 Abs. 2 lit. i)	Beibehalten wohl auch ohne Modifikation in Form einer Erweiterung um angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen des Betroffenen	Anforderungen des spezifischen Charakters der Maßnahme unklar hinsichtlich einer Umsetzungsnotwendigkeit im Gesetz selbst.
Abs. 2 Nr. 9	Art. 9 Abs. 2 lit. g	Dito	Der Hinweis auf den spezifischen Charakter der Maßnahme spricht für eine eigenständige Absicherung.

§ 14: Datenspeicherung, -veränderung und -nutzung

a. Abs. 1: Datenspeicherung, -veränderung und -nutzung durch öffentliche Stellen

§ 14 Abs. 1 BDSG bezieht sich auf das Speichern, Verändern und Nutzen personenbezogener Daten durch öffentliche Stellen, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Das Speichern, Verändern und Nutzen ist vom Verarbeitungsbegriff des Art. 4 Nr. 2 (ex Art. 4 Nr. 3) DSGVO eingeschlossen. Als zusätzliche Voraussetzung ist dies nur möglich für solche Zwecke, für die die Daten *erhoben* worden sind, bzw. in den Fällen des § 14 Abs. 1 S. 2 BDSG, für die Zwecke, zu denen sie gespeichert worden sind. Eine solche Zweckbegrenzung ist gem. Art. 6 Abs. 3 S. 3 DSGVO möglich. Damit kann § 14 Abs. 1 BDSG aus denselben Gründen aufrechterhalten werden wie § 13 Abs. 1 BDSG[533].

[533] Vgl. hierzu ausführlich oben § 13 Abs. 1.

b. Abs. 2: Zweckänderung

§ 14 Abs. 2 BDSG regelt Fälle der Zweckänderung. Art. 6 Abs. 4 (ex Abs. 3a) DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, Bestimmungen zu erlassen oder aufrechterhalten, die Zweckänderungen auch für mit dem ursprünglichen Zweck inkompatible Zwecke zulassen, sofern dies eine notwendige und verhältnismäßige Maßnahme in einer demokratischen Gesellschaft zum Schutz der in Art. 23 Abs. 1 lit. a bis j (ex Art. 21 Abs. 1 lit. aa bis g) DSGVO aufgelisteten Ziele darstellt.
Die Datenschutz-Grundverordnung geht in Art. 6 Abs. 4 (ex Abs. 3a) DSGVO davon aus, dass eine Zweckänderung für kompatible Zwecke grundsätzlich ohne zusätzliche Zulässigkeitsnorm möglich ist. Darüber hinaus können Mitgliedstaaten aber auch Aufgaben und Zwecke bestimmen, in denen eine Zweckänderung als kompatibel mit dem ursprünglichen Zweck und rechtmäßig erachtet wird, sofern die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Dies stellt EG 50 S. 3 (ex EG 40 S. 3) DSGVO klar. Eine Weiterverarbeitung für mit dem ursprünglichen Zweck vereinbare Zwecke muss nicht einem der in Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO niedergelegten Ziele dienen, wie sich aus einem Umkehrschluss des Art. 6 Abs. 4 (ex Abs. 3a) DSGVO ergibt.[534] Dies ermöglicht weitgehend eine Aufrechterhaltung der in § 14 Abs. 2 BDSG angelegten Zweckänderungsbestimmungen. Allerdings empfiehlt sich für jeden in § 14 Abs. 2 BDSG geregelten Fall eine gesetzliche Klarstellung, die zwischen Zweckänderungen für inkompatible Zwecke und solchen für kompatible Zwecke unterscheidet. Insgesamt sollte § 14 Abs. 2 BDSG demnach dahin gehend umstrukturiert werden, dass zwischen Zweckänderungen unterschieden wird, die mit dem ursprünglichen Zweck kompatibel oder inkompatibel sind. Sodann muss der nationale Gesetzgeber für kompatible Zwecke überlegen, ob er eine Konkretisierung/Modifikation der Zweckänderungsmöglichkeit nach Art. 6 Abs. 4 (ex Abs. 3a) DGSVO vornehmen möchte. Hier ist fraglich, ob Art. 6 Abs. 4 (ex Abs. 3a) DSGVO insoweit eine Öffnungsmöglichkeit vorsieht. Art. 6 Abs. 4 (ex Abs. 3a) und

[534] Vgl. hierzu ausführlich S. 38.

Abs. 2a, 3 DSGVO können aber zusammengelesen werden, so dass eine mitgliedstaatliche Konkretisierungsbefugnis für die Fälle des Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO besteht. Für inkompatible Zwecke ist dagegen Art. 6 Abs. 4 (ex Abs. 3a) DSGVO mit dem Verweis auf Art. 23 Abs. 1 lit. a bis j (ex Art. 21 Abs. 1 lit. aa bis g) DSGVO selbst die Öffnungsklausel.
Im Einzelnen gilt für die jeweiligen Teilregelungen des § 14 BDSG also Folgendes:

c. Abs. 2 Nr. 1

§ 14 Abs. 2 Nr. 1 BDSG regelt, dass die Datenspeicherung, -veränderung oder -nutzung für andere Zwecke zulässig ist, wenn eine Rechtsvorschrift dies vorsieht oder zwingend erfordert. Dieser Hinweis ist als Verweis „Schaltnorm“ auf andere Rechtsvorschriften, beispielsweise einschlägige Normen in bereichsspezifischen Gesetzen, zu verstehen, als solche aber wie schon § 13 Abs. 2 Nr. 1 Alt. 1 BDSG überflüssig, da sich die entsprechenden Anforderungen ohnehin aus der spezifischen Norm ergeben müssen. Die Norm ist daher zu streichen.

d. Abs. 2 Nr. 2

§ 14 Abs. 2 Nr. 2 kann gestrichen werden, da die Fälle der Zweckänderung, die durch Einwilligung des Betroffenen legitimiert sind, bereits in Art. 6 Abs. 4 (ex Abs. 3a) DSGVO geregelt sind, und hinsichtlich der Einwilligung in die Zweckänderung von Art. 6 Abs. 4 (ex Abs. 3a) DSGVO kein Spielraum für die Mitgliedstaaten vorgesehen ist. Im Übrigen muss durch die Übereinstimmung die Norm auch nicht aufrechterhalten werden, um das bestehende Datenschutzniveau zu erhalten.

e. Abs. 2 Nr. 3

§ 14 Abs. 2 Nr. 3 BDSG lässt Zweckänderungen zu, die offensichtlich im Interesse des Betroffenen liegen, und wenn kein Grund besteht zur Annahme, dass er die Einwilligung hierzu verweigern würde. Gem. Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i (ex Art. 21 Abs. 1 lit. f) DSGVO können Mitgliedstaaten Zweckänderungen regeln, die eine notwendige und verhältnismäßige Maßnahme darstellen und dem Schutz des Betroffenen dienen.

Damit setzt Art. 23 Abs. 1 lit. i (ex Art. 21 Abs. 1 lit. f) DSGVO höhere Anforderungen als § 14 Abs. 2 Nr. 3 BDSG, da die Zweckänderung dem *Schutz* des Betroffenen dienen und nicht lediglich in seinem Interesse sein muss. Auch wenn sich in der Praxis viele Fälle dahin gehend überschneiden werden, empfiehlt sich hier eine Änderung des Wortlauts, damit die Norm – in modifizierter Weise – auch für Zweckänderungen zu inkompatiblen Zwecken aufrechterhalten werden kann.

f. Abs. 2 Nr. 4

§ 14 Abs. 2 Nr. 4 BDSG regelt Fälle, in denen offensichtliche Anhaltspunkte für die Unrichtigkeit der Angaben des Betroffenen gegeben sind. Diesen Fall deckt keines der Ziele in Art. 23 Abs. 1 lit. a bis j (ex Art. 21 Abs. 1 lit. aa bis g) DSGVO explizit ab. Die Norm kann deswegen nur zu Zweckänderungen für kompatible Zwecke aufrechterhalten werden und sollte entsprechend gekennzeichnet werden. Für inkompatible Zwecke kann sie nur aufrechterhalten werden, sofern die Änderung zu Erreichung einer der Zwecke des Art. 23 Abs. 1 lit. a bis j (ex Art. 21 Abs. 1 lit. aa bis g) DSGVO erforderlich sein sollte. Dann kann aber direkt auf jene entsprechenden Gründe zurückgegriffen werden.

g. Abs. 2 Nr. 5

§ 14 Abs. 2 Nr. 5 BDSG regelt Fälle, in denen die Daten allgemein zugänglich sind oder durch die öffentliche Stelle veröffentlicht werden dürften. Sowohl zur Sicherstellung der öffentlichen Sicherheit als auch zum Schutz der Rechte und Freiheiten von einzelnen Personen und finanziellen Interessen eines Mitgliedstaates, etwa Steuerbetrug oder Sozialmissbrauch, könnte eine Auswertung aus allgemein zugänglichen Quellen erforderlich sein, auch wenn die Zurverfügungstellung der Daten selbst anderen Zwecken diente. Auch weitere Ziele in Art. 23 Abs. 1 lit. a bis j (ex Art. 21 Abs. 1 lit. aa bis g) DSGVO könnten betroffen sein. Dann dürften allerdings regelmäßig bereits die spezielleren Zulässigkeitstatbestände greifen. Insofern ist die Zulässigkeit der Regelung des Zugriffs speziell auf allgemein zugängliche bzw. veröffentlichungsoffene Daten fraglich. Die Norm kann aber jedenfalls zu Zweckänderungen für kompatible Zwecke aufrechterhalten werden.

h. Abs. 2 Nr. 6 Var. 1, 3

§ 14 Abs. 2 Nr. 6 Var. 1, 3 BDSG regeln die Zulässigkeit der Zweckänderung, sofern es für die Abwehr erheblicher Nachteile für das Gemeinwohl bzw. zur Wahrung erheblicher Belange desselben erforderlich ist. Diese Normen können gem. Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. e (ex Art. 21 Abs. 1 lit. c) DSGVO aufrechterhalten werden.

i. Abs. 2 Nr. 6 Var. 2

§ 14 Abs. 2 Nr. 6 Var. 2 BDSG ermöglicht eine erforderliche Zweckänderung zur Abwehr einer Gefahr für die öffentliche Sicherheit. Diese Norm kann gem. Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. c (ex Art. 21 Abs. 1 lit. a) DSGVO aufrechterhalten werden.

j. Abs. 2 Nr. 7

§ 14 Abs. 2 Nr. 7 BDSG lässt erforderliche Zweckänderungen zur Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Vollstreckung oder zum Vollzug von Straftaten oder Maßnahmen im Sinne des § 11 Abs. 1 Nr. 8 StGB oder von Erziehungsmaßregeln oder Zuchtmitteln im Sinne des JGG oder zur Vollstreckung von Bußgeldbescheiden zu. Hier könnte die Regelung der Zweckänderung durch die Mitgliedstaaten nach Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. d (ex Art. 21 Abs. 1 lit. b) DSGVO eröffnet sein. Dies dürfte allerdings wohl nur für Straftaten gelten. Soweit die Norm auch Zweckänderungen zur Verfolgung von Ordnungswidrigkeiten umfasst, muss dies auf Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. e (ex Art. 21 Abs. 1 lit. c) DSGVO gestützt werden. Andernfalls dürfte die Vorschrift insoweit nur für die Zweckänderung zu kompatiblen Zwecken gelten.

k. Abs. 2 Nr. 8

§ 14 Abs. 2 Nr. 8 BDSG, der die Zweckänderung zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person zulässt, kann aufgrund von Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) DSGVO aufrechterhalten werden.

l. Abs. 2 Nr. 9

§ 14 Abs. 2 Nr. 9 BDSG regelt Fälle der Zweckänderung zur Durchführung wissenschaftlicher Forschung. Diesen Fall deckt zwar keines der Ziele in Art. 23 Abs. 1 lit. a bis j (ex Art. 21 Abs. 1 lit. aa bis g) DSGVO ab. Die Norm kann deswegen nur zu Zweckänderungen für kompatible Zwecke aufrechterhalten werden und müsste entsprechend gekennzeichnet werden. Art. 5 Abs. 1 lit. b DSGVO geht jedoch im Rahmen einer Fiktion davon aus, dass eine entsprechende Zweckänderung immer zweckkompatibel ist. Daher besteht insoweit an sich kein Bedürfnis, die Vorschrift aufrechtzuerhalten, da sich eine zulässige zweckkompatible Zweckänderung ohnehin schon aus der Datenschutz-Grundverordnung ergibt.

m. Abs. 3: Vom Primärzweck umfasste Zwecke

§ 14 Abs. 3 BDSG bestimmt, dass im Falle der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen keine Zweckänderung vorliegt, sieht diese Fälle also als vom Primärzweck umfasst an. Selbiges soll gem. § 14 Abs. 3 S. 2 BDSG auch für die Verarbeitung oder Nutzung zu Ausbildungs- und Prüfungszwecken gelten, soweit nicht überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Letztlich normiert die Bestimmung damit die Fiktion einer Zweckidentität. In der Logik der Datenschutz-Grundverordnung dürften darin zum Teil in der Tat Zweckidentitäten vorliegen, da etwa Aufsichts- und Kontrollbefugnisse von der verantwortlichen Stelle regelmäßig in Erfüllung ihrer ursprünglichen Zwecke erfüllt werden. Dafür spricht auch, dass Art. 6 Abs. 3 S. 3 DSGVO den Mitgliedstaaten einen Konkretisierungsspielraum eröffnet, „Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung“ zu ergreifen, wozu auch die Wahrnehmung von Aufsichts- und Kontrollbefugnisse gefasst werden können.
Sofern gleichwohl keine Zweckidentität i. S. d. Datenschutz-Grundverordnung vorliegt, wird regelmäßig eine Zweckkompatibilität gegeben sein. So ist zur Aufrechterhaltung einer Aufgabenerfüllung auch eine diesbezügliche Ausbildung erforderlich und dass diese im Rahmen der Übung mit „echten Sachverhalten“ eingebunden werden, so dass jedenfalls gemessen

an den Leitparametern des Art. 6 Abs. 4 (ex Abs. 3a) lit. a bis e DSGVO eine Kompatibilität vorliegen wird. Daher könnte insoweit auf die Fiktion der fehlenden Zweckänderung in § 14 Abs. 3 BDSG verzichtet und ohne weitere Klarstellung davon ausgegangen werden, dass in den genannten Fällen eine Zweckidentität, jedenfalls aber eine zulässige Zweckänderung im Rahmen kompatibler Zwecke vorliegt. Die Aufrechterhaltung der jetzigen Formulierung ist dagegen problematisch, da die Einordnung als Zweckänderung und als kompatible bzw. inkompatible Zwecke letztlich der Datenschutz-Grundverordnung und nicht dem nationalen Recht unterliegt. Hier müsste also argumentiert werden, dass auf Basis von Art. 6 Abs. 2, 3 und 4 (ex Abs. 3a) DSGVO eine zulässige Konkretisierung erfolgt, was angesichts der insoweit fehlenden Öffnungsklausel für zweckkompatible Zweckänderungen zweifelhaft erscheint.

n. Abs. 4: Zweckbegrenzung

§ 14 Abs. 4 BDSG bestimmt als Grenze (des § 9 BDSG), dass personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert wurden, nur für diese Zwecke verwendet werden dürfen. Die Bestimmung einer solchen Zweckbegrenzung wird von Art. 6 Abs. 3 S. 3 DSGVO („Maßnahmen zur Gewährleistung [...]“) ermöglicht.

o. Abs. 5: Zweckänderung bei besonderen Arten personenbezogener Daten

§ 14 Abs. 5 BDSG regelt Fälle der Zulässigkeit der Speicherung, Veränderung oder Nutzung besonderer Arten personenbezogener Daten durch öffentliche Stellen für andere Zwecke als jene, zu denen die Daten erhoben wurden. Die Zulässigkeit der Verarbeitung besonderer Arten personenbezogener Daten ist in der Datenschutz-Grundverordnung in Art. 9 DSGVO geregelt. Die Verarbeitung i. S. d. DSGVO schließt gem. Art. 4 Nr. 2 (ex Art. 4 Nr. 3) DSGVO auch das Speichern, Verändern und Nutzen ein. Eine Zweckänderung der Verarbeitung bei besonderen Arten personenbezogener Daten regelt die Datenschutz-Grundverordnung nicht gesondert. Ein Rückgriff auf Art. 6

Abs. 4 DSGVO (ex Art. 6 Abs. 3a) ist insoweit nicht möglich, sofern das Verhältnis von Art. 9 und 6 DGSVO so bestimmt wird, dass Art. 6 DSGVO nur für die allgemeine Verarbeitung personenbezogener Daten gilt und Art. 9 DSGVO für die Verarbeitung besonderer Arten personenbezogener Daten hierzu speziell ist. Art. 6 Abs. 4 (ex Abs. 3a) DSGVO findet dann keine Anwendung auf Art. 9 DSGVO (siehe dazu oben S. 54). Art. 9 Abs. 1 DSGVO stellt insofern klar, dass eine Verarbeitung besonderer personenbezogener Daten grundsätzlich verboten ist. Dies schließt wohl auch die zweckändernde Verarbeitung jener Daten mit ein (siehe dazu oben S. 54). Ausnahmen bestehen nur im Rahmen von Art. 9 Abs. 2 DSGVO. Die Zweckänderung ist bei der Verarbeitung personenbezogener Daten nach diesem Verständnis dann möglich, wenn sie selbst eine Rechtsgrundlage in Art. 9 Abs. 2 DSGVO bzw. in den aufgrund von Öffnungsklauseln in Art. 9 Abs. 2 DSGVO aufrechterhaltenen oder geschaffenen nationalen Normen findet.

Eine ähnliche Vorschrift fand sich bereits in Art. 8 RL 95/46/EG. Auch hier war eine zweckändernde Verarbeitung nicht vorgesehen. Vor diesem Hintergrund dürfte § 14 Abs. 5 BDSG insoweit diesen Anforderungen genügen: Die Vorschrift verlangt, dass die Voraussetzungen für eine Erhebung besonderer Arten personenbezogener Daten nach § 13 Abs. 2 BDSG vorliegen. Ist dies gegeben, hat die weitere Speicherung, Veränderung oder Nutzung jedoch gleichzeitig eine Rechtsgrundlage, die für sich den Anforderungen des Art. 9 Abs. 2 DSGVO genügt. Auch wenn insoweit Restzweifel verbleiben, bestanden diese wohl bereits mit Blick auf die Vorgaben der RL 95/46/EG.

Der Verweis auf § 13 Abs. 2 BDSG kann aber nur insofern aufrechterhalten werden, als die entsprechenden Nummern des § 13 Abs. 2 BDSG aufrechterhalten werden können. Weniger problematisch wäre es, das Speichern, Verändern oder Nutzen besonderer Arten personenbezogener Daten in einer eigenen Rechtsgrundlage und ohne den Verweis auf die Zweckänderung zu regeln, was innerhalb des von den Öffnungsklauseln in Art. 9 DSGVO markierten Spielraums unproblematisch im selben Umfang wie das Erheben besonderer Arten personenbezogener Daten möglich wäre. Damit wäre auch das Problem gelöst, dass § 14 Abs. 5 BDSG nur das Speichern, Verändern und

Nutzen für andere Zwecke regelt und bisher eine Regelungslücke für Fälle besteht, in denen keine Erhebung vorausging.[535]
Demnach ist eine Aufrechterhaltung von § 14 Abs. 5 BDSG nur möglich, soweit § 13 Abs. 2 BDSG aufrechterhalten werden kann, und ist wegen der Zweckänderung, die in Art. 9 DSGVO nicht angelegt ist, nicht ohne Restrisiko. Sinnvoller erscheint es, das Verändern, Speichern und Nutzen besonderer Arten personenbezogener Daten nach Maßgabe des Art. 9 DSGVO und der dort enthaltenen Öffnungsklauseln gesondert zu regeln.

p. Abs. 6: Verweis auf § 13 Abs. 2 Nr. 7 BDSG

Die Problematik der Zweckänderung stellt sich für § 14 Abs. 6 BDSG nicht. Hier wird für die Speicherung, Veränderung oder Nutzung für die Fälle des § 13 Abs. 2 Nr. 7 BDSG auf die Voraussetzungen, insbesondere auch auf das hierfür zuständige Fachpersonal verwiesen. Damit genügt die Vorschrift den Anforderungen des Art. 9 Abs. 2 lit. h i. V. m. Abs. 4 (ex Art. 9 Abs. 5) DSGVO und kann ebenso wie § 13 Abs. 2 Nr. 7 BDSG bestehen bleiben.

§ 14 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Insgesamt	Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1, Abs. 4 (ex Abs. 3a); Art. 23 Abs. 1 lit. a bis j (ex Art. 21 lit. aa bis g)	Umstrukturierung mit klarerer Unterscheidung (und gegebenenfalls Beschränkung) auf inkompatible Zwecke (Abgrenzung von kompatiblen Zwecken, da diesbezügliche Zweckänderungen nach DSGVO prinzipiell zulässig)	Art. 6 Abs. 4 (ex Abs. 3a) DSGVO erfasst nur inkompatible Zweckänderungen; Art. 5 lit. b DSGVO lässt kompatible Zweckänderungen zu.

[535] *Albers*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 14 BDSG, Rn. 64.

Abs. 1	Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1	Ggf. leichte Modifikation	§ 14 Abs. 1 BDSG stimmt mit Anforderungen aus Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1 DSGVO überein. Art. 6 Abs. 2 (ex Abs. 2a), 3 DSGVO fordert Präzisierung und Spezifizierung der mitgliedstaatlichen Norm, daher ggf. geringfügige Konditionierung nötig, um Restzweifel zu beseitigen.
Abs. 2 Nr. 1	-	Streichen	Verweis auf andere Rechtsvorschriften wg. eventuellen Erlaubnistatbeständen in bereichsspezifischen Gesetzen nicht nötig und so unkonditioniert auch nicht von Öffnungsklauseln gedeckt.
Abs. 2 Nr. 2	Art. 6 Abs. 4 (ex Abs. 3a) Alt. 1	Streichen	Keine Öffnungsklausel; keine Notwendigkeit zur Aufrechterhaltung, da entsprechende Regelung in DSGVO
Abs. 2 Nr. 3	Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i (ex Art. 21 Abs. 1 lit. f)	Modifikation für inkompatible Zwecke	Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i (ex Art. 21 Abs. 1 lit. f) DSGVO hat höhere Anforderungen als § 14 Abs. 2 Nr. 3 BDSG.
Abs. 2 Nr. 4	Art. 6 Abs. 4 (ex Art. 6 Abs. 3a)	Beibehalten für kompatible Zwecke zulässig, aber nicht notwendig, da im Übrigen aus DSGVO	Zweckänderung für *kompatible* Zwecke müssen nicht einem in Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO gelisteten Ziel dienen.
Abs. 2 Nr. 5	Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) (Art. 23 Abs. 1 lit. a bis j [ex Art. 21 lit. aa bis g])	Beibehalten für kompatible Zwecke zulässig, aber nicht notwendig, da im Übrigen aus DSGVO; Beibehalten für inkompatible Zwecke fraglich, da insoweit spezielle Tatbestände eher einschlägig	Zweckänderung für *kompatible* Zwecke müssen nicht einem in Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO gelisteten Ziel dienen; Zweckänderung im Übrigen fraglich, da Art. 23 Abs. 1 lit. a bis j (ex Art. 21 Abs. 1 lit. aa bis g) DSGVO zwar einschlägig sein können, aber nicht speziell auf besonders zugängliche Daten abstellen, so dass insoweit wohl die übrigen Zulässigkeitstatbestände spezieller wären.

Abs. 2 Nr. 6 Var. 1, 3	Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i (ex Art. 21 Abs. 1 lit. f)	Beibehalten auch für inkompatible Zwecke	§ 14 Abs. 2 Nr. 6 Var. 1, 3 BDSG erfüllen die Anforderungen des Art. 6 Abs. 4 i. V. m. Art. 23 Abs. 1 lit. j (ex Art. 6 Abs. 3a i. V. m. Art. 21 Abs. 1 lit. g DSGVO).
Abs. 2 Nr. 6 Var. 2	Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. c (ex Art. 21 Abs. 1 lit. a)	Beibehalten auch für inkompatible Zwecke	§ 14 Abs. 2 Nr. 6 Var. 2 BDSG erfüllt die Anforderungen des Art. 6 Abs. 4 i. V. m. Art. 23 Abs. 1 lit. c (ex Art. 6 Abs. 3a i. V. m. Art. 21 Abs. 1 lit. a) DSGVO.
Abs. 2 Nr. 7	Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. d/e (ex Art. 21 Abs. 1 lit. b/c)	Beibehalten auch für inkompatible Zwecke insbesondere hinsichtlich Strafprävention/-verfolgung	§ 14 Abs. 2 Nr. 7 BDSG erfüllt die Anforderungen des Art. 6 Abs. 4 i. V. m. Art. 23 Abs. 1 lit. d (ex Art. 6 Abs. 3a i. V. m. Art. 21 Abs. 1 lit. b) DSGVO nur hinsichtlich Strafverhütung/-verfolgung.
Abs. 2 Nr. 8	Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2)	Beibehalten auch für inkompatible Zwecke	§ 14 Abs. 2 Nr. 8 BDSG erfüllt die Anforderungen des Art. 6 Abs. 4 i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 6 Abs. 3a i. V. m. Art. 21 Abs. 1 lit. f Alt. 2) DSGVO.
Abs. 2 Nr. 9	Art. 6 Abs. 4 (ex Art. 6 Abs. 3a)/Art. 5 Abs. 1 lit. b	Streichen/Beibehalten nicht notwendig und zweifelhaft	DSGVO fingiert Zweckkompatibilität und sieht Zweckänderung als zulässig an.
Abs. 3	(Art. 6 Abs. 3, 4 [ex 3a])	Streichen/Beibehalten nicht notwendig und zweifelhaft	In Logik der DSGVO entweder schon keine Zweckänderung oder jedenfalls zulässige Zweckänderung.

Abs. 4	Art. 6 Abs. 3 S. 3	Beibehalten	Zweckbegrenzung möglich durch Art. 6 Abs. 3 S. 3.
Abs. 5	Art. 9 Abs. 2 lit. a, c, e, g	Modifikation; Regelung in eigener Rechtsgrundlage	§ 14 Abs. 5 BDSG kann nur aufrechterhalten werden, soweit § 13 Abs. 2 BDSG aufrechterhalten werden kann. Eine Regelung in einer eigenen Rechtsgrundlage wäre sinnvoll, um Regelungslücken zu vermeiden, und das Erfordernis einer eigenen Rechtsgrundlage für zweckändernde Veränderungen, Nutzungen oder Speicherungen besonderer Arten personenbezogener Daten klarzustellen.
Abs. 6	Art. 9 Abs. 2 lit. h i. V. m. Abs. 3 (ex Art. 9 Abs. 4)	Beibehalten; Streichen zulässig aber untunlich	Die Norm erfüllt die Voraussetzungen der Öffnungsklausel.

§ 15: Datenübermittlung an öffentliche Stellen

a. Abs. 1: Zulässigkeit der Datenübermittlung an öffentliche Stellen

§ 15 Abs. 1 BDSG bezieht sich auf das Übermitteln personenbezogener Daten durch öffentliche Stellen an öffentliche Stellen, wenn die Übermittlung zur Erfüllung der Aufgaben der verantwortlichen oder empfangenden Stelle erforderlich ist. Das Übermitteln ist vom Verarbeitungsbegriff des Art. 4 Nr. 2 (ex Art. 4 Nr. 3) DSGVO umfasst. § 15 Abs. 1 BDSG kann ebenso und aus denselben Gründen wie § 13 Abs. 1 BDSG[536] und § 14 Abs. 1 BDSG aufrechterhalten werden.[537]

b. Abs. 2: Für die Übermittlung Verantwortlicher

§ 15 Abs. 2 BDSG legt den für die Übermittlung Verantwortlichen fest. Diese Bestimmung ist von Art. 4 Nr. 7 (ex Art. 4 Nr. 5) DSGVO gedeckt, die es den

[536] Vgl. hierzu ausführlich oben § 13 Abs. 1.
[537] Vgl. hierzu ausführlich oben § 14 Abs. 1.

Mitgliedstaaten eröffnet, den Verantwortlichen zu bestimmen oder Modalitäten zu seiner Benennung festzulegen.

c. Abs. 3: Zweckbegrenzung

§ 15 Abs. 3 BDSG stellt klar, dass die übermittelten Daten von der Empfängerstelle nur zu dem Zweck verwendet werden dürfen, für den sie übermittelt wurden, normiert für diese Fälle also ausdrücklich den Zweckbindungsgrundsatz. Eine solche Zweckbegrenzung ist wegen Art. 6 Abs. 3 S. 3 DSGVO möglich.

d. Abs. 4: Übermittlung an Stellen öffentlich-rechtlicher Religionsgemeinschaften

§ 15 Abs. 4 BDSG regelt die Zulässigkeit der Übermittlung personenbezogener Daten an Stellen der öffentlich-rechtlichen Religionsgemeinschaften, sofern die Voraussetzungen des § 15 Abs. 1 BDSG zutreffen. Sofern die Übermittlung erforderlich ist, um in der Zuständigkeit der übermittelnden Stelle Aufgaben zu erfüllen, kann diese Norm zulässigerweise aufrechterhalten werden. Für Stellen öffentlich-rechtlicher Religionsgemeinschaften kann dies nur gelten, soweit diese hoheitliche Gewalt ausüben (Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 2 DSGVO) und zur Erfüllung dieser Aufgaben die Übermittlung erforderlich ist oder ein anderer Rechtfertigungsgrund nach der Datenschutz-Grundverordnung greift, etwa weil die Zweckänderung zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist (Art. 6 Abs. 4 [ex Art. 6 Abs. 3a] i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 [ex Art. 21 Abs. 1 lit. f Alt. 2] DSGVO). Für diese Fälle kann die Norm aufrechterhalten werden. Insoweit empfiehlt sich ein dahin gehender Hinweis in der Norm.

e. Abs. 5: Verbundene personenbezogene Daten

Gem. § 15 Abs. 5 BDSG ist die Übermittlung von personenbezogenen Daten zulässig, die untrennbar oder nur mit unvertretbarem Aufwand trennbar mit den zu übermittelnden Daten gem. § 15 Abs. 1 BDSG verbunden sind. Ge-

meint sind damit etwa Daten in Akten oder Dateien.[538] Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1 DSGVO lässt seinem Wortlaut nach die Verarbeitung – also auch die Übermittlung, § 4 Nr. 3 DSGVO – personenbezogener Daten zu, die für die Wahrnehmung der Aufgabe, die im öffentlichen Interesse liegt, erforderlich ist. Damit ist die Verarbeitung nur der personenbezogenen Daten zulässig, die tatsächlich verarbeitet werden sollen. Die Verarbeitung von damit verbundenen personenbezogenen Daten ist davon nicht gedeckt. Allerdings bieten Art. 6 Abs. 2 (ex Abs. 2a), 3 DSGVO den Mitgliedstaaten einen weiten Spielraum zur Anpassung der Anwendung des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO. Zudem stellt § 15 Abs. 5 BDSG hohe Hürden an die Zulässigkeit der Übermittlung solcher personenbezogenen Daten und verbietet deren Nutzung. Damit kann § 15 Abs. 5 BDSG aufrechterhalten werden.

f. Abs. 6: Verbundene personenbezogene Daten innerhalb einer öffentlichen Stelle

Da § 15 Abs. 5 BDSG aufrechterhalten werden kann, gilt dies auch für § 15 Abs. 6 BDSG, der sich auf § 15 Abs. 5 BDSG bezieht.

§ 15 BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1	Art. 6 Abs. 1 UAbs. 1 lit. e	Ggf. leichte Modifikation	§ 15 Abs. 1 BDSG stimmt mit Anforderungen aus Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1 DSGVO überein. Art. 6 Abs. 2 (ex Abs. 2a), 3 DSGVO fordert Präzisierung und Spezifizierung der mitgliedstaatlichen Norm, die durch Differenzierung der verantwortlichen Stelle und der Datenverarbeitungsvorgänge erfüllt.
Abs. 2	Art. 4 Nr. 7 (ex Art. 4 Nr. 5)	Beibehalten; Streichen zulässig aber untunlich	Aufrechterhaltung durch Art. 4 Nr. 7 (ex Art. 4 Nr. 5) DSGVO möglich.
Abs. 3	Art. 6 Abs. 3 S. 3	Beibehalten; Streichen zulässig aber untunlich	Aufrechterhaltung durch Art. 6 Abs. 3 S. 3 DSGVO möglich.

[538] *Albers*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 15 BDSG, Rn. 46.

Abs. 4	Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 2	Modifikation	Ergänzung um Hinweis, dass Aufgabenerfüllung der öffentlich-rechtlichen Religionsgemeinschaft i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 2 DSGVO erfolgen muss bzw. ausnahmsweise sonstiger Grund im Sinne der DSGVO vorliegt.
Abs. 5	Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1	Beibehalten; Streichen zulässig	Gem. Art. 6 Abs. 2 (ex Abs. 2a), 3 DSGVO weiter Spielraum zur Anpassung der Anwendung des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO.
Abs. 6	Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1	Beibehalten; Streichen zulässig	Gem. Art. 6 Abs. 2 (ex Abs. 2a), 3 DSGVO weiter Spielraum zur Anpassung der Anwendung des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO.

§ 16: Datenübermittlung an nicht-öffentliche Stellen

Abs. 1: Zulässigkeit der Datenübermittlung an nicht-öffentliche Stellen

a. Abs. 1 Nr. 1

§ 16 Abs. 1 BDSG bezieht sich auf das Übermitteln personenbezogener Daten durch öffentliche Stellen an nicht-öffentliche Stellen, wenn die Übermittlung zur Erfüllung der Aufgaben der verantwortlichen oder empfangenden Stelle erforderlich ist. Das Übermitteln ist vom Verarbeitungsbegriff des Art. 4 Nr. 2 (ex Art. 4 Nr. 3) DSGVO umfasst. § 16 Abs. 1 BDSG kann ebenso und aus denselben Gründen wie § 13 Abs. 1 BDSG[539], § 14 Abs. 1 BDSG[540] und § 15 Abs. 1 BDSG[541] aufrechterhalten werden.

b. Abs. 1 Nr. 2

§ 16 Abs. 1 Nr. 2 BDSG regelt das Übermitteln personenbezogener Daten an nicht-öffentliche Stellen, wenn diese ein berechtigtes Interesse glaubhaft darlegen können. Diese Zulässigkeitsnorm fällt weder unter die Öffnungsklausel des Art. 6 Abs. 1 UAbs. 1 lit. c noch lit. e DSGVO. Damit ist dieser Fall von

[539] Vgl. hierzu ausführlich oben § 13 Abs. 1.
[540] Vgl. hierzu ausführlich oben § 14 Abs. 1.
[541] Vgl. hierzu ausführlich oben § 15 Abs. 1.

keiner Öffnungsklausel der DSGVO gedeckt. Es greift jedoch Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Diese Norm bedarf jedoch keiner nationalen Umsetzung, so dass die diesbezügliche Implementierung an sich gegen das Wiederholungsverbot verstieße. Vorliegend wird jedoch umfassend die zulässige Datenverarbeitung durch die öffentliche Stelle geregelt, wozu auch die Übermittlungsbefugnisse an nicht-öffentliche Stellen zählen. Diese kann daher die DSGVO-Regelung insoweit mit Blick auf den Handlungsrahmen für die öffentliche Stelle mitregeln. § 16 Abs. 1 Nr. 2 BDSG kann daher zulässigerweise aufrechterhalten werden, sollte aber an Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO angepasst werden.

c. Abs. 2: Für die Übermittlung Verantwortlicher

§ 16 Abs. 2 BDSG legt den für die Übermittlung Verantwortlichen fest. Diese Bestimmung ist von Art. 4 Nr. 7 (ex Art. 4 Nr. 5) DSGVO gedeckt, die den Mitgliedstaaten eröffnet, den Verantwortlichen zu bestimmen oder Modalitäten zu seiner Benennung festzulegen. Sie kann daher aufrechterhalten werden.

d. Abs. 3: Unterrichtung des Betroffenen

§ 16 Abs. 3 BDSG sieht eine Unterrichtungspflicht im Fall des § 16 Abs. 1 Nr. 2 BDSG vor, der so von der Datenschutz-Grundverordnung (und auch der Art. 13 (ex Art. 14), 14a) nicht erfasst wird. Die Bestimmung ist aber von der Konkretisierungsbefugnis des Art. 6 Abs. 3 DSGVO gedeckt.

e. Abs. 4: Zweckbegrenzung

§ 16 Abs. 4 BDSG bestimmt, dass die übermittelten Daten von der Empfängerstelle nur zu dem Zweck verwendet werden dürfen, für den sie übermittelt wurden, normiert für diese Fälle also ausdrücklich den Zweckbindungsgrundsatz. Eine solche Zweckbegrenzung ist wegen Art. 6 Abs. 3 S. 3 DSGVO möglich.

§ 16 BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1 Nr. 1	Art. 6 Abs. 1 UAbs. 1 lit. e	Ggf. leichte Modifikation	§ 16 Abs. 1 BDSG stimmt mit Anforderungen aus Art. 6 Abs. 1 UAbs. 1 lit. e Alt. 1 DSGVO überein. Art. 6 Abs. 2 (ex Abs. 2a), 3 DSGVO fordert Präzisierung und Spezifizierung der mitgliedstaatlichen Norm, daher ggf. geringfügige Konditionierung nötig, um Restzweifel zu beseitigen.
Abs. 1 Nr. 2	Art. 6 Abs. 1 UAbs. 1 lit. f	Modifikation	Zwar von keiner Öffnungsklausel gedeckt, aber angepasste Konkretisierung des Art. 6 Abs. 1 UAbs. 1 lit. f insoweit zulässige Wiederholung.
Abs. 2	Art. 4 Nr. 7 (ex Art. 4 Nr. 5 DSGVO)	Beibehalten; Streichen zulässig aber untunlich	Aufrechterhaltung durch Art. 4 Nr. 7 (ex Art. 4 Nr. 5) DSGVO möglich.
Abs. 3	-/(Art. 6 Abs. 3 S. 3)	Beibehalten	-
Abs. 4	Art. 6 Abs. 3 S. 3	Beibehalten	Aufrechterhaltung durch Art. 6 Abs. 3 S. 3 DSGVO möglich.

§ 18: Durchführung des Datenschutzes in der Bundesverwaltung

§ 18 Abs. 1 BDSG ist Ausdruck des Gebots der Polizeifestigkeit von Hoheitsträgern. Diese stellen die Einhaltung der Regeln, an die sie auf der Grundlage des Art. 22 Abs. 4 (ex Art. 20 Abs. 3) DSGVO gebunden sind, grundsätzlich selbst sicher. Dieses Konstrukt ist dem Unionsrecht fremd. Die Vorschrift ist entweder zu streichen oder zu modifizieren. Nach dem Regelungssystem der Datenschutz-Grundverordnung sind öffentliche Stellen den Aufsichtsmaßnahmen der Aufsichtsbehörden ausgesetzt.[542]

[542] *Schaar* (Fn. 155), (64); *Voßhoff/Hermerschmidt* (Fn. 473), 59, die Datenschutzbehörden künftig als „spezifische Rechtsaufsichtsbehörden“ sehen. Sie halten das für erforderlich, da die Beanstandung eines datenschutzrechtswidrigen Verhaltens von öffentlichen Stellen kein probates Mittel zur Sicherstellung des Datenschutzes sei.

Auf einer anderen Ebene bewegt sich § 18 Abs. 2 BDSG. Er legt öffentlichen Stellen[543] im Interesse des Persönlichkeitsschutzes auf, ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen zu führen. Mangels entsprechender Öffnungsklausel in Art. 30, Art. 13 (ex Art. 28, 14) DSGVO als sedes materiae bleibt mit Blick auf das unionsrechtliche Wiederholungsverbot für seine Aufrechterhaltung grundsätzlich kein Raum.

§ 18 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 S. 1	-	Streichen oder ergänzen um den Passus „Dies dispensiert die genannten Stellen nicht von der Aufsicht durch die Aufsichtsbehörde gemäß Art. 51 ff. (ex Art. 46 ff.) DSGVO.“	Die DSGVO enthält keine dem Grundgedanken der Polizeifestigkeit von Hoheitsträgern verpflichtete Sonderregelung für die in § 18 Abs. 1 BDSG genannten Stellen. Die DSGVO differenziert insbesondere nicht danach, ob die Verarbeitung durch eine oberste Bundesbehörde durchgeführt wird, sondern kennt eine einheitliche Verantwortlichkeit des Verarbeiters und eine damit korrespondierende Aufsicht (Art. 51 Abs. 1 [ex Art. 46 Abs. 1] DSGVO). Die DSGVO stellt die Behörden mithin nicht von einer Aufsicht frei. Das ergibt sich auch im Umkehrschluss aus Art. 83 Abs. 7 (ex Art. 79 Abs. 3b) DSGVO: Die Mitgliedstaaten sind zwar frei darin, ob sie den Aufsichtsbehörden die Befugnis einräumen, gegen Behörden und öffentliche Stellen Geldbußen zu verhängen. Sie müssen den Aufsichtsbehörden aber Abhilfebefugnisse einräumen („unbeschadet der Abhilfebefugnisse der Aufsichtsbehörden gemäß Art. 58 Abs. 2“ [ex Art. 53 Abs. 1b]). § 18 Abs. 1 S. 1 BDSG sollte daher entweder gestrichen oder als deklaratorischen Hinweis auf die Verpflichtung der Bundesbehörden

[543] Also solchen, die unter diesen Abschnitt des BDSG fallen, vgl. § 12 Abs. 1 BDSG. Am Wettbewerb teilnehmende öffentlich-rechtliche Unternehmen sind somit nicht Normadressat des § 18 Abs. 2.

			zur Wahrung des Datenschutzes verstanden und um einen Hinweis auf die Befugnis der Aufsichtsbehörden ergänzt werden.
Abs. 1 S. 2	-	Streichen	Da die Deutsche Postbank AG, die Deutsche Telekom AG und die Deutsche Post AG nicht mehr über ein ausschließliches Recht nach dem Postgesetz verfügen, ist Abs. 1 S. 2 obsolet und zu streichen.[544]
Abs. 2 S. 1	Art. 30 Abs. 1 lit. g, Abs. 2 e, EG 82 (ex Art. 28 Abs. 1 lit. h, Abs. 2a lit. e, EG 65)	Streichen	§ 18 Abs. 2 S. 1 verpflichtet die öffentlichen Stellen, ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen zu führen. Die DSGVO enthält eine ähnliche Regelung: Gemäß Art. 30 Abs. 1 lit. g (ex Art. 28 Abs. 1 lit. h) hat der Verantwortliche im Verzeichnis der Verarbeitungstätigkeiten, wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherung eines angemessenen Schutzniveaus (Art. 32 Abs. 1 [ex Art. 30 Abs. 1] DSGVO) anzufügen. Gleiches gilt gemäß Art. 30 Abs. 2 lit. d (ex Art. 28 Abs. 2a lit. e) für den Auftragsverarbeiter. Anders als § 18 Abs. 2 S. 1 BDSG schreibt das Unionsrecht nicht ausdrücklich ein Hardwareverzeichnis vor. Ein solches Verzeichnis lässt sich als den Vorschriften des Art. 30 Abs. 1 lit. g i. V. m. Art. 32 Abs. 1 (ex Art. 28 Abs. 1 lit. h i. V. m. Art. 30 Abs. 1) DSGVO immanent erachten, da es dazu dienen kann, Sicherheitslücken für die Betroffenen aufzudecken bzw. Verletzungen des Datenschutzes schneller aufzuheben (dann bedarf es nicht zwingend einer nationalen Regelung). Falls das nicht der Fall ist, ist eine nationale Regelung mangels durch Öffnungsklausel ermöglichten Regelungsspielraum unzulässig. Die besseren Gründe sprechen daher für eine Streichung der Vorschrift.

[544] *Plath*, in: ders. (Hrsg.), BDSG, 2013, § 18, Rn. 3.

Abs. 2 S. 2	Art. 30, Art. 13 Abs. 1 lit. b (ex Art. 28, 14 Abs. 1 lit. b)	Streichen	Die Vorschrift des § 18 Abs. 2 S. 2 BDSG begründet eine Pflicht zur schriftlichen[545] Darlegung der Rechtsgrundlage der Verarbeitung sowie inhaltliche Mitteilungspflichten. Nach Art. 13 Abs. Abs. 1 lit. c (ex 14 Abs. 1 lit. b) DSGVO ist die Rechtsgrundlage zwar dem Betroffenen mitzuteilen, eine Pflicht zur Aufnahme in das Verzeichnis nach Art. 30 (ex Art. 28) DSGVO besteht aber nicht. Der Schutz des BDSG geht hier somit weiter. Vom Sinn und Zweck und der systematischen Einordnung her gedacht, erscheint es naheliegend, die Rechtsgrundlage ebenfalls in das Verzeichnis nach Art. 30 (ex Art. 28) DSGVO aufzunehmen: Es entsteht kein substanzieller Mehraufwand für den Verantwortlichen, da ihm dies Art. 13 Abs. 1 lit. c (ex Art. 14 Abs. 1 lit. b) DSGVO ohnehin auferlegt. Des Weiteren setzt sich der Verantwortliche auch mit dem Tatbestand und den Rechtsfolgen der jeweiligen Rechtsgrundlage ggf. vertieft auseinander, was zusätzlich dem Schutz der Betroffenenrechte dienen kann. Allerdings lässt sich die weitergehende Pflicht nicht ohne Weiteres als Präzisierung der Angabe der Verarbeitungszwecke gemäß Art. 30 Abs. 1 lit. b (ex Art. 28 Abs. 1 lit. c) DSGVO ansehen. Vor allem enthält Art. 30 (ex Art. 28) keine Öffnungsklausel, die es den Mitgliedstaaten ermöglicht, eigene Regelungsvorstellungen zu entwickeln oder Normwiederholungen vorzunehmen.
Abs. 2 S. 3	Art. 30 (ex Art. 28)	Streichen	§ 18 Abs. 2 S. 3 BDSG erlaubt eine (ermessensgesteuerte) Ausnahme von der Pflicht, ein Verzeichnis zu führen, wenn die automatisierte Verarbeitung lediglich allgemeinen Verwaltungszwecken dient. Eine solche Ausnahme von der Pflicht des Art. 30 (ex Art. 28) sieht die DSGVO nicht vor. § 18 Abs. 2 S. 3 BDSG ist daher zu streichen.

[545] Siehe die Präzisierung in Art. 30 Abs. 3 (ex 28 Abs. 3a).

Abs. 2 S. 4	Art. 30, 35 Abs. 10 (ex Art. 28, 33 Abs. 5)	Streichen	Ähnlich gelagerte automatisierte Verarbeitungen erlaubt § 18 Abs. 2 S. 4 BDSG zusammenzufassen. Eine korrespondierende Norm enthält Art. 30 (ex Art. 28) DSGVO nicht. Lediglich Art. 35 Abs. 10 (ex Art. 33 Abs. 5) DSGVO regelt einen annäherungsweise ähnlichen Fall: Danach ist die Pflicht zur Durchführung einer Folgenabschätzung ausnahmsweise entbehrlich. Beide Fälle bewegen sich aber auf unterschiedlichen Ebenen. Mangels Öffnungsklausel ist den Mitgliedstaaten kein Regelungsspielraum eröffnet. Die Vorschrift ist daher zu streichen.

§§ 19 – 21: Rechte des Betroffenen bei Datenverarbeitung der öffentlichen Stellen

Vorbemerkung

Die §§ 19 – 21 BDSG regeln die Rechte des Betroffenen bei einer Datenverarbeitung durch öffentliche Stellen. Sie umfassen das Auskunftsrecht (§ 19 BDSG), die Benachrichtigungspflicht der verantwortlichen Stelle (§ 19a BDSG), die Ansprüche auf Berichtigung, Löschung und Sperrung von Daten, das Widerspruchsrecht (§ 20 BDSG) sowie ein damit korrespondierendes Recht auf Anrufung der BfDI (§ 21 BDSG). Das § 19 BDSG entsprechende Auskunftsrecht findet sich in der Datenschutz-Grundverordnung in Art. 15 DSGVO. Die Benachrichtigungspflicht in § 19a BDSG korrespondiert mit den wesentlich weiter gefassten Informationspflichten gemäß Art. 13 (ex Art. 14) und Art. 14 (ex 14a) DSGVO, die teilweise noch durch die Transparenzpflichten des Art. 12 DSGVO ergänzt werden. § 20 BDSG fasst in einer Norm mehrere Rechte zusammen, die in verschiedenen Bestimmungen der Datenschutz-Grundverordnung geregelt sind, nämlich das Recht auf Berichtigung in Art. 16 DSGVO, das Recht auf Löschung in Art. 17 DSGVO sowie das Recht auf Einschränkung der Verarbeitung in Art. 18 (ex Art. 17a) DSGVO und das Widerspruchsrecht in Art. 21 (ex Art. 19) DSGVO, das der Sperrung von Daten und dem Widerspruchsrecht in § 20 Abs. 4 und 5 BDSG entspricht.

Dabei sind die Betroffenenrechte der Datenschutz-Grundverordnung tendenziell umfassender und adressieren sowohl öffentliche als auch nichtöffentliche Stellen. Es werden auch gänzlich neue Rechte geschaffen, wie insbesondere das Recht auf Datenübertragbarkeit aus Art. 20 (ex Art. 18) DSGVO. Insoweit muss der deutsche Gesetzgeber nicht zwingend handeln, wenn er diese Vorschrift mit voller Wirkkraft belassen möchte. Will er diese einschränken, kann er dies, sofern Art. 23 (ex Art. 21) DSGVO greift.
Art. 23 (ex Art. 21) DSGVO verschafft den Mitgliedstaaten unter den geschilderten Voraussetzungen[546] umfassend die Möglichkeit, gerade im öffentlichen Bereich Beschränkungen und Modifikationen der Betroffenenrechte vorzunehmen. Allerdings muss die nationale Norm dem Katalog des Art. 23 Abs. 2 (ex Art. Art. 21 Abs. 2) DSGVO genügen.[547] Das verlangt jedenfalls zunächst, dass eine entsprechende Einschränkung tatsächlich notwendig ist. Hier stellt sich die Frage, ob für einzelne der in den Art. 12 ff. DSGVO vorgesehenen Rechte der Betroffenen und Pflichten der Verarbeiter derartige Gründe pauschal für die Datenverarbeitung der öffentlichen Hand vorliegen. Insgesamt dürfte der Ansatz sinnvoll sein, möglichst umfassend von den Regelungen der Datenschutz-Grundverordnung auszugehen und nur in den wenigen Fällen – vor allem im öffentlichen Bereich – Änderungen in einer Sondernorm vorzusehen, wo Abweichungen notwendig sind.

§ 19: Auskunft an den Betroffenen

§ 19 Abs. 1 BDSG regelt das Auskunftsrecht und korrespondiert mit Art. 15 DSGVO. Die Öffnungsklausel nach Art. 23 (ex Art. 21) DSGVO lässt zwar eine abweichende Regelung zu. Die Diskrepanz zwischen Art. 15 DSGVO und § 19 BDSG, die teils auf Formulierungsunterschieden, vor allem aber auf im Detail unterschiedlichen Inhalten des Auskunftsrechts gründet (etwa Hinweise zur Speicherdauer in Art. 15 Abs. 1 lit. d), lässt sich grundsätzlich nicht durch die Rechtfertigungsgründe des Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO pauschal rechtfertigen.

[546] Siehe ausführlich S. 68.
[547] Dazu ausführlich S. 71.

§ 19 Abs. 2 Alt. 1 BDSG normiert einen Ausschluss vom Auskunftsrecht für archivierte Daten. Diese finden in Art. 15 DSGVO nicht als Problem Erwähnung; auch Art. 23 (ex Art. 21) DSGVO dürfte nicht einschlägig sein. Dies gilt jedenfalls soweit entsprechende Auskunftsansprüche nicht in einem Umfang überhandnehmen, der das finanzielle Interesse der öffentlichen Hand als wichtiges Ziel in Art. 23 Abs. 1 lit. e (ex Art. 21 Abs. 1 lit. c) DSGVO angesichts einer unverhältnismäßigen Kostenbelastung bei der öffentlichen Stelle greifen lässt.
§ 19 Abs. 2 Alt. 2 BDSG regelt hingegen einen Ausschluss für Daten, die ausschließlich der Datensicherung und Datenschutzkontrolle dienen (etwa Sicherungskopien oder Protokolldaten), soweit eine Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde. Auch diese Daten erwähnt Art. 15 DSGVO als Problem nicht; Art. 23 (ex Art. 21) DSGVO dürfte ebenso wenig einschlägig sein. Dies gilt auch hier, soweit entsprechende Auskunftsansprüche nicht angesichts einer unverhältnismäßigen Kostenbelastung der Behörde das Ziel des Art. 23 Abs. 1 lit. e (ex Art. 21 Abs. 1 lit. c) DSGVO eingreifen lassen. Damit ließe sich auch der Ansatz einer Verhältnismäßigkeitsprüfung hinsichtlich des entstehenden Aufwands unter der Geltung der DSGVO fortführen. Dass eine entsprechende Ausnahme greift, wird aber regelmäßig schon deshalb nicht der Fall sein, weil und soweit diese Sicherungskopien keine weiteren personenbezogenen Daten enthalten.
§ 19 Abs. 3 BDSG regelt eine Zustimmungspflichtigkeit für die Auskunft über eine Übermittlung von Daten an Sicherheitsbehörden. Art. 23 Abs. 1 lit. a (ex Art. 21 Abs. 1 lit. aa) (Schutz der nationalen Sicherheit) und lit. c (ex lit. a) (Schutz der öffentlichen Sicherheit) DSGVO rechtfertigen eine entsprechende Einschränkung der Beauskunftung. Dabei muss die Vorschrift jedoch an den Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO angepasst werden. Unter dieser Voraussetzung kann die Vorschrift, sofern rechtspolitisch erwünscht, beibehalten werden.
Weitere Ausnahmen bzw. Auskunftsverbote sieht § 19 Abs. 4 BDSG vor. Soweit dies bei einer Gefährdung in Nr. 1 der Aufgabenerfüllung, in Nr. 2 Var. 2 der öffentlichen Ordnung sowie in Var. 3 des Wohls des Bundes oder eines Landes der Fall ist, ist Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO nur bedingt einschlägig. Dieser sieht zwar eine ganze Reihe von Rechtfertigungstatbeständen vor. Jedoch stellen diese nicht allgemein auf die Erfüllung öf-

fentlicher Aufgaben ab. Daher müsste eine Eingrenzung der Beschränkung auf die dort angeführten Ziele erfolgen. Ferner ist der Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeiten. § 19 Abs. 4 Nr. 2 Var. 1 stellt hingegen konkret auf die öffentliche Sicherheit und Nr. 3 auf die Geheimhaltungspflicht ab. Art. 23 Abs. 1 lit. c (ex Art. 21 Abs. 1 lit. a) (öffentliche Sicherheit) und lit. i Alt. 2 (ex lit. f Alt. 2) (Rechte und Freiheiten anderer Personen) deckt diese Ausnahmen ab. Auch hier ist jedoch der Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeiten.
Die Abs. 5 und 6 sind des Weiteren mit Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO vereinbar, bzw. gestalten diesen hinreichend (jedoch noch nicht vollständig) aus. Nach Art. 23 Abs. 2 lit. h (ex Art. 21 Abs. 2 lit. h) DSGVO gehört zu dem abzuarbeitenden Katalog auch eine Unterrichtungspflicht, „sofern dies nicht dem Zweck der Beschränkung abträglich ist“. Das wird durch die Bestimmung des § 19 Abs. 5 BDSG umgesetzt. Ferner gehören zu dem nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeitenden Katalog prozedurale Sicherungsmechanismen, wozu die Auskunftspflicht nach § 19 Abs. 6 BDSG zählt.
Die in § 19 Abs. 7 BDSG geregelte Unentgeltlichkeit normiert nun Art. 12 Abs. 5 DSGVO. Er lässt im Einzelfall auch eine Kostenpflichtigkeit zu. Ob der nationale Gesetzgeber hiervon für seine eigenen, öffentlichen Stellen generell abweichen darf und generelle Kostenfreiheit vorsehen kann, ist unklar. Für eine solche Befugnis spricht, dass es sich bei dem Recht, Kosten zu erheben, um eine „kann“-Vorschrift handelt und der Gesetzgeber diese wohl für seine öffentlichen Stellen generell zugunsten einer Kostenfreiheit i.S. e. ermessenslenkenden Vorschrift ausfüllen darf.

§ 19 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	Art. 15	Streichen	Die Regelung wird durch Art. 15 DSGVO substituiert. Die Öffnungsklausel nach Art. 23 (ex Art. 21) DSGVO lässt zwar eine abweichende Regelung zu, rechtfertigt aber nicht die vorliegenden Abweichungen.

Abs. 2 Alt. 1 (Ausschluss für archivierte Daten)	-	Wohl Streichung oder erhebliche Einschränkung	So weitgehend nicht von Art. 23 (ex Art. 21) DSGVO gedeckt.
Abs. 2 Alt. 2 (Ausschluss für Datensicherung und Datenschutzkontrolle)	-	Wohl Streichung oder erhebliche Einschränkung	Dito
Abs. 3 (Übermittlung an Sicherheitsbehörden)	Art. 15; Öffnungsklausel: Art. 23 Abs. 1 lit. a und c (ex Art. 21 Abs. lit. aa und lit. a)	Wohl Beibehalten möglich	Wohl durch Art. 23 Abs. 1 lit. a (ex Art. 21 Abs. 1 lit. aa) (Schutz der nationalen Sicherheit) und lit. c (ex lit. a) (Schutz der öffentlichen Sicherheit) gedeckt.
Abs. 4 Nr. 1 (Gefährdung der Aufgabenerfüllung) und Nr. 2 Var. 2 (öffentliche Ordnung) und Var. 3 (Wohle des Bundes oder eines Landes)	Art. 15; Öffnungsklausel: Art. 23 Abs. 1 (ex Art. 21 Abs. 1)	Beibehalten mit Modifikation möglich	So von Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO nicht umfassend gedeckt. Daher müsste eine Eingrenzung der Beschränkung auf die dort angeführten Ziele erfolgen. Ferner ist der Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeiten.
Abs. 4 Nr. 2 Var. 1 (öffentliche Sicherheit) und Nr. 3 (Geheimhaltungspflicht)	Art. 15; Öffnungsklausel: Art. 23 Abs. 1 lit. c und lit. i Alt. 2 (ex 21 Abs. 1 lit. a und lit. f	Beibehalten möglich	Art. 23 Abs. 1 lit. c (ex Art. 21 Abs. 1 lit. a) (öffentliche Sicherheit) und lit. i Alt. 2 (ex lit. f Alt. 2) (Rechte und Freiheiten anderer Personen) deckt diese Ausnahmen ab. Es ist der Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeiten.

	Alt. 2)		
Abs. 5 (begrenzte Begründungspflicht bei Ablehnung)	Art. 15; Öffnungsklausel: Art. 23 (ex Art. 21)	Beibehalten möglich	Element des Katalogs nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO.
Abs. 6 (Auskunft an die BfDI)	Art. 15; Öffnungsklausel: Art. 23 (ex Art. 21)	Beibehalten möglich	Dito
Abs. 7 (Unentgeltlichkeit)	Art. 12 Abs. 5	Beibehalten wohl möglich	Der Gesetzgeber kann mit der Anordnung der Kostenfreiheit für Auskünfte seiner öffentlichen Stellen die „kann"-Vorschrift des Art. 12 Abs. 5 S. 2 DSGVO generell ermessensleitend ausfüllen.

§ 19a: Benachrichtigung

§ 19a BDSG regelt die Benachrichtigungspflicht und korrespondiert mit Art. 14 (ex Art. 14a) DSGVO, weicht aber von dieser Vorgabe ab. § 19a BDSG bezieht sich nach überkommener Auslegung (und in Abgrenzung von § 4 Abs. 3 BDSG) nur auf die geheime Erhebung von Daten – sei es beim Betroffenen oder bei Dritten. Damit unterscheidet sie prima vista anders als die DSGVO in Art. 13 und 14. Ihnen scheint es dem Wortlaut nach alleine darum zu gehen, wo die Daten erhoben werden, nicht aber wie. Damit würde § 19a BDSG sowohl mit Art. 14 als auch mit Art. 13 DSGVO korrespondieren. Dieses Verständnis der Abgrenzung von Art. 13 und 14 DSGVO überzeugt jedoch nicht. Art. 13 DSGVO erfasst vielmehr nur die nicht-geheime Erhebung von Daten unmittelbar beim Betroffenen. Dies macht insbesondere ein Vergleich der Ausschlussgründe nach Art. 13 Abs. 4 und Art. 14 Abs. 5 DSGVO deutlich: Nur bei Art. 14 Abs. 5 DSGVO erlaubt eine bestehende gesetzliche Verarbeitungspflicht, von der Benachrichtigung abzusehen. (Nur) in Fällen der gesetzlich angeordneten geheimen Erhebung ist ein solches Absehendürfen zwingend. Sonst wäre nämlich die Geheimhaltung gefährdet.

Die Öffnungsklausel nach Art. 23 (ex Art. 21) DSGVO lässt zwar eine abweichende Regelung zu. Die Diskrepanz zwischen Art. 14 (ex Art. 14a) DSGVO und § 19a Abs. 1 BDSG, die teils in Formulierungsunterschieden, vor allem aber in im Detail unterschiedlichen Inhalten der Benachrichtigungspflicht begründet ist (etwa Hinweise zur Speicherdauer in Art. 14 Abs. 2 lit. a [ex Art. 14a Abs. 2 lit. b]), lässt sich grundsätzlich nicht durch die Rechtfertigungsgründe des Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO pauschal rechtfertigen.
Die Ausnahmevorschrift in § 19a Abs. 2 BDSG ist im Unionsrecht vorgesehen.
In Bezug auf § 19a Abs. 3 BDSG gilt schließlich das zu § 19 Abs. 2 bis 4 BDSG Gesagte.

§ 19a BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	Art. 14 (ex Art. 14a); Öffnungsklausel: Art. 23 (ex Art. 21)	Streichen	Abweichende Regelung ist nicht durch die Rechtfertigungsgründe des Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO pauschal gerechtfertigt.
Abs. 2 Nr. 1, 2, 3	Art. 14 Abs. 5 lit. a, b, c (ex Art. 14a Abs. 4 lit. a; b; c)	Streichen	Regelung ist im Unionsrecht vorgesehen.
Abs. 3 verweist auf § 19 Abs. 2-4	s.o. bei § 19 Abs. 2 bis 4 BDSG	Beibehalten, aber Verweisung auf entsprechend modifizierte § 19 Abs. 2 bis 4, s.o.	s.o. bei § 19 Abs. 2 bis 4 BDSG

§ 20: Berichtigung, Löschung und Sperrung von Daten; Widerspruchsrecht

§ 20 BDSG korrespondiert sub specie der Berichtigung, Löschung und Sperrung von Daten sowie dem Widerspruchsrecht mit verschiedenen Normen in der Datenschutz-Grundverordnung, namentlich den Art. 16, 17, 18 und 21 (ex Art. 17a und Art. 19). Die Öffnungsklausel nach Art. 23 (ex Art. 21) DSGVO lässt zwar eine abweichende Regelung zu. Die Diskrepanz zwischen Art. 17, 18 und 21 (ex Art. 17a und Art. 19) DSGVO einerseits und § 20 Abs. 1 bis 8 BDSG andererseits, die teils in Formulierungsunterschieden, vor allem aber in einer umfassenderen Reichweite der Normen der Datenschutz-Grundverordnung liegt, lässt sich grundsätzlich nicht durch die angeführten Öffnungsklauseln des Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO pauschal rechtfertigen. § 20 ist daher zu streichen und von den Art. 16, 17, 18 und 21 (ex Art. 17a und Art. 19) substituiert. Ferner müssen die im deutschen Datenschutzrecht nicht vergleichbar umfangreichen Regelungen des Art. 13 (ex Art. 14) und 14 (ex 13) DSGVO greifen.

Etwas anderes gilt lediglich für § 20 Abs. 9 BDSG, der Sonderregelungen mit Blick auf das Bundesarchivgesetz vorsieht. Die Betroffenenrechte der Art. 15, 16, 18, 19, 20 und 21 (ex Art. 17a, Art. 17b, Art. 18 und Art. 19) DSGVO können gemäß Art. 89 Abs. 3 (ex Art. 83 Abs. 3) DSGVO zum Zweck der Verarbeitung für im öffentlichen Interesse liegende Archivzwecke durch mitgliedstaatliche Regelungen unter Wahrung der Anforderungen des Art. 89 Abs. 1 (ex Art. 83 Abs. 1) DGSVO ausgeschlossen werden. Dies deckt grundsätzlich die Regelung des § 21 Abs. 9 BDSG mit dem Verweis auf das Bundesarchivgesetz, da Art. 89 Abs. 3 DSGVO insgesamt weitreichende Einschränkungen der Betroffenenrechte mit Blick auf Archivzwecke eröffnet. In der Sache ist dies jedoch eine Frage der Ausgestaltung des Bundesarchivgesetzes und sollte dort geregelt werden. Dies gilt allerdings nur, sofern sich Abs. 9 nicht auf einen Löschungsanspruch bezieht. Denn der Hinweis soll die Spezialität des Bundesarchivgesetzes sichern und damit v. a. gewährleisten, dass Datenbestände vor einem etwaigen Löschen dem Bundesarchiv überlassen werden. Die Ausnahmen von der Löschung regelt Art. 17 Abs. 3 DSGVO abschließend, so dass die Vorschrift des Abs. 9, soweit sie eine Ausnahme von der Löschung vorsieht, allenfalls wiederholend im nationalen Recht aufrechterhalten bleiben kann.

§ 20 BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1 – 8	Art. 16, 17, 18 und 21 (ex Art. 17a und Art. 19); Öffnungsklausel: Art. 23 (ex Art. 21)	Streichen	Die Diskrepanz zwischen Art. 17, 18 und 21 (ex Art. 17a und Art. 19) DSGVO einerseits und § 20 BDSG andererseits lässt sich grundsätzlich nicht durch die Öffnungsklausel des Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO pauschal rechtfertigen
Abs. 9 (Bundesarchivgesetz), sofern er sich *nicht* auf den Löschungsanspruch bezieht	Art. 89 Abs. 3 (ex Art. 83 Abs. 3)	ggf. modifiziert im Bundesarchivgesetz regeln	Dies ist eine Frage der Ausgestaltung des Bundesarchivgesetzes und sollte dort geregelt werden.
Abs. 9 (Bundesarchivgesetz), sofern er sich auf den Löschungsanspruch bezieht	Art. 17 Abs. 3 lit. d	Beibehalten nicht tunlich – streichen	Die Ausnahme vom Löschanspruch ist in Art. 17 Abs. 3 DSGVO abschließend geregelt – Art. 89 Abs. 3 DSGVO sieht keine Öffnungsklausel vor, die ein Abweichen von Art. 17 DSGVO gestattet. Die Vorschrift kann allenfalls wiederholend im nationalen Recht aufrechterhalten bleiben, um eine konsistente Regelung zu behalten.

§ 21: Anrufung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

§ 21 BDSG regelt, unter welchen Voraussetzungen sich ein Betroffener an den Beauftragten für den Datenschutz und die Informationsfreiheit wenden kann. Die Vorschrift korrespondiert in S. 1 mit dem allgemeinen Beschwerderecht aus Art. 77 DSGVO. Die Beschränkung auf Tätigkeiten von Gerichten des Bundes in Verwaltungsangelegenheiten ergibt sich aus der entsprechenden Begrenzung der Zuständigkeit der Aufsichtsbehörde in Art. 55 Abs. 3 DSGVO. Eine Beschwerde, die außerhalb der Zuständigkeit der Aufsichtsbehörde liegt, ist unzulässig, jedenfalls unbegründet.

§ 21 BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
S. 1	Art. 77 (ex Art. 73)	Streichen	§ 21 S. 1 BDSG geht im allgemeinen Beschwerderecht nach Art. 77 DSGVO auf.
S. 2	Art. 55 Abs. 3 (ex Art. 51 Abs. 3)	Streichen	S. 2 nimmt Datenschutzverstöße, die Gerichte des Bundes begangen haben, von dem Recht zur Anrufung der BfDI grundsätzlich aus. Etwas anderes gilt für den Bereich, in dem Gerichte nicht in ihrer rechtsprechenden Tätigkeit, sondern als Verwaltungsbehörden tätig werden. Die Vorschrift des § 21 S. 2 BDSG konfligiert nicht zwingend mit Art. 58 Abs. 5 (ex Art. 53 Abs. 3) DSGVO. Denn diese regelt lediglich die Klagebefugnis der Aufsichtsbehörden, nicht aber das Recht, sich an die Aufsichtsbehörde zu wenden. Vielmehr entspricht § 21 S. 2 der Zuständigkeitsbegrenzung der Aufsichtsbehörden durch Art. 55 Abs. 3 (ex Art. 51 Abs. 3 DSGVO): Für die Überwachung der von Gerichten im Rahmen ihrer gerichtlichen Tätigkeit vorgenommenen Verarbeitungen sind die Aufsichtsbehörden nicht zuständig – Beschwerden sind damit unzulässig oder jedenfalls unbegründet. Eine mitgliedstaatliche Regelung ist nicht erforderlich. Für sie lässt die unmittelbar geltende DSGVO auch keinen Raum.

§§ 22 – 26: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

Entsprechend der Ausdifferenzierung der materiell-rechtlichen Vorgaben für öffentliche und nicht-öffentliche Stellen sieht das BDSG auch divergierende Regelungen für die Datenschutzaufsicht vor. Die §§ 22 – 26 BDSG regeln dabei die Kontrolle im öffentlichen Bereich des Bundes und gestalten insoweit die Behörde der BfDI aus. § 22 BDSG regelt dabei die Wahl und Unabhängigkeit der BfDI, § 23 BDSG deren Rechtsstellung, § 24 BDSG die Kon-

trollbefugnisse und § 25 BDSG gestaltet insbesondere das Beanstandungsrecht aus. Schließlich regelt § 26 BDSG eine Reihe weiterer Aufgaben insbesondere in Form der Berichts- und Gutachtentätigkeit.
Insbesondere Art. 52 Abs. 3 – 5, Art. 53 Abs. 1 und Art. 54 DSGVO geben den Mitgliedstaaten hinsichtlich dieser Regelungsgegenstände pro futuro zahlreiche Sicherstellungs- und Regelungsaufträge mit auf den Weg.

§ 22: Wahl und Unabhängigkeit der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

§ 22 Abs. 1 S. 1 BDSG sieht als Legitimationsweg der Bestellung der BfDI die Wahl durch den Deutschen Bundestag auf Vorschlag der Bundesregierung vor. Die Ernennung erfolgt gemäß § 22 Abs. 1 S. 3 BDSG durch den Bundespräsidenten. Die Ernennung nimmt damit nach deutschem Recht das Staatsoberhaupt i. S. d. Art. 53 Abs. 1 Spstr. 3 (ex Art. 48 Abs. 1 Spstr. 3) DSGVO vor; eine arbeitsteilige Beteiligung weiterer Staatsorgane ist trotz der als Alternativen ausgestalteten Formulierung in Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO unschädlich. Der dabei vorgesehene Verzicht auf eine Aussprache kann zwar die Transparenz des Verfahrens im Sinne des Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO in Frage stellen, ist aber als eine zulässige Verfahrenskonkretisierung zu verstehen („Die Mitgliedstaaten sehen vor…“). Daher können die Sätze 1 und 3 des § 22 Abs. 1 BDSG so beibehalten werden.
Hinsichtlich der Qualifikation der BfDI regelt das BDSG in § 22 Abs. 1 S. 2 BDSG alleine das (Mindest-)Alter von 35 Jahren. Dies ist mit Blick auf die notwendige Lebenserfahrung noch als zulässige Mindestanforderung der Qualifikation anzusehen. Die Vorschrift wird jedoch zu ergänzen sein, um die Anforderungen aus Art. 53 Abs. 2 (ex Art. 48 Abs. 2) und auch aus Art. 54 Abs. 1 lit. b (ex Art. 49 Abs. 1 lit. b) DSGVO an die Normierung der materiellen Anforderungen (z. B. fachliche Qualifikation) zu erfüllen.
§ 22 Abs. 2 BDSG sieht einen Amtseid vor. Die Datenschutz-Grundverordnung regelt ihn nicht explizit. Bei dem Amtseid handelt es sich jedoch um eine formelle Konkretisierung des Ernennungsvorgangs, die eine zulässige Konkretisierung der Anforderungen des Art. 54 Abs. 1 lit. c (ex Art. 49 Abs. 1 lit. c) DSGVO darstellt.

§ 22 Abs. 3 BDSG regelt die Länge der Amtszeit (fünf Jahre) und eröffnet die Möglichkeit zur einmaligen Wiederwahl. Beides bewegt sich im Bereich dessen, was die Datenschutz-Grundverordnung in Art. 54 Abs. 1 lit. d und e (ex Art. 49 Abs. 1 lit. d und e) für zulässig erachtet. Mit Blick auf die Amtszeit der derzeitigen Mitglieder der Aufsichtsbehörden lässt die DSGVO in Art. 54 Abs. 1 lit. d Hs. 2 (ex Art. 49 Abs. 1 lit. d Hs. 2) eine kürzere Frist als vier Jahre zu, „wenn eine zeitlich versetzte Ernennung zur Wahrung der Unabhängigkeit der Aufsichtsbehörde notwendig ist".

§ 22 Abs. 4 S. 2 BDSG verbürgt der BfDI Unabhängigkeit. Die Vorschrift entspricht – nach der jüngsten Novellierung des BDSG – der Unabhängigkeitsanforderung des Art. 52 Abs. 2 (ex Art. 47 Abs. 2) DSGVO, da die BfDI als oberste Bundesbehörde ausgestaltet ist und weder einer Rechts- noch einer Fach- noch einer Dienstaufsicht unterliegt[548]. Die Ausgestaltung als „öffentlich-rechtliches Amtsverhältnis" in § 22 Abs. 4 S. 1 BDSG schafft dabei ein „Dienstverhältnis eigener Art"[549], das die Unabhängigkeit wahrt, indem es etwa die Anwendung des Disziplinarrechts[550] ausschließt. Es handelt es sich insoweit um eine zulässige mitgliedstaatliche Konkretisierung der Stellung, welche die Aufsichtsbehörde genießt.

§ 22 Abs. 5 S. 1 BDSG nimmt jene unabhängigkeitswahrende Ausgestaltung als oberste Bundesbehörde vor und gewährleistet damit gleichermaßen die Unabhängigkeitsanforderung des Art. 52 Abs. 2 (ex Art. 47 Abs. 2) DSGVO, aber auch die Personalhoheit nach Art. 52 Abs. 5 (ex Art. 47 Abs. 6) DSGVO. Die Regelung des Dienstsitzes in § 22 Abs. 5 S. 2 BDSG ist unionsrechtlich nicht vorgezeichnet und daher der mitgliedstaatlichen Ausgestaltung überlassen; das gilt auch für die körperschaftliche Zuweisung der Mitarbeiter der BfDI als solche des Bundes im Beamtenverhältnis. Dies ermöglicht die Wahrung entsprechender Unabhängigkeitsanforderungen auch in Bezug auf die Bediensteten der Aufsichtsbehörde.

§ 22 Abs. 6 BDSG schafft eine Vertretungsregelung für den Fall, dass der BfDI verhindert ist. Die Datenschutz-Grundverordnung sieht insoweit keine

[548] Siehe zur Änderung der diesbezüglichen Rechtslage aufgrund der unionsrechtlichen Anforderungen bereits aus der DSRL 95/46/EG *Kühling/Seidel/Sivridis* (Fn. 44), S. 230 f.
[549] So *von Lewinski*, in: Auernhammer (Hrsg.), BDSG, 4. Aufl., 2014, § 22, Rn. 15.
[550] So zutreffend *von Lewinski* (Fn. 549), § 22, Rn. 17.

Regelung vor; es handelt sich um eine sinnvolle Konkretisierung bzw. Ausgestaltung der Aufsichtsbehörde, die zugleich durch den Verweis in § 22 Abs. 6 S. 2 BDSG auf die Unabhängigkeit nach § 22 Abs. 4 S. 2 BDSG die nach Art. 52 Abs. 1, 2 (ex Art. 47 Abs. 1, 2) DSGVO erforderliche Unabhängigkeit gewährleistet.

§ 22 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 S. 1 (Wahl auf Vorschlag der BReg durch BT)	Art. 53 Abs. 1 (ex Art. 48 Abs. 1)	Wohl beibehalten; allenfalls geringfügig modifizieren („Aussprache“)	Sowohl die Beteiligung mehrerer Kreationsorgane als auch der Verzicht auf eine Aussprache kann noch als zulässige Konkretisierung des Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO angesehen werden.
Abs. 1 S. 2 (Mindestalter)	Art. 53 Abs. 2; Art, 54 Abs. 1 lit. b (ex Art. 48 Abs. 2; Art. 49 Abs. 1 lit. b)	Beibehalten; Ergänzung um weitere Anforderungen an die Qualifikation	§ 22 Abs. 1 S. 2 BDSG setzt die Vorgabe des Art. 53 Abs. 2 (ex Art. 48 Abs. 2) DSGVO hinsichtlich der erforderlichen Erfahrung um – allerdings nicht vollständig, so dass eine Ergänzung erforderlich ist.
Abs. 1 S. 3 (Ernennung durch BP)	Art. 53 Abs. 1; Art, 54 Abs. 1 lit. c (ex Art. 48 Abs. 1; Art. 49 Abs. 1 lit. c)	Beibehalten	Setzt die Vorgabe der Art. 53 Abs. 1 (ex Art. 48 Abs. 1) DSGVO und Art. 54 Abs. 1 lit. c (ex Art. 49 Abs. 1 lit. c) DSGVO um.
Abs. 2 (Amtseid)	- / (Art. 54 Abs. 1 lit. c [ex Art. 49 Abs. 1 lit. c])	Beibehalten	Die Datenschutz-Grundverordnung thematisiert einen Amtseid nicht explizit. Insoweit liegt jedoch eine zulässige Konkretisierungsvorgabe des Ernennungsverfahrens vor.

Abs. 3 (Amtszeit; Wiederwahl)	Art. 54 Abs. 1 lit. d (ex Art. 49 Abs. 1 lit. d und e)	Beibehalten	Die Regelung zur Länge der Amtszeit und auch die Möglichkeit zur einmaligen Wiederwahl bewegen sich im Bereich dessen, was die DSGVO für zulässig erachtet. Mit Blick auf die Amtszeit der jetzigen BfDI lässt die DSGVO in Art. 54 Abs. 1 lit. d Hs. 2 (ex Art. 49 Abs. 1 lit. d Hs. 2) unter bestimmten Voraussetzungen eine Verkürzung der vierjährigen Mindest-Amtszeit zu.
Abs. 4 S. 1 (öffentlich-rechtliches Amtsverhältnis)	- / (Art. 52 Abs. 1 und 2 [ex Art. 47 Abs. 1und 2])	Beibehalten	Zulässige Konkretisierung der Amtsstellung und Unabhängigkeit der Aufsichtsbehörde.
Abs. 4 S. 2 (Unabhängigkeit)	Art. 52 Abs. 1 und 2 (ex Art. 47 Abs. 1 und 2)	Beibehalten wohl möglich	Die Norm entspricht den Vorgaben der DSGVO und kann als Teil eines weit verstandenen Errichtungsauftrags (Art. 54 Abs. 1 lit. a DSGVO) und einer in sich konsistenten nationalen Ausgestaltungsregelung wohl aufrechterhalten bleiben.
Abs. 5 S. 1 (oberste Bundesbehörde)	Art. 52 Abs. 1, Abs. 5 (ex Art. 47 Abs. 1, Abs. 6)	Beibehalten	Die Norm dient der Umsetzung der EuGH-Rechtsprechung zur „völligen Unabhängigkeit“ und gewährleistet auch die Personalhoheit nach Art. 52 Abs. 5 (ex Art. 47 Abs. 6) DSGVO.
Abs. 5 S. 2 (Dienstsitz)	-	Beibehalten	Zum Dienstsitz trifft die Datenschutz-Grundverordnung keine Aussage, dies bleibt der mitgliedstaatlichen Entscheidung überlassen.
Abs. 5 S. 3 (Bundesbeamte)	- / (Art. 52 Abs. 5 [ex Art. 47 Abs. 6])	Beibehalten	Die körperschaftliche Zuweisung (*Bundes*beamte) bleibt der Konkretisierung durch die Mitgliedstaaten überlassen; die Beamteneigenschaft (Bundes*beamten*) stärkt die Unabhängigkeit der Bediensteten.
Abs. 6 S. 1 (Vertretungsregelung)	-	Beibehalten	Auch hier entbehrt die Datenschutz-Grundverordnung einer Aussage. Die Schaffung einer Vertretungsregelung ist aber eine sinnvolle Konkretisierung bzw. Ausgestaltung des Amtes der Aufsichtsbehörde.

Abs. 6 S. 2 (Unabh. bei Vertretung)	- / (Art. 52 Abs. 1, 2 [ex Art. 47 Abs. 1, 2])	Beibehalten	Zwar trifft die DSGVO in Bezug auf die Vertretung keine Aussagen, jedoch ist es angezeigt, auch dem Vertreter der BfDI eine sachliche Unabhängigkeit zu gewähren.

§ 23: Rechtsstellung der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

§ 23 BDSG bestimmt die Rechtsstellung der BfDI näher. Abs. 1 normiert den Beginn und das Ende ihrer Amtszeit. Zu dem in Abs. 1 S. 1 geregelten Beginn des Amtsverhältnisses sieht die DSGVO keine Regelung vor, so dass das BDSG insoweit eine zulässige und auch zweckmäßige nationale Regelung trifft. Anderes gilt für die Entlassungsgründe. Für diese nimmt § 23 Abs. 1 S. 2 und 3 BDSG Bezug auf § 21 DRiG, der wesentlich weiter gefasst ist als Art. 53 Abs. 4 (ex Art. 48 Abs. 4) DSGVO. Hier bedarf es einer Anpassung: Amtsenthebungsgründe sind entsprechend Art. 53 Abs. 4 (ex Art. 48 Abs. 4) DSGVO auf Fälle einer schweren Verfehlung bzw. des Wegfalls der Voraussetzungen für die Wahrnehmung der Aufgaben zu begrenzen. Weitere Gründe für das Ende der Amtszeit sind deren Ablauf und der Rücktritt.
§ 23 Abs. 1 S. 4 und 5 BDSG konkretisiert den auch in Art. 53 Abs. 3 (ex Art. 48 Abs. 3) DSGVO vorgesehenen Entlassungsvorgang, der dort jedoch nicht näher geregelt ist (Entlassungsurkunde und deren Aushändigung als Wirksamkeitsvoraussetzung und Markierung des Wirksamkeitszeitpunkts). Es handelt sich um eine in Deutschland übliche Regelung für Ämter, die sachgerecht ist und beibehalten werden sollte, um insoweit klare Verhältnisse zu schaffen. Dasselbe gilt für § 23 Abs. 1 S. 6 BDSG, der für den Fall des regulären Endes des Amtes durch Ablauf der Amtszeit eine Interimslösung schafft: Die bisherige BfDI bleibt auf Ersuchen des Präsidenten des Bundestages bis zur Nachfolgeregelung im Amt.
§ 23 Abs. 2 BDSG verbietet der BfDI umfassend eine anderweitige Berufsausübung. Die Norm bildet den Regelungsgehalt des Art. 52 Abs. 3 (ex Art. 47 Abs. 3) DSGVO und des Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f) DSGVO jedoch nur teilweise ab. Es fehlt namentlich ein Verbot, auch unentgeltliche Tätigkeiten auszuüben, die mit dem Amt nicht zu vereinbaren sind. Zudem ist die Norm in ihrem sachlichen Bezugspunkt zu eng. Die Datenschutz-Grundverordnung verlangt, *sämtliche* mit dem Amt nicht zu vereinba-

renden Handlungen zu unterlassen. Schlussendlich fehlt es an einer Regelung im BDSG, die ein mit dem Amt unvereinbares Verhalten auch *nach* der Amtszeit erfasst. Daher ist hier eine Modifikation der Regelung erforderlich.
§ 23 Abs. 3 BDSG trifft eine für die Wahrung der Unabhängigkeit notwendige und sinnvolle Regelung der Annahme von Geschenken. Sie findet keine entsprechende Regelung in der Datenschutz-Grundverordnung. Die Regelungen passen aber in den thematischen Kontext der Art. 52 Abs. 2 (ex Art. 47 Abs. 3) DSGVO und Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f) DSGVO. Sie können daher als sinnvolle Konkretisierung beibehalten werden.
§ 23 Abs. 4 BDSG regelt das Zeugnisverweigerungsrecht der BfDI und ihrer Mitarbeiterinnen, das in den thematischen Kontext der Verschwiegenheitspflicht gemäß Art. 54 Abs. 2 (ex Art. 49 Abs. 2) DSGVO gehört und eine effektive Aufgabenwahrnehmung der Behörde ermöglichen soll. Auch wenn die Norm in der Datenschutz-Grundverordnung keine passgenaue Entsprechung findet, ist sie als zulässige Konkretisierung der Ausgestaltung der Aufsichtsbehörde und der Verschwiegenheitspflicht nach Art. 54 Abs. 2 (ex Art. 49 Abs. 2) DSGVO anzusehen und daher beizubehalten.
§ 23 Abs. 5 BDSG regelt umfassend die Verschwiegenheitspflicht. Die Norm enthält ein fein austariertes System, das den Anforderungen des Art. 54 Abs. 2 (ex Art. 49 Abs. 2) DSGVO wohl entspricht.
§ 23 Abs. 6 BDSG normiert die Möglichkeit und die Einschränkungen des Zeugenaussagerechts und gehört damit ebenfalls in den Kontext der Verschwiegenheitspflicht nach Art. 54 Abs. 2 (ex Art. 49 Abs. 2) DSGVO. Auch hier gilt, dass die Bestimmung als entsprechende konkretisierende Ausgestaltung der Datenschutz-Grundverordnung („gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten“) aufrechterhalten bleiben kann.
§ 23 Abs. 7 BDSG regelt die Besoldung und Versorgung. Die Datenschutz-Grundverordnung enthält insoweit keine explizite Vorgabe. Die Regelung der Besoldung und Versorgung der BfDI ist nicht zuletzt jedoch ein Element des mitgliedstaatlichen Sicherstellungsauftrags zur angemessenen finanziellen Ausgestaltung im Sinne des Art. 52 Abs. 4 (ex Art. 47 Abs. 5) DSGVO, das auch die Unabhängigkeit wahren soll. Sie kann daher als konkretisierende Regelung beibehalten werden.
§ 23 Abs. 8 BDSG erklärt die Regelungen zur Verschwiegenheitspflicht und spezieller die Wahrung der bundesrechtlichen Geheimnisschutzbestimmun-

gen in § 23 Abs. 5 S. 5 – 7 BDSG auch für die Landesdatenschutzbeauftragten für anwendbar. Dies soll die Bundesbelange trotz der diesbezüglichen Landeskompetenz für die Ausgestaltung der Landesdatenschutzbeauftragten absichern, die eine Frage der mitgliedstaatlichen Kompetenzverteilung ist. Der Verweis kann daher ebenso aufrechterhalten bleiben wie die Regelung in § 23 Abs. 5 S. 5 – 7 BDSG selbst.

§ 23 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 S. 1 (Beginn der Amtszeit)	-	Beibehalten	Zum Beginn des Amtsverhältnisses trifft die Datenschutz-Grundverordnung keine Aussage.
Abs. 1 S. 2 und 3 (Ende der Amtszeit; Entlassungsgründe)	Art. 53 Abs. 2 – 4; Art. 54 Abs. 1 lit. f (ex Art. 48 Abs.–2 - 4; Art. 49 Abs. 1 lit. f)	Modifizieren; einschränken	Entlassungsgründe sind mit Bezugnahme auf § 21 DRiG wesentlich weiter gefasst als Art. 53 Abs. 4 (ex Art. 48 Abs. 4) DSGVO, so dass insoweit eine Anpassung an Art. 53 Abs. 4 (ex Art. 48 Abs. 4) DSGVO erfolgen muss.
Abs. 1 S. 4, 5 (Entlassung)	-	Beibehalten u. U. möglich	Formelle Konkretisierung der Entlassung.
Abs. 1 S. 6 (Interimsamtszeit)	-	Beibehalten	Sinnvolle Norm zur Regelung der Übergangszeit bis zum Amtsantritt der oder des neuen BfDI.
Abs. 2 (Verbot anderweitiger Berufsausübung)	Art. 52 Abs. 3 (ex Art. 47 Abs. 3); Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f)	Modifizieren; ergänzen	Die Norm ist enger gefasst als Art. 52 Abs. 3 (ex Art. 47 Abs. 3) DSGVO und Art. 49 Abs. 1 lit. f (ex Art. 54 Abs. 1 lit. f) DSGVO (kein Verbot, auch unentgeltliche Tätigkeiten auszuüben, die mit dem Amt nicht zu vereinbaren sind, und sämtliche mit dem Amt nicht zu vereinbarenden Handlungen zu unterlassen; keine Wirkung nach Amtszeitende). Sie bedarf daher einer Ergänzung, wenn sie im Grundsatz aufrechterhalten bleiben soll.

Abs. 3 (Geschenke)	- / (Art. 52 Abs. 3 [ex Art. 47 Abs. 3]; Art. 54 Abs. 1 lit. f [ex Art. 49 Abs. 1 lit. f])	Beibehalten	Die Regelungen können als sinnvolle Konkretisierung von Art. 52 Abs. 3 (ex Art. 47 Abs. 3) DSGVO sowie Art. 54 Abs. 1 lit. f (ex Art. 49 Abs. 1 lit. f) DSGVO beibehalten werden.
Abs. 4 (Zeugnisverweigerungsrecht)	- / (Art. 54 Abs. 2 [ex Art. 49 Abs. 2])	Beibehalten	Die Norm findet in der DSGVO keine passgenaue Entsprechung. Sie passt aber in den thematischen Kontext der Verschwiegenheitspflicht gem. Art. 54 Abs. 2 (ex Art. 49 Abs. 2) DSGVO und kann als zulässige Konkretisierung („gemäß dem Unionsrecht oder dem Recht der Mitgliedstaaten“) beibehalten werden.
Abs. 5 (Verschwiegenheitspflicht)	Art. 54 Abs. 2 (ex Art. 49 Abs. 2)	Beibehalten	Die Norm enthält ein fein austariertes System, das den Anforderungen und nationalen Regelungsspielräumen/-aufträgen des Art. 54 Abs. 2 (ex Art. 49 Abs. 2) DSGVO wohl entspricht.
Abs. 6 (Zeugenaussagen)	- / (Art. 54 Abs. 2 [ex Art. 49 Abs. 2])	Beibehalten	Die Norm findet in der Datenschutz-Grundverordnung keine passgenaue Entsprechung. Sie gehört aber in den thematischen Kontext der Verschwiegenheitspflicht, für die Art. 54 Abs. 2 (ex Art. 49 Abs. 2) DSGVO den Mitgliedstaaten einen Regelungsspielraum/-auftrag gibt. Sie kann daher als zulässige Konkretisierung beibehalten werden.
Abs. 7 (Besoldung/Versorgung)	- / (Art. 52 Abs. 4 [ex Art. 47 Abs. 5})	Beibehalten	Die Datenschutz-Grundverordnung enthält keine explizite diesbezügliche Vorgabe. Die Regelung ist als konkretisierende Regelung und Ausgestaltung des Amtes zulässig.
Abs. 8 (Entsprechungsklausel Landesrecht)	-	Beibehalten	Die Norm dient der Sicherung der Bundesbelange im Rahmen der Geheimnisschutzregelungen.

§ 24: Kontrolle durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Hinsichtlich der Regelung der Befugnisse stellt sich die Frage, inwieweit neben Art. 58 (ex Art. 53) DSGVO überhaupt eine nationale Normierung zulässig und zweckmäßig ist. Insoweit ist zu differenzieren: Die Befugnisse des Art. 58 (ex Art. 53) DSGVO regelt im Wesentlichen die Verordnung selbst. Sie bedürfen daher keiner parallelen Ausgestaltung im BDSG.
Ob wegen der Ausgestaltung des Zugangsrechts zu den Geschäftsräumen in Art. 58 Abs. 2 lit. f (ex Art. 53 Abs. 1 lit. db) DSGVO, die eine mitgliedstaatliche Regelung erfordert, und Art. 58 Abs. 6 S. 1 DSGVO, der den Mitgliedstaaten Freiraum für zusätzliche Befugnisse zugesteht, eine Wiederholung der gesamten Befugnisse im BDSG denkbar ist, ist demgegenüber unklar. Eine solche Regelung wäre zwar der Zielrichtung zuträglich, eine insgesamt kohärente und transparente Kodifikation vorzunehmen. Das gilt auch vor dem Hintergrund, dass das BDSG bislang über die Datenschutz-Grundverordnung teilweise hinausgeht – noch mehr für § 25 BDSG (dazu sogleich zu § 25 Abs. 1 Hs. 2 BDSG). Die Öffnungsklausel des Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO lässt eine Ergänzung der in der Datenschutz-Grundverordnung vorgesehenen Befugnisse auch zu. Sollte der Bundesgesetzgeber an diesen Ergänzungen festhalten, spricht Manches für eine insgesamt umfassende kohärente Regelung mit entsprechenden – im Wortlaut parallelen – Wiederholungen der in der Datenschutz-Grundverordnung vorgesehenen Befugnisse. Allerdings streiten – auch regelungstechnisch – gute Gründe dafür, eher allgemein auf die Befugnisse des Art. 58 (ex Art. 53) DSGVO zu verweisen – mit der Maßgabe, dass im Übrigen begrenzte spezifische Regelungen gemäß dem BDSG greifen. Andernfalls besteht die Gefahr, dass die Vollharmonisierung unterlaufen und die Herkunft der Befugnisse unmittelbar aus dem Unionsrecht verschleiert wird.
Die Datenschutz-Grundverordnung unterscheidet nicht wie das BDSG strikt zwischen der Kontrolle öffentlicher und nicht-öffentlicher Stellen. Dies ergibt sich schon aus EG 122 (ex EG 95a) DSGVO, der allgemein die Ausübung der Befugnisse verlangt – unabhängig davon, ob „Behörden oder private Einrichtungen, die im öffentlichen Interesse handeln“, oder sonstige Stellen Daten verarbeiten. In Bezug auf öffentliche Stellen sieht die Datenschutz-Grundverordnung auch keine spezifischen Öffnungsklauseln bei der Ausge-

staltung der Aufsichtsbefugnisse vor. Allein mit Blick auf die Zuständigkeitsfrage findet sich in Art. 55 Abs. 3 (ex Art. 51 Abs. 3) DSGVO eine Sonderregelung:[551] Die Überwachung „von Gerichten im Rahmen ihrer gerichtlichen Kontrolle“ bleibt von der Zuständigkeit der Datenaufsichtsbehörden ausgenommen.

§ 24 BDSG weist einige Besonderheiten auf: So erstreckt § 24 Abs. 1 S. 1 Nr. 1 BDSG den Kontrollbereich auch auf Daten, die dem Fernmeldegeheimnis unterliegen. Durch den Hinweis auf Art. 10 GG in § 24 Abs. 1 S. 2 BDSG wird das BDSG dem Zitiergebot gerecht. Soweit das BDSG in Zukunft insgesamt auf die Befugnisse der Datenschutz-Grundverordnung verweist, wäre dies nicht erforderlich, da sich die entsprechende Erstreckung der Befugnis dann unmittelbar aus dem Unionsrecht ergibt und das Zitiergebot insoweit nicht greift. Sollte hingegen (soweit zulässig) eine wiederholende Formulierung der Befugnisse auch aus der Datenschutz-Grundverordnung verbunden mit den Ergänzungen auf nationaler Ebene erfolgen, kann die Regelung aus Klarstellungsgründen entsprechend beibehalten werden– ihr Fehlen könnte gleichwohl die Befugnisse aus der DSGVO ebenso wenig verkürzen wie verhindern, dass sich der Grundrechtsschutz insoweit aus der GrCh ergibt. Ebenso ist angesichts der Regelung des § 30 AO wohl § 24 Abs. 2 S. 1 Nr. 2 BDSG in Bezug auf Steuerdaten weiterhin erforderlich, um eine entsprechende Befugnis für das Offenbaren im Sinne des § 30 AO abzusichern.

§ 24 Abs. 2 S. 3 und 4 BDSG regelt die Kontrolle des Umgangs mit besonders geheim zu haltenden Daten, die dem BfDI entzogen wird. Dies betrifft in Satz 3 den Fall der Kontrolle durch die G 10-Kommisison des Bundestages (§ 15 G 10) und im Fall des Satzes 4 Daten, die aus Sicherheitsüberprüfungsakten stammen (§§ 18 – 23 SÜG). Es ist davon auszugehen, dass der Umgang mit diesen Daten außerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung liegt, da insoweit die Ausnahmebestimmungen des Art. 2 Abs. 2 lit. b und d (ex lit. c und e) DSGVO für die Datenverarbeitung im Bereich Gemeinsame Außen- und Sicherheitspolitik (Titel V Kapitel 2 EUV)

[551] Eine Sonderregelung mit Bezug insbesondere auf öffentlicher Stellen enthält auch Art. 55 Abs. 2 (ex Art. 51 Abs. 2) DSGVO. Sein Regelungsanspruch erstreckt sich aber nur auf die Bestimmung der Zuständigkeit und des Abstimmungsverfahrens, nicht die Regelungsbefugnisse.

und im Bereich der Strafverfolgung und der Gefahrenabwehr greifen. Daher kann diese Sonderbestimmung (vorbehaltlich hier nicht zu vertiefender besonderer Umsetzungsbedarfe, die sich aus den Umsetzungsverpflichtungen der Richtlinie RL 2016/680 für den Datenschutz bei Polizei und Strafjustiz ergeben), aufrechterhalten bleiben.

Die Regelung des § 24 Abs. 3 BDSG entspricht Art. 55 Abs. 3 (ex Art. 51 Abs. 3) DSGVO und sollte daher gestrichen oder aber vom Wortlaut her im Rahmen einer wiederholenden Regelung an die Verordnung angepasst werden.

Dasselbe gilt für die Regelung der Unterstützungspflicht in § 24 Abs. 4 S. 1 und S. 2 Nr. 1 BDSG, der die Unterstützungspflicht und die Einsicht in Unterlagen durch den BfDI regelt. Die Vorschrift ist wegen des tendenziell weiter gefassten Art. 58 Abs. 1 lit. a und e (ex Art. 53 Abs. 1 lit. a und lit. da) DSGVO zu streichen und für den Fall einer wiederholenden Normierung zumindest an den Wortlaut der Verordnung anzupassen. Die Besonderheiten für die Sicherheitsbehörden in § 24 Abs. 4 S. 2 und 3 BDSG können wiederum – wie § 24 Abs. 2 S. 3 und 4 BDSG – aufrechterhalten bleiben, da die Datenverarbeitung außerhalb des Anwendungsbereichs der Datenschutz-Grundverordnung liegt. Denn auch insoweit greifen die Ausnahmebestimmungen des Art. 2 Abs. 2 lit. b und d (ex c und e) DSGVO.

§ 24 Abs. 4 S. 2 Nr. 2 BDSG regelt Betretungsrechte für die Diensträume. Zwar spricht Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db) DSGVO nur von Geschäftsräumen, so dass unklar ist, ob davon auch Diensträume erfasst werden. Das kann jedoch dahin stehen, da entweder jene Öffnungsklausel oder die des Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DGVO aktiviert werden kann. Die Vorschrift kann jedenfalls so beibehalten werden.

§ 24 Abs. 5 BDSG regelt eine allgemeine Mitteilungspflicht der BfDI für Kontrollergebnisse. Eine allgemeine Mitteilungspflicht ist so in der Datenschutz-Grundverordnung nicht explizit geregelt, ergibt sich aber als sinnvolle Aufgabenwahrnehmung aus dem Gesamtumfang der Aufgaben und Befugnisse der Aufsichtsbehörde nach Art. 57 und 58 (ex Art. 52 und 53) DSGVO. Sie kann daher im Rahmen einer Normierung der Befugnisse als Pflicht wohl entsprechend aufrechterhalten bleiben.

§ 24 Abs. 5 BDSG erklärt ähnlich wie § 23 Abs. 8 BDSG die Regelungen zur Wahrung der bundesrechtlichen Geheimnisschutzbestimmungen in § 24

Abs. 2 S. 2 und 3 BDSG auch für die Landesdatenschutzbeauftragten für anwendbar. Damit soll auch insoweit (trotz der diesbezüglichen Landeskompetenz) eine Absicherung der Bundesbelange für die Ausgestaltung der Landesdatenschutzbeauftragten erfolgen. Das ist eine zulässige Ausgestaltung der mitgliedstaatlichen Kompetenzverteilung. Der Verweis kann daher ebenso aufrechterhalten bleiben wie die Regelung in § 24 Abs. 2 S. 2 und 3 BDSG selbst.
Tabellarisch zusammengefasst ergibt sich Folgendes:

§ 24 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 (Allgemeine Kontrollbefugnis)	(Art. 57 Abs. 1 lit. a [ex Art. 52 Abs. 1 lit. a])	Modifizieren	§ 24 Abs. 1 BDSG formuliert eine allgemeine Aufgabe der Kontrolle. Die Formulierung sollte an die der DSGVO in Art. 57 Abs. 1 lit. a [ex Art. 52 Abs. 1 lit. a] angepasst werden.
Abs. 2 S. 1 Nr. 1, 2 und 3 (Daten nach Art. 10 GG)	(Art. 57 Abs. 1 lit. a [ex Art. 52 Abs. 1 lit. a])	Ggf. beibehalten	Sofern eine wiederholende Normierung der Befugnisse erfolgt, kann eine entsprechende Regelung gerechtfertigt sein.
Abs. 2 S. 1 Nr. 2 (Steuerdaten)	(Art. 57 Abs. 1 lit. a [ex Art. 52 Abs. 1 lit. a])	Wohl beibehalten	Die Norm ist wohl wegen der Regelung in § 30 AO erforderlich, um Befugnis für Offenbarung zu gewährleisten.
Abs. 2 S. 3 und 4 (geheim zu haltende Daten)	(Art. 2 Abs. 2 lit. b und d [ex lit. c und e])	Wohl beibehalten	Soweit die nach § 24 Abs. 2 S. 3 und 4 BDSG geheim zu haltenden Daten, die im Fall des Satzes 3 der Kontrolle durch die G 10-Kommisison des Bundestages unterliegen (§ 15 G 10), bzw. im Fall des Satzes 4 aus Sicherheitsüberprüfungsakten stammen (§§ 18 – 23 SÜG), außerhalb des Anwendungsbereichs der DSGVO liegen, da die Ausnahmebestimmungen des Art. 2 Abs. 2 lit. b und d (ex lit. c und e) Art. 2 Abs. 2 lit. c und e DSGVO greifen, kann diese Sonderbestimmung aufrechterhalten bleiben.

Abs. 3 (begrenzte Überwachung der Gerichte)	Art. 55 Abs. 3 (ex Art. 51 Abs. 3)	Streichen oder modifizieren	Die Vorschrift ist wegen Art. 55 Abs. 3 (ex Art. 51 Abs. 3) DSGVO zu streichen und für den Fall einer wiederholenden Normierung zumindest an den Wortlaut der Verordnung anzupassen.
Abs. 4 S. 1; S. 2 Nr. 1 (Unterstützungspflicht; Einsicht in Unterlagen)	Art. 58 Abs. 1 lit. a und e (ex Art. 53 Abs. 1 lit. a und lit. da)	Streichen oder modifizieren	Dito
Abs. 4 S. 2 Nr. 2 (Betretungsrechte)	Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db) DSGVO	Beibehalten	Zwar spricht Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db) DSGVO nur von Geschäftsräumen, so dass unklar ist, ob davon auch Diensträume erfasst werden. Das kann jedoch dahin stehen, da entweder jene Öffnungsklausel oder die des Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO aktiviert werden kann.
Abs. 4 S. 3 und 4 (Sicherheitsbehörden)	(Art. 2 Abs. 2 lit. b und d [ex lit. c und e])	Beibehalten	Wie bei § 24 Abs. 2 S. 3 und 4 BDSG erfolgt die Datenverarbeitung hier außerhalb des Anwendungsbereichs der DSGVO, da die Ausnahmebestimmungen des (Art. 2 Abs. 2 lit. b und d [ex lit. c und e]) DSGVO greifen. Daher können die Bestimmungen aufrechterhalten bleiben.
Abs. 5 (Mitteilung des Kontrollergebnisses)	(allgemein Art. 58 [ex Art. 52 und 53])	Beibehalten wohl zulässig	Eine allgemeine Mitteilungspflicht regelt die DSGVO nicht explizit. Sie ergibt sich aber als sinnvolle Aufgabenwahrnehmung aus dem Gesamtumfang der Aufgaben und Befugnisse der Aufsichtsbehörde nach Art. 57 und 58 (ex Art. 52 und 53) DSGVO.
Abs. 6 (Entsprechungsklausel Landesrecht)	-	Beibehalten	Bundesbelange im Rahmen der Geheimnisschutzregelungen zu sichern, steht dem Mitgliedstaat im Rahmen seiner Kompetenzordnung frei.

§ 25: Beanstandungen durch die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Über § 24 BDSG hinausgehende Befugnisse der BfDI normiert § 25 BDSG. Diese überschreiten teilweise den Rahmen, den die Datenschutz-

Grundverordnung zieht, da sie beispielsweise eine Stellungnahmepflicht wie in § 25 Abs. 1 S. 1 Hs. 2 BDSG so explizit in der Verpflichtung nach Art. 58 Abs. 1 lit. a (ex Art. 53 Abs. 1 lit. a) DSGVO, Informationen bereitzustellen, nicht zwingend enthält. Insoweit darf auf der Basis der Öffnungsklausel in Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO eine Ergänzung der Datenschutz-Grundverordnung erfolgen. § 25 BDSG bleibt aber in anderen Teilen hinter den in Art. 58 (ex Art. 53) DSGVO vorgesehenen Befugnissen zurück. So ist der Tadel nach Art. 58 Abs. 2 lit. b (ex Art. 53 Abs. 1b lit. b) DSGVO wohl schärfer als die Beanstandung nach § 25 Abs. 1 und 2 BDSG. Vor allem aber sieht die Datenschutz-Grundverordnung eine Vielzahl weiterer, teils ergänzender, teils abweichender Maßnahmen vor, wie z. B. die Verpflichtung zur Benachrichtigung des Betroffenen in Art. 58 Abs. 2 lit. e (ex Art. 53 Abs. 1b lit. da) DSGVO, die vom Benachrichtigungsrecht der BfDI in § 23 Abs. 5 S. 7 BDSG abweicht.

Im Übrigen gilt das zu § 24 BDSG Ausgeführte auch hier: Es spricht Einiges dafür, pauschal auf die Rechte nach der Datenschutz-Grundverordnung zu verweisen und diese dann zu ergänzen, soweit dies gewünscht ist. Alternativ dürfen die DSGVO-Regeln bei weitem Verständnis des Wiederholungsverbots[552] aber auch zur Klarstellung als Teil einer in sich konsistenten und verständlichen Regelung wiederholt werden. Dabei kann dann auch eine Präzisierung erfolgen, beispielsweise an wen genau die Beanstandung zu erfolgen hat, wie es § 25 Abs. 1 BDSG näher regelt.

Tabellarisch zusammengefasst ergibt sich Folgendes:

§ 25 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1, 2 (Beanstandungsrecht)	Art. 58 Abs. 2 lit. b (ex Art. 53 Abs. 1b lit. b)	Modifizieren; ergänzen	Die DSGVO geht schon in Art. 58 Abs. 2 lit. b (ex Art. 53 Abs. 1b lit. b) weiter, sieht aber vor allem eine ganze Reihe weiterer Befugnisse für die Aufsichtsbehörde vor. Diese dürfen entweder wiederholend in das

[552] Immerhin regelt Art. 58 DSGVO die Befugnisse der Aufsichtsbehörde (von der Öffnungsklausel in Art. 58 Abs. 6 abgesehen) unmittelbar und grundsätzlich abschließend. Vgl. dazu auch S. 461 ff.

			BDSG wortlautgleich aufgenommen und ergänzen werden oder es erfolgt zunächst ein pauschaler Verweis auf die Befugnisse der DSGVO. Im Übrigen kann bei der wiederholenden und ergänzenden Normierung auch die Konkretisierung der Beanstandungsadressaten erfolgen.
Abs. 1 S. 2 Hs. 2, Abs. 3 (Aufforderung zur Stellungnahme)	Art. 58 Abs. 1 lit. a; Abs. 5 (ex Art. 53 Abs. 1 lit. a; Abs. 3)	Ggf. beibehalten	Die Notwendigkeit der Behörde, eine Stellungnahme abgeben zu müssen, geht wohl weiter als die bloße Pflicht zur Bereitstellung von Informationen in Art. 58 Abs. 1 lit. a DSGVO. Art. 58 Abs. 5 (ex Art. 53 Abs. 3) DSGVO sieht insoweit eine Öffnungsklausel für die Einräumung weiterer Befugnisse vor.

§ 26: Weitere Aufgaben der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

§ 26 BDSG regelt als weitere Aufgaben der BfDI die Anfertigung eines Tätigkeitsberichts, die Information der Öffentlichkeit sowie eine Beratungs- und Gutachtentätigkeit. Schließlich sieht sie eine allgemeine Kooperationspflicht mit anderen Datenschutzkontrollstellen vor. Damit korrespondiert die Bestimmung mit der Norm über Tätigkeitsberichte in Art. 59 (ex Art. 54) DSGVO, aber auch mit der allgemeinen Aufgabennorm der Datenschutz-Grundverordnung. So treten insbesondere ergänzend die allgemeinen Aufklärungsaufgaben nach Art. 57 Abs. 1 lit. b (ex Art. 52 Abs. 1 lit. aa) DSGVO hinzu. Dabei hat die Datenschutz-Grundverordnung jedoch teils abweichende Regelungen getroffen. Insoweit ist zu differenzieren:
§ 26 Abs. 1 S. 1 BDSG normiert zunächst die Pflicht, einen Tätigkeitsbericht vorzulegen, sieht hierzu jedoch – abweichend von Art. 59 S. 1 (ex Art. 54 S. 1) DSGVO – nicht einen Jahres-, sondern einen Zweijahreszeitraum vor. Insoweit kann die nationale Vorschrift gestrichen werden. Da aber das nationale Recht den Adressatenkreis nach Art. 59 S. 2 (ex Art. 54 S. 2) DSGVO näher bestimmen darf, kann das deutsche Recht die Frist wohl auch wiederholen, um insgesamt eine kohärente Regelung auch in Bezug auf die Bestimmung des Adressaten zu erreichen. Dabei sollte im BDSG deutlich gemacht werden, dass der Bericht gegenüber dem Bundestag erfolgt.

Das Recht zur Unterrichtung der Öffentlichkeit normiert die Datenschutz-Grundverordnung in Art. 57 Abs. 1 lit. b (ex Art. 52 Abs. 1 lit. aa) DSGVO und in Art. 58 Abs. 3 lit. b (ex Art. 53 Abs. 1c lit. aa) DSGVO umfassend, so dass die Regelung in § 26 Abs. 1 S. 2 BDSG sich überholt, aber wohl im Rahmen einer Kohärenz wahrenden wiederholenden Normierung an den Wortlaut der Datenschutz-Grundverordnung angepasst werden darf.

§ 26 Abs. 2 BDSG bestimmt, dass die BfDI für den in der Vorschrift näher bezeichneten Kreis auf Aufforderung Gutachten zu erstellen und Berichte zu erstatten sowie entsprechenden Hinweisen nachzugehen hat. Damit normiert das BDSG Handlungspflichten, die sich so nicht vergleichbar im Aufgabenkatalog des Art. 57 (ex Art. 52) DSGVO finden. Allerdings kann dies wohl noch als im Einklang mit der Öffnungsklausel innerhalb der Beratungsaufgabe nach Art. 57 Abs. 1 lit. c (ex Art. 53 Abs. 1 lit. ab) DSGVO („im Einklang mit dem Recht der Mitgliedstaaten“) und damit als zulässige Konkretisierung angesehen werden.

§ 26 Abs. 3 BDSG normiert eine weit gefasste Empfehlungs- und Beratungsaufgabe der BfDI. Eine Beratungsaufgabe sieht auch Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab) DSGVO vor, wenn auch mit leicht abweichender Formulierung. Hier ist zu erwägen, die Bestimmung dem Wortlaut des Unionsrechts anzupassen, wobei die Adressaten der Beratung angesichts der Öffnungsklausel („im Einklang mit dem einzelstaatlichen Recht“; „und andere Einrichtungen“) weit gefasst werden können. Jedenfalls sollte klargestellt werden, dass § 26 Abs. 3 BDSG als Beratungsrecht und nicht als Beratungspflicht zu verstehen ist.

Die Kooperationspflicht innerhalb Deutschlands und mit EU-Behörden gemäß § 26 Abs. 4 BDSG ist im Rahmen der Umsetzung der Kooperationspflichten nach der Datenschutz-Grundverordnung gemäß den Art. 60 ff. (ex Art. 54a ff.) DSGVO – dem Zusammenarbeitsverfahren – entsprechend an- und in dieses künftig umfassendere Regelungsgefüge einzupassen. Das Zusammenarbeitsverfahren der DSGVO (und damit auch das Konzept der federführenden Aufsichtsbehörde) findet nach Art. 55 Abs. 2 S. 2 DSGVO jedoch keine Anwendung, wenn sich eine Verarbeitung auf Art. 6 Abs. 1 UAbs. 1 lit. c und e DSGVO stützt. Dies dürfte das Gros der öffentlichen Verarbeitungstätigkeit betreffen. Ist in diesen Fällen trotzdem eine Zusammenarbeit gewünscht, sollte die Regelung (sicherheitshalber) aufrechterhalten werden.

§ 26 BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1 S. 1 (Tätigkeitsbericht)	Art. 59 (ex Art. 54)	Modifizieren	Die Frist und das Parlament als Adressat benennt die DSGVO selbst. Es besteht jedoch eine obligatorische Öffnungsklausel für den Adressaten. Hier ist eine Klarstellung im BDSG indiziert. Jedenfalls ist eine Anpassung an die Jahresfrist erforderlich.
Abs. 1 S. 2 (Information der Öffentlichkeit)	Art. 57 Abs. 1 lit. b (ex Art. 52 Abs. 1 lit. aa); Art. 58 Abs. 3 lit. b (ex Art. 53 Abs. 1c lit. aa)	Modifizieren	Anpassung an Wortlaut der Art. 57 Abs. 1 lit. b (ex Art. 52 Abs. 1 lit. aa); Art. 58 Abs. 3 lit. b (ex Art. 53 Abs. 1c lit. aa) DSGVO.
Abs. 2 (Gutachten; Sonderberichte)	Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab)	Ggf. beibehalten	Wohl noch von der Öffnungsklausel der Beratungsaufgabe gemäß Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab) DSGVO gedeckt.
Abs. 3 (Empfehlung und Beratung)	Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab)	Beibehalten; modifizieren	Eine Beratungsaufgabe sieht auch Art. 57 Abs. 1 lit. c (ex Art. 52 Abs. 1 lit. ab) DSGVO vor, wenn auch mit leicht abweichender Formulierung. Hier ist zu erwägen, die Bestimmung dem Wortlaut des Unionsrecht anzupassen, wobei die Adressaten der Beratung angesichts der Öffnungsklausel („im Einklang mit dem einzelstaatlichen Recht“; „und andere Einrichtungen“) weit gefasst werden können.
Abs. 4 (Zusammenarbeit mit anderen Datenschutzkon-	(Art. 60 ff. [ex Art. 54a ff.])	Ggf. aufrechterhalten; regeln im Zusammenhang mit Normierung	Aufrechterhaltung sinnvoll, für Bereiche in denen nach Art. 55 Abs. 2 DSGVO das Konzept der federführenden Aufsichtsbehörde und damit auch das Verfahren der Zusammenarbeit (Art. 60 ff. DSGVO) keine Anwendung findet.

trollstellen)		der Zusammenarbeit	

§§ 27 – 32: Rechtsgrundlagen der Datenverarbeitung durch nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen

Während sich für öffentliche Stellen wegen der in Art. 6 Abs. 1 UAbs. 1 lit. c und e, Abs. 2a, Abs. 3 DSGVO enthaltenen Öffnung große Handlungsspielräume für den nationalen Gesetzgeber eröffnen, der auch eine Aufrechterhaltung der bestehenden Normen zu weiten Teilen möglich macht, sieht die Datenschutz-Grundverordnung für den nicht-öffentlichen Bereich keine entsprechende weitgehende Öffnungsklausel vor. Dies führt dazu, dass Zulässigkeitstatbestände im nicht-öffentlichen Bereich sich zukünftig europarechtlich weitgehend einheitlich aus der Datenschutz-Grundverordnung ergeben werden, jedenfalls vorbehaltlich nationaler Regelungen über rechtliche Verpflichtungen i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO. Für Zweckänderungen hingegen findet sich auch für den nicht-öffentlichen Bereich eine Öffnungsklausel in Art. 6 Abs. 4 (ex Abs. 3a) DSGVO[553] i. V. m. Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO, insbesondere (bei weiter Interpretation) durch Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 lit. f Alt. 2) DSGVO. Hier können nicht nur Bestimmungen, die den zweckverändernden Umgang mit personenbezogenen Daten regeln, aufrechterhalten werden; die Öffnungsklausel ermöglicht mitunter womöglich auch eine Modifikation bestehender Normen dahin gehend, dass diese nur noch Zweckänderungen regeln und würde auch eine Neuschaffung solcher Normen ermöglichen, die den zweckverändernden Datenumgang in den Grenzen des Art. 6 Abs. 4 (ex Art. 6 Abs. 3a) i. V. m. Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO regeln.

[553] Zu den – im Einzelnen unklaren – Grenzen dieser Öffnungsklausel oben unter S. 43.

§ 27: Anwendungsbereich

§ 27 BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Insgesamt	Art. 4 Nr. 7 (ex Art. 4 Nr. 5 DSGVO)	Beibehalten; Streichen möglich, sofern Aufgabe der überkommenen Unterscheidung von öffentlichen und nicht-öffentlichen Stellen	Die Unterscheidung von öffentlichen und nicht-öffentlichen Stellen ist in der DSGVO zwar nicht angelegt, wegen Art. 4 Nr. 7 (ex Art. 4 Nr. 5 DSGVO) DSGVO möglich.

§ 28: Datenerhebung und -speicherung für eigene Geschäftszwecke

a. Abs. 1

§ 28 Abs. 1 BDSG regelt die Zulässigkeit der Datenerhebung und-speicherung für eigene Geschäftszwecke. Für § 28 Abs. 1 BDSG findet sich keine Öffnungsklausel in der Datenschutz-Grundverordnung, die ein Aufrechterhaltung ermöglichen würde. Dies ist nur möglich, soweit die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO) oder für die Wahrnehmung einer Aufgabe im öffentlichen Interesse bzw. für die Ausübung hoheitlicher Gewalt (Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO) erforderlich ist, wie sich aus Art. 6 Abs. 2 (ex Abs. 2a), 3 DSGVO ergibt. Dies ist hier nicht der Fall. Entsprechende Zulässigkeitstatbestände ergeben sich allerdings ohnehin direkt aus Art. 6 Abs. 1 DSGVO, so dass eine Aufrechterhaltung auch nicht notwendig ist.

b. Abs. 2

§ 28 Abs. 2 BDSG regelt die Zulässigkeit der zweckändernden Übermittlung und Nutzung. Für inkompatible Zwecke ergibt sich eine Öffnungsklausel direkt aus Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. a bis j (ex Art. 21 Abs. 1 lit. aa bis g) DSGVO. Zweckänderungen für *kompatible* Zwecke benötigen nach der normativen Wertung der Datenschutz-

Grundverordnung keine eigene Rechtsgrundlage. Mitgliedstaaten können diese auch nur aus dem Zusammenspiel von Art. 6 Abs. 4 (ex Abs. 3a) mit Art. 6 Abs. 2 (ex Abs. 2a), 3 DSGVO konkretisieren, also nur für Rechtsgrundlagen für Verarbeitungen gem. Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO. Dies wäre aber ohnehin nur für eine *Einschränkung* der Zweckänderung für kompatible Zwecke interessant, da diese ohne eigene Rechtsgrundlage gem. Art. 6 Abs. 4 (ex Abs. 3a) DSGVO zulässig ist.[554] Die Zweckänderungen in § 28 Abs. 2 BDSG müssen also einem in Art. 23 Abs. 1 lit. a bis j (ex Art. 21 Abs. 1 lit. aa bis g) DSGVO niedergelegten Ziel dienen, um aufrechterhalten werden zu können, da § 28 BDSG weder rechtliche Verpflichtungen i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. c DSGVO noch die Wahrnehmung von Aufgaben im öffentlichen Interesse i. S. d. Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO regelt. In diesem Sinne ist es jedoch denkbar, § 28 Abs. 2 Nr. 1 i. V. m. § 28 Abs. 1 Nr. 2 BDSG in der Weise modifiziert aufrechtzuerhalten, dass die Zweckänderung dem *Schutz* der Rechte und Freiheiten der verantwortlichen Stelle und nicht lediglich ihrer berechtigten Interessen dient. Allerdings gilt Art. 23 Abs. 1 lit. i DSGVO nur für „andere". Dabei meint „Freiheiten anderer Personen" womöglich nur die Freiheiten mittelbar betroffener Dritter, nicht aber des Verantwortlichen selbst. Lit. i bündelt nach diesem Verständnis die Schutzrechte derjenigen, die von einer Verarbeitung betroffen sind. Denkbar ist, dass jene Norm nicht auch die gegenläufigen Interessen der Verarbeiter als Schutzgut im gleichen Tatbestand im Auge hat. Dies wäre dann Aufgabe des Art. 23 Abs. 1 lit. j DSGVO: Er schützt die Rechte des Verarbeiters insoweit, als er auf die Verarbeitung für die Durchsetzung zivilrechtlicher Ansprüche angewiesen ist. Daraus lässt sich zwar womöglich im Umkehrschluss schließen, dass seine Rechte im Übrigen keinen Schutz genießen, der eine Ausnahme nach Art. 23 DSGVO rechtfertigt. Dies wäre allerdings vor dem Hintergrund der Grundrechtspositionen der verantwortlichen Stelle ein sehr enges Verständnis. Je nachdem, ob man die Öffnungsklausel vor dem Hintergrund eines umfassenden Grundrechtsschutzes auch des Verantwortlichen weit versteht, ist eine entsprechende Aufrechterhaltung der Norm möglich.

[554] Vgl. ausführlich S. 38 sowie S. 382.

§ 28 Abs. 2 Nr. 2 lit. a BDSG kann aufgrund von Art. 6 Abs. 4 (ex Abs. 3a) DSGVO i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2 DSGVO), und § 28 Abs. 2 Nr. 2 lit. b BDSG aufgrund von Art. 6 Abs. 4 (ex Abs. 3a) DSGVO i. V. m. Art. 23 Abs. 1 lit. a (ex Art. 21 Abs. 1 lit. aa) (nationale Sicherheit), lit. c (ex lit. a) (öffentliche Sicherheit), lit. d (ex lit. b) (Strafverfolgung) DSGVO aufrechterhalten werden. § 28 Abs. 2 Nr. 3 BDSG kann nicht nach Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. a bis j (ex Art. 21 Abs. 1 lit. aa bis g) DSGVO aufrechterhalten werden, da er hiervon nicht gedeckt ist. Art. 5 Abs. 1 lit. b DSGVO geht jedoch im Rahmen einer Fiktion davon aus, dass eine entsprechende Zweckänderung immer zweckkompatibel ist. Daher besteht hier auch kein Bedürfnis, die Vorschrift aufrechtzuerhalten, da sich eine zulässige zweckkompatible Zweckänderung aus der Datenschutz-Grundverordnung selbst ergibt. Inwieweit die Vorschrift nach der Öffnungsklausel des Art. 85 Abs. 2 DSGVO zulässt, der Abweichungen für wissenschaftliche Zwecke zum Schutz der Informationsfreiheit, enthält, ist sehr fraglich. Denn Abs. 2 Nr. 3 dient nicht per se der Informationsfreiheit, diese greift vielmehr nur begrenzt, zum Beispiel bei Daten aus öffentlich zugänglichen Quellen.

c. Abs. 3

§ 28 Abs. 3 BDSG stellt eine zu § 28 Abs. 1 BDSG abschließende, spezielle Zulässigkeitsnorm für die Verarbeitung und Nutzung personenbezogener Daten für Zwecke des Adresshandels und der Werbung dar.[555] Als *Zulässigkeitstatbestand* kann § 28 Abs. 3 BDSG mangels Öffnungsklausel in Art. 6 DSGVO nicht aufrechterhalten werden.[556] Für Zweckänderungen hingegen können gegebenenfalls die in § 28 Abs. 3 BDSG genannten Bestimmungen aufrechterhalten werden. So könnte die Norm dann aufrechterhalten werden, wenn sie dahin gehend modifiziert wird, dass sie nur zweckändernde Verarbeitungen und Nutzungen für Zwecke des Adresshandels und der Werbung regelt. Die entsprechende Öffnungsklausel wäre hier Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2)

[555] *Wolff*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 28 BDSG, Rn. 112.
[556] Vgl. oben §§ 27 ff. BDSG.

DSGVO – zum Schutz der Rechte und Freiheiten der verantwortlichen Stelle, insbesondere ihrer Berufsfreiheit. Voraussetzung wäre allerdings, dass trotz der angeführten Bedenken die Öffnungsklausel so verstanden wird, dass sie auch die Verantwortliche Stelle als „andere Person“ ansieht.

d. Abs. 3a: Bestätigung des Einwilligungsinhalts

§ 28 Abs. 3a BDSG erfordert eine Bestätigung des Einwilligungsinhalts unter bestimmten Voraussetzungen und bezieht sich damit auf § 4 Abs. 1 i. V. m. § 4a BDSG. Allerdings ist die Zulässigkeit der Datenverarbeitung aufgrund einer Einwilligung des Betroffenen in Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO ohne Öffnungsklausel normiert; die Voraussetzungen der Einwilligung sind in Art. 7 DSGVO normiert. Der Verweis auf die Einwilligung in § 4 Abs. 1 BDSG kann nur aus Gründen der Klarstellung aufrechterhalten werden.[557] Damit ist eine gesonderte Regelung hier nicht möglich, aber auch nicht nötig, da sie keinen Fall mehr betrifft, der im BDSG geregelt werden kann.

e. Abs. 3b: Kopplungsverbot

§ 28 Abs. 3b BDSG normiert ein Kopplungsverbot für Zwecke der Werbung und des Adresshandels. Das Kopplungsverbot ist in der Datenschutz-Grundverordnung allgemein in Art. 7 Abs. 4 DSGVO ohne Öffnungsklausel normiert. Der Absatz kann daher nicht aufrechterhalten werden; die Regelung in der Datenschutz-Grundverordnung erhält dabei das Datenschutzniveau aufrecht.

f. Abs. 4: Widerspruchsrecht

§ 28 Abs. 4 BDSG regelt Widerspruchsrechte des Betroffenen für die Verarbeitung zu Zwecken der Werbung oder der Markt- oder Meinungsforschung. Widerspruchsrechte sind in Art. 21 (ex Art. 19) DSGVO geregelt, für Zwecke der Werbung explizit in Art. 21 Abs. 2, 3 (ex Art. 19 Abs. 2, 2a) DSGVO. Eine Aufrechterhaltung ist deswegen nicht nötig; es gilt aber das zu § 35 Abs. 5 BDSG ausführlicher Dargelegte, d. h. im Rahmen der Öffnungsklausel des Art. 23 Abs. 2 lit. f Alt. 2 (ex Art. 21 Abs. 2 lit. f Alt. 2) DSGVO ist hier

[557] Vgl. oben § 4 Abs. 1 BDSG.

unter Wahrung der Anforderungen des Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO gegebenenfalls auch eine Aufrechterhaltung möglich, wenn auch wenig sinnvoll.

g. Abs. 5

§ 28 Abs. 5 S. 1 BDSG normiert den Zweckbindungsgrundsatz für die Übermittlung an Dritte, nimmt also auch Bezug auf die Möglichkeit der Übermittlung für andere Zwecke nach § 28 Abs. 2 BDSG. Art. 5 Abs. 1 lit. b DSGVO normiert den allgemeinen Zweckbindungsgrundsatz, eine weitere Normierung ist deswegen nicht nötig und von der Öffnungsklausel des Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO auch nicht vorgesehen.
Man kann jedoch davon ausgehen, dass eine Wiederholung von Art. 5 Abs. 1 lit. b DSGVO nicht gegen das Wiederholungsgebot verstößt, da die Aufrechterhaltung des Zweckbindungsgrundsatzes in § 28 Abs. 5 BDSG Klarheit für den Normadressaten schafft. § 28 Abs. 5 S. 2 BDSG, der wiederum Fälle der zulässigen Zweckänderung normiert, kann aufrechterhalten werden, sofern § 28 Abs. 2 BDSG bzw. § 14 Abs. 2 BDSG, auf die § 28 Abs. 5 S. 2 BDSG verweist, aufrechterhalten werden. Da § 28 Abs. 3 BDSG in seiner bisher bestehenden Form nicht aufrechterhalten werden kann, geht der Verweis in § 28 Abs. 5 S. 2 auf § 28 Abs. 3 BDSG fehl.

h. Abs. 6 Hs. 1

§ 28 Abs. 6 Hs. 1 BDSG sieht die Zulässigkeit der Erhebung besonderer Arten personenbezogener Daten vor, soweit der Betroffene eingewilligt hat. Er entspricht im Wesentlichen Art. 9 Abs. 2 lit. a DSGVO. Allerdings setzt § 28 Abs. 6 Hs. 1 BDSG eine Einwilligung nach § 4a Abs. 3 BDSG voraus. Geht man davon aus, dass die Öffnungsklausel angesichts der weit gehenden mitgliedstaatlichen Gestaltungsbefugnis als Minus auch das Aufstellen zusätzlicher Anforderungen an die Einwilligung abdeckt[558] und dass § 4a Abs. 3 BDSG weiterreichende Anforderungen aufstellt als Art. 4 Nr. 11 (ex Art. 4

[558] Vgl. hierzu ausführlich S. 49.

Nr. 8) DSGVO[559], kann § 28 Abs. 6 BDSG zulässigerweise aufrechterhalten werden. Die Sonderregelung kann jedoch auch gestrichen werden, was ausschließlich einer rechtspolitischen Bewertung unterliegt.

i. Abs. 6 Nr. 1

§ 28 Abs. 6 Nr. 1 BDSG kann gestrichen werden, da dieser Art. 9 Abs. 2 lit. c DSGVO entspricht und dort keine Öffnungsklausel für die Mitgliedstaaten enthalten ist.

j. Abs. 6 Nr. 2

Dito.

k. Abs. 6 Nr. 3

Dito.

l. Abs. 6 Nr. 4

§ 28 Abs. 6 Nr. 4 BDSG regelt die Zulässigkeit der Erhebung besonderer Arten personenbezogener Daten zu Zwecken der wissenschaftlichen Forschung. Dieser Fall ist in Art. 9 Abs. 2 lit. j (ex lit. i) DSGVO geregelt. Art. 9 Abs. 2 lit. j (ex lit. i) DSGVO verlangt jedoch neben der Wahrung des Verhältnismäßigkeitsgrundsatzes und des Wesensgehalts des Rechts auf Datenschutz, dass das mitgliedstaatliche Recht „angemessene und spezifische Maßnahmen“ vorsehen muss, um jene Rechte zu schützen. Insoweit kann auf die Ausführungen zu § 13 Abs. 2 Nr. 1 Alt. 1 BDSG[560] verwiesen werden. Damit gilt hier, dass § 28 Abs. 6 Nr. 4 BDSG in seiner bestehenden Form wohl auch ohne Modifikationen aufrechterhalten werden kann. Inwieweit daneben die Öffnungsklausel des Art. 85 Abs. 2 DSGVO greift, erscheint fraglich.

[559] Vgl. hierzu ausführlich S. 49.
[560] Vgl. oben § 13 Abs. 2.

m. Abs. 7

§ 28 Abs. 7 BDSG bestimmt die Zulässigkeit der Erhebung besonderer Arten personenbezogener Daten u. a. zum Zweck der Gesundheitsvorsorge und medizinischen Diagnostik, sofern die Verarbeitung durch ärztliches Personal oder sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, erfolgt. Die Voraussetzungen des § 28 Abs. 2 S. 1 BDSG decken sich somit mit den Voraussetzungen des Art. 9 Abs. 2 lit. h i. V. m. Art. 9 Abs. 3 (ex Abs. 4) DSGVO, wobei hier eine mitgliedstaatliche Regelung erforderlich ist, um den jetzigen Zustand zu wahren, da Art. 9 Abs. 2 lit. h i. V. m. Art. 9 Abs. 3 (ex Abs. 4) DSGVO insoweit als Öffnungsklausel greift. § 28 Abs. 7 S. 3 BDSG erfüllt in der jetzigen Formulierung nicht die Anforderungen an die für die Verarbeitung zuständigen Personen. Somit kann § 28 Abs. 7 S. 3 BDSG nur dahin gehend modifiziert aufrechterhalten werden, dass eine Geheimhaltungspflicht auch insoweit vorgegeben wird.

n. Abs. 8

§ 28 Abs. 8 BDSG regelt Fälle der Zulässigkeit der Verarbeitung besonderer Arten personenbezogener Daten für andere Zwecke als eigene Geschäftszwecke. Eine Zweckänderung der Verarbeitung bei besonderen Arten personenbezogener Daten regelt die Datenschutz-Grundverordnung nicht gesondert. Ein Rückgriff auf Art. 6 Abs. 4 (ex Abs. 3a) DSGVO ist nicht möglich, da Art. 6 DSGVO nur für die Verarbeitung personenbezogener Daten gilt und Art. 9 DSGVO für die Verarbeitung besonderer Arten personenbezogener Daten hierzu speziell ist. Art. 9 Abs. 1 DSGVO stellt klar, dass eine Verarbeitung personenbezogener Daten grundsätzlich verboten ist. Dies schließt aber auch die zweckändernde Verarbeitung jener Daten mit ein. Ausnahmen bestehen nur im Rahmen von Art. 9 Abs. 2 DSGVO. Die Zweckänderung ist bei der Verarbeitung personenbezogener Daten also dann möglich, wenn sie selbst eine Rechtsgrundlage in Art. 9 Abs. 2 DSGVO bzw. den aufgrund von Öffnungsklauseln in Art. 9 Abs. 2 DSGVO aufrechterhaltenen oder geschaffenen nationalen Normen findet.
Da Art. 9 Abs. 2 DSGVO eine Zweckbegrenzung für eigene Geschäftszwecke, wie § 28 BDSG sie indiziert, nicht vorsieht, könnte eine Datenverarbeitung besonderer Arten personenbezogener Daten auch durch nicht-öffentliche

Stellen in einer eigenen Rechtsgrundlage geregelt werden, die nicht auf die Verarbeitung für eigene Geschäftszwecke begrenzt ist, soweit Art. 9 DSGVO dahin gehende Öffnungsklauseln enthält. Daher könnte man auch erwägen, die Verarbeitung besonderer Arten personenbezogener Daten in einer eigenen Rechtsgrundlage und ohne den Verweis auf die Zweckänderung zu regeln, was innerhalb des von den Öffnungsklauseln in Art. 9 DSGVO markierten Spielraums möglich wäre.

o. Abs. 9

§ 28 Abs. 9 BDSG kann nicht aufrechterhalten werden, da er identisch mit Art. 9 Abs. 2 lit. d DSGVO ist, der keine Öffnungsklausel enthält.

§ 28 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	Art. 6 Abs. 1 UAbs. 1 lit. b, f	Streichen	Von keiner Öffnungsklausel gedeckt, Zulässigkeitstatbestände in Art. 6 Abs. 1 DSGVO geregelt.
Abs. 2 Nr. 1 i. V. m. Abs. 1 S. 1 Nr. 2	Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i (ex Art. 21 Abs. 1 lit. f)	Modifikation	Verweis auf § 28 Abs. 1 BDSG muss geändert werden, da Streichung des Abs. 1 indiziert; Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) DSGVO setzt voraus, dass die Zweckänderung dem *Schutz* der Rechte und Freiheiten anderer Personen dient, nicht lediglich berechtigter Interessen.
Abs. 2 Nr. 1 i. V. m. Abs. 1 S. 1 Nr. 1, 3	-	Streichen	Von keinem der in Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO niedergelegten Ziele gedeckt.
Abs. 2 Nr. 2	Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. a, c, e, I (ex Art. 21 Abs. 1 lit. aa, a, c, f)	Beibehalten	Aufrechterhaltung von der Öffnungsklausel gedeckt.

Abs. 2 Nr. 3	Art. 5 Abs. 1 lit. Hs. 2	Streichen	Von keinem der in Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO niedergelegten Ziele gedeckt. Das Unionsrecht erfasst diesen Fall unmittelbar in Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO (ohne Öffnungsklausel). Da aber zweckkompatible Zweckänderung nach Art. 5 Abs. 1 lit. b DSGVO auch kein Regelungsbedürfnis. Inwieweit die Öffnungsklausel des Art. 85 Abs. 2 DSGVO greift, ist fraglich.
Abs. 3	Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2)	Modifikation	Die Norm kann als Zulässigkeitstatbestand nicht aufrechterhalten werden; als Norm, die eindeutig eine Zweckveränderung normiert, wäre sie von Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) gedeckt.
Abs. 3a	Art. 6 Abs. 1 UAbs. 1 lit. a	Streichen	Von keiner Öffnungsklausel gedeckt; in Art. 6 Abs. 1 UAbs. 1 lit. a und 7 DSGVO geregelt.
Abs. 3b	Art. 7 Abs. 4	Streichen	Von keiner Öffnungsklausel gedeckt; in Art. 7 Abs. 4 DSGVO geregelt.
Abs. 4	Art. 21 Abs. 2, 3 (ex Art. 19 Abs. 2, 2a); Öffnungsklausel: Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) DSGVO	Streichen; ggf. Beibehalten	In Art. 21 Abs. 2, 3 (ex Art. 19 Abs. 2, 2a) DSGVO geregelt. Die Öffnungsklausel in Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) ermöglicht aber auch eine Aufrechterhaltung, die aber nicht zweckmäßig ist; vgl. die Ausführungen zu § 35 Abs. 5 BDSG.
Abs. 5 S. 1	Art. 5 Abs. 1 lit. b	Ggf. Beibehalten; Streichen	Zweckbindungsgrundsatz in Art. 5 Abs. 1 lit. b DSGVO normiert; Aufrechterhaltung aus Gründen der Klarheit ggf. auch ohne Verstoß gegen das Wiederholungsverbot möglich.
Abs. 5 S. 2	-	Beibehalten, soweit Bei-	Soweit die Normen, auf die § 28 Abs. 5 S. 2 BDSG verweist, aufrechterhalten werden,

		behalten der Normen, auf die verwiesen wird	kann die Norm auch aufrechterhalten werden.
Abs. 6 Hs. 1	Art. 9 Abs. 2 lit. a	Beibehalten; Streichen möglich	Aufrechterhaltung möglich, sofern man davon ausgeht, dass die Öffnungsklausel angesichts der weit gehenden mitgliedstaatlichen Gestaltungsbefugnis als Minus auch das Aufstellen zusätzlicher Anforderungen an die Einwilligung abdeckt, und dass § 4 Abs. 3a BDSG weiterreichende Anforderungen aufstellt als Art. 4 Nr. 11 (ex Art. 4 Nr. 8) DSGVO.
Abs. 6 Nr. 1	Art. 9 Abs. 2 lit. c	Streichen	Von keiner Öffnungsklausel gedeckt; im Übrigen muss durch die Übereinstimmung die Norm auch nicht beibehalten werden, um das bestehende Datenschutzniveau zu erhalten.
Abs. 6 Nr. 2	Art. 9 Abs. 2 lit. e	Streichen	Dito
Abs. 6 Nr. 3	Art. 9 Abs. 2 lit. f	Streichen	Dito
Abs. 6 Nr. 4	Art. 9 Abs. 2 lit. j (ex lit. i)	Beibehalten wohl auch ohne Modifikation in Form einer Erweiterung um angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen des Betroffenen	Anforderungen des spezifischen Charakters der Maßnahme unklar hinsichtlich einer Umsetzungsnotwendigkeit im Gesetz selbst.
Abs. 7 S. 1, 2	Art. 9 Abs. 2 lit. h, Abs. 3 (ex Abs. 4)	Beibehalten	Von der Öffnungsklausel des Art. 9 Abs. 2 lit. h DSGVO gedeckt; erfüllt die Anforderungen des Art. 9 Abs. 3 (ex Abs. 4) DSGVO.
Abs. 7 S. 3	Art. 9 Abs. 2 lit. h	Modifikation	Erfüllt die Anforderungen des Art. 9 Abs. 3 (ex Abs. 4) DSGVO nicht und ist um eine Geheimhaltungsverpflichtung zu ergänzen.
Abs. 8	Art. 9 Abs. 2	Modifikati-	Aufrechterhaltung nur, sofern die Normen,

		on; Regelung in eigener Rechtsgrundlage	auf die § 28 Abs. 8 BDSG verweist, aufrechterhalten werden. Eine Regelung in einer eigenen Rechtsgrundlage wäre sinnvoll, um Regelungslücken zu vermeiden, und das Erfordernis einer eigenen Rechtsgrundlage für zweckändernde Veränderungen, Nutzungen oder Speicherungen besonderer Arten personenbezogener Daten klarzustellen.
Abs. 9	Art. 9 Abs. 2 lit. d	Streichen	Von keiner Öffnungsklausel gedeckt; in Art. 9 Abs. 2 lit. j (ex lit. i) DSGVO geregelt.

§ 28a: Datenübermittlung an Auskunfteien

§ 28a BDSG regelt die Zulässigkeit der Übermittlung an Auskunfteien. Gegenstand der Norm sind somit Daten, die bereits erhoben wurden. Die Datenschutz-Grundverordnung kennt keinen Zulässigkeitstatbestand, der speziell die Übermittlung an Auskunfteien abdeckt. Entscheidend ist vorliegend, ob die Übermittlung solcher Daten als inkompatible zweckverändernd eingestuft wird (dazu oben S. 41). Soweit dies der Fall ist, können die Mitgliedstaaten nur die Öffnungsklausel des Art. 6 Abs. 4 (ex Abs. 3a) DSGVO i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) DSGVO aktivieren, d. h. Regelungen erlassen, die eine zweckändernde Verarbeitung zulässt, sofern sie einem in Art. 23 (ex Art. 21 Abs. 1) DSGVO niedergelegten Ziel dient – gegebenenfalls etwa dem Schutz der Rechte und Freiheiten anderer Personen i. S. d. Art. 23 Abs. lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) DSGVO – und Art. 6 Abs. 4 (ex Abs. 3a) DSGVO diese Vorschrift erfasst (dazu oben S. 43). Im Übrigen bietet auch Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO (ebenso wie Art. 6 Abs. 4 DSGVO bei einer Einordnung als zweckkompatible Zweckänderung) einen Zulässigkeitstatbestand für solche Übermittlungen, deren Reichweite allerdings noch im Rahmen der Anwendung der Datenschutz-Grundverordnung zu klären sein wird. Eine Aufrechterhaltung ist damit nur dann erforderlich, wenn der Regelungsgegenstand nicht als zweckkompatible Weiterverarbeitung qualifiziert werden kann.

§ 28a BDSG	Korrespondierende Norm in der DSG-VO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1	Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 1)	Beibehalten möglich	Übermittlung an Auskunfteien gegebenenfalls zweckändernd; Öffnungsklausel des Art. 6 Abs. 4 (ex Abs. 3a) DSGVO fraglich; in Betracht kommt aber eine „implizite“ Öffnungsklausel aufgrund einer Regelungslücke.
Abs. 2	Dito	Dito	Dito
Abs. 3	Dito	Dito	Dito

§ 28b: Scoring

§ 28b hegt das das Scoring durch eine Sonderregelung rechtlich ein. Die Vorschrift beschränkt sich auf das vertragsbezogene Scoring im nicht-öffentlichen Bereich.[561] Scoring bezeichnet die Berechnung eines Wahrscheinlichkeitswertes für ein bestimmtes *zukünftiges* Verhalten des Betroffenen anhand zuvor erhobener Daten. Anwendungsbereiche sind vor allem das Kreditwesen, bestimmte Versicherungen, Versandhandel und Wohnraumvermietung. Scoring gehört zu den klassischen „Big Data“-Technologien. Von ihrer Anwendung können sensible Auswirkungen auf die Persönlichkeitsentfaltung ausgehen. Daher hat § 28b BDSG dessen Geschäftsmodell Grenzen gezogen.

§ 28b BDSG regelt die Zulässigkeit, Art und Umfang des Scoring-Verfahrens und dessen Datengrundlagen. Gegenstand ist die Nutzung *bereits erhobener und gespeicherter* Daten; die Zulässigkeit der Speicherung regeln § 29 (Übermittlung bei Auskunftei) und § 28 (Nutzung in allen sonstigen Fällen) BDSG. § 28b enthält dabei keine umfassende Verarbeitungsgrundlage, son-

[561] Erfasst sind nicht-öffentliche Stellen sowie teilweise öffentlich-rechtliche Unternehmen (vgl. § 27 Abs. 1 S. 1 Nr. 2 BDSG).

dern verweist hierfür auf das allgemeine Datenschutzrecht (*Nr. 2*).[562] Daneben regelt die Vorschrift allgemeine materielle sowie verfahrensbezogene Erfordernisse. *Nr. 1* verpflichtet zur Zugrundelegung eines validen, also wissenschaftlich anerkannten mathematisch-statistischen Verfahrens. *Nr. 3* enthält ein Verbot der Berechnung alleine auf der Grundlage von Anschriftendaten (hierunter fällt z. B. das sog. Geo-Scoring). *Nr. 4* regelt eine Unterrichtungs- und Dokumentationspflicht im Falle der Verwendung von Anschriftendaten.

Die Datenschutz-Grundverordnung hält keine gesonderte Parallelvorschrift zum Scoring vor. Das indiziert auf den ersten Blick die Unzulässigkeit einer nationalstaatlichen Sonderregelung: Die nationalstaatliche Privilegierung des Scorings bzw. seine Beschränkung könnte namentlich womöglich das unionsrechtliche Schutzniveau untergraben. Das Scoring steht in einer unmittelbaren sachlichen Nähe zu dem grundsätzlich verbotenen Profiling (Art. 22 [ex Art. 20] DSGVO). Die Datenschutz-Grundverordnung enthält allerdings insoweit in Art. 22 Abs. 2 lit. b (ex Art. 20 Abs. 1a lit. b) DSGVO eine Öffnungsklausel. Die Vorschrift ermöglicht den Mitgliedstaaten, vom Verbot einer automatisierten Generierung von Einzelentscheidungen Ausnahmen vorzusehen, wenn geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person vorgesehen sind.[563]

Die Öffnungsklausel ist freilich nicht unmittelbar einschlägig. Scoring trifft nämlich nicht unbedingt eine ausschließlich automatisierte Entscheidung. Es bereitet eine Entscheidung vielmehr vor („zum Zwecke der Entscheidung", § 28b BDSG). § 28b BDSG geht davon aus, dass dem Scoring typischerweise eine menschliche Entscheidung folgt, die Entscheidung sich also nicht alleine auf eine automatisierte Verarbeitung stützt, sondern eine Person noch einen (nicht nur rein formalen) Entscheidungsspielraum ausübt. Ein verbleibender mitgliedstaatlicher Regelungsspielraum lässt sich dann allenfalls unter Rückgriff auf einen Erst-recht-Schluss herleiten: Wenn die Mitgliedstaaten auto-

[562] *von Lewinski*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 28b BDSG, Überblick vor Rn. 1.

[563] Eine Aufrechterhaltung des § 28b BDSG daher für zulässig haltend *Ehmann*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 28b, Rn. 79; s. o. zu § 28a BDSG.

matisierte Einzelentscheidungen zulassen dürfen, dann womöglich erst recht auch Entscheidungen, denen eine Einzelentscheidung vorausgeht.[564] Eine solche Weite der Interpretation würde aber das System des einheitlichen Datenschutzniveaus und der Öffnungsklauseln im Unionsrecht unterwandern. Die Öffnungsklauseln sind auf spezifische Kontexte bezogen und darauf beschränkt. Insbesondere setzen sie voraus, dass der Tatbestand einer Rechte und Pflichten regelnden Norm der Datenschutz-Grundverordnung berührt ist. Im Falle des Art. 22 DSGVO ist das aber nur bei weiter Auslegung des Abs. 1 der Vorschrift gegeben, nämlich dann, wenn man unter sie auch solche Konstellationen subsumiert bei denen die Entscheidung ganz überwiegend und nicht nur ausschließlich auf einer automatisierten Verarbeitung beruht.

Eine mitgliedstaatliche Regelungsbefugnis für die Rechtmäßigkeit der Scoring-Verarbeitung ergibt sich aber womöglich aus Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO. Die Ermittlung der Kreditwürdigkeit kann einem überwiegenden berechtigten Interesse der Kreditwirtschaft und der entsprechenden Institute entsprechen. Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. i (ex Art. 21 Abs. 1 lit. f) DSGVO lässt prima facie auch die mit einem Scoring typischerweise verbundene Zweckänderung der erhobenen Daten zu. Denn die Zweckänderung dient dem Schutz der wirtschaftlichen Freiheiten betroffener Kreditinstitute. Allerdings ist unklar, ob Art. 23 Abs. 1 lit. i gegebenenfalls nicht die Freiheiten des Verantwortlichen, sondern sonstiger von einer Verarbeitung betroffener Personen. Jedenfalls regelt § 28b BDSG (anders als § 28a BDSG) nicht selbst die Zulässigkeit der Zweckänderung, sondern den Mechanismus einer Aggregation von Daten, um daraus eine Entscheidungsgrundlage zu entwickeln.

In Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO eröffnet die Datenschutz-Grundverordnung den Mitgliedstaaten nicht ausdrücklich einen Regelungsspielraum. Dies tut sie vielmehr nur für die Buchstaben lit. c und lit. e. Das legt einen Umkehrschluss nahe: Dürfen die Mitgliedstaaten nur für diese Regelungen „spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung beibehalten oder einführen“, gilt das für die anderen Tatbestände des Art. 6 Abs. 1 gerade nicht. Ohne Konkretisierung bleibt Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO zugleich allerdings nahezu voll-

[564] In diesem Sinne auch *Taeger* (Fn. 106), 95.

zugsunfähig. Die Regelung bewegt sich auf einem Abstraktionsniveau, das nicht in allen Fällen Ableitungen mit klaren Handlungsanleitungen für die Kollisionslage zwischen Persönlichkeitsschutz und wirtschaftlichen Interessen ermöglicht. Das streitet dafür, den Mitgliedstaaten auch im Interesse einer Rechtssicherheit für die betroffenen Akteure einen konkretisierenden Spielraum zuzugestehen. Der Mitgliedstaat übernähme dann die Aufgabe, eine normative Auskleidung vorzunehmen, die dem Normanwender sonst versagt bliebe. Die verbindliche Auslegung ihres normativen Inhalts weist die Datenschutz-Grundverordnung im Gefolge ihrer unmittelbaren Anwendbarkeit (kraft der Ermächtigung der Mitgliedstaaten) freilich grundsätzlich dem EuGH, nicht dem nationalen Gesetzgeber zu. Über einen eigenen Regelungsspielraum verfügen die Mitgliedstaaten nur noch, soweit die Verordnung ihnen diesen ausdrücklich zugesteht. Die Mitgliedstaaten dürfen Regelungen treffen, um die Kohärenz zu wahren und Rechtsvorschriften verständlicher zu machen – allerdings nur, „wenn in dieser Verordnung Präzisierungen oder Einschränkungen ihrer Vorschriften durch das Recht der Mitgliedstaaten vorgesehen sind“ (EG 8 [ex EG 6a] DSGVO). Letzteres trifft auf Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO nicht zu. Präzisierungen sind den Mitgliedstaaten dann grundsätzlich verwehrt.

Von der Beantwortung der Frage, ob den Mitgliedstaaten die Befugnis zusteht, Regelungslücken, welche die Verordnung hinterlässt, im Interesse der Rechtssicherheit auch dann zu schließen, wenn die Verordnung nicht ausdrücklich eine Öffnungsklausel ausweist, zu schließen, hängt ab, ob § 28b BDSG aufrechterhalten bleiben kann. Die Frage ist im Grundsatz zu verneinen, bleibt aber letztlich der Klärung durch den EuGH vorbehalten.

Gerechtfertigt ist eine Ausnahme von den Betroffenenrechten der Art. 12 – 22 (ex Art. 12 – 20) DSGVO (Art. 23 Abs. 1 lit. i [ex Art. 21 Abs. 1 lit. f]). Das gilt insbesondere für die Pflicht, aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer Verarbeitung im Wege automatisierter Entscheidungsfindung zu erhalten (Art. 14 Abs. 2 lit. g DSGVO). Art. 23 Abs. 1 lit. i und j DSGVO gestatten davon Ausnahmen. Im Kontext der Regelung einer solchen Ausnahme darf der Gesetzgeber im Interesse einer in sich konsistenten und verständlichen Regelung (vgl. EG 8 [ex EG 6a] DSGVO) Wiederholungen des Unionsrechts vornehmen. Ob der deutsche Gesetzgeber von der Pflicht des Art. 14

Abs. 2 lit. g DSGVO aber wirklich entbinden sollte und ob davon dann auch eine – Rechtssicherheit schaffende – Vollregelung getragen werden kann, ist aber sehr zweifelhaft.
Die Regelung des § 28b darf der deutsche Gesetzgeber danach nur bei einem sehr großzügigen Verständnis der Öffnungsklauseln des Art. 22 Abs. 2 lit. b (insbesondere einem weiten Verständnis des Begriffs „Entscheidung"), Art. 6 Abs. 4 DSGVO und Art. 23 Abs. 1 lit. i DSGVO sowie des unionsrechtlichen Wiederholungsverbots aufrechterhalten.

§ 28b BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Nr. 1 (Scoring unter Zugrundelegung eines validen Verfahrens)	Keine spezielle Regelung des Scorings. Anknüpfungspunkte aber in Art. 6 Abs. 1 UAbs. 1 lit. f, Abs. 4, Art. 14 Abs. 2 lit. g, Art. 15 Abs. 1 lit. h; Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2), Art. 22 (ex Art. 20) sowie EG 71 (ex EG 58).	Beibehalten eher nicht möglich, wohl streichen; u. U. empfiehlt sich ein Verweis auf den (ggf. modifizierten) § 6a BDSG (siehe ebenda) und/oder Art. 22 DSGVO.	Für die Vorschrift besteht (ungeachtet ihrer rechtspolitischen Sinnhaftigkeit) wohl kein nationaler Aufrechterhaltungsspielraum. Insbesondere Art. 6 Abs. 1 UAbs. 1 lit. f DSGVO gesteht den Mitgliedstaaten keinen Konkretisierungsspielraum zu. Denkbar ist zwar ein Rekurs auf die Öffnungsklausel des Art. 22 Abs. 2 lit. b DSGVO (vgl. auch EG 71 UAbs. 1 S. 1). Sie erstreckt sich aber nur auf ausschließlich automatisierte Entscheidungen, denen keine menschliche Entscheidung vorausgeht. Das Scoring selbst ist aber wohl noch keine rechtliche Entscheidung i. S. d. Art. 22 Abs. 1 DSGVO (auch wenn § 28b BDSG von „Entscheidung" spricht), sondern bereitet eine solche vor. Zwar muss der Verantwortliche dem Betroffenen die „involvierte Logik" kundtun (Art. 14 Abs. 2 lit. g, Art. 15 Abs. 1 lit. h DSGVO). Eine Offenlegungspflicht für den Score-Algorithmus besteht wegen schutzwürdiger Geheimhaltungsinteressen (Betriebs-/Geschäftsgeheimnisse) des Verarbeiters jedoch grundsätzlich nicht, vgl. EG 63 S. 4 (ex EG 51 S. 4) DSGVO. Erwägenswert ist aber – wie auch sonst bei der Überprüfung von geheimhaltungsbedürftigen Informationen in Gerichtsverfahren – eine *In-camera-*

			Kontrolle der Score-Formel durch geeignete Instanzen.
Nr. 2	-	Beibehalten eher nicht möglich, wohl streichen	Dito
Nr. 3	-	Beibehalten eher nicht möglich, wohl streichen	Die Untersagung *ausschließlich* auf Adressdaten beruhenden Scorings ist zum Schutz der betroffenen Rechte sachgerecht. Art. 6 Abs. 1 UAbs. 1 lit f DSGVO belässt dem Mitgliedstaat aber keinen Konkretisierungsspielraum.
Nr. 4	-	Beibehalten eher nicht möglich, wohl streichen	Dito

§ 29: Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung

a. Abs. 1, 2

§ 29 Abs. 1, 2 BDSG kann aus denselben Gründen wie § 28 Abs. 1 BDSG nicht aufrechterhalten werden. Insoweit greifen allerdings auch die Legitimationsgründe des Art. 6 Abs. 2 lit. b und f der DSGVO. Einzig § 29 Abs. 1 S. 2 BDSG und § 29 Abs. 2 S. 2 BDSG können mit dem Verweis auf § 28 Abs. 3 BDSG aufrechterhalten werden, soweit es sich dabei um eine zweckändernde Verarbeitung handelt.

b. Abs. 3

§ 29 Abs. 3 BDSG bestimmt, dass die Aufnahme personenbezogener Daten in bestimmten Verzeichnissen unterbleiben muss, wenn aus dem zugrunde liegenden Register ersichtlich ist, dass der Wille des Betroffenen dem entgegensteht. Die Zulässigkeit der Aufnahme in solche Register kann nur mitglied-

staatlich geregelt werden, wenn es sich hier um eine zweckändernde Verarbeitung i. S. d. Art. 6 Abs. 4 (ex Abs. 3a) i. V. m. Art. 23 Abs. 1 lit. a bis j (ex Art. 21 Abs. 1 lit. aa bis g) DSGVO handelt. In solchen Fällen ist es sachgerecht, auch Einschränkungen dieser zweckändernden Weiterverarbeitung mitgliedstaatlich zu regeln. Im Übrigen greift jedoch auch der Legitimationsgrund des Art. 6 Abs. 1 UAbs. 1 lit. f der DSGVO.

c. Abs. 4

§ 29 Abs. 4 BDSG kann nur aufrechterhalten werden, sofern die §§ 28 Abs. 4, 5 BDSG aufrechterhalten werden.

d. Abs. 5

§ 29 Abs. 5 BDSG kann aufrechterhalten werden, soweit die Bestimmungen des § 28 BDSG, auf die verwiesen wird, aufrechterhalten werden.

e. Abs. 6, 7

§ 29 Abs. 6 BDSG kann nicht aufrechterhalten werden, da dieser lediglich bestimmt, dass Anfragen über die Kreditwürdigkeit aus der EU mit Anfragen aus dem Inland gleichzustellen sind, was sich angesichts der einheitlichen Anwendung der Datenschutz-Grundverordnung und auch des BDSG-neu auf in- und ausländische nicht-öffentliche Stellen der EU ohnehin ergibt. § 29 Abs. 7 BDSG kann soweit aufrechterhalten werden, wie die Verbraucherkreditrichtlinie speziellerer gegenüber der Datenschutz-Grundverordnung ist.

§ 29 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 S. 1, Abs. 2 S. 1, S. 3 – 5	Art. 6 Abs. 1 UAbs. 1 lit. b, f	Streichen	Von keiner Öffnungsklausel gedeckt, Zulässigkeitstatbestände in Art. 6 Abs. 1 DSGVO geregelt.
Abs. 1 S. 2,	-	Beibehalten soweit Beibehalten der	Sofern die Normen, auf die § 29 Abs. 1 S. 2, Abs. 2 S. 2 BDSG verweisen aufrechterhalten

Abs. 2 S. 2		Normen, auf die verwiesen wird.	werden, können auch § 29 Abs. 1 S. 2, Abs. 2 S. 2 BDSG aufrechterhalten werden.
Abs. 3	-	Beibehalten für zweckändernde Aufnahme in Verzeichnisse möglich	Soweit sich die Norm auf die zweckändernde Aufnahme in Verzeichnisse i. S. d. § 29 Abs. 3 BDSG bezieht, ist eine Einschränkung dieser Verzeichnisse von der Öffnungsklausel mit umfasst.
Abs. 4	-	Beibehalten	Aufrechterhaltung der Norm möglich, sofern die Bestimmungen des § 28 BDSG, auf die § 29 Abs. 4 BDSG verweist, aufrechterhalten werden.
Abs. 5	-	Beibehalten	Aufrechterhaltung der Norm möglich, sofern die Bestimmungen des § 28 BDSG, auf die § 29 Abs. 5 BDSG verweist, aufrechterhalten werden.
Abs. 6	-	Streichen	Nach DSGVO und BDSG-neu sind inländische und EU-ausländische Datenverarbeiter ohnehin gleich zu behandeln.
Abs. 7	Verbraucherkreditrichtlinie	Beibehalten	Nach Verbraucherkreditrichtlinie.

§ 30: Geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form

§ 30 Abs. 1 BDSG regelt die geschäftsmäßige Datenerhebung und -speicherung zum Zweck der Übermittlung in anonymisierter Form. Allerdings enthält § 30 Abs. 1 BDSG keinen eigenen Zulässigkeitstatbestand, d. h. die Erhebung oder Speicherung dieser Daten muss sich auf einen anderen Zulässigkeitstatbestand stützen.[565] Soweit die Übermittlung der Daten in anonymisierter Form stattfinden soll, ist diese ohnehin aus dem Anwendungsbereich des BDSG (vgl. § 1 Abs. 1 BDSG) bzw. der Datenschutz-Grundverordnung (vgl. Art. 1 Abs. 1 DSGVO) ausgenommen. Die Bestimmung über das Verändern der Daten i. S. d. § 30 Abs. 2 BDSG kann nicht aufrechterhalten werden, da sich hierfür keine Öffnungsklausel in der Datenschutz-Grundverordnung findet. Insoweit greift aber der Legitimationsgrund des Art. 6 Abs. 2 lit. f DSGVO.

[565] *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 30, Rn. 3.

§ 30 Abs. 5 BDSG, der auf § 28 Abs. 6 – 9 BDSG verweist, kann aufrechterhalten werden, soweit § 28 Abs. 6 – 9 BDSG aufrechterhalten werden. Hier wäre auch eine Zusammenfassung der Zulässigkeitstatbestände für den Umgang mit besonderen Arten personenbezogener Daten im Rahmen der von Art. 9 Abs. 2 DSGVO markierten Öffnungen möglich.

§ 30 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	-	Streichen	Von keiner Öffnungsklausel gedeckt, Zulässigkeitstatbestände in Art. 6 Abs. 1 DSGVO geregelt.
Abs. 2	(Art. 6 Abs. 1 UAbs. 1 lit. f)	Streichen	Dito
Abs. 3	-	Streichen	Streichung, da nicht nötig, wenn Abs. 1, 2 gestrichen werden.
Abs. 4	-	Streichen	Dito
Abs. 5	-	Beibehalten; Modifikation	Aufrechterhaltung, soweit Normen des § 28 Abs. 6 – 9 BDSG aufrechterhalten werden, oder Regelung der Verarbeitung besonderer Arten personenbezogener Daten in eigener Vorschrift.

§ 30a: Geschäftsmäßige Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung

§ 30a Abs. 1 – 4 BDSG kann gestrichen werden, da insoweit, wie bei § 28 Abs. 1 und § 29 Abs. 1, 2 BDSG, keine Öffnungsklausel für den Zulässigkeitstatbestand des § 30a Abs. 1 BDSG in der Datenschutz-Grundverordnung besteht und somit auch die Zweckbindung und Anonymisierungspflichten in § 30 a Abs. 2 bzw. 3 BDSG sowie der Hinweis auf § 29 BDSG entfallen. § 30a Abs. 5 BDSG, der auf die Datenverarbeitung besonderer Arten personenbezogener Daten in § 28 Abs. 6 – 9 BDSG verweist, kann nur aufrechterhalten werden, soweit § 28 Abs. 6 – 9 BDSG aufrechterhalten werden. Hier wäre auch eine Zusammenfassung der Zulässigkeitstatbestände für den Um-

gang mit besonderen Arten personenbezogener Daten im Rahmen der von Art. 9 Abs. 2 DSGVO markierten Öffnungen möglich. Der Verweis auf § 28 Abs. 4 BDSG hingegen kann gestrichen werden, da er ohne die anderen Vorschriften des § 30a BDSG nicht mehr notwendig ist.

§ 30a BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	(Art. 6 Abs. 1 UAbs. 1 lit. f)	Streichen	Von keiner Öffnungsklausel gedeckt; Zulässigkeitstatbestände in Art. 6 Abs. 1 DSGVO geregelt.
Abs. 2	(Art. 6 Abs. 1 UAbs. 1 lit. f)	Streichen	Von keiner Öffnungsklausel gedeckt; Zulässigkeitstatbestände in Art. 6 Abs. 1 DSGVO geregelt.
Abs. 3	-	Streichen	Streichung, da nicht nötig, wenn Abs. 1, 2 gestrichen werden.
Abs. 4	-	Streichen	Streichung, da nicht nötig, wenn Abs. 1, 2, 3 gestrichen werden.
Abs. 5	-	Beibehalten; Modifikation	Aufrechterhaltung, soweit Normen des § 28 Abs. 6 – 9 BDSG aufrechterhalten werden; Verweis auf § 28 Abs. 4 BDSG kann gestrichen werden, da nicht nötig, wenn § 30a Abs. 1 – 4 BDSG gestrichen werden.

§ 31: Besondere Zweckbindung

§ 31 BDSG bestimmt als Grenze (des § 9 BDSG), dass personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert wurden, nur für diese Zwecke verwendet werden dürfen. Diese Zweckbegrenzung kann im nicht-öffentlichen Bereich schwerlich aufrechterhalten werden, da sich hierfür keine Öffnungsklausel findet. Insbesondere auf die Öffnungsklausel des Art. 6 Abs. 3 S. 3 DSGVO kann nur zurückgegriffen werden, sofern es sich um Rechtsgrundlagen zur Anpassung der Bestimmungen des Art. 6 Abs. 1 UAbs. 1 lit. c bzw. e DSGVO handelt. Dies wird im nicht-öffentlichen Bereich aber selten der Fall sein;

jedenfalls kann eine pauschale Norm wie § 31 BDSG nicht aufrechterhalten werden. Dies ist aber auch nicht nötig, da der Zweckbindungsgrundsatz in Art. 5 Abs. 1 lit. b DSGVO normiert ist. Abweichungen hiervon lässt die DSGVO nach Art. 6 Abs. 4 DSGVO nur in sehr begrenztem Umfang, dort aber grundsätzlich ohne Präzisierungs- oder Abweichungsrecht der Mitgliedstaaten zu.

§ 31 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Insgesamt	Art. 5 Abs. 1 lit. b	Streichen	Von keiner Öffnungsklausel gedeckt, Zweckbindungsgrundsatz in Art. 5 Abs. 1 lit. b DSGVO normiert.

§ 32: Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

§ 32 BDSG regelt den Arbeitnehmerdatenschutz. Art. 88 (ex Art. 82) DSGVO eröffnet den Mitgliedstaaten umfassende Handlungsmöglichkeiten auf dem Gebiet des Arbeitnehmerdatenschutzes und letztlich die Möglichkeit, den Arbeitnehmerdatenschutz eigenständig zu regeln. Eine nähere Konditionierung erfolgt in Art. 88 (ex Art. 82) DSGVO nicht.[566] Damit kann der § 32 BDSG aufrechterhalten oder auch weiter ausdifferenziert werden.[567]

§ 32 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Insgesamt	Art. 88 (ex Art. 82)	Beibehalten	Weitreichende Gestaltungsbefugnisse der Mitgliedstaaten durch Art. 88 (ex Art. 82) DSGVO.

[566] Vgl. hierzu S. 298.
[567] So auch *Wybitul/Sörup/Pötters*, ZD 2015, 559 (561); *Sörup/Marquardt*, ArbRAktuell 2016, 103 (105).

§§ 33 – 35: Rechte des Betroffenen bei Datenverarbeitung der nicht-öffentlichen Stellen

Vorbemerkung

Für den Bereich der nicht-öffentlichen Stellen sehen die §§ 33 – 35 BDSG eine ähnliche Regelungsstruktur vor wie für den öffentlichen Bereich.[568] Sie umfassen in leicht abweichender, eher der logischen Reihenfolge und auch dem Ansatz der Datenschutz-Grundverordnung entsprechender Abfolge gleichermaßen die Dreiteilung vor:

1) die Benachrichtigungspflicht der verantwortlichen Stelle gegenüber dem Betroffenen (§ 33 BDSG), die wiederum korrespondiert mit den wesentlich weiter gefassten Informationspflichten gemäß Art. 13 und Art. 14 (ex Art. 14 und 14a) DSGVO, die teilweise noch durch die Transparenzpflichten des Art. 12 DSGVO ergänzt werden,

2) das Auskunftsrecht des Betroffenen (§ 34 BDSG), das sich in Art. 15 DSGVO findet und

3) die in § 35 BDSG zusammengefassten Ansprüche auf Berichtigung, Löschung und Sperrung von Daten, die mit Art. 16 DSGVO (Berichtigung), Art. 17 DSGVO (Recht auf Löschung) sowie dem Recht auf Einschränkung der Verarbeitung in Art. 18 (ex Art. 17a) DSGVO (ergänzt um das Widerspruchsrecht in Art. 21 [ex Art. 19] DSGVO), korrespondieren.

Für den nicht-öffentlichen Bereich greift auf den ersten Blick der Beschränkungstatbestand des Art. 23 Abs. 1 lit. i (ex Art. 21 Abs. 1 lit. f) DSGVO mit dem Schutzziel „der Rechte und Freiheiten anderer Personen“ (sub specie der von der Berufsfreiheit gedeckten Datenverarbeitungsziele. Möglicherweise meint „Freiheiten anderer Personen“ allerdings auch nur die Freiheiten mittelbar betroffener Dritter, nicht aber des Verantwortlichen selbst. Unabhängig davon muss auch hier wiederum umfassend der Katalog des Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abgearbeitet werden.[569] Das verlangt jedenfalls zunächst, dass eine entsprechende Einschränkung tatsächlich notwendig ist. Teilweise sehen die in der Datenschutz-Grundverordnung normierten Betroffenenrechte aber auch sogleich Einschränkungen selbst vor und überlassen

[568] Vgl. §§ 19 ff. BDSG.
[569] Dazu ausführlich S. 70.

dies nicht den Mitgliedstaaten. Insgesamt ist in der rein rechtlichen Bewertung eine strukturelle Orientierung an den Ausführungen zum öffentlichen Bereich möglich, wobei allerdings Einschränkungen in geringerem Umfang auf der Basis des Art. 23 Abs. 1 lit. i (ex Art. 21 Abs. 1 lit. f) DSGVO gerechtfertigt sein dürften. Im Übrigen ist es für den nicht-öffentlichen Bereich in rechtspolitischer Hinsicht sehr fraglich, ob überhaupt abweichende Regelungen vorgesehen werden sollen.
Im Einzelnen gilt in Anlehnung an die Ausführungen zum öffentlichen Bereich Folgendes:

§ 33: Benachrichtigung des Betroffenen

§ 33 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	Art. 14 (ex Art. 14a); Öffnungsklausel: Art. 23 (ex Art. 21)	Streichen und durch Art. 13, 14 (ex Art. 14, 14a) DSGVO substituieren	Die Öffnungsklausel nach Art. 23 (ex Art. 21) DSGVO lässt zwar eine abweichende Regelung zu. Die Diskrepanz zwischen Art. 14 (ex Art. 14a) DSGVO und § 33 BDSG, die teils in Formulierungsunterschieden, vor allem aber in einer umfassenderen Reichweite des Art. 14 DSGVO begründet ist (etwa Hinweise zur Speicherdauer in Art. 13 Abs. 2 lit. a [ex Art. 14 Abs. 2 lit. b]), lässt sich grundsätzlich nicht durch die Rechtfertigungsgründe des Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO pauschal rechtfertigen. Ferner müssen die im deutschen Datenschutzrecht nicht vergleichbar umfangreichen Regelungen des Art. 13 (ex Art. 14) DSGVO greifen.
Abs. 2 S. 1 Nr. 1 – 9 dem Grunde nach	Art. 14 Abs. 5 lit. a – d (ex Art. 14a Abs. 4 lit. a – d) dem Grunde nach	Streichen/Wiederholung, dann aber Anpassung an Formulierung der DSGVO	Die Regelung ist im Unionsrecht – wenn auch in teils modifizierter, sogar weiter gehender Form – vorgesehen und daher ist keine Absicherung im nationalen Recht erforderlich. Sollte eine Wiederholung im nationalen Recht erfolgen, dann wäre zumindest eine Anpassung an die Formulierung in der DSGVO erforderlich. Das gilt grundsätzlich auch für die teils sehr ausdifferenzierte Regelung der Unverhältnismäßigkeit (etwa für listenmäßige

			Daten in § 33 Abs. 1 S. 1 Nr. 8 lit. b BDSG), da dies von der generellen Unverhältnismäßigkeitsregelung des Art. 14 Abs. 5 lit. b Hs. 1 Alt. 2 (ex Art. 14a Abs. 4 lit. b Hs. 1 Alt. 2) DSGVO grundsätzlich erfasst ist. Eine Aktivierung der Öffnungsklausel zur Absicherung des Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) DSGVO („Rechte und Freiheiten anderer Personen") wäre daher fraglich und hängt auch davon ab, ob sich jene Rechtspositionen nur auf Dritte oder auch auf den Verantwortlichen erstrecken. Dann wäre jedenfalls der Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeiten.
Speziell Abs. 2 S. 1 Nr. 6 Var. 1 (öffentliche Sicherheit) und Nr. 3 (Geheimhaltungspflicht)	Art. 14 (ex Art. 14a); Öffnungsklausel: Art. 23 Abs. 1 lit. c und lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. a und lit. f Alt. 2)	Beibehalten möglich	Art. 23 Abs. 1 lit. c (ex Art. 21 Abs. 1 lit. a) – öffentliche Sicherheit – und lit. i Alt. 2 (ex lit. f Alt. 2) – Rechte und Freiheiten anderer Personen – deckt diese Ausnahmen ab. Es ist der Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeiten.
Speziell Abs. 2 S. 1 Nr. 6 Var. 2 (öffentliche Ordnung) und Var. 3 (Wohle des Bundes oder eines Landes)	Art. 14 (ex Art. 14a); Öffnungsklausel: Art. 23 Abs. 1 (ex Art. 21 Abs. 1)	Beibehalten mit Modifikation möglich	Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO sieht eine ganze Reihe von Rechtfertigungstatbeständen vor, die jedoch nicht allgemein auf die Erfüllung öffentlicher Aufgaben abstellen, was weiter gefasst ist. Daher müsste eine Eingrenzung der Beschränkung auf die dort angeführten Ziele erfolgen. Ferner ist der Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeiten.

§ 34: Auskunft an den Betroffenen

§ 34 BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Norm insgesamt	Art. 15	Streichen und durch Art. 15 DSGVO substituieren	Die Öffnungsklausel nach Art. 23 (ex Art. 21) DSGVO lässt zwar eine abweichende Regelung zu. Die Diskrepanz zwischen Art. 15 DSGVO und § 34 BDSG, die teils in Formulierungsunterschieden, vor allem aber in einer umfassenderen Reichweite des Art. 15begründet ist (etwa Hinweise zur Speicherdauer in Art. 15 Abs. 1 lit. d), lässt sich grundsätzlich nicht durch die Rechtfertigungsgründe des Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO pauschal rechtfertigen.
Speziell Abs. 1 S. 3, 4; Abs. 3 S. 2 (Geschäftsgeheimnisse; Geheimhaltungsinteresse)	Öffnungsklausel: Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2)	Beibehalten möglich	Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) DSGVO (Rechte und Freiheiten anderer Personen) deckt diese Ausnahme ab.
Speziell Abs. 1a	Öffnungsklausel: Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2)	Beibehalten wohl möglich	Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) DSGVO (Rechte und Freiheiten anderer Personen) deckt diese Ausnahme wohl ab, da wohl auch eine Konditionierung einzelner Auskunftsmöglichkeiten in Bezug auf die Empfänger nach Art. 15 Abs. 1 lit. c DSGVO möglich ist.
Speziell Abs. 2 und 4 (Scoring)	s. Ausführungen zu § 28b BDSG	s. Ausführungen zu § 28b BDSG	s. Ausführungen zu § 28b BDSG
Abs. 5 (Zweckbindung)	-	Beibehalten möglich	Jedenfalls als Ausgestaltung nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO als entsprechende zusätzliche Schranke zulässig.

Abs. 6, 8, 9 (Verfahren und Form; Entgeltpflichtigkeit der Auskunftserteilung)	Art. 12 Abs. 5, Art. 15; Öffnungsklausel: Art. 23 (ex Art. 21)	Streichen; beibehalten u. U. möglich	Art. 12 Abs. 5 DSGVO sieht grundsätzlich die Entgeltfreiheit vor. Ob Art. 23 (ex Art. 21) DSGVO eine Ausnahme deckt, ist fraglich.
Abs. 7 (Verweis auf § 33 Abs. 2 S. 1 Nr. 2, 3, 4, 5, 6, 7)	Art. 15; Öffnungsklausel: Art. 23 (ex Art. 21)	Beibehalten möglich, soweit § 33 Abs. 2 S. 1 Nr. 2, 3, 4, 5, 6, 7 BDSG aufrechterhalten werden kann; dazu s.o. § 33 BDSG	s. o. § 33 BDSG.

§ 35: Berichtigung, Löschung und Sperrung von Daten

§ 35 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Gesamte Bestimmung, v. a. Ansatz in Abs. 1, 2, 3, 4, 5, 6	Art. 16, 17, 18, 21 (ex Art. 17a, Art. 19); Öffnungsklausel: Art. 23 (ex Art. 21)	Grundsätzlich Streichen und durch Art. 16, 17, 18, 21 (ex Art. 17a, Art. 19) DSGVO substituieren	Die Öffnungsklausel nach Art. 23 (ex Art. 21) DSGVO lässt zwar eine abweichende Regelung zu. Die Diskrepanz zwischen Art. 17, 18 und 21 (ex Art. 17a und Art. 19) DSGVO einerseits und § 35 BDSG, die teils in Formulierungsunterschieden, vor allem aber in einer umfassenderen Reichweite der Normen der DSGVO liegt, kann grundsätzlich nicht durch die Rechtfertigungsgründe des Art. 23 Abs. 1 (ex Art. 21 Abs. 1) DSGVO pauschal gerechtfertigt werden. Andere Regelungsansätze wie die in § 35 Abs. 6 als Ausnahmen vom Berichtigungsanspruch sollten eher gestrichen werden, sofern nicht starke rechtspolitische Gründe für sie sprechen. Sonst wäre die Einschränkung auf Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) (Rechte und

			Freiheiten anderer Personen) abzustützen. Dann wäre der Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeiten.
Speziell Abs. 2 Nr. 4	-	Kann wohl aufrecht-erhalten werden.	Auch Konkretisierungen wie § 35 Abs. 2 Nr. 4 sind vor diesem Hintergrund zumindest rechtspolitisch fraglich. Allerdings deckt Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) DSGVO (Rechte und Freiheiten anderer Personen) diese Konkretisierung wohl ab. Es ist der Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeiten.
Speziell Abs. 3 Nr. 1 (Aufbewahrungsfristen)	Art. 17 Abs. 3 lit. b	Streichen (allenfalls wiederholende Aufrecht-erhaltung)	Dient der Erfüllung einer rechtlichen Verpflichtung. Diese Ausnahme ist aber bereits in Art. 17 Abs. 3 lit. b DSGVO vorgesehen und bedarf keiner mitgliedstaatlichen Wiederholung. Vielmehr sind entsprechende Aufbewahrungspflichten im nationalen Recht zu regeln.
Speziell Abs. 3 Nr. 2 (schutzwürdige Interessen des Betroffenen)	Art. 23 Abs. 1 lit. i Alt. 1 (ex Art. 21 Abs. 1 lit. f Alt. 1)	Beibehalten möglich	Art. 23 Abs. 1 lit. i Alt. 1 (ex Art. 21 Abs. 1 lit. f Alt. 1) DSGVO deckt diese Ausnahme ab. Es ist dann der Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeiten.
Speziell Abs. 3 Nr. 3 (hoher Aufwand)	Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2)	Beibehalten wohl möglich	Art. 23 Abs. 1 lit. i Alt. 2 (ex Art. 21 Abs. 1 lit. f Alt. 2) DSGVO (Rechte und Freiheiten anderer Personen) deckt diese Ausnahme wohl ab, da wohl auch der Fall unverhältnismäßigen Aufwands erfasst ist. Es ist dann der Katalog nach Art. 23 Abs. 2 (ex Art. 21 Abs. 2) DSGVO abzuarbeiten. Die DSGVO geht allerdings in Art. 12 Abs. 5 lit. a (ex Abs. 4) davon aus, dass Unverhältnismäßigkeiten über Entgelteinnahmen ausgeglichen werden.
Speziell Abs. 4a (keine Übermittlung der Tatsache der	Art. 18 Abs. 2 (ex Art. 17a Abs. 2)	Beibehalten fraglich	Art. 18 Abs. 2 (ex Art. 17a Abs. 2) DSGVO kann so verstanden werden, dass im Fall einer Einschränkung der Verarbeitung auch nicht der Umstand der Einschränkung mitgeteilt werden darf, wie es § 35 Abs. 4a BDSG explizit regelt, da andernfalls eine effektive

Sperrung)			Wahrung des Sperrungsinteresses nicht gewährleistet ist. Dann wäre eine Konkretisierung fraglich, da es sich insoweit nicht um eine Öffnungsklausel handelt.
Speziell Abs. 8 Nr. 1 (Sperre und wissenschaftliche Zwecke)	Art. 89 Abs. 2 (ex Art. 83 Abs. 2)	Beibehalten möglich	Art. 89 Abs. 2 (ex Art. 83 Abs. 2) DSGVO eröffnet eine entsprechende Ausnahme von Art. 18 (ex Art. 17a) DSGVO.

§ 35a BDSG-neu: Rechteausübung bei Tod des Betroffenen

EG 27 (ex EG 23aa) DSGVO ermöglicht den Mitgliedstaaten, Vorschriften für die Verarbeitung der Daten Verstorbener beizubehalten oder zu erlassen. Die Datenschutz-Grundverordnung findet auf Daten Verstorbener selbst keine Anwendung.[570] Für die Nationalstaaten empfiehlt es sich, Regelungen zum postmortalen Persönlichkeitsschutz Verstorbener in das nationale BDSG zu integrieren. Mit der wachsenden Zahl von „digital natives“ wächst nämlich auch die Bedeutung des digitalen Nachlasses. Internetnutzer hinterlassen unablässig digitale Spuren im Netz. So entsteht ein Abziehbild der Persönlichkeit, das den Tod des Nutzers überdauert und nicht den Gesetzen der Vergänglichkeit unterliegt.[571] Diese Daten sind zumeist nur mit einem digitalen Schlüssel, namentlich den korrekten Zugangsdaten des Nutzer-Accounts erreichbar. Sind diese Passwörter nicht greifbar, hat auch der Diensteanbieter technische Möglichkeiten, um den hinter den Zugangshindernissen schlummernden Datenschatz zu heben.[572] Ob der Verstorbene diese Daten Angehörigen überhaupt preisgeben oder aber z. B. Onlineliebesbriefe einer geheimen Romanze lieber mit ins Grab nehmen wollte, lässt sich nicht ohne Weiteres ergründen.

[570] Dazu im Einzelnen S. 21.
[571] *Martini* (Fn. 27), 1146.
[572] *Martini* (Fn. 27), 1146.

a. Erbrechtliche Dimension des digitalen Nachlasses

Da das Erbrecht alleine die vermögensrechtliche Rechtsnachfolge regelt, nicht aber den Persönlichkeitsschutz Verstorbener, hält es keine für den Datenschutz des Verstorbenen angemessene Antwort bereit, insbesondere erfolgt keine Universalsukzession bei höchstpersönlichen Daten (soweit sie nicht untrennbar mit vermögensrechtlichen Positionen verwoben sind, die dem Erben als Teil seiner vermögensrechtlichen Position zufallen).[573]

b. Datenschutzrechtliche Dimension des digitalen Nachlasses

Ob Verstorbene de lege lata Schutzsubjekt des Datenschutzrechts sind, ist nicht abschließend geklärt: Einige lesen in der datenschutzrechtlichen Begriffsbestimmung „personenbezogene Daten" das Wort „lebend" als ungeschriebene Voraussetzung mit.[574] Zwar setzt das Allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG als Keimzelle des Datenschutzrechts die Fähigkeit zur Entfaltung der Persönlichkeit voraus. Diese erlischt mit dem Tode (nicht aber der Persönlichkeitsschutz in toto). Das einfachgesetzliche Datenschutzrecht ist indes noch nicht allein aus diesem Grunde auf den Schutz lebender Menschen beschränkt: Entscheidend ist, dass die Daten *zum Zeitpunkt der Entstehung* einen Personenbezug zu einem lebenden Menschen aufweisen. Sinn und Zweck des Datenschutzes gebieten, die Daten Verstorbener nicht zum „Plünderungsobjekt" der Nachwelt degenerieren zu lassen, was überdies Auswirkungen auf das Verhalten und die Persönlichkeitsentfaltung zu Lebzeiten hätte.[575] Ein Vergleich mit § 35 Abs. 5 SGB I (Sozialdaten Verstorbener) und § 22 S. 3 KunstUrhG (Recht am eigenen

---

[573] *Martini* (Fn. 27), 1147 f.; a. A. *Klas/Möhrke-Sobolewski* (Fn. 33), 3474, die auch nichtvermögensrechtliche Positionen als vererbbar ansehen, da eine Differenzierung nicht ohne Weiteres möglich sei; gleichwohl wollen sie die höchstpersönlichen Positionen von der Universalsukzession ausnehmen; ohne letztere Unterscheidung, *Steiner/Holzer*, ZEV 2015, 262 (263); LG Berlin, Urt. v. 17.12.2015 – 20 O 172/15, juris Rn. 24 f., hier beruhte der Antrieb der Erben, Auskunft über die Daten der Erblasserin zu erhalten, letztlich auf finanziellen Erwägungen, da sie als Eltern der Verstorbenen weitere Schadensersatzansprüche des beim Tod ihres Kindes geschädigten U-Bahnfahrers befürchteten, wenn es sich um einen Suizid gehandelt hätte. Diese Konstellation ist nicht mit solchen vergleichbar, in denen Angehörige nicht aus vermögensrechtlichen, sondern persönlichen Motiven heraus die Daten Verstorbener einsehen wollen.

[574] So etwa *Dammann* (Fn. 26), § 3, Rn. 17; zustimmend LG Berlin, Urt. v. 17.12.2015 – 20 O 172/15, juris Rn. 41; ebenso *Klas/Möhrke-Sobolewski* (Fn. 33), 3476.

[575] *Martini* (Fn. 27), 1148 f.

Bild) zeigt, dass es sinnvoll sein kann, dem Schutz der Daten Verstorbener einen Stellenwert einzuräumen. So geht § 35 Abs. 5 S. 1 SGB I im Rahmen der Verarbeitungsbefugnis von Daten Verstorbener implizit davon aus, dass ihre Sozialdaten weiter unter das Sozialgeheimnis fallen und grundsätzlich einen besonderen Geheimhaltungsschutz genießen.[576] Eine ähnliche Wertung formuliert § 203 Abs. 2 StGB für das Verhältnis zwischen Patient und Arzt: Das Arztgeheimnis wirkt auch über den Tod hinaus.

Telemedienrechtliche Diensteanbieter befinden sich in einer ähnlichen Rolle wie der Inhaber der Krankenakte: Sie halten einen Schlüssel in den Händen, der alleine den Zugang zu den in dem Account verborgenen Daten eröffnet. § 13 Abs. 4 Nr. 3 TMG verpflichtet Diensteanbieter dazu, die Nutzung der Telemedien gegen die Kenntnisnahme Dritter zu schützen, Letzteren also keinen Zugang zu eröffnen.[577] Insoweit sind sie als „Gatekeeper" mit Berufsgeheimnisträgern wie Ärzten vergleichbar, so dass die Geheimhaltungspflicht Hauptpflicht des Vertrages mit dem Nutzer ist.[578] Diese einfachgesetzliche Wertung unterfüttert das Verfassungsrecht mit einem besonderen postmortalen Persönlichkeitsschutz: Dem Verstorbenen fließt aus der Menschenwürde des Art. 1 Abs. 1 GG ein Achtungsanspruch und ein sozialer Geltungswert zu, der den Schutz der lebenslangen Persönlichkeitsentfaltung vor postmortalen Verfälschungen oder Ausspähungen als wesensgleiches Minus zum Persönlichkeitsschutz Lebender umfasst.[579] Insbesondere der Schutz vor Ausspähungen kann schon das Verhalten des lebenden Nutzers bestimmen; namentlich vertraut er darauf, dass seine zu Lebzeiten geschützten persönlichen Daten, etwa die heimliche Liebschaft, auch nach dem Ableben geheim bleiben und gerade nicht einem Angehörigen oder sonstigem Dritten offenbar werden.[580]

---

[576] *Martini* (Fn. 27), 1149.

[577] Der vor dem LG Berlin verhandelte Fall betraf die besondere Konstellation, in der die Eltern als Erben ihres Kindes Auskunft verlangten und zugleich Sachwalter des Persönlichkeitsrechts ihres Kindes waren, LG Berlin, Urt. v. 17.12.2015 – 20 O 172/15, juris Rn. 32.

[578] *Martini* (Fn. 30), S. 96 ff.

[579] *Martini* (Fn. 27), 1150.

[580] *Martini* (Fn. 27), 1151 f.

c. Rechtspolitische Handlungsempfehlungen

Gute Argumente streiten dafür, dass de lege lata auch schon personenbezogene Daten Verstorbener unter den Schutz des BDSG fallen.[581] Das sollte der Gesetzgeber gegebenenfalls klarstellen. Jedenfalls im Hinblick auf Betroffenenrechte sollte der Gesetzgeber den Angehörigen Verstorbener das Wahrnehmungsrecht ausdrücklich zusprechen. [582] Die Regelung eines neuen § 35a BDSG könnte lauten: „Datenschutzrechtliche Rechte nehmen nach dem Tod des Betroffenen dessen Angehörige wahr. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Betroffenen und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Nutzers.“ Anderenfalls laufen die Daten Verstorbener in einer modernen Big-Data-Welt Gefahr, zum kommerziellen Plünderungsobjekt von Datenauswertungskonzernen zu werden. Hinsichtlich des Zugangs zu Passwort geschützten Inhalten sollte der Gesetzgeber die Diensteanbieter grundsätzlich dazu verpflichten, sicherzustellen, dass die Nutzer durch geeignete Einstellungsmöglichkeiten Regelungen für den Umgang mit ihren Daten nach dem Tod treffen.[583]

§ 35a BDSG n. F.	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Norm insgesamt	EG 27 (ex EG 23aa)	Neu einfügen; Vorschlag: „Datenschutzrechtliche Rechte nehmen nach dem Tod des Betroffenen dessen Angehörige wahr. Angehörige im Sinne dieses Ge-	De lege ferenda sollte der Gesetzgeber die Generalüberholung des nationalen Datenschutzrechts nutzen, vor allem durch Rechtsprechung und Literatur behandelten Fälle, in denen Angehörige die Persönlichkeitsrechte wahrgenommen haben, zu normieren. Dafür enthält EG 27 (ex EG 23aa) DSGVO eine Öffnungsklausel, die dem Mitgliedstaat trotz des engen Wortlauts weitreichende Rege-

[581] Fällt mit der Novellierung des BDSG auch die Definition des personenbezogenen Datums im deutschen Recht weg, entfällt insbesondere das bisher in der Diskussion dominierende Argument, der Begriff des personenbezogenen Datums impliziere eine lebende Person.
[582] *Martini* (Fn. 30), S. 114-116.
[583] Siehe dazu oben S. 14 sowie *Martini* (Fn. 30), S. 110, 122 f.

		setzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Betroffenen und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Nutzers“	lungsbefugnisse für den Datenschutz Verstorbener einräumt.

§§ 36 – 38a: Aufsichtsbehörde

§§ 36, 37 weggefallen.

§ 38: Aufsichtsbehörde

Entsprechend den Bestimmungen der §§ 22 - 26 BDSG für die Kontrolle öffentlicher Stellen regelt § 38 BDSG die Datenschutzaufsicht über *nicht-öffentliche* Stellen. Hier finden sich tendenziell weiter reichende Befugnisse der Aufsichtsbehörden als im Rahmen der Kontrolle der *öffentlichen* Stellen gemäß den §§ 22 - 26 BDSG. Gleichwohl gilt auch hier: Die Aufgaben und Befugnisse in Art. 57 und 58 (ex Art. 52 und 53) DSGVO reichen jedenfalls in Teilen weiter als diejenigen in § 38 BDSG. Das gilt etwa für die Einsicht in geschäftliche Unterlagen nach § 38 Abs. 4 S. 2 BDSG, die mit einer weiter gefassten Zugriffsbefugnis auf alle relevanten personenbezogenen Daten und Informationen in Art. 58 Abs. 1 lit. e (ex Art. 53 Abs. 1 lit. da) DSGVO korrespondiert. Zahlreiche Bestimmungen sind allerdings auch deckungsgleich, wie etwa die Befugnis zur Übermittlung von Daten an andere Aufsichtsbehörden in § 38 Abs. 1 S. 4 BDSG, die Art. 57 Abs. 1 lit. g Var. 2 (ex Art. 52 Abs. 1 lit. c Var. 2) DSGVO entspricht. Daher ist unabhängig von der erwägenswerten Zusammenführung der Aufsichtsregeln in einem gemeinsamen Teil für öffentliche und nicht-öffentliche Stellen auch für die nicht-öffentlichen Stellen zu prüfen, ob nicht ein pauschaler Verweis auf die Befugnisse der Datenschutz-Grundverordnung mit punktuellen Regelungen im

Rahmen der Öffnungsklauseln der Datenschutz-Grundverordnung (soweit zulässig) sinnvoller ist als eine Wiederholung der DSGVO-Regeln im Rahmen einer die Öffnungsklauseln ausschöpfenden kohärenten und transparenten Gesamtregelung.

Im Einzelnen gilt (in Teilergebnissen kann auf die obigen Ausführungen zur Aufsicht über nicht-öffentliche Stellen[584] verwiesen werden, etwa mit Blick auf § 38 Abs. 1 S. 7 BDSG, für den entsprechende Ergebnisse gelten wie für § 26 Abs. 1 S. 1 BDSG):

§ 38 Abs. 1 S. 1 BDSG normiert die allgemeine Kontrollbefugnis der Aufsichtsbehörde. Die Bestimmung entspricht Art. 55 Abs. 1 (ex Art. 51 Abs. 1) DSGVO, weicht im Wortlaut jedoch von dieser Bestimmung ab, so dass sie gestrichen oder im Wortlaut angepasst werden sollte. Eine Wiederholung bewegt sich an den absoluten Grenzen des Wiederholungsverbots. Es ist nicht vollständig gesichert, dass die Regelung weiterreichender Befugnisse unter Berufung auf die Öffnungsklausel des Art. 58 Abs. 4 (ex Art. 53 Abs. 4) DSGVO und das damit ausgelöste Interesse an einer kohärenten Gesamtregelung hierfür genügt. Das gilt auch für die sich anschließenden Absätze.

§ 38 Abs. 1 S. 2 BDSG normiert die Beratung und Unterstützung der Datenschutzbeauftragen. Das BDSG geht hier mit seiner generellen Befugnis weiter als die Datenschutz-Grundverordnung in Art. 53 Abs. 3 lit. a (ex Art. 53 Abs. 1c lit. a) DSGVO; Art. 57 Abs. 1 lit. d (ex Art. 52 Abs. 1 lit. ac) DSGVO. Das ist gemäß der Öffnungsklausel des Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO jedoch unproblematisch möglich.

§ 38 Abs. 1 S. 3 BDSG regelt besondere Datenverarbeitungsbefugnisse für die Durchführung der Aufsicht. Die Datenverarbeitung durch die Datenschutzaufsicht ist jedoch durch Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO gedeckt und bedarf keiner gesonderten Regelung, auch wenn eine solche ggf. nach Art. 6 Abs. 2 (ex Abs. 2a) und Abs. 3 DSGVO zulässig ist. Es empfiehlt sich daher, die Vorschrift zu streichen.

§ 38 Abs. 1 S. 4 und 5 BDSG zur Übermittlung von Daten an andere Aufsichtsbehörden und zur Amtshilfe und Art. 57 Abs. 1 lit. g Var. 2 und 3 (ex Art. 52 Abs. 1 lit. c Var. 2 und 3) DSGVO sind deckungsgleich. Die Vorschrift im BDSG sollte gestrichen oder im Wortlaut angepasst werden. Die

[584] Siehe S. 409 ff.

Vorschrift sollte im Rahmen der Regeln über die Zusammenarbeit der Aufsichtsbehörden neu aufgenommen werden.

§ 38 Abs. 1 S. 6 Hs. 1 BDSG zur Unterrichtung von Betroffenem bei Verstoß gegen Datenschutzbestimmungen geht weiter als Art. 58 Abs. 2 lit. e (ex Art. 53 Abs. 1b lit. da) DSGVO, da die Vorschrift auch die Möglichkeit der unmittelbaren Information des Betroffenen vorsieht. Dies kann wegen Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO aufrechterhalten bleiben. Dann sollte aber ausgehend von einem an die Datenschutz-Grundverordnung angepassten Wortlaut eine entsprechende explizite Ergänzung erfolgen.

§ 38 Abs. 1 S. 6 Hs. 2 BDSG zur Anzeige von Datenschutzverstößen bei zuständigen Stellen geht ebenfalls weiter als die Datenschutz-Grundverordnung in Art. 58 Abs. 5 (ex Art. 53 Abs. 3), da jene nicht nur Justizbehörden, sondern alle „zuständigen Stellen“ erfasst. Dies kann mit Blick auf Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO aufrechterhalten bleiben. Dann sollte aber wiederum ausgehend von einem an die Datenschutz-Grundverordnung angepassten Wortlaut eine entsprechende explizite Ergänzung erfolgen. Die Anzeigepflicht gegenüber der Sanktionsstelle wird allerdings nur erforderlich, wenn der Gesetzgeber nach Art. 83 Abs. 7 (ex Art. 79 Abs. 3b) DSGVO die Zuständigkeit für Bußgelder nicht bei der/dem BfDI ansiedelt.

Die Anzeigepflicht in § 38 Abs. 1 S. 6 Hs. 2 BDSG gegenüber den Gewerbeaufsichtsbehörden sieht die Datenschutz-Grundverordnung so nicht vor. Die Norm ist aber wegen Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO als zusätzliche Befugnis von der Öffnungsklausel gedeckt.

In Bezug auf den Tätigkeitsbericht nach § 38 Abs. 1 S. 7 BDSG gilt das zu § 26 Abs. 1 S. 1 BDSG (dazu S. 425) Gesagte.

Da die Meldepflicht und das entsprechende Register entfällt (siehe oben § 4d und § 4e BDSG), bedarf es auch keiner entsprechenden Aufgaben- und Befugniszuweisung. § 38 Abs. 2 BDSG kann daher gestrichen werden.

§ 38 Abs. 3 BDSG entspricht tendenziell Art. 58 Abs. 1 lit. a (ex Art. 53 Abs. 1 lit. a) DSGVO, sieht jedoch angesichts des Hinweises auf eine „unverzüglich“ zu erteilende Auskunft wohl eine Verschärfung vor, die von der Öffnungsklausel des Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO gedeckt ist. Sie kann also beibehalten werden. Dann sollte aber wiederum ausgehend von einem an die Datenschutz-Grundverordnung angepassten Wortlaut eine ent-

sprechende explizite Ergänzung erfolgen. Die Konkretisierung des Zeugnisverweigerungsrechts ist gerade dann sinnvoll.
Die in § 38 Abs. 4 S. 1 BSDG geregelten Nachschaurechte sind von der Öffnungsklausel des Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db) DSGVO gedeckt und können so aufrechterhalten bleiben. Allerdings geht Art. 58 Abs. 1 lit. d (ex Art. 53 Abs. 1 lit. d) DSGVO hinsichtlich der Einsicht in geschäftliche Unterlagen ggf. weiter. Um unnötige Rechtsunsicherheiten insoweit zu vermeiden, sollte wiederum ausgehend von einem an die Datenschutz-Grundverordnung angepassten Wortlaut eine entsprechende explizite Ergänzung erfolgen.
Die Anordnungsbefugnisse in § 38 Abs. 5 S. 1 und 2 BDSG entsprechen weitgehend Art. 58 Abs. 2 lit. d und f (ex Art. 53 Abs. 1b lit. d und lit. e) DSGVO, wobei lit. f (ex lit. e) aber etwas abweichend explizit auch auf den Zeitraum verweist, innerhalb dessen die Anpassung durch die verantwortliche Stelle zu erfolgen hat. Auch hier sollte also im Falle einer gewünschten Kohärenz wahrenden Wiederholung der Wortlaut der Datenschutz-Grundverordnung übernommen werden.
Die in § 38 Abs. 5 S. 3 BDSG vorgesehene Möglichkeit, die Abberufung des Datenschutzbeauftragten zu verlangen, ist so nicht in der Datenschutz-Grundverordnung vorgesehen, aber von der Öffnungsklausel des Art. 56 Abs. 6 (ex Art. 53 Abs. 4) DSGVO gedeckt. Sie kann also beibehalten werden.
Tabellarisch zusammengefasst ergibt sich Folgendes:

§ 38 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 S. 1 (Kontrollbefugnis)	Art. 57 Abs. 1 lit. a; Abs. 2 (ex Art. 52 Abs. 1 lit. a; Abs. 4	Streichen; modifizieren	§ 38 Abs. 1 S. 1 BDSG entspricht Art. 55 Abs. 1 (ex Art. 51 Abs. 1 DSGVO), weicht im Wortlaut jedoch von dieser Bestimmung ab.
Abs. 1 S. 2 (Beratung und Unterstützung)	Art. 58 Abs. 3 lit. a (ex Art. 53 Abs. 1c	Ggf. beibehalten	BDSG geht weiter als die DSGVO, da generelle Befugnis, die nach Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO auch aufrechterhalten werden kann.

	lit. a); Art. 57 Abs. 1 lit. d (ex Art. 52 Abs. 1 lit. ac); Art. 53 Abs. 6 (ex Art. 53 Abs. 4)		
Abs. 1 S. 3 (Datenverarbeitungsbefugnisse)	Art. 6 Abs. 1 UAbs. 1 lit. e; Abs. 2 (ex Abs. 2a), Abs. 3	Besser streichen	Die Datenverarbeitung ist durch Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO gedeckt.
Abs. 1 S. 4, 5 (Übermittlung von Daten an andere Aufsichtsbehörden; Amtshilfe)	Art. 57 Abs. 1 lit. g Var. 2, 3 (ex Art. 52 Abs. 1 lit. c Var. 2, 3)	Streichen	§ 38 Abs. 1 S. 4 und 5 BDSG und Art. 57 Abs. 1 lit. g Var. 2, 3 (ex Art. 52 Abs. 1 lit. c Var. 2, 3) DSGVO sind deckungsgleich.
Abs. 1 S. 6 Hs. 1 (Unterrichtung von Betroffenem bei Verstoß)	Art. 58 Abs. 2 lit. e; Art. 58 Abs. 6 (ex Art. 53 Abs. 1b lit. da; Art. 53 Abs. 4)	Ggf. beibehalten;	§ 38 Abs. 1 S. 6 Hs. 1 BDSG geht weiter als Art. 58 Abs. 2 lit. e (ex Art. 53 Abs. 1b lit. da) DSGVO, da die Vorschrift auch die Möglichkeit der unmittelbaren Information des Betroffenen vorsieht.
Abs. 1 S. 6 Hs. 2 (Anzeige bei zuständigen Stellen)	Art. 58 Abs. 5; Abs. 6 (ex Art. 53 Abs. 3; Abs. 4)	Beibehalten	§ 38 Abs. 1 S. 6 Hs. 2 BDSG geht weiter als Art. 58 Abs. 5 (ex Art. 53 Abs. 3) DSGVO, da nicht nur Justizbehörden, sondern alle „zuständigen Stellen“ erfasst werden.
Abs. 1 S. 6 Hs. 3 (Anzeige bei Gewerbe-	Art. 58 Abs. 5; Abs. 6 (ex Art. 53	Streichen; beibehalten	Diese Anzeigepflicht ist so in der DSGVO nicht vorgesehen.

aufsicht)	Abs. 3; Abs. 4)		
Abs. 1 S. 7 (Tätigkeits-bericht)	Art. 59 (ex Art. 54)	Modifizieren	Es gilt insoweit das zu § 26 Abs. 1 S. 1 BDSG Gesagte.
Abs. 2 (Register)	-	Streichen	Keine Entsprechung in DSGVO.
Abs. 3 (Auskunfts-recht)	Art. 58 Abs. 1 lit. a (ex Art. 53 Abs. 1 lit. a)	Modifizieren	§ 38 Abs. 3 BDSG entspricht tendenziell Art. 58 Abs. 1 lit. a (ex Art. 53 Abs. 1 lit. a) DSGVO, sieht jedoch angesichts des Hinweises auf eine „unverzüglich" zu erteilende Auskunft wohl eine Verschärfung vor, die von der Öffnungsklausel des Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO gedeckt ist.
Abs. 4 (Nachschau-rechte)	Art. 58 Abs. 1 lit. f und e (ex Art. 53 Abs. 1 lit. db und lit. da)	Ggf. beibe-halten	Die in § 38 Abs. 4 S. 1 BSDG geregelten Nachschaurechte sind von der Öffnungsklau-sel des Art. 58 Abs. 1 lit. f (ex Art. 53 Abs. 1 lit. db) DSGVO gedeckt und können so aufrechterhalten bleiben.
Abs. 5 (Anord-nungsbefug-nisse)	Art. 58 Abs. 2 lit. d und f (ex Art. 53 Abs. 1b lit. d und lit. e)	Modifizie-ren; (strei-chen bzw. Verweis auf DSGVO)	§ 38 Abs. 5 S. 1 und 2 BDSG entspricht weitgehend Art. 58 Abs. 2 lit. d und f (ex Art. 53 Abs. 1b lit. d und lit. e) DSGVO, wobei lit. f aber etwas abweichend explizit auch auf den Zeitraum verweist, innerhalb dessen die Anpassung durch die verantwortli-che Stelle zu erfolgen hat. Auch hier sollte also im Falle einer gewünschten Kohärenz wahrenden Wiederholung der Wortlaut der DSGVO übernommen werden.
Abs. 5 S. 3 (Abberu-fungsverla-gen des Daten-schutzbeauf-tragten)	Art. 58 Abs. 6 (ex Art. 53 Abs. 4)	Beibehalten	Die in § 38 Abs. 5 S. 3 BDSG vorgesehene Möglichkeit, die Abberufung des Daten-schutzbeauftragten zu verlangen, ist so nicht in der Datenschutz-Grundverordnung vorge-sehen, aber von der Öffnungsklausel des Art. 58 Abs. 6 (ex Art. 53 Abs. 4) DSGVO gedeckt.

§ 38a: Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen

§ 38a BDSG eröffnet die Möglichkeit für Zusammenschlüsse spezifischer datenverarbeitender Stellen, Verhaltensregeln zu entwerfen und diese sodann der zuständigen Aufsichtsbehörde zur Prüfung und Anerkennung vorzulegen (Abs. 1 und 2). Die Norm ist Ausdruck des Steuerungskonzepts regulierter Selbstregulierung. Unter dem Regime des BDSG ist sein sinnvoller und gerade für das Datenschutzrecht als dynamisches Rechtsgebiet prädestinierter Regelungsansatz im Grundsatz kaum gelebt worden.[585] Lediglich zwei Kodizes sind zur Anerkennung gelangt. Die Datenschutz-Grundverordnung will der Selbstregulierung im Datenschutz neues Leben einhauchen. Sie etabliert insbesondere das Instrument des Datenschutzsiegels. Daneben enthalten Art. 40 f. (ex Art. 38 f.) DSGVO detailreiche Vorschriften zu Verhaltensregeln und deren Genehmigung durch die Aufsichtsbehörden. Diese lassen für mitgliedstaatliche Regelungen kaum Spielraum übrig. Die Regelungskompetenz beschränkt sich auf die Akkreditierung von Zertifizierungsstellen im Sinne des Art. 43 Abs. 1 S. 2 (ex Art. 39a Abs. 1 S. 2) DSGVO, rechtfertigt aber keine mitgliedstaatliche Vollregelung.

§ 38a BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1	Art. 40 (ex Art. 38) und i. w. S. Art. 43 (ex Art. 39a)	Streichen	Zwar begründet Art. 40 Abs. 1 (ex Art. 38 Abs. 1) DSGVO eine Förderungsverpflichtung der Mitgliedstaaten. Diese erstreckt sich aber nicht darauf, von Art. 40 (ex Art. 38) DSGVO abweichende Regelungen zu erlassen. § 38a BDSG enthält auch keine Regelungen, die nicht schon die DSGVO etabliert. Im Gegenteil enthält Art. 40 (ex Art. 38) DSGVO eine detaillierte Regelung für Codes of Conduct. Es handelt sich um eine Vollharmonisierung.

[585] Dazu *Martini* (Fn. 439) ff.

Abs. 2	Art. 40 Abs. 5 (ex Art. 38 Abs. 2)	Streichen	Dito
Neue BDSG-Vorschrift	Art. 43 Abs. 1 i. V. m. Art. 42 (ex Art. 39a Abs. 1 S. 2 DSGVO i. V. m. Art. 39)	Bestimmung, wer die Zertifizierungsstellen akkreditiert (zuständige Aufsichtsbehörde und/oder nationale Akkreditierungsstelle oder nationale Akkreditierungsstelle auf der Grundlage des Akkreditierungsstellengesetzes)	Die Bestimmung der Zertifizierungsstellen legt die DSGVO in die Hände der Mitgliedstaaten (Art. 43 Abs. 1 S. 2 [ex Art. 39a Abs. 1 S. 2] DSGVO). Hinsichtlich der Voraussetzungen für die Akkreditierung und ihr Handeln enthält die DSGVO grundsätzlich eine Vollregelung, die nicht auf eine mitgliedstaatliche Konkretisierung angelegt ist.

§§ 39-42a: Sondervorschriften

§ 39: Zweckbindung bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen

§ 39 BDSG regelt die Zweckbindung für Fälle des Umgangs mit personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen.

Damit normiert § 39 BDSG speziell, was in Art. 5 Abs. 1 lit. b DSGVO als allgemeiner Verarbeitungsgrundsatz niedergelegt ist. Angesichts der Festlegung des Zweckbindungsgrundsatzes in Art. 5 Abs. 1 lit. b DSGVO für jeden Umgang mit personenbezogenen Daten muss § 39 BDSG nicht aufrechterhalten werden; Art. 5 Abs. 1 lit. b DSGVO sieht hierfür auch keine Öffnungsklausel vor. Erwägenswert ist lediglich, ob, unter Einhaltung des Wiederholungsverbots, eine Klarstellung in den entsprechenden im BDSG-neu aufrechterhaltenen Regelungen sinnvoll ist, um Klarheit für den Normanwender zu schaffen. Dies ist allerdings für die in Frage kommenden Normen jeweils gesondert zu prüfen.

§ 39 BDSG	Korrespondierende Norm in der DSGVO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1	Art. 5 Abs. 1 lit. b	Streichen	Zweckbindungsgrundsatz in Art. 5 Abs. 1 lit. b normiert, der keine Öffnungsklausel vorsieht.
Abs. 2	Art. 5 Abs. 1 lit. b	Streichen	Zweckbindungsgrundsatz in Art. 5 Abs. 1 lit. b normiert, der keine Öffnungsklausel vorsieht.

§ 40: Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

§ 40 BDSG konkretisiert, wie personenbezogene Daten durch Forschungseinrichtungen verarbeitet und genutzt werden dürfen, d. h. § 40 BDSG stellt keinen Zulässigkeitstatbestand dar. Ähnliche Bedingungen finden sich in Art. 89 (ex Art. 83) DSGVO. Zwar enthält Art. 89 Abs. 2, 3 (ex Art. 83 Abs. 2, 3) DSGVO eine Öffnungsklausel für die Mitgliedstaaten, jedoch gilt diese nur für die Beschränkung von Betroffenenrechten, nicht aber für eine Konkretisierung der Verarbeitungsbedingungen. § 40 Abs. 1 BDSG normiert den Zweckbindungsgrundsatz, der in der Datenschutz-Grundverordnung in Art. 5 Abs. 1 lit. b DSGVO niedergelegt ist, und für den keine Öffnungsklausel durch die Mitgliedstaaten vorgesehen ist. Ferner betrifft Art. 5 Abs. 1 lit. b Hs. 2 DSGVO gerade nicht die Fälle von § 40 Abs. 1 BDSG, da Art. 5 Abs. 1 lit. b Hs. 2 DSGVO eine Vereinbarkeit des ursprünglichen Zwecks für – unter anderem – die Verarbeitung zu wissenschaftlichen Forschungszwecken fingiert, und § 40 Abs. 1 BDSG eine Zweckbindung bestimmt, wenn bereits eine Erhebung und Speicherung für wissenschaftliche Zwecke stattgefunden hat. Eine Aufrechterhaltung ist deswegen nicht möglich, aber auch nicht nötig, um das bestehende Schutzniveau zu erhalten.

§ 40 Abs. 2 BDSG bestimmt eine Anonymisierungspflicht für zu wissenschaftlichen Forschungszwecken erhobene und gespeicherte personenbezogene Daten. Art. 89 Abs. 1 (ex Art. 83 Abs. 1) DSGVO bestimmt, dass die Verarbeitung für wissenschaftliche Forschungszwecke angemessenen Garantien für die Rechte und Freiheiten unterliegt. Dies ist zwar weniger konkret als § 40 Abs. 1 BDSG. Allerdings nennt Art. 89 Abs. 1 (ex Art. 83 Abs. 1)

DSGVO beispielhaft die Pseudonymisierung der personenbezogenen Daten als eine solche Garantie. Auch hier ist eine Aufrechterhaltung daher mangels Öffnungsklausel nicht möglich, aber auch nicht nötig.
Denkbar wäre jedoch, dass eine dem § 40 Abs. 1 BDSG ähnliche Regelung vom Umfang der Öffnungsklausel des Art. 9 Abs. 2 lit. j (ex Art. 9 Abs. 2 lit. i) DSGVO umfasst ist. Art. 9 Abs. 2 lit. j (ex Art. 9 Abs. 2 lit. i) DSGVO macht eine Ausnahme vom Verbot der Verarbeitung besonderer Arten personenbezogener Daten für – unter anderem – wissenschaftliche Forschungszwecke und enthält hierfür eine Öffnungsklausel für die Mitgliedstaaten; die Öffnungsklausel verlangt für die Verarbeitung besonderer Arten personenbezogener Daten zu wissenschaftlichen Forschungszwecken, dass das mitgliedstaatliche Gesetz angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der Betroffenen vorsieht. Anonymisierungspflichten könnten eine solche spezifische Maßnahme sein. Dies müsste allerdings nur in Bezug auf die Verarbeitung besonderer Arten personenbezogener Daten geregelt werden, und nicht wie in § 40 Abs. 1 BDSG in einer generellen Norm.
§ 40 Abs. 1 BDSG kann daher nicht aufrechterhalten werden.

§ 40 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	Art. 5 Abs. 1 lit. b	Streichen	Zweckbindungsgrundsatz in Art. 5 Abs. 1 lit. b normiert, der keine Öffnungsklausel vorsieht.
Abs. 2	Art. 89 Abs. 1 (ex Art. 83 Abs. 1)	Streichen	Von keiner Öffnungsklausel gedeckt.
Abs. 3 Nr. 1	Art. 89 Abs. 1 (ex Art. 83 Abs. 1), Art. 6 Abs. 1 UAbs. 1 lit. a, Art. 9 Abs. 2 lit. a	Streichen	Von keiner Öffnungsklausel gedeckt und als allgemeiner Grundsatz in der DSGVO enthalten.

Abs. 3 Nr. 2	Art. 85 Abs. 2	u. U. beibehalten möglich	Die Aufrechterhaltung der Norm lässt sich auf Art. 85 Abs. 2 DSGVO stützen, wenn man den Begriff der Informationsfreiheit auch dahin gehend auslegt, dass sie auch eine Veröffentlichung von wissenschaftlichen Forschungsergebnissen deckt.

§ 41: Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Medien

§ 41 BDSG setzt, zusammen mit § 47 RStV sowie den jeweiligen Ländervorschriften, die Vorgaben des Art. 85 (ex Art. 80) DSGVO bereits um, allerdings nicht vollständig, sondern nur bezogen auf die Medien und nicht allgemein auf die Meinungsfreiheit. Insoweit ist eine Ergänzung zu überlegen.

§ 41 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1	Art. 85 (ex Art. 80)	Beibehalten/Ergänzen	§ 41 BDSG erfasst den Regelungsauftrag des Art. 85 Abs. 1 (ex Art. 80 Abs. 1) DSGVO teilweise.
Abs. 2	Art. 85 Abs. 1 (ex Art. 80 Abs. 1)	Beibehalten	Setzt die Vorgaben des Art. 85 Abs. 1 (ex Art. 80 Abs. 1) DSGVO um.
Abs. 3 S. 1	Art. 15	Beibehalten möglich	Dient als Grundlage für § 41 Abs. 3 S. 2 BDSG und ist daher erforderlich.
Abs. 3 S. 2	Art. 85 Abs. 2 (ex 80 Abs. 2)	Beibehalten möglich	Setzt Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO um.
Abs. 3 S. 3 i. V. m. § 20 Abs. 1	Art. 16	Modifizieren	Die Regelung muss an Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO angepasst werden, um die Vorgaben der DSGVO zu konkretisieren. Bislang sind noch keine derartigen Ausnahmen vorgesehen.
Abs. 4	Art. 85 Abs. 2 (ex Art. 80 Abs. 2)	Beibehalten	Die Vorschrift setzt Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO um.

§ 42: Datenschutzbeauftragter der Deutschen Welle

Die Sondervorschrift des § 42 BDSG regelt eigens die Datenschutzkontrolle bei der Rundfunkanstalt des Bundes. Dessen Datenschutzbeauftragter tritt gem. § 42 Abs. 1 S. 1 an die Stelle des Bundesdatenschutzbeauftragten (vgl. § 21). Er wird für vier Jahre durch den Verwaltungsrat der Deutschen Welle gewählt. Die Abs. 2 bis 4 regeln Aufgaben und Status, Abs. 5 eröffnet der Deutschen Welle eine bereichsspezifische eigene Regelungskompetenz.

a. Eigener Beauftragter für den Datenschutz, § 42 Abs. 1 S. 1 BDSG

Die Pflicht zur Bestellung eines eigenen (rundfunkinternen) Datenschutzbeauftragten kann wegen Art. 37 Abs. 1 (ex Art. 35 Abs. 1) und Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO bestehen bleiben. Die Verpflichtung zur Bestellung eines Datenschutzbeauftragten ist nicht zuletzt Ausdruck der Staatsferne der Rundfunkanstalt.[586]

Die Ausgliederung der Deutschen Welle aus dem für die öffentlichen Stellen des Bundes etablierten System der Datenschutzaufsicht ist mit der Datenschutz-Grundverordnung vereinbar. Diese Sonderstellung ist aufgrund der aus der Rundfunkfreiheit (Art. 5 Abs. 1 S. 2 GG) resultierenden Staatsferne der Bundesrundfunkanstalt auch für den Bereich des Datenschutzes gerechtfertigt.[587] Art. 37 Abs. 1 (ex Art. 35 Abs. 1), 85 Abs. 2 sowie EG 153 S. 2 (ex EG 121 S. 2) DSGVO tragen dem Rechnung. Art. 85 Abs. 2 (ex Art. 80 Abs. 2) DSGVO gestattet ausdrücklich Sonderregelungen für den Bereich journalistischer Zwecke auch im Hinblick auf die Wahrnehmung der Aufsicht („Abweichungen oder Ausnahmen von den Bestimmungen (…) des Kap. 6 (unabhängige Aufsichtsbehörden)"), sodass die mit der Verpflichtung einhergehenden Vorschriften ebenfalls beibehalten werden können.

Jedoch sollte die Terminologie des BDSG an die der Datenschutz-Grundverordnung angepasst werden: Gegenüber „bestellen" in § 42 Abs. 1 S. 1 BDSG ist „bestimmen" (vgl. z. B. Art. 51 Abs. 3 [ex Art. 46 Abs. 2] DSGVO) oder „benennen" (vgl. z. B. Art. 70 Abs. 3 [ex Art. 64 Abs. 3] DSGVO) vorzugswürdig.

---

[586] Vgl. *Gola/Klug/Körffer*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 42, Rn. 1.
[587] *Gola/Klug/Körffer* (Fn. 586), § 42, Rn. 1.

b. Modus der Bestellung, § 42 Abs. 1 S. 2 BDSG

Auch der Modus der Bestellung ist mit dem Gedanken des Art. 54 Abs. 1 (ex 48 Abs. 1) DSGVO vereinbar. Ebenso ist die Amtszeit von vier Jahren (Art. 54 Abs. 1 lit. d [ex Art. 49 Abs. 1 lit. d] DSGVO) sowie die Möglichkeit der Wiederbestellung (Art. 54 Abs. 1 lit. e [ex Art. 49 Abs. 1 lit. e] DSGVO) zulässig.

c. Keine Unvereinbarkeit mit anderen Aufgaben, § 42 Abs. 1 S. 3 BDSG

Nach Art. 52 Abs. 3 (ex Art. 47 Abs. 3) DSGVO dürfen Mitglieder der Aufsichtsbehörde keine mit dem Amt nicht zu vereinbarende Tätigkeit ausüben. Die Wahrnehmung von anderen Aufgaben innerhalb der Deutschen Welle ist damit grundsätzlich in Einklang zu bringen. Im Zweifelsfall (wie z. B. der gleichzeitigen Leitung des Archivs) ist eine verordnungskonforme Auslegung angezeigt.

d. Aufgaben, § 42 Abs. 2 S. 1 BDSG

Die Aufgabenzuweisung deckt sich mit Art. 57 Abs. 1 lit. a und v (ex Art. 52 Abs. 1 lit. a und lit. k) DSGVO. Insofern liegt jedoch eine grundsätzlich zu streichende Normwiederholung vor.

e. Unabhängigkeit, § 42 Abs. 2 S. 2, 3 BDSG

Die Regelung zur Unabhängigkeit (§ 42 Abs. 2 S. 2 BDSG) ist als Normwiederholung grundsätzlich zu streichen, kann aber im Rahmen einer einheitlichen Regelung als zulässige Wiederholung sinnvoll sein. Die Regelung zur Dienst- und Rechtsaufsicht im Übrigen kann bestehen bleiben und ist wegen der Möglichkeit der Übernahme von sonstigen Aufgaben mit der Datenschutz-Grundverordnung vereinbar.

f. Jedermann-Anrufungsrecht, § 42 Abs. 3 BDSG

Das Beschwerderecht aus § 42 Abs. 3 i. V. m. § 21 S. 1 BDSG entspricht Art. 77 Abs. 1 (ex Art. 73 Abs. 1) DSGVO (vgl. auch EG 141 [ex EG 111] DSGVO). In entsprechender Anwendung des § 21 S. 1 BDSG steht das Recht aus § 42 Abs. 3 BDSG nach dem Wortlaut aber nur dem Betroffenen zu, der

sich in seinen Rechten verletzt sieht. Gleichwohl kann der Datenschutzbeauftragte auch Beanstandungen Dritter nachgehen.[588] Das folgt aus seiner Unabhängigkeit (vgl. § 42 Abs. 2 S. 2 BDSG, damit korrespondierend Art. 52 Abs. 1 [ex Art. 47 Abs. 1] DSGVO). Insofern ergibt sich im Hinblick auf Art. 77 Abs. 1 (ex Art. 73 Abs. 1) DSGVO kein Regelungsbedarf. Ein entsprechender Verweis in § 42 Abs. 3 BDSG kann aus Gründen der Klarstellung aber sinnvoll sein.

g. Tätigkeitsbericht, § 42 Abs. 4 S. 1, 3 BDSG

Der Zweijahresturnus ist mit Art. 59 S. 1 (ex Art. 54 S. 1) DSGVO, der einen Einjahresturnus vorsieht, nicht zu vereinbaren. Für einen längeren Turnus streiten keinerlei Interessen der Meinungsäußerung und der Informationsfreiheit (vgl. Art. 85 Abs. 2 [ex Art. 80 Abs. 2] DSGVO). Die journalistische Arbeit wird nicht übergebührlich behindert. Die Regelung ist zu streichen oder als Klarstellung anzupassen und beizubehalten.
Die Regelung sub specie der Adressaten, also den Organen der Deutschen Welle, sowie die Übermittlung an den BfDI, sind mit der Datenschutz-Grundverordnung vereinbar. Insoweit liegt zwar eine Abweichung von Art. 59 S. 2 und 3 (ex Art. 54 S. 2 und 3) DSGVO vor. Beide sind jedoch gerechtfertigt. Einerseits ist der Bericht nicht wie in Art. 59 S. 2 (ex Art. 54 S. 2) DSGVO vorgesehen dem Parlament und der Regierung zu übermitteln. Dies findet seine Rechtfertigung jedoch in dem Ziel, die Unabhängigkeit der Presse in besonderer Weise zu schützen. Insoweit fehlt es insbesondere der Bundesregierung und dem Bundestag auch an (politischen wie rechtlichen) Einflussmöglichkeiten auf die Deutsche Welle, von denen sie als Reaktion auf Verstöße gegen Datenschutzvorschriften Gebrauch machen könnten. Andererseits ist der Bericht auch nicht – wie es Art. 59 S. 3 (ex Art. 54 S. 3) DSGVO vorsieht – der Öffentlichkeit, der Kommission und dem EDA zugänglich zu machen. Auch dies ist der Unabhängigkeit der Presse und hier gleichzeitig einem verminderten Abstimmungsbedarf der Tätigkeit mit den europäischen Einrichtungen geschuldet und ist insoweit gerechtfertigt.
Die Pflicht zur Übermittlung an den BfDI ist hingegen bereits von der Öffnungsklausel des Art. 59 S. 2 (ex Art. 54 S. 2) DSGVO gedeckt und deshalb

[588] *Gola/Klug/Körffer* (Fn. 586), § 42, Rn. 6.

zulässig. Die BfDI ist eine „andere Behörde“ (vgl. § 22 Abs. 5 S. 1 BDSG) im Sinne dieser Vorschrift.

p. Erstattung besonderer Berichte, § 42 Abs. 4 S. 2 BDSG

Die Pflicht zur Erstattung besonderer Berichte ist mit der Datenschutz-Grundordnung vereinbar. Diese kennt selbst die Pflicht von Aufsichtsbehörden, auf Antrag bestimmter Stellen Stellungnahmen abzugeben (Art. 58 Abs. 3 lit. b [ex Art. 53 Abs. 1c lit. aa] DSGVO). Eine Berichtspflicht ist ihr deshalb nicht wesensfremd. Dass antragsberechtigt insoweit nur Organe des Selbstverwaltungsträgers sind, ist wiederum wegen der Unabhängigkeit der Presse als Ausnahme gerechtfertigt.

q. Ermächtigung der Deutschen Welle zur Regelung im Wege der Selbstverwaltung, § 42 Abs. 5 S. 1 BDSG

Die Übertragung von Regelungsbefugnissen an die Deutsche Welle ist mit der Datenschutz-Grundverordnung vereinbar, da diese nicht in die mitgliedstaatliche Kompetenzordnung eingreift (vgl. Art. 51 Abs. 3 [ex Art. 46 Abs. 2] DSGVO). Die durch die Deutsche Welle (im Rahmen der angepassten §§ 23 bis 26 BDSG) getroffenen Regelungen müssen dann aber selbst mit der Datenschutz-Grundverordnung vereinbar sein. Die Deutsche Welle ist unmittelbar Verpflichtete.

§ 42 BDSG	Korrespondierende Norm in der DSG-VO	Gesetzgeberische Handlungsoption	Begründung
Abs. 1-4	Art. 37 (ex Art. 35), Art. 85 Abs. 2 (ex Art. 80 Abs. 2)	Beibehalten in Teilen möglich	Deutschland kommt damit auch dem Regelungsauftrag nach, den die DSG-VO ihm auferlegt. Die bestehenden Regelungen bedürfen nicht aus unionsrechtlichen Gründen einer Anpassung.
Abs. 5 S. 1	Art. 37 (ex Art. 35), Art. 85 Abs. 2 (ex 80 Abs. 2)	Beibehalten möglich	Räumt die DSGVO den Mitgliedstaaten Regelungsautonomie zur konkreten Ausgestaltung der Position des Datenschutzbeauftragten öffentlicher Stellen ein, dürfen sie auch in Teilen – wie hier – der öffentlichen Stelle Rege-

			lungsautonomie einräumen, soweit dadurch die Zielsetzungen des Art. 85 (ex Art. 80), die freie Meinungsäußerung und den Persönlichkeitsschutz in Einklang zu bringen, befördert werden.
Abs. 5 S. 2	Art. 37 (ex Art. 35)	Dito	Der Verweis auf die allgemeinen Regelungen zum Datenschutzbeauftragten, die auch nach Inkrafttreten der DSGVO teilweise bestehen bleiben können, ist vom nationalen Regelungsspielraum gedeckt.

§ 42a: Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Art. 33 und 34 (ex Art. 31 und 32) DSGVO regeln umfassende Informations- und Meldepflichten des Verantwortlichen bei der Verletzung des Schutzes personenbezogener Daten. Die Datenschutz-Grundverordnung belässt nach ihrem Inkrafttreten für die bisherige Regelung des § 42a BDSG keinen Regelungsspielraum.

§ 42a BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
S. 1	Art. 33 Abs. 1; Art. 34 Abs. 1 (ex Art. 31 Abs. 1; Art. 32 Abs. 1)	Streichen	Die DSGVO unterscheidet bei Verletzungen des Schutzes personenbezogener Daten zwischen der Meldepflicht gegenüber der Aufsichtsbehörde (Art. 33 [ex Art. 31] DSGVO) und der Benachrichtigungspflicht gegenüber den Betroffenen (Art. 34 [ex Art. 32] DSGVO). Die Meldepflicht beschränkt sich nicht auf die Datenschutzverstöße bei *bestimmten* personenbezogenen Daten (§ 42a S. 1 Nr. 1-4 BDSG), sondern die Verpflichtung besteht ohne Rücksicht auf die Art der Daten. Eine Ausnahme von der Meldepflicht besteht nur, wenn die „Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt“, Art. 33 Abs. 1 S. 1 a. E. [ex

			Art. 31 Abs. 1 S. 1 a. E.] DSGVO. Daneben heben Art. 33 f. [ex Art. 31 f.] DSGVO auch nicht auf die unrechtmäßige Übermittlung oder sonstige unrechtmäßige Kenntniserlangung Dritter ab, sondern verlangen lediglich einen Verstoß gegen den Schutz personenbezogener Daten. Das Unionsrecht regelt den Inhalt der Informationspflichten umfänglich, ohne eine Öffnungsklausel für das nationale Recht vorzusehen. Für eine ergänzende nationale Regelung in § 42a S. 1 BDSG lässt die DSGVO keinen Raum mehr.
S. 2	Art. 33 Abs. 1 S. 1 (ex Art. 31 Abs. 1 S. 1)	Streichen	§ 42a S. 2 BDSG fordert eine unverzügliche Meldung an die Aufsichtsbehörde. Ganz ähnlich untersagt Art. 33 Abs. 1 S. 1 (ex Art. 31 Abs. 1 S. 1) DSGVO eine unangemessene Verzögerung nach Kenntnisnahme, wobei die Information „möglichst binnen höchstens 72 Stunden“ erfolgt. Damit verdrängt das Unionsrecht kraft seines Anwendungsvorrangs § 42a S. 2 BDSG, ohne dass ein nationaler Regelungsspielraum verbliebe. Die Vorschrift muss demnach gestrichen werden.
S. 3	Art. 34 Abs. 2 i. V. m. Art. 33 Abs. 3 lit. b, c und d (ex Art. 32 Abs. 2 i. V. m. Art. 31 Abs. 3 lit. b, d und e)	Streichen	Art. 34 Abs. 2 (ex Art. 32 Abs. 2) DSGVO verpflichtet den Verantwortlichen, Betroffene verständlich und klar über die Art der Verletzung zu unterrichten und Empfehlungen gemäß Art. 33 Abs. 1 lit. d (ex Art. 31 Abs. 3 lit. e) zur Behebung der Verletzung bzw. zur Eindämmung deren Folgen abzugeben. Dies wiederholt – wenn auch in anderen Worten – § 42a S. 3 BDSG. Mangels nationalstaatlicher Öffnungsklausel ist Vorschrift im BDSG zu streichen.
S. 4	Art. 33 Abs. 3 lit. c, d Hs. 1 (ex Art. 31 Abs. 3 lit. d, e Hs. 1)	Streichen	Gemäß § 42a S. 4 BDSG hat der Verantwortliche mögliche nachteilige Folgen der Verletzung und dagegen ergriffene Maßnahmen der Aufsichtsbehörde mitzuteilen. Dies entspricht der Verpflichtung des Art. 33 Abs. 3 lit. c, d Hs. 1 (Art. 31 Abs. 3 lit. d, e Hs. 1) DSGVO. Mangels Öffnungsklausel besteht kein natio-

			naler Regelungsspielraum. Die Bestimmung ist daher zu streichen.
S. 5	Art. 34 Abs. 3 lit. c (ex Art. 32 Abs. 3 lit. c)	Streichen	Art. 34 Abs. 3 lit. c (ex Art. 32 Abs. 3 lit. c) DSGVO verlangt keine Benachrichtigung, wenn diese einen unverhältnismäßigen Aufwand zu Folge hätte; stattdessen muss die Verletzung dann öffentlich bekannt gemacht werden. Ganz ähnlich verpflichtet § 42a S. 5 BDSG zur öffentlichen Bekanntmachung auf eine wirksame, geeignete Weise, etwa durch Anzeigen in mindestens zwei bundesweit erscheinenden Tageszeitungen. Auch wenn dies als eine sachgerechte Konkretisierung der unionalen Pflicht erscheinen mag, besteht mangels Öffnungsklausel – wie auch in den anderen Fällen des § 42a BDSG – kein Regelungsspielraum.
S. 6	i. w. S. Art. 83 Abs. 2 lit. h (ex Art. 79 Abs. 2a lit. h)	Streichen bzw. modifizieren	Eine Benachrichtigung darf gegen den zur Mitteilung Verpflichteten nur mit dessen Zustimmung in Strafverfahren oder Ordnungswidrigkeitenverfahren verwendet werden (§ 42a S. 6 BDSG). Das Substrat für diese Regelung fällt mit der Streichung der anderen Vorschriften des § 42a BDSG weg. Für die unionsrechtliche Meldepflicht auf der Grundlage des Art. 33 und 34 (ex Art. 31 und 32) DSGVO enthält die DSGVO keine Regelung eines Verwertungsverbotes. Es findet sich lediglich Art. 83 Abs. 2 lit. h (ex Art. 79 Abs. 2a lit. h) DSGVO, wonach die Umstände des Bekanntwerdens der Verletzung, insbesondere ob der Verantwortliche bzw. Auftragsverarbeiter den Verstoß mitgeteilt hat, im Rahmen der Bemessung der Geldbuße zu berücksichtigen sind. Das spricht dafür, dem Mitgliedstaat einen Regelungsspielraum abzusprechen. Anderes ist dann denkbar, wenn man die gerichtliche Verwertung von Informationen als Teil der originären mitgliedstaatlichen Regelungsautonomie versteht, auf die sich die

			DSGVO a priori nicht erstreckt. Allerdings erhebt die DSGVO gerade den Anspruch, das Sanktionsregime grundsätzlich abschließend mit zu erfassen.

§§ 43 - 44: Schlussvorschriften

Der 5. Abschnitt des BDSG regelt im Interesse wirksamer Sicherung der Persönlichkeit vor datenschutzrechtlichen Pflichtverletzungen Bußgeld- und darauf aufbauende Strafvorschriften. Sofern andere datenschutzrechtliche Regelungen kein eigenes Sanktionsregime enthalten, waren die Vorschriften des § 43 und 44 BDSG bislang – vorbehaltlich § 1 Abs. 3, 4, 5 – anwendbar.[589]
Die Datenschutz-Grundverordnung enthält nunmehr für diesen Bereich unmittelbar geltende Vorgaben, welche für einen großen Teil der bisherigen Bestimmungen keinen Spielraum mehr belässt. Ein solcher Spielraum kann sich künftig lediglich in dem Umfang des Art. 83 Abs. 7 DSGVO sowie des Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO ergeben.
Besonders zu beachten ist jeweils die *Meldepflicht* der Mitgliedstaaten nach Art. 83 Abs. 9 S. 3 DSGVO und Art. 84 Abs. 2 (ex Art. 79b Abs. 3) DSGVO. Ihr müssen die Mitgliedstaaten bis zum Inkrafttreten der Datenschutz-Grundverordnung nachkommen.

§ 43: Bußgeldvorschriften

§ 43 Abs. 1 BDSG sanktioniert überwiegend formelle Pflichtverstöße, Abs. 2 materielle Datenschutzverstöße und damit Verstöße gegen das Verbot mit Erlaubnisvorbehalt (§ 4 Abs. 1). Erfasst ist jeweils vorsätzliches und fahrlässiges Handeln.
Art. 83 (ex Art. 79) DSGVO legt konkret fest, wann Geldbußen verhängt werden können. § 43 BDSG ist damit grundsätzlich nicht mehr vonnöten und verstößt gegen das Wiederholungsverbot. Anders verhält sich dies lediglich insoweit, wie der deutsche Gesetzgeber von der Öffnungsklausel des Art. 83

[589] *Ehmann* (Fn. 406), § 43, Rn. 18 f.

Abs. 7 (ex Art. 79 Abs. 3b) DSGVO (Befugnis des Mitgliedstaates, gegen Behörden und öffentliche Stellen, die in dem betreffenden Mitgliedstaat niedergelassen sind, Geldbußen zu verhängen) Gebrauch macht. Außerhalb dieser Öffnungsklausel darf der deutsche Gesetzgeber – auch nicht gestützt auf Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO – grundsätzlich keine weiteren Tatbestände vorsehen, die es erlauben, Geldbußen zu verhängen. Gleiches gilt im Hinblick auf den Regelungsauftrag der Union, „angemessene Verfahrensgarantien (…) einschließlich wirksamer gerichtlicher Rechtsbehelfe und ordnungsgemäßer Verfahren" vorzusehen (Art. 83 Abs. 8 DSGVO, der aber keine Befugnis zum Erlass neuer Bußgeldtatbestände impliziert). Eine Ausnahme gilt lediglich für diejenigen Bereiche, in denen dem Mitgliedstaat aufgrund einer in der Datenschutz-Grundverordnung enthaltenen Öffnungsklausel ein eigener Regelungsspielraum zukommt. Dieser Bereich wird durch Art. 83 (ex Art. 79) DSGVO nicht harmonisiert, sodass der mitgliedstaatliche Gesetzgeber, gestützt auf Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO, selbst Bußgeldtatbestände schaffen darf.[590]

Aus Gründen der Rechtssicherheit sollte der deutsche Gesetzgeber mit Blick auf seinen Regelungsauftrag aus Art. 83 Abs. 8 DSGVO aber im neuen BDSG einen Verweis auf die Geltung des OWiG aufnehmen, um sicherzustellen, dass auf die Verhängung von Geldbußen nach Art. 83 DSGVO das verfahrensrechtliche Rechtsregime Anwendung findet.

§ 44: Strafvorschriften

§ 44 BDSG regelt an § 43 Abs. 2 BDSG anknüpfende Straftatbestände, die gegenüber den bereichsspezifischen Strafnormen zum Schutz vor Persönlichkeitsverletzungen (z. B. §§ 201a, 203 StGB) subsidiär verfolgbar sind.[591] Einen Straftatbestand im Sinne dieser Norm erfüllt, wer eine vorsätzliche Ordnungswidrigkeit nach § 43 Abs. 2 BDSG gegen Entgelt oder mit Bereicherungs- oder Schädigungsabsicht begeht (Abs. 1). Die Tat wird nur auf Antrag verfolgt. Den Kreis der Antragsberechtigten erweitert § 44 Abs. 2

[590] Ausführlicher hierzu oben auf S. 281 f.

[591] *Holländer*, in: Wolff/Brink (Hrsg.), Datenschutzrecht in Bund und Ländern, 2013, § 44 BDSG, Rn. 18.

BDSG gegenüber § 77 StGB (Abs. 2). Im Übrigen finden die Vorschriften des allgemeinen Teils des StGB ergänzend Anwendung. Dadurch ist auch eine Begehung durch pflichtwidriges Unterlassen (§ 13 StGB) möglich.[592] Der Versuch eines Verstoßes gegen § 43 Abs. 2 BDSG ist nicht strafbar, denn die Straftaten gemäß § 44 BDSG stellen keine Verbrechen dar (vgl. §§ 12, 23 Abs. 1 StGB).

Verurteilungen gem. § 44 BDSG waren wegen der hohen tatbestandlichen Anforderungen der Strafvorschrift bisher selten.[593] Auch die Ahndung von Datenschutzverstößen mit den Instrumenten des Strafrechts rückt jedoch zunehmend ins Zentrum der öffentlichen Aufmerksamkeit; Betroffene wenden sich immer öfter an die Aufsichtsbehörden für Datenschutz. Die Datenschutz-Grundverordnung hat auch aus diesem Grunde den Sanktionsrahmen ausgeweitet und will mit seinen Regelungen in Art. 83 und 84 (ex Art. 79 und 79b) DGSVO zu einem wirksamen Datenschutz beitragen.

Die Vorschrift des § 44 Abs. 1 BDSG hat auf der Grundlage des nationalen Rechtsrahmens den Regelungsspielraum ausgefüllt, für den Art. 84 (ex Art. 79b) DSGVO nunmehr lediglich eingeschränkt Raum lässt. Art. 84 (ex Art. 79b) DSVGO lässt diese Freiheit namentlich nur für solche Tatbestände, die nicht bereits auf der Grundlage des Art. 83 (ex Art. 79) DSGVO unmittelbar unionsrechtlich harmonisiert sind. Insbesondere bedürfen die Bußgeldtatbestände des Art. 83 (ex Art. 79) DSGVO nach Inkrafttreten der Datenschutz-Grundverordnung keiner ergänzenden Regelung im nationalen Recht. Dies verstieße gegen das Wiederholungsverbot.[594] Die Norm des § 44 Abs. 1 BDSG bedarf insoweit der Anpassung. Die Mitgliedstaaten dürfen aber „beispielsweise bei schweren Verstößen gegen diese Verordnung“ strafrechtliche Sanktionen verhängen (EG 152 S. 1 [ex 120a S. 1] DSGVO), soweit die Datenschutz-Grundverordnung keine Vollharmonisierung vorgenommen hat. Belegt die Datenschutz-Grundverordnung einen Verstoß mit einer in der Höhe begrenzten Geldbuße, darf der Mitgliedstaat darüber nicht hinausgehen – wohl auch nicht, indem er aus einem Bußgeldtatbestand einen Straftatbestand für besonders schwere Verstöße macht. Denn sonst könnte er die Harmonisie-

[592] *Ehmann*, in: Simitis (Hrsg.), BDSG, 8. Aufl., 2014, § 44, Rn. 3.
[593] Erklärungsversuch bei *Ehmann* (Fn. 592), § 44, Rn. 4 m. w. N.
[594] Dazu im Einzelnen S. 274 ff.

rungsbestrebungen der Datenschutz-Grundverordnung (vgl. EG 13 S. 1 [ex EG 11 S. 1] DSGVO: „gleichwertige Sanktionen in allen Mitgliedstaaten") leichter Hand umgehen. Straftatbestände kommen daher grundsätzlich nur für solche Verstöße gegen Tatbestände der Datenschutz-Grundverordnung oder des nationalen (auf der Grundlage von Öffnungsklauseln erlassenen) Datenschutzrechts in Betracht, welche nicht die Datenschutzgrundverordnung selbst mit einem Bußgeldtatbestand belegt.[595]

§ 44 BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
Abs. 1 (Strafbarkeit der qualifizierten Begehung einer Bußgeldtat i. S. d. § 43 Abs. 2	Art. 84 (ex Art. 79b), EG 149, 152 (ex EG 119, 120a)	Überwiegend streichen, teilweise in modifizierter Form aufrechterhalten	Straftatbestände kommen nur für solche Verstöße gegen Tatbestände der Datenschutz-Grundverordnung oder des nationalen (auf der Grundlage von Öffnungsklauseln erlassenen) Datenschutzrechts in Betracht, welche nicht die Datenschutz-Grundverordnung selbst mit einem Bußgeldtatbestand belegt.
Abs. 2 S. 1 (Strafantragserfordernis)	Art. 84 (ex Art. 79b), EG 149, 152 (ex EG 119, 120a)	Beibehalten möglich	Soweit der nationale Regelungsspielraum aufgrund Art. 83 Abs. 7 (ex Art. 79 Abs. 3b) DSGVO und Art. 84 (ex Art. 79b) DSGVO reicht, darf der nationale Gesetzgeber davon durch ein Strafantragserfordernis Gebrauch machen. Es ist zudem Ausdruck des Verhältnismäßigkeitsprinzips, das auch Art. 84 Abs. 1 S. 2 (ex Art. 79b Abs. 1 S. 2) DSGVO und Art. 83 Abs. 1 (ex Art. 79 Abs. 1a)

[595] Vgl. auch den Wortlaut des Art. 84 Abs. 1 (ex Art. 79b Abs. 1) DSGVO: „*insbesondere* für Verstöße, die keiner Geldbuße gemäß Artikel 83 unterliegen" (Hervorhebung durch die Verfasser).

			DSGVO festschreiben.
Abs. 2 S. 2 (Antragsberechtigung)	Art. 84 (ex Art. 79b)	Dito	Dito

§§ 45 – 48: Übergangsvorschriften

Die §§ 45 – 48 BDSG normieren Übergangsvorschriften, die allesamt inzwischen überholt sind und durch Nachfolgevorschriften ersetzt werden müssen.

BDSG	**Korrespondierende Norm in der DSGVO**	**Gesetzgeberische Handlungsoption**	**Begründung**
§ 45	-	Streichen	Die in der Vorschrift genannten Fristen sind abgelaufen.
§ 46 (Weitergeltung von Begriffsbestimmungen)	-	Streichen / Modifizieren	Für bereichsspezifische Gesetze kann diese Regelung durchaus noch relevant sein. Die Norm könnte jedoch auch gestrichen werden, um den Anpassungsdruck auf den bereichsspezifischen Gesetzgeber zu erhöhen, zumal Begriffsverständnisse im Rahmen der Anwendung jener Normen ohnehin im Rahmen der genetischen Auslegung berücksichtigt werden können. Das spricht auch gegen eine entsprechende Nachfolgeregelung mit Blick auf die terminologische Anpassung des § 3 BDSG (siehe dort).
§ 47 (Übergangsregelung)	-	Streichen	Die in der Vorschrift genannten Fristen sind abgelaufen.
§ 48 (Bericht der Bundesregierung)	-	Streichen	Dito

Literaturverzeichnis

Anonymous, Data Protection Authorities, http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm (5.2.2016).

Ashkar, Daniel, Durchsetzung und Sanktionierung des Datenschutzrechts nach den Entwürfen der Datenschutz-Grundverordnung, DuD 2015, S. 796–800.

Auernhammer, Herbert (Hrsg.), BDSG, 4. Aufl., Köln, 2014.

Bäcker, Matthias/*Hornung*, Gerrit, EU-Richtlinie für die Datenverarbeitung bei Polizei und Justiz in Europa, Einfluss des Kommissionsentwurfs auf das nationale Strafprozess- und Polizeirecht, ZD 2012, S. 147–152.

Bloehs, Joachim/*Frank*, Torben (Hrsg.), Akkreditierungsrecht, VO (EG) Nr. 765/2008, Akkreditierungsstellengesetz, Verordnung über die Beleihung der Akkreditierungsstelle nach dem Akkreditierungsstellengesetz, Kostenverordnung der Akkreditierungsstelle, Verordnung zur Gestaltung und Verwendung des Akkreditierungssymbols der Akkreditierungsstelle, Kommentar, München, 2015.

Born, Tobias, Die Datenschutzaufsicht und ihre Verwaltungstätigkeit im nicht-öffentlichen Bereich, Frankfurt am Main, 2014.

Braun Binder, Nadja, Elektronische Bekanntgabe von Verwaltungsakten über Behördenportale, NVwZ 2016, S. 342–347.

Breuer, Marten, Auslandswirkung von Hoheitsakten, in: Schöbener, Burkhard (Hrsg.), Völkerrecht, Lexikon zentraler Begriffe und Themen, Heidelberg, 2014.

Bruns, Alexander, Informationsansprüche gegen Medien, Tübingen, 1997.

Calliess, Christian/*Ruffert*, Matthias (Hrsg.), Das Verfassungsrecht der Europäischen Union mit Europäischer GRundrechtecharta, Kommentar, 4. Aufl., München, 2011.

Dammann, Ulrich/*Simitis*, Spiros, EG-Datenschutzrichtlinie, Kommentar, Baden-Baden, 1997.

Dörr, Dieter/*Schiedermair*, Stephanie, Rundfunk und Datenschutz, Die Stellung des Datenschutzbeauftragten des Norddeutschen Rundfunks, 2002, http://www.ndr.de/der_ndr/unternehmen/organisation/studie16.pdf (5.2.2016).

Ehmann, Eugen/*Helfrich*, Marcus, EG-Datenschutzrichtlinie, Kurzkommentar, Köln, 1999.

Epping, Volker/*Hillgruber*, Christian (Hrsg.), Beck'scher Online-Kommentar GG, 27. Ed., 2015.

Fechner, Frank, Medienrecht, 15. Aufl., Tübingen, 2014.

Funke, Andreas, Der Anwendungsvorrang des Gemeinschaftsrechts, Einige Problemfälle und ein Präzisierungsvorschlag, DÖV 2007, S. 733–740.

Gerhard, Thorsten, Vereinbarkeit einer Verbandsklage im Datenschutzrecht mit Unionsrecht, Grundsätzliche Fragen zur Rechtmäßigkeit des UKlaG-E v. 4.2.2015 (BT-Drucks. 18/4631) aus Sicht des EU-Rechts, CR 2015, S. 338–344.

Gola, Peter/*Klug*, Christoph, Grundzüge des Datenschutzrechts, München, 2003.

Gola, Peter/*Piltz*, Carlo, Die Datenschutz-Haftung nach geltendem und zukünftigem Recht - ein vergleichender Ausblick auf Art. 77 DS-GVO, RDV 2015, S. 279–285.

Gola, Peter/*Schomerus*, Rudolf (Hrsg.), BDSG, 12. Aufl., München, 2015.

Gola, Peter/*Wronka*, Georg, Datenschutzrecht im Fluss, RDV 2015, S. 3–10.

Grabitz, Eberhard/*Hilf*, Meinhard (Hrsg.), Das Recht der Europäischen Union, Verbraucher- und Datenschutzrecht, 57. Erg.-Lfg., München, 2015.

Gröpl, Christoph, Die Reform der Medienkontrolle durch den Zehnten Rundfunkänderungsstaatsvertrag, Anforderungen an eine vertragsgemäße Umsetzung durch die Landesmedienanstalten, ZUM 2009, S. 21–29.

Hahn, Werner/*Vesting*, Thomas (Hrsg.), Beck'scher Kommentar zum Rundfunkrecht, Rundfunkstaatsvertrag, Rundfunkgebührenstaatsvertrag, Rundfunkfinanzierungsstaatsvertrag, Jugendmedienschutzstaatsvertrag, 3. Aufl., München, 2012.

Härting, Niko, Starke Behörden, schwaches Recht - der neue EU-Datenschutzentwurf, BB 2012, S. 459–466.

– Datenschutz-Grundverordnung, Anwendungsbereich, Verbotsprinzip, Einwilligung, ITRB 2016, S. 36–40.

Herzog, Roman, § 59 Zusammensetzung und Verfahren des Bundesrates, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, 3. Aufl., Heidelberg, 2005.

Herzog, Stephanie, Der digitale Nachlass – ein bisher kaum gesehenes und häufig missverstandenes Problem, NJW 2013, S. 3745–3751.

Hill, Hermann/*Martini*, Mario/*Wagner*, Edgar (Hrsg.), Facebook, Google & Co, Chancen und Risiken; [Vorträge aus der Tagung „Facebook, Google & Co Chancen und Risiken" an der Universität Speyer vom 26. bis 27. April 2012] Bd. 23, Baden-Baden, 2013.

Hillenbrand-Beck, Renate, Aufsichtsbehörden, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München, 2003, S. 816–851.

Hobe, Stephan, Einführung in das Völkerrecht, 10. Aufl., 2014.

Holznagel, Bernd/*Sonntag*, Matthias, 4.8 Einwilligung des Betroffenen, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München, 2003.

Hornung, Gerrit/*Städtler*, Stephan, Europas Wolken, Die Auswirkungen des Entwurfs für eine Datenschutz-Grundverordnung auf das Cloud Computing, CR 2012, S. 638–645.

Immenga, Ulrich/*Mestmäcker*, Ernst-Joachim (Hrsg.), Wettbewerbsrecht, Band 2. GWB, 5. Aufl., München, 2014.

Isensee, Josef/*Kirchhof*, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, 3. Aufl., Heidelberg, 2005.

Jarass, Hans D./*Pieroth*, Bodo (Hrsg.), Grundgesetz für die Bundesrepublik Deutschland, 13. Aufl., 2014.

Kahler, Thomas, Die Europarechtswidrigkeit der Kommissionsbefugnisse in der Grundverordnung, Oder: Die überfällige Reform der deutschen und europäischen Datenschutzaufsicht, RDV 2013, S. 69–73.

Kiefer, Günther, Regelungsbedarf und Gestaltungsspielräume bei der Beleihung, LKRZ 2009, S. 441–445.

Kilian, Wolfgang/*Heussen*, Benno (Hrsg.), Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis, 32. EL, München, 2013.

Kingreen, Thorsten/*Kühling*, Jürgen, Weniger Schutz durch mehr Recht: Der überspannte Parlamentsvorbehalt im Datenschutzrecht, Eine Problemskizze am Beispiel des Gesundheitsdatenschutzrechts, JZ 2015, S. 213–221.

Klas, Benedikt/*Möhrke-Sobolewski*, Christine, Digitaler Nachlass - Erbenschutz trotz Datenschutz, NJW 2015, S. 3473–3478.

Klug, Christoph, BDSG-Interpretation, Materialien zur EU-konformen Auslegung, 3. Aufl., Frechen, 2007.

Krüger, Wolfgang/*Rauscher*, Thomas (Hrsg.), Münchener Kommentar zur Zivilprozessordnung, Band 3, 4. Aufl., München, 2013.

Kühling, Jürgen, Auf dem Weg zum vollharmonisierten Datenschutz!?, EuZW 2012, S. 281–282.

– Rückkehr des Rechts: Verpflichtung von „Google & Co." zu Datenschutz , EuZW 2014, S. 527–532.

Kühling, Jürgen/*Martini*, Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, S. 448–454.

Kühling, Jürgen/*Seidel*, Christian/*Sivridis*, Anastasios, Datenschutzrecht, 3. Aufl., Heidelberg, 2015.

Leupold, Andreas/*Glossner*, Silke (Hrsg.), Münchener Anwaltshandbuch IT-Recht, 3. Aufl., München, 2013.

Loewenheim, Ulrich/*Meessen*, Karl M./*Riesenkampff*, Alexander (Hrsg.), Kartellrecht, 2. Aufl., München, 2009.

Martini, Mario, Verwaltungsprozessrecht, Systematische Darstellung in Grafik-Text-Kombination, 5. Aufl., München, 2011.

– Der digitale Nachlass und die Herausforderung postmortalen Persönlichkeitsschutzes im Internet, JZ 2012, S. 1145–1155.

– Wenn ich einmal soll scheiden…Der digitale Nachlass und seine unbewältigte rechtliche Abwicklung, in: Hill, Hermann/Martini, Mario/Wagner, Edgar (Hrsg.), Facebook, Google & Co, Chancen und Risiken; [Vorträge aus der Tagung „Facebook, Google & Co Chancen und Risiken" an der Universität Speyer vom 26. bis 27. April 2012], Bd. 23, Baden-Baden, 2013, S. 77–125.

– Die IMK als Gegenstand des Informationsrechts, Berlin, 2015.

– Wie neugierig darf der Staat im Cyberspace sein?, Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen, VerwArch. 2016, S. 307–358.

– Do it yourself im Datenschutzrecht, Der „Geo Business Code of Conduct" als Erprobungsfeld regulierter Selbstregulierung, NVwZ-Extra 3/2016, S. 1–13.

Martini, Mario/*Fritzsche*, Saskia, Mitverantwortung in sozialen Netzwerken, Fanpage-Betreiber in der datenschutzrechtlichen Grauzone, NVwZ-Extra 2015/21, S. 1–16, http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2015_21.pdf.

Maunz, Theodor/*Dürig*, Günter (Hrsg.), Grundgesetz, Loseblatt-Kommentar, München, 2015.

Maurer, Hartmut, Allgemeines Verwaltungsrecht, 18. Aufl., München, 2011.

Meyer, Jürgen (Hrsg.), Charta der Grundrechte der Europäischen Union, Online-Ausg, Baden-Baden, Wien, Basel, 2014.

Nettesheim, Martin, § 61 Amt und Stellung des Bundespräsidenten in der grundgesetzlichen Demokratie, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, 3. Aufl., Heidelberg, 2005.

Nguyen, Alexander M., Die Subsidiaritätsrüge des Deutschen Bundesrates gegen den Vorschlag der EU-Kommission für eine Datenschutz-Grundverordnung, ZeuS 2012, S. 277–305.

– Die Verhandlungen um die EU-Datenschutzgrundverordnung unter litauischer Ratspräsidentschaft, RDV 2014, S. 26–30.
– Die zukünftige Datenschutzaufsicht in Europa, Anregungen für den Trilog zu Kap. VI bis VII der DS-GVO, ZD 2015, S. 265–270.

Paal, Boris P./*Pauly*, Daniel (Hrsg.), Datenschutz-Grundverordnung, Kommentar, München, 2016.

Plath, Kai-Uwe (Hrsg.), BDSG, Kommentar zum BDSG sowie den Datenschutzbestimmungen von TMG und TKG, Köln, 2013.

Polenz, Sven, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes, in: Kilian, Wolfgang/Heussen, Benno (Hrsg.), Computerrechts-Handbuch, Informationstechnologie in der Rechts- und Wirtschaftspraxis, 32. EL, München, 2013.

Preuß, Tamina, Das Datenschutzrecht der Religionsgesellschaften, Eine Untersuchung de lege lata und de lege ferenda nach Inkrafttreten der DS-GVO, ZD 2015, S. 217–225.

Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München, 2003.

– Unabhängigkeit der Datenschutzaufsicht, Zweites Gesetz zur Änderung des BDSG, ZD 2015, S. 106–111.

Rudolf, Walter, § 141 Kooperation im Bundesstaat, in: Isensee, Josef/Kirchhof, Paul (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, 3. Aufl., Heidelberg, 2005.

Sachs, Michael (Hrsg.), Grundgesetz, Kommentar, 7. Aufl., München, 2014.

Schaar, Peter, Datenschutz-Grundverordnung: Arbeitsauftrag für den deutschen Gesetzgeber, PinG 2016, S. 62–65.

Schaffland, Hans-Jürgen/*Wiltfang*, Noeme, Bundesdatenschutzgesetz, Ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Berlin, 2012.

Scheffczyk, Fabian, "Karenzzeit“ für Bundesminister und Parlamentarische Staatssekretäre, ZRP 2015, S. 133–135.

Schmidt-Bleibtreu, Bruno/*Hofmann*, Hans/*Henneke*, Hans-Günter (Hrsg.), Kommentar zum Grundgesetz, 13. Aufl., Köln, 2014.

Schöbener, Burkhard (Hrsg.), Völkerrecht, Lexikon zentraler Begriffe und Themen, Heidelberg, 2014.

Schweitzer, Michael, Staatsrecht III, 10. Aufl., Heidelberg, München, Landsberg, Frechen, Hamburg, 2010.

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden, 2014.

Sörup, Thorsten/*Marquardt*, Sabrina, Auswirkungen der EU-Datenschutzgrundverordnung auf die Datenverarbeitung im Beschäftigungskontext, ArbRAktuell 2016, S. 103–106.

Spindler, Gerald/*Schuster*, Fabian (Hrsg.), Recht der elektronischen Medien, Kommentar, 3. Aufl., München, 2015.

Steiner, Anton/*Holzer*, Anna, Praktische Empfehlungen zum digitalen Nachlass, ZEV 2015, S. 262–266.

Streinz, Rudolf (Hrsg.), EUV/AEUV, 2. Aufl., München, 2012.

Taeger, Jürgen, Scoring in Deutschland nach der EU-Datenschutzgrundverordnung, ZRP 2016, S. 72–75.

Taeger, Jürgen/*Gabel*, Detlev (Hrsg.), BDSG, 2. Aufl., Frankfurt am Main, 2013.

Thomé, Sarah, Die Unabhängigkeit der Bundesdatenschutzaufsicht, VuR 2015, S. 130–133.

Tinnefeld, Marie-Theres, Grundlagen des Datenschutzes, in: Roßnagel, Alexander (Hrsg.), Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München, 2003, S. 188–193.

von der Groeben, Hans/*Schwarze*, Jürgen/*Hatje*, Armin (Hrsg.), Europäisches Unionsrecht, Vertrag über die Europäische Union - Vertrag über die Arbeitsweise der Europäischen Union - Charta der Grundrechte der Europäischen Union, 7. Aufl., Baden-Baden, 2015.

von Lewinski, Kai, Europäisierung des Datenschutzrechts, Umsetzungsspielraum des deutschen Gesetzgebers und Entscheidungskompetenz des BVerfG, DuD 2012, S. 564–570.

– Unabhängigkeit des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, ZG 2015, S. 228–245.

– , Datenschutzaufsicht in Europa als Netzwerk (Entwurfsfassung vom 24.2.2015), in: Ziekow, Jan (Hrsg.), Verwaltung in Netzwerken, 2016 (in Vorbereitung).

Voßhoff, Andrea/*Hermerschmidt*, Sven, Endlich! - Was bringt uns die Datenschutz-Grundverordnung?, PinG 2016, S. 56–59.

Westphal, Dietrich, Föderale Privatrundfunkaufsicht im demokratischen Verfassungsstaat, Verwaltungs- und verfassungsrechtliche Analyse der Kommission zur Ermittlung der Konzentration im Medienbereich (KEK), Berlin, 2007.

Wieczorek, Mirko, Der räumliche Anwendungsbereich der EU-Datenschutz-Grundverordnung, DuD, S. 644–649.

Wolff, Heinrich Amadeus, Rechtsvorgaben für die Besetzung der Art. 29-Gruppe, Kurzgutachten im Auftrag der BfDI, 2015.

Wolff, Heinrich Amadeus/*Brink*, Stefan (Hrsg.), Datenschutzrecht in Bund und Ländern, Grundlagen, bereichsspezifischer Datenschutz, BDSG, München, 2013.

Wybitul, Tim/*Sörup*, Thorsten/*Pötters*, Stephan, Betriebsvereinbarungen und § 32 BDSG: Wie geht es nach der DS-GVO weiter?, Handlungsempfehlungen für Unternehmen und Betriebsräte, ZD 2015, S. 559–564.

Ziebarth, Wolfgang, Demokratische Legitimation und Unabhängigkeit der deutschen Datenschutzbehörden, Warum das durch die Rechtsprechung des EuGH (Rs. C-518/07, CR 2010, 339 und Rs. C-614/10) Erreichte durch den Entwurf für eine Datenschutz-Grundverordnung gefährdet wird, CR 2013, S. 60–68.

Ziekow, Jan (Hrsg.), Verwaltung in Netzwerken, 2016 (in Vorbereitung).