NomosKommentar

Sydow | Marsch [Hrsg.]

DS-GVO | BDSG

Datenschutz-Grundverordnung Bundesdatenschutzgesetz

Handkommentar

3. Auflage

Nomos DIKE MANZ

NomosKommentar

Prof. Dr. Gernot Sydow
Prof. Dr. Nikolaus Marsch [Hrsg.]

DS-GVO | BDSG

Datenschutz-Grundverordnung Bundesdatenschutzgesetz

Handkommentar

3. Auflage

Dr. Linda Bienemann | Arnd Böken | Andreas Braun | Prof. Dr. Daniel Ennöckl |Dr. Holger Greve | Dr. Nikolas Guggenberger | Prof. Dr. Michael Heghmans | Prof. Dr. Marcus Helfrich | Prof. Dr. Ansgar Hense | Prof. Dr. Albert Ingold | Paul C. Johannes | Dr. David Kampert | Prof. Dr. Bernhard Kreße | Dr. Reto Mantz | Prof. Dr. Nikolaus Marsch | Dr. Marian Müller | Dr. Nicholas Otto | PD Dr. Enrico Peuker | Prof. Dr. Andreas Popp | Prof. Dr. Nicolas Raschauer | Bartholomäus Regenhardt | Prof. Dr. Philipp Reimer | Prof. Dr. Bettina Schöndorf-Haubold | Sabine Schwendemann | Prof. Dr. Gernot Sydow | Dr. Jens Tiedemann | Prof. Dr. Emanuel V. Towfigh | Jacob Ulrich | Robert Weinhold | Maria Wilhelm-Robertson | Prof. Dr. Wolfgang Ziebarth

Nomos DIKE MANZ

Zitiervorschlag: Sydow/Marsch DS-GVO/BDSG

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-8487-7290-2
(Nomos Verlagsgesellschaft mbH & Co. KG, Baden-Baden)

ISBN 978-3-03891-514-0
(Dike Verlag, Zürich/St. Gallen)

ISBN 978-3-214-02605-9
(MANZ'sche Verlags- u. Universitätsbuchhandlung GmbH, Wien)

3. Auflage 2022

Vorwort

Die Datenschutz-Grundverordnung ist exakt vor vier Jahren am 25. Mai 2018 in Kraft getreten. In dieser Zeit hat sich der vorliegende Handkommentar als Kommentierung etabliert, die die materiellen Datenschutznormen ebenso wie die institutionellen und prozeduralen Neuregelungen der Datenschutz-Grundverordnung umfassend interpretiert und Lösungen für die zahlreichen Anwendungsfragen des materiellen Rechts erarbeitet.

Mit der 3. Auflage dieses Kommentars sind nicht nur umfassende Aktualisierungen der einzelnen Kommentierungen verbunden, sondern auch einige wesentliche konzeptionelle Neuerungen: Die Normen des BDSG, die bislang einen eigenständigen Kommentarband gebildet hatten, sind jetzt in den DS-GVO-Kommentar integriert. Er umfasst damit jetzt die beiden datenschutzrechtlichen Kerngesetze in einem Band und ist dadurch in seinem Umfang wesentlich gewachsen. Ergänzend erscheinen in derselben Reihe bei Nomos weitere Handkommentare zu den Landesdatenschutzgesetzen und zum bereichsspezifischen Datenschutz, die von unterschiedlichen Herausgebern betreut werden (2021 bereits erschienen: Sydow [Hrsg.], Kirchliches Datenschutzrecht).

Nikolaus Marsch, der bereits als Autor am BDSG-Handkommentar beteiligt war und durch grundlegende Publikationen zum Datenschutzrecht dieses Rechtsgebiet mit prägt, ist mit der 3. Auflage nun zum Mitherausgeber des Kommentars geworden. Auch der Autorenkreis umfasst durch die Zusammenführung der beiden Kommentierungen nun über 30 Autorinnen und Autoren aus Wissenschaft, Anwaltschaft, Justiz und Verwaltung. Ihr Erfahrungsschatz und ihre Versiertheit in der datenschutzrechtlichen Praxis haben diesen Kommentar maßgeblich geformt und ihn zu einer zentralen Kommentierung des Datenschutzrechts gemacht.

Unsere Aufgaben als Herausgeber sind durch die Mitarbeiterinnen und Mitarbeiter beider Lehrstühle in vielfältiger Weise unterstützt worden. Unser Dank für die Mitwirkung an der 3. Auflage gilt Maike Herrlein, Vera Kolb, Silvia Marx, Caroline Nacke, Jan Niermann, Nicholas Otto, Felicitas Scholz, Pia Marie Siebert, Alban Spielkamp, Luise Teubner, Johanna Werpers, Lena Westphal, Beyza Nur Yeşilyurt Dur, Philipp Ziemons und Lara Zölck (Institut für internationales und vergleichendes öffentliches Recht, Münster) sowie Annabelle Aumann, Christian Backes, Audrey Dakhil, Sofía Maria Fölsch Schroh, David Gölz, Cedric Henke, Alexander Ihl, Michelle Metzger, Laura Palige, Michael Rauber, Tim Templin, Clara Schirmeister und Danielle Schreiner (Lehrstuhl für Deutsches und Europäisches Öffentliches Recht und Rechtsvergleichung, Saarbrücken). Unser Dank gilt schließlich dem Nomos-Verlag für die hervorragende verlegerische Begleitung.

Münster/Saarbrücken, 25. Mai 2022

Gernot Sydow
Nikolaus Marsch

Inhaltsverzeichnis

Kapitel VII
Zusammenarbeit und Kohärenz

Abschnitt 1: Zusammenarbeit

Abschnitt 2: Kohärenz

Abschnitt 3: Europäischer Datenschutzausschuss

Kapitel VIII
Rechtsbehelfe, Haftung und Sanktionen

Kapitel IX
Vorschriften für besondere Verarbeitungssituationen

Abschnitt 2: Besondere Verarbeitungssituationen

Kapitel 2
Rechte der betroffenen Person

Kapitel 3
Pflichten der Verantwortlichen und Auftragsverarbeiter

Kapitel 4
Aufsichtsbehörde für die Datenverarbeitung durch nichtöffentliche Stellen

Kapitel 5
Sanktionen

Kapitel 6
Rechtsbehelfe

Teil 3
Bestimmungen für Verarbeitungen zu Zwecken gemäß Artikel 1 Absatz 1 der Richtlinie (EU) 2016/680

Kapitel 1
Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Kapitel 2
Rechtsgrundlagen der Verarbeitung personenbezogener Daten

Kapitel 3
Rechte der betroffenen Person

Kapitel 4
Pflichten der Verantwortlichen und Auftragsverarbeiter

Bearbeiterverzeichnis

Dr. Linda Bienemann, Rechtsanwältin, Köln	Art. 15, 85, 86 DS-GVO, §§ 34, 57 BDSG
Arnd Böken, Rechtsanwalt und Notar, Partner Graf von Westphalen, Berlin	§§ 1, 2 BDSG
Andreas Braun, M.A., LL.M., Wissenschaftlicher Mitarbeiter, Universität Münster	§ 86 BDSG
Prof. Dr. Daniel Ennöckl, LL.M., Universität für Bodenkultur Wien	Art. 2, 3, 4 Nr. 6 DS-GVO
Dr. Holger Greve, Regierungsdirektor, Bundesministerium des Inneren	Art. 12 DS-GVO, §§ 32, 33 BDSG
Dr. Nikolas Guggenberger, LL.M., Executive Director, Information Society Project, Yale Law School	§§ 30, 31 BDSG
Prof. Dr. Michael Heghmans, Universität Münster	§§ 41–43, 84 BDSG
Prof. Dr. Marcus Helfrich, Rechtsanwalt, FOM Hochschule München	Art. 4 Nr. 4, Art. 21, 22, 37–39 DS-GVO, §§ 5–7, 36–39, 54 BDSG
Prof. Dr. Ansgar Hense, Rheinische Friedrich-Wilhelms-Universität Bonn	Art. 87, 89, 91 DS-GVO, §§ 27, 28, 40, 50 BDSG
Prof. Dr. Albert Ingold, Johannes Gutenberg-Universität Mainz	Art. 4 Nr. 8, 11, Art. 7, 13, 14, 26–30 DS-GVO
Paul C. Johannes, LL.M., Rechtsanwalt, stellv. Geschäftsführer provet, Universität Kassel	§§ 45, 47, 49, 51–53, 62–81 BDSG
Dr. David Kampert, RiVG, VG Gelsenkirchen	Art. 4 Nr. 13–15, 25, Art. 8–11 DS-GVO, §§ 22, 48, 85 BDSG
Prof. Dr. Bernhard Kreße, LL.M., Maître en droit, Technische Universität Dortmund	Art. 79–82 DS-GVO, §§ 44, 83 BDSG
Dr. Reto Mantz, Dipl.-Inf., RiLG, LG Frankfurt a. M.	Art. 4 Nr. 12, Art. 25, 32 DS-GVO

Prof. Dr. Nikolaus Marsch, D.I.A.P., Universität des Saarlandes	§§ 4, 23–25, 46 BDSG
Dr. Marian Müller, Richter, LG Münster	§ 55 BDSG
Dr. Nicholas Otto, Wissenschaftlicher Mitarbeiter, Universität Münster	§§ 56, 58, 59 BDSG
PD Dr. Enrico Peuker, Akad. Rat a. Z., Humboldt-Universität zu Berlin	Art. 4 Nr. 24, Art. 16–19, 23, 56, 60–62 DS-GVO, §§ 35, 82 BDSG
Prof. Dr. Andreas Popp, M.A., Universität Konstanz	Art. 83, 84 DS-GVO
Prof. Dr. Nicolas Raschauer, HSSH Schaffhausen	Art. 4 Nr. 7, Art. 24, 40–43 DS-GVO
Bartholomäus Regenhardt, LL.B., Rechtsanwalt, Cooley LLP, Brüssel	Art. 4 Nr. 9, Art. 73–76 DS-GVO
Prof. Dr. Philipp Reimer, Universität Konstanz	Art. 4 Nr. 2, Art. 5, 6, 36 DS-GVO, § 3 BDSG
Prof. Dr. Bettina Schöndorf-Haubold, Justus-Liebig-Universität Gießen	Art. 63–72 DS-GVO, §§ 17, 19 BDSG
Sabine Schwendemann, Rechtsanwältin, München	Art. 35 DS-GVO
Prof. Dr. Gernot Sydow, M.A., Universität Münster	Einl., Art. 1, 20, 77, 78, 92–95, 97–99 DS-GVO, §§ 20, 21, 60, 61 BDSG
Dr. Jens Tiedemann, DirArbG, ArbG Siegburg	Art. 88, 90 DS-GVO, § 26 BDSG
Prof. Dr. Emanuel V. Towfigh, EBS Universität für Wirtschaft und Recht, Wiesbaden, Research Affiliate am Max-Planck-Institut zur Erforschung von Gemeinschaftsgütern	Art. 4 Nr. 20, 26, Art. 44–50, 96 DS-GVO
Jacob Ulrich, M.A., EBS Universität für Wirtschaft und Recht, Wiesbaden	Art. 4 Nr. 20, 26, Art. 44–50, 96 DS-GVO

Robert Weinhold, Rechtsanwalt, Orrick, Herrington & Sutcliffe, LLP, Düsseldorf	§§ 45, 47, 49, 51–53, 62–81 BDSG
Maria Wilhelm-Robertson, Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg, derzeit abgeordnet zum Staatsministerium Baden-Württemberg	Art. 20, 33–34 DS-GVO, §§ 18, 29 BDSG
Prof. Dr. Wolfgang Ziebarth, Hochschule für Polizei Baden-Württemberg, Villingen-Schwenningen	Art. 4 A, C, Art. 4 Nr. 1, 3, 5, 10, 16–19, 21–23, Art. 31, 51–55, 57–59 DS-GVO, §§ 8–16 BDSG

Einleitung

1 Die europäische **Datenschutz-Grundverordnung (DS-GVO)**[1] hat das Datenschutzrecht mit ihrem Inkrafttreten am **25.5.2018** grundlegend umgestaltet, und zwar auf zahlreichen Ebenen. So wurden nicht nur zahlreiche neue materielle Institute wie das Recht auf Vergessenwerden (Art. 17 Abs. 2 DS-GVO) installiert, auch die Durchsetzung einschließlich eines deutlich verschärften Bußgeldkatalog (Art. 83, 84 DS-GVO) wurden neu geregelt. Folge dieser Rechtssetzung war auch auf nationaler Ebene eine Neustrukturierung des Datenschutzrechts. So ist am **26.11.2019** das **zweite Datenschutz-Anpassungs- und Umsetzungsgesetz (2. DSAnpUG-EU)**[2] in Kraft getreten, das neben Änderungen am BDSG auch zahlreiche bereichsspezifische Gesetze angepasst hat sowie das bisherige Umsetzungsgesetz[3] ergänzt und teilweise abändert.

2 Neben etlichen inhaltlichen Neuerungen haben es Rechtsanwender also seit der europäischen Datenschutzreform mit einem ganz neuen **Geflecht aus europarechtlichen und nationalen Normen** zu tun. Die Rechtsanwen-

1 VO (EU) Nr. 2016/697 vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der RL 95/46/EG, ABl. 2016 L 119, 1; in Kraft getreten am 25.5.2016, Anwendung bzw. Geltung seit dem 25.5.2018 (Art. 99 Abs. 2 DS-GVO; zur entsprechenden Terminologie der DS-GVO → Art. 99 Rn. 2 f.); zu den Schritten des Gesetzgebungsprozesses Sydow DS-GVO/*Sydow,* 2. Aufl. 2018, Einleitung Rn. 18 ff.

2 Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU) vom 20.11.2019, BGBl. 2019 I 1626.

3 Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und Umsetzungsgesetz-EU – DSAnpUG-EU) vom 30.6.2017, BGBl. 2017 I 2097.

dung ist um einiges komplizierter geworden. Genügte früher im Wesentlichen die Kenntnis des nationalen Rechts und waren europäische Richtlinien maximal als Auslegungshilfen heranzuziehen, muss nun für die Ermittlung der Rechtslage der Blick zwischen verschiedenen europäischen und nationalen Gesetzen hin- und herwandern.

Zudem lassen sich mehr als drei Jahre nach Inkrafttreten der neuen Regelungen im Datenschutzrecht einige praktische Anwendungsprobleme sowie neue Herausforderungen, mit denen die Regelungen der DS-GVO und des BDSG konfrontiert werden, ausmachen. 3

Dementsprechend geht es nachfolgend um 4

- einen Überblick zum Mehrebenensystem des Datenschutzrechts (A.),
- die DS-GVO im Spezifischen (B.),
- das BDSG im Spezifischen (C.),
- die Rechtsanwendung im Mehrebenensystem (D.) und
- eine Bewertung des neuen Datenschutzregimes (E.).

A. Überblick: Datenschutzrecht – ein Mehrebenensystem

I. Rechtsgrundlagen

Die Rechtsgrundlagen des Datenschutzrechts sind schon lange nicht mehr in einem einheitlichen Gesetz zu finden. Bei der Materie des Datenschutzrechts handelt es sich nämlich um ein Rechtsgebiet, welches stark durch das europäische Recht geprägt ist. So muss Ausgangspunkt jeder datenschutzrechtlichen Beurteilung zunächst die **Prüfung der Anwendbarkeit der DS-GVO** nach Art. 2 und 3 DS-GVO sein. Ist diese zu bejahen, so ist die DS-GVO vorrangig heranzuziehen. Das nationale Recht kann dann nur als Ergänzung dienen. Wenn der Anwendungsbereich der DS-GVO nicht eröffnet ist, ist ausschließlich das deutsche Recht heranzuziehen (dazu → Rn. 126 ff.). 5

Auf nationaler Ebene gibt es aufgrund der föderalen Struktur Deutschlands und der nicht vorhandenen gebündelten Gesetzgebungskompetenz für das Datenschutzrecht verschiedene Datenschutzgesetze. So sind zunächst das **BDSG** und die **Landesdatenschutzgesetze** zu nennen, die sich auf den allgemeinen Datenschutz in Bezug auf öffentliche Stellen des Bundes (BDSG) oder der Länder (Landesdatenschutzgesetze) sowie in Bezug auf nichtöffentliche Stellen (BDSG) beziehen. Daneben sind in zahlreichen **bereichsspezifischen Gesetzen** Regelungen in Bezug auf den Datenschutz zu finden, die den allgemeinen Regelungen von BDSG und den Landesdatenschutzgesetzen vorgehen. Prominentestes Beispiel ist das Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG)[4], welches jüngst in Kraft getreten ist. Für den richtigen Umgang mit dem Datenschutzrecht ist es daher stets erforderlich, den Blick zu öffnen und die Rechtsgrundlagen in verschiedenen Gesetzen zu suchen (zur Methode der Herausarbeitung der richtigen Rechtsgrundlage → Rn. 107 ff.). 6

4 Artikel 1 des Gesetzes zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien vom 23.6.2021, BGBl. 2021 I 1982.

II. Verhältnis europäisches und nationales Datenschutzrecht

7 Aufgrund der unterschiedlichen normativen Ebenen der einschlägigen Rechtsgrundlagen im Bereich des Datenschutzrechts ist es zwingend notwendig, deren Rang und Verhältnis zueinander zu bestimmen.

1. Unmittelbare Geltung und Anwendungsvorrang der DS-GVO

8 Ziel der DS-GVO ist es, Unterschiede im Datenschutz, die auf einer uneinheitlichen Umsetzung der vorherigen RL 95/46/EG in den Mitgliedstaaten oder auf divergierenden Aufsichtspraktiken beruhen, zu beseitigen und so einen freien Datenverkehr im Binnenmarkt zu ermöglichen.[5] Dieses Ziel soll gerade durch einen Wechsel der Handlungsform erreicht werden.[6] Denn als Verordnung ist die DS-GVO an sich gemäß Art. 288 Abs. 2 S. 2 AEUV in all ihren Teilen verbindlich und gilt unmittelbar in den Mitgliedstaaten. Soweit die DS-GVO diese Regelung nicht im Einzelfall selbst durch an die Mitgliedstaaten gerichtete Regelungsaufträge und Öffnungsklauseln wieder durchbricht, bedarf es also für die DS-GVO – anders als unter der vorherigen RL 95/46/EG – grundsätzlich **keiner mitgliedstaatlichen Umsetzungsakte** mehr.[7] Die Normen der DS-GVO haben daneben **Anwendungsvorrang** vor nationalem Recht. Entgegenstehende Bestimmungen im nationalen Recht sind seit dem 25.5.2018 unanwendbar.[8]

9 Der EuGH geht über den Anwendungsvorrang europäischer Verordnungen noch hinaus: Er hat aus dem Prinzip der Rechtsklarheit ein rechtliches **Gebot zur förmlichen Aufhebung** entgegenstehender Bestimmungen des nationalen Rechts abgeleitet.[9] Zudem waren die nationalen Gesetzgeber verpflichtet, auch mit der DS-GVO inhaltsgleiches Recht bis zum 25.5.2018 aufzuheben. Deutschland veröffentlichte als erster Mitgliedstaat bereits am 30.6.2017 ein neues Bundesdatenschutzgesetz, das ebenfalls am 25.5.2018 in Kraft getreten ist und der Umsetzung der DS-GVO dient. Bzgl. des BDSG aF ist der Gesetzgeber dabei seiner Aufhebungspflicht nachgekommen. Es ist am 25.5.2018 als Ganzes außer Kraft getreten. Auch die Län-

5 Erwägungsgrund 9; Erwägungsgrund 12 DS-GVO benennt daher auch Art. 16 Abs. 2 AEUV als Kompetenzgrundlage.
6 Erwägungsgrund 13 S. 1 DS-GVO: „… ist eine Verordnung erforderlich …".
7 So stellt nun auch § 1 Abs. 5 BDSG klar, dass das BDSG keine Anwendung findet, soweit die DS-GVO unmittelbar gilt.
8 Allgemein zum Anwendungsvorrang ua Calliess/Ruffert/*Ruffert* AEUV Art. 1 Rn. 19 ff.
9 EuGH 26.4.1988 – 74/86, ECLI:EU:C:1988:198 Rn. 10 – Kommission / Deutschland.

der sind ihrer entsprechenden Verpflichtung nachgekommen und haben neue Datenschutzgesetze verabschiedet.[10]

2. Verhältnis der DS-GVO zum bereichsspezifischen Datenschutz im TTDSG

Nach der Grundkonzeption der DS-GVO, die eine technikneutrale Regelung des Datenschutzes vorsieht,[11] bleibt kein Raum mehr für nationales Datenschutzrecht, welches spezifische Regelungen mit Rücksicht auf die verwendete Technik aufstellt.[12] Andererseits sollen nach Art. 95 DS-GVO Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste keine zusätzlichen Pflichten auferlegt werden, soweit sie besonderen Pflichten aus der RL 2002/58/EG unterliegen, die dasselbe Ziel verfolgen. Nationale Umsetzungsvorschriften zur RL 2002/58/EG unterliegen also nicht dem Vorrang der DS-GVO.[13] Das deutsche Recht regelt den Telekommunikations- und Telemediendatenschutz neuerdings im **Telekommunikations-** 10

10 Baden-Württemberg: Gesetz zur Anpassung des allgemeinen Datenschutzrechts und sonstiger Vorschriften an die Verordnung (EU) 2016/679 vom 12.6.2018, GBl. S. 173; Bayern: Bayerisches Datenschutzgesetz (BayDSG) vom 15.5.2018, GVBl. S. 230; Berlin: Gesetz zur Anpassung des Berliner Datenschutzgesetzes und weiterer Gesetze an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Berliner Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – BlnDSAnpUG-EU) vom 13.6.2018; Brandenburg: Gesetz zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 8.5.2018, GVBl. I/18 [Nr. 17]; Bremen: Bremisches Ausführungsgesetz zur EU-Datenschutz-Grundverordnung (BremDS-GVO-AG) vom 8.5.2018, Brem.GBl. 2018, S. 131; Hamburg: Gesetz zur Anpassung des Hamburgischen Datenschutzgesetzes sowie weiterer Vorschriften an die Verordnung (EU) 2016/679 vom 18.5.2018, HmbGVBl. S. 145; Hessen: Hessisches Gesetz zur Anpassung des Hessischen Datenschutzrechts an die Verordnung (EU) Nr. 2016/679 und zur Umsetzung der Richtlinie (EU)Nr. 2016/680 und zur Informationsfreiheit vom 3.5.2018, GVBl. S. 82; Mecklenburg-Vorpommern: Gesetz zur Anpassung des Landesdatenschutzgesetzes und weiterer datenschutzrechtlicher Vorschriften im Zuständigkeitsbereich des Ministeriums für Inneres und Europa Mecklenburg-Vorpommern an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 22.5.2018, GVOBl. M-V 2018, S. 193; Niedersachsen: Gesetz zur Neuordnung des niedersächsischen Datenschutzrechts vom 2.5.2018, Nds. GVBl. S. 66; Nordrhein-Westfalen: Gesetz zur Anpassung des allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Nordrhein-Westfälisches Datenschutz-Anpassungs- und Umsetzungsgesetz EU – NRWDSAnpUG-EU) vom 17.5.2018, GV. NRW S. 244; Rheinland-Pfalz: Landesdatenschutzgesetz vom 8.5.2018, GVBl. 2018, S. 93; Saarland: Gesetz Nr. 1941 zur Anpassung des Saarländischen Datenschutzgesetzes an die Verordnung (EU) 2016/679 vom 16.5.2018, Amtsbl. I S. 254; Sachsen: Sächsisches Datenschutzdurchführungsgesetz (SächsDSDG) vom 26.4.2018, SächsGVBl. S. 198, 199; Sachsen-Anhalt: Gesetz zur Ausfüllung der Verordnung (EU) 2016/679 und zur Anpassung des allgemeinen Datenschutzrechts in Sachsen-Anhalt (Datenschutz-Grundverordnungs-Ausfüllungsgesetz Sachsen-Anhalt – DSAG LSA) vom 18.2.2020, GVBl. LSA 2020, S. 25; Schleswig-Holstein: Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 2.5.2018, GVOBl. S. 162; Thüringen: Thüringer Gesetz zur Anpassung des Allgemeinen Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vom 6.6.2018, GVBl. S. 229.

11 Erwägungsgrund 15 S. 1 DS-GVO; *Sydow/Kring* ZD 2014, 271 (271).

12 *Buchner* DuD 2016, 155 (161).

13 *Nebel/Richter* ZD 2012, 407 (408).

Telemedien-Datenschutzgesetz (TTDSG). Das TTDSG gilt seit dem 1.12.2021 und hat die früheren Datenschutzregelungen im TMG und TKG abgelöst.

11 Unproblematisch anwendbar ist das TTDSG dann, wenn es um Einzelverhältnisse von rechtsfähigen **juristischen Personen** geht. Auf diese ist das TTDSG nach § 1 Abs. 2 anwendbar, von der DS-GVO sind juristische Personen hingegen nicht umfasst, sofern keine Zuordnung zu einer natürlichen Person nach Art. 4 Nr. 1 DS-GVO möglich ist.[14] Daneben bezieht auch Art. 1 Abs. 2 S. 1 RL 2002/58/EG juristische Personen ein, so dass insoweit Art. 95 DS-GVO ebenfalls zum Tragen kommt.

12 Wie auch schon früher muss für die Gültigkeit der einzelnen Regelungen in Bezug auf die Datenverarbeitung **natürlicher Personen** differenziert werden, ob sie auf der RL 2002/58/EG beruhen oder nicht. Ist dies nicht der Fall, müssen derartige Normen mangels Eingreifens von Art. 95 DS-GVO an der DS-GVO gemessen werden. Trotz der Bemühungen des Gesetzgebers, durch das TTDSG rechtssichere Regelungen für das Zusammenspiel von bereichsspezifischem Datenschutz im Bereich der Telekommunikation und der Telemedien und dem Datenschutzregime der DS-GVO zu schaffen, ist dieses Ziel nicht durchgehend geglückt.

13 Bereits in Bezug auf den Adressatenkreis der jeweiligen Norm lässt sich eine überschießende Regelung feststellen. So beschränkt die RL 2002/58/EG diesen auf die Verarbeitung personenbezogener Daten in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Gemeinschaft, mithin also auf Anbieter von öffentlichen Kommunikationsdiensten und Betreiber von öffentlichen Kommunikationsnetzen.[15] Lediglich § 13 TTDSG nimmt diese Beschränkung des Adressatenkreises vor, weitere Normen wie §§ 9 ff. TTDSG verweisen für den Adressatenkreis auf die zur Wahrung des Fernmeldegeheimnisses Verpflichteten in § 3 Abs. 2 S. 1 TTDSG. Darunter fallen zum einen Anbieter, Betreiber sowie Mitwirkende öffentlich zugänglicher Telekommunikationsdienste, zum anderen auch Anbieter, Betreiber sowie Mitwirkende geschäftsmäßig und damit nicht öffentlich oder nicht öffentlich zugänglich angebotener Telekommunikationsdienste. Das Merkmal der „Geschäftsmäßigkeit" ist allerdings weder der RL 2002/58/EG noch Art. 95 DS-GVO bekannt. Für Datenverarbeitungen durch geschäftsmäßige Anbieter, Betreiber sowie daran Mitwirkende ist demnach einzig die DS-GVO maßgeblich.[16]

14 Auch weitere Normen des TTDSG werden in ihrer Anwendbarkeit durch die DS-GVO begrenzt. Hierunter fällt beispielsweise § 7 Abs. 3 TTDSG, denn die Anfertigung einer Kopie stellt bereits einen automatisierten Verarbeitungsvorgang dar. Auch § 10 TTDSG setzt die RL 2002/58/EG teilweise überschießend um: So wird die Situation der Entgelteinziehung durch einen Dritten zwar in § 10 Abs. 1 S. 2 TTDSG, nicht aber in der RL vorgesehen,

14 Dazu auch *Kühling/Sauerborn* CR 2021, 271 (273).
15 Art. 3 Abs. 1, Art. 5 Abs. 1 RL 2002/58/EG.
16 Hierzu und zum Folgenden *Kühling/Sauerborn* CR 2021, 271 (273 f.), die bereits im Gesetzgebungsprozess des TTDSG auf dieses Problem erfolglos hinwiesen; ebenso *Kiparski* CR 2021, 482 (484).

zudem enthält Abs. 2 engere Vorgaben in Bezug auf die Entgeltabrechnung als der insoweit zugrundeliegende Art. 6 Abs. 2 RL 2002/58/EG. Die aus § 97 Abs. 4 TKG aF in § 10 Abs. 3 TTDSG übernommene Erlaubnis zur Verarbeitung der Daten im Falle der Leistungserbringung durch mehrere Dienstanbieter steht weiterhin im Widerspruch zur RL 2002/58/EG. In Bezug auf die Verarbeitung von Standortdaten sieht § 13 Abs. 1 S. 4 TTSDSG ein Schriftlichkeitserfordernis für die Einwilligung vor; ein solches ist hingegen nicht durch Art. 9 Abs. 1 RL 2002/58/EG vorgesehen. Weiter ist das Verhältnis von § 25 TTDSG, der sich auf den Schutz der Privatsphäre bei Endeinrichtungen, mithin auf Cookies und vergleichbare Technologien, bezieht und damit Art. 5 Abs. 3 RL 2002/58/EG fast wortlautgleich übernimmt, zur DS-GVO nicht eindeutig. § 25 Abs. 1 TTDSG stellt eine Speicherung der Informationen in der Endeinrichtung des Endnutzers unter ein striktes Einwilligungserfordernis, Ausnahmen davon sind nur in den in § 25 Abs. 2 TTDSG normierten Fällen möglich. Hierbei ist zwar fraglich, ob der nationale Gesetzgeber überhaupt befugt war, derartige Ausnahmen vom Einwilligungserfordernis zu normieren. Praktisch relevant wird diese Frage regelmäßig nicht sein; schließlich wird, wenn ein Ausnahmetatbestand des § 25 Abs. 2 TTDSG einschlägig ist, stets auch ein Zulässigkeitstatbestand aus Art. 6 Abs. 1 DS-GVO vorliegen. Für eine sich anschließende Verarbeitung der beim Endnutzer auf seinem Endgerät erhobenen Daten ist dagegen unproblematisch die DS-GVO maßgebend.[17]

Die Rechtsfindung im Telekommunikations- und Telemediendatenschutz gestaltet sich damit im Einzelfall weiterhin sehr schwierig. Um diese Abgrenzungsschwierigkeiten zu vermeiden, soll die **RL 2002/58/EG** seit längerem einer **Revision** unterzogen werden.[18] Dementsprechend hat die Kommission am 10.1.2017 einen Gesetzesentwurf[19] vorgelegt, nach dem die RL 2002/58/EG aufgehoben[20] und durch eine neue ePrivacy-Verordnung ersetzt werden soll.[21] Nach dem ursprünglichen Plan der Kommission hätte die neue Verordnung wie auch die DS-GVO ab dem 25.5.2018 anwendbar sein sollen.[22] Dieser ambitionierte Zeitplan konnte nicht eingehalten werden. Am 26.10.2017 hatte zwar das Europäische Parlament dem

15

17 Dazu auch die Praxishilfe der GDD zum Umgang mit dem TTDSG vom Juni 2021, S. 5, abrufbar unter: https://www.gdd.de/downloads/praxishilfen/prax-praxishilfen-neustrukturierung/gdd-praxishilfe-ttdsg-im-ueberblick (zuletzt abgerufen am 04.1.2022).

18 Art. 98 S. 1, Erwägungsgrund 173 S. 2 und 3 DS-GVO.

19 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der RL 2002/58/EG (2017/0003 (COD)) vom 10.1.2017, COM(2017) 10 final (im Folgenden: ePrivacy-VO-E Kom).

20 Art. 27 Abs. 1 ePrivacy-VO-E Kom.

21 Siehe hierzu die vielen kritischen Stimmen zum Entwurf *Engeler* ZD 2017, 549 ff.; *Engeler/Felber* ZD 2017, 251 ff.; *Schleipfer* ZD 2017, 460 ff.; *Maier/Schaller* ZD 2017, 373 ff.; *Bihlmayer/Ehmann/Lesch* DuD 2018, 241 ff.

22 Art. 29 Abs. 2 ePrivacy-VO-E Kom.

Entwurf des federführenden LIBE-Ausschusses[23] zugestimmt und damit seinen Verhandlungstext für das Trilogverfahren festgelegt.[24] Darin waren 168 Änderungsanträge enthalten. Nachdem daraufhin mehrere Versuche gescheitert waren, einen konsensfähigen Ratsentwurf zu verabschieden, gelang dies unter portugiesischer Ratspräsidentschaft erst am 10.2.2021.[25] Der Entwurf sieht zahlreiche Lockerungen in Bezug auf die Einwilligung und die Datenverarbeitung bei Endnutzern vor, ua zum Umgang mit Cookies und anderen Tracking-Diensten. Mittlerweile konnten neue Trilog-Verhandlungen aufgenommen werden. Die Positionen von Rat und Parlament sind nach wie vor konträr, so dass mit einer endgültigen Verabschiedung frühestens 2022 zu rechnen ist.

3. Zulässigkeit nationaler Regelungen aufgrund von Öffnungsklauseln in der DS-GVO

16 Trotz ihres Charakters als Grund-Verordnung beinhaltet die DS-GVO zahlreiche Öffnungsklauseln, die den nationalen Gesetzgeber dazu ermächtigen, Konkretisierungen oder Abweichungen einiger Bestimmungen der DS-GVO zu normieren (dazu unten → Rn. 46 ff., 65 ff.). Den Mitgliedsstaaten kommen damit zahlreiche Gestaltungsmöglichkeiten zu. Die DS-GVO ermächtigt unter anderem dazu, „spezifischere Bestimmungen“[26] als die DS-GVO zu erlassen oder „zusätzliche Bedingungen, einschließlich Beschränkungen“[27] einzuführen, aufrechtzuerhalten oder schlicht von der DS-GVO abzuweichen.[28] Verschiedene Artikel formulieren explizite Gesetzgebungsaufträge an die Mitgliedstaaten, insbesondere Vorschriften über Sanktionen bei Verstößen gegen die DS-GVO zu erlassen[29] und durch Rechtsvorschriften den Datenschutz mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.[30] Weitere Nor-

23 Entwurf einer legislativen Entschließung des Europäischen Parlaments in: Bericht des Ausschusses für bürgerliche Freiheiten Justiz und Inneres (LIBE), Berichterstatterin Marju Lauristin, über den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) (COM(2017)0010 – C8–0009/2017–2017/0003(COD)) vom 20.10.2017, A8–0324/2017 (im Folgenden: ePrivacy-VO-E LIBE).

24 P8_PV(2017)10–26 (9.5) vom 26.10.2017.

25 Entwurf einer Verordnung über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation) vom 10.2.2021, Doc. No. 6087/21 (im Folgenden: ePrivacy-VO-E Rat).

26 Art. 6 Abs. 2, Abs. 3 DS-GVO für Datenverarbeitungen in Ausübung öffentlicher Gewalt oder im öffentlichen Interesse (Art. 6 Abs. 1 lit. e, Abs. 3 DS-GVO) sowie für verschiedenste weitere Konstellationen (Art. 6 Abs. 1 lit. c und lit. d DS-GVO).

27 Art. 9 Abs. 4 DS-GVO für die Verarbeitung von genetischen, biometrischen und Gesundheitsdaten.

28 Art. 8 Abs. 1 DS-GVO: Festlegung der Altersgrenze für die Einwilligungsfähigkeit von Kindern in Abweichung von der 16-Jahre-Grenze der DS-GVO; Art. 14 Abs. 5 lit. c DS-GVO: Informationspflichten über Datenerhebungen; Art. 35 Abs. 10 iVm Art. 6 Abs. 1 lit. c oder e DS-GVO: Verzicht auf eine Datenschutz-Folgeabschätzung in bestimmten Fällen.

29 Art. 84 Abs. 1 DS-GVO.

30 Art. 85 Abs. 1 DS-GVO.

men der DS-GVO ermöglichen den Mitgliedstaaten den Erlass eigenständiger Regelungen, nämlich für die Datenverarbeitung im Beschäftigungskontext[31] oder für nationale Kennziffern.[32] Dabei besteht teilweise die Möglichkeit, durch nationales Recht von den Normen der Kapitel II bis VII der DS-GVO abzuweichen oder Ausnahmen vorzusehen.[33]

17 Eine **Gemengelage von europäischem und nationalem Recht** findet sich auch in einer so zentralen Frage wie den Befugnissen der Aufsichtsbehörden: Sie ergeben sich teils unmittelbar aus der DS-GVO,[34] teilweise sind sie durch nationales Recht vorzusehen,[35] teilweise können sie über die DS-GVO hinaus durch nationales Recht eingeräumt werden.[36] Zudem gewähren Art. 78 ff. DS-GVO verschiedenste datenschutzrechtliche Rechtsbehelfe; die konkreten Gerichtsverfahren in einem Mitgliedstaat sollen aber nach den Erwägungsgründen zur DS-GVO „im Einklang mit dem Verfahrensrecht dieses Mitgliedstaats durchgeführt werden."[37] Die DS-GVO setzt also die Existenz nationaler Prozessordnungen voraus und knüpft für datenschutzrechtliche Rechtsbehelfe daran an, so dass man die bestehenden nationalen Prozessordnungen für datenschutzrechtliche Klagen letztlich als Umsetzungsnormen für Art. 78 ff. DS-GVO lesen muss.

18 Schließlich öffnet sich die DS-GVO nicht nur gegenüber staatlichem, sondern auch gegenüber **nicht-staatlichem Datenschutzrecht**, indem sie die weitere Anwendung von Datenschutzbestimmungen von **Kirchen und religiösen Vereinigungen** (an Stelle der DS-GVO) ermöglicht, sofern diese Bestimmungen mit der DS-GVO in Einklang gebracht werden (dazu unten → Rn. 106).[38] Auch in diesem Fall ist die DS-GVO nicht unmittelbar anwendbar, sondern entfaltet gegenüber nicht-staatlichem Recht eine richtlinienartige Wirkung.

B. DS-GVO

I. Regelungsgehalte

19 Die Kernregelungen der DS-GVO zum materiellen Datenschutzrecht sind in den Kapiteln II und III der Verordnung niedergelegt; sie machen etwa ein Drittel der insgesamt 99 Artikel der DS-GVO aus.[39] Einen vergleichbar breiten Raum nehmen institutionelle, kompetenzielle und verfahrensrecht-

31 Art. 88 Abs. 1 DS-GVO.
32 Art. 87 DS-GVO.
33 Art. 85 Abs. 2 DS-GVO für Datenverarbeitungen zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken; Art. 89 Abs. 3 DS-GVO für wissenschaftliche, historische und statistische Zwecke; ähnlich Art. 83 Abs. 9 DS-GVO für Geldbußen, wenn das Recht eines Mitgliedstaats keine administrativen, sondern nur gerichtliche Geldbußen kennt.
34 Art. 58 Abs. 1 bis 3 DS-GVO.
35 Art. 58 Abs. 5 DS-GVO.
36 Art. 58 Abs. 6 DS-GVO.
37 Erwägungsgrund 143 Satz 7, 2. Halbsatz DS-GVO (an versteckter Stelle im Rahmen dieses zwei Absätze und insgesamt 12 Sätze langen Erwägungsgrundes, der drei eigenständige Rechtsschutzkomplexe betrifft: Nichtigkeitsklagen vor dem EuGH, mitgliedstaatlicher Rechtsschutz, Vorabentscheidungsverfahren).
38 Art. 91 Abs. 1 DS-GVO; Erwägungsgrund 165 DS-GVO; hierzu *Hoeren* NVwZ 2018, 373 (373 f.).
39 Art. 5 bis 36 DS-GVO.

liche Bestimmungen ein, nämlich zum Datenschutzbeauftragten,[40] zu den Aufsichtsbehörden[41] und zu Rechtsbehelfen, Haftung und Sanktionen.[42] Ihnen schließen sich noch einmal materielle Vorschriften für besondere Datenverarbeitungssituationen an.[43] Hinzu kommen einleitende Normen zu den Zielen, dem Anwendungsbereich und den Begriffsbestimmungen der DS-GVO[44] und Schlussbestimmungen über das Inkrafttreten und das Verhältnis zu anderen datenschutzrechtlichen Regelungen.[45] Die DS-GVO normiert demzufolge nicht allein das **materielle Datenschutzrecht**, sondern regelt auch – in einem weit verstandenen Sinn – seine **Durchsetzung**.

20 Im Einzelnen regelt die DS-GVO folgende Fragen:

- Kapitel 1: Allgemeine Bestimmungen
  - Gegenstand und Ziele, Anwendungsbereich und Begriffsbestimmungen (Art. 1 bis 4 DS-GVO).
- Kapitel 2: Grundsätze
  - Grundsätze für die Verarbeitung personenbezogener Daten und Rechtmäßigkeit der Verarbeitung (Art. 5, 6 DS-GVO), Bedingungen für die Einwilligung (Art. 7, 8 DS-GVO), Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9, 10 DS-GVO) und Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist (Art. 11 DS-GVO).
- Kapitel 3: Rechte der betroffenen Person
  - Transparenz und Modalitäten (Art. 12 DS-GVO), Informationspflichten und Recht auf Auskunft zu personenbezogenen Daten (Art. 13 bis 15 DS-GVO), Berichtigung und Löschung (Art. 16 bis 20 DS-GVO), Widerspruchsrecht und automatisierte Entscheidungsfindung im Einzelfall (Art. 21, 22 DS-GVO), Beschränkungen (Art. 23 DS-GVO).
- Kapitel 4: Verantwortlicher und Auftragsverarbeiter
  - Allgemeine Pflichten (Art. 24 bis 31 DS-GVO);
  - Sicherheit personenbezogener Daten (Art. 32 bis 34 DS-GVO);
  - Datenschutz-Folgenabschätzung und vorherige Konsultation (Art. 35, 36 DS-GVO);
  - Datenschutzbeauftragter (Art. 37 bis 39 DS-GVO);
  - Verhaltensregeln und Zertifizierung (Art. 40 bis 43 DS-GVO).
- Kapitel 5: Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen
  - Allgemeine Grundsätze der Datenübermittlung (Art. 44 DS-GVO), Datenübermittlung auf der Grundlage eines Angemessenheitsbeschlusses (Art. 45 DS-GVO) und vorbehaltlich geeigneter Garantien (Art. 46 DS-GVO), verbindliche interne Datenschutzvorschriften (Art. 47 DS-GVO), nach dem Unionsrecht nicht zulässige Übermitt-

40 Art. 37 bis 39 DS-GVO.
41 Art. 51 bis 59 DS-GVO.
42 Art. 77 bis 84 DS-GVO.
43 Art. 85 bis 91 DS-GVO.
44 Art. 1 bis 4 DS-GVO.
45 Art. 94 bis 99 DS-GVO.

lung oder Offenlegung (Art. 48 DS-GVO), Ausnahmen für bestimmte Fälle (Art. 49 DS-GVO);
  - Internationale Zusammenarbeit zum Schutz personenbezogener Daten (Art. 50 DS-GVO).
- Kapitel 6: Unabhängige Aufsichtsbehörden
  - Unabhängigkeit (Art. 51 bis 54 DS-GVO);
  - Zuständigkeit, Aufgaben und Befugnisse (Art. 55 bis 59 DS-GVO).
- Kapitel 7: Zusammenarbeit und Kohärenz
  - Zusammenarbeit, gegenseitige Amtshilfe, gemeinsame Maßnahmen (Art. 60 bis 62 DS-GVO);
  - Kohärenz, Streitbeilegung, Informationsaustausch (Art. 63 bis 67 DS-GVO);
  - Europäischer Datenschutzausschuss (Art. 68 bis 76 DS-GVO).
- Kapitel 8: Rechtsbehelfe, Haftung und Sanktionen (Art. 77 bis 84 DS-GVO).
- Kapitel 9: Vorschriften für besondere Verarbeitungssituationen (Art. 85 bis 91 DS-GVO).
- Kapitel 10: Delegierte Rechtsakte und Durchführungsrechtsakte (Art. 92, 93 DS-GVO).
- Kapitel 11: Schlussbestimmungen (Art. 94 bis 99 DS-GVO).

II. Regelungskompetenzen für das europäische Datenschutzrecht

1. Kompetenzgrundlage für die DS-GVO

Die DS-GVO beruht auf dem Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf **Art. 16 AEUV**.[46] Dessen Absatz 1 normiert in Entsprechung zu Art. 8 GRCh das Recht auf Schutz personenbezogener Daten (näher unten → Rn. 24 ff.). Art. 16 Abs. 2 AEUV überträgt der Europäischen Union die Kompetenz, im Wege des ordentlichen Gesetzgebungsverfahrens[47] Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und über den freien Datenverkehr zu treffen. Art. 16 Abs. 2 AEUV bezieht sich dabei auf zwei Konstellationen: auf die Verarbeitung personenbezogener Daten durch die **Organe, Einrichtungen und sonstigen Stellen der Union** und auf Datenverarbeitungen durch die **Mitgliedstaaten** im Rahmen der Ausübung von Tätigkeiten, die in den **Anwendungsbereich des Unionsrechts** fallen. 21

Auch die Regelungen der DS-GVO zur Durchsetzung des Datenschutzrechts (Bestimmungen über Institutionen, Rechtsbehelfe, Sanktionen und Haftung) beruhen auf Art. 16 Abs. 2 AEUV. Ihre Aufnahme in die DS-GVO begründet ein **Spannungsverhältnis zur mitgliedstaatlichen Orga-** 22

46 Einleitungssatz zur DS-GVO vor den Erwägungsgründen.
47 Dh durch übereinstimmende Mehrheitsentscheidungen im Europäischen Parlament und im Rat; im Einzelnen: Art. 294 AEUV.

nisations- und Verfahrensautonomie.[48] Die Autonomie der Mitgliedstaaten ist aber weder in institutioneller und verfahrensrechtlicher noch in verwaltungsprozessualer Hinsicht absolut: Die Autonomieformel bezeichnet nicht mehr als einen Grundsatz, der aus den Prinzipien der begrenzten Einzelermächtigung, der Verhältnismäßigkeit, des Subsidiaritätsgebots und des Effektivitätsgebots abgeleitet werden kann.[49] Im Rahmen dieser Primärrechtsbestimmungen kann das nationale Recht nicht nur materiellrechtlich, sondern auch in Bezug auf Organisation und Verfahren des Verwaltungsvollzugs und des Rechtsschutzes europarechtlichen Vorgaben unterworfen werden. Dabei ist es unerheblich, ob entsprechende Vorgaben durch den EuGH aus allgemeinen Rechtsgrundsätzen entwickelt werden oder – wie im Falle der DS-GVO – auf europäischer Gesetzgebung beruhen.

23 Art. 16 AEUV ist auch Kompetenzgrundlage der zeitgleich zur DS-GVO erlassenen Richtlinie 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 (JI-RL)[50]. Besondere Kompetenzbestimmungen bestehen für den Datenschutz im Bereich der gemeinsamen Außen- und Sicherheitspolitik, nämlich in Art. 39 EUV, der nur einen Ratsbeschluss statt des ordentlichen Gesetzgebungsverfahrens durch Rat und Parlament erfordert.

2. Materielle Vorgaben des Primärrechts für die europäische Datenschutzgesetzgebung

a) Datenschutzgrundrecht aus Art. 8 GRCh, 16 Abs. 1 AEUV

aa) Verhältnis der grundrechtlichen Gewährleistungen zueinander

24 Art. 8 Abs. 1 GRCh und Art. 16 Abs. 1 AEUV gewährleisten beide den Schutz personenbezogener Daten. Dieses **Datenschutzgrundrecht** bildet den normativen Rahmen, in dem das datenschutzrechtliche Sekundärrecht der Union zu entwickeln ist, und ist daher für Verständnis und Auslegung die-

48 Die Autonomieformel geht zurück auf EuGH 11.2.1971 – Rs. 39/70, ECLI:EU:C:1971:16 S. 58 – Norddeutsches Vieh- und Fleischkontor GmbH/Hauptzollamt Hamburg-St. Annen und EuGH 15.12.1971 – Rs. 51/71, ECLI:EU:C:1971:128 S. 1116 – International Fruit Company ua/Produktschap voor Groenten en fruit; aus der jüngeren Rechtsprechung EuGH 24.4.2008 – C-55/06, ECLI:EU:C:2008:244 Rn. 166, 170 – Arcor.

49 Aus der kritischen Diskussion der Autonomieformel *Kadelbach*, Allgemeines Verwaltungsrecht, 1999 S. 113; *Classen* Die Verwaltung 1998, 307 ff.; *Galetta*, Procedural Autonomy of EU Member States, 2010; *Frenz* VerwArch 2011, 134 (148); Hatje/Müller-Graff Europäisches Organisations- und Verfahrensrecht EnzEuR Bd. 1/*Sydow*, 2. Aufl. 2021, § 17 Rn. 47 mwN; zu den entsprechenden Anforderungen an Sekundärrechtsakte auch EuGH 18.6.2015 – C-508/13, ECLI:EU:C:2015:403 – Estland/Parlament und Rat.

50 RL (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.4.2016 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. 2016 L 119, 89.

ses Sekundärrechts von grundlegender Bedeutung.[51] Ferner zieht der EuGH zur Beurteilung datenschutzgrundrechtlicher Sachverhalte teilweise auch Art. 8 Abs. 1 EMRK und dessen Auslegung durch den EGMR heran, auch wenn diese Norm kein explizites Datenschutzgrundrecht enthält, sondern allgemeiner das Privat- und Familienleben schützt.[52]

25 **Art. 8 Abs. 1 GRCh** und **Art. 16 Abs. 1 AEUV** sind in der Umschreibung des grundrechtlichen Schutzbereichs wortlautidentisch. Anders als Art. 8 GRCh gewährleistet Art. 16 AEUV das Datenschutzgrundrecht jedoch schrankenlos. Dies führt zur Frage, inwieweit das **Verhältnis beider Gewährleistungen** der Regel des Art. 52 Abs. 2 GRCh unterliegt,[53] nach der sich die Ausübung eines Charta-Grundrechts nach den in den Verträgen festgelegten Bedingungen richtet, sofern ein in der Charta niedergelegtes Grundrecht auch dort normiert ist. Eine Anwendung des Art. 52 Abs. 2 GRCh hätte zur Folge, dass auch Art. 8 Abs. 1 GRCh schrankenlos gewährleistet wäre[54] mit der Folge, dass nur die allgemeinen Schranken des Art. 52 Abs. 1 GRCh greifen würden.

26 Art. 52 Abs. 2 GRCh dürfte indes nach seiner systematischen Stellung innerhalb der GRCh ausschließlich mit dem Ziel konzipiert worden sein, spezifische Schrankenregelungen, die für einzelne grundrechtliche Gewährleistungen bereits bei Erlass der Charta in den bestehenden europäischen Verträgen normiert waren, auf die Gewährleistungen der GRCh zu übertragen. Art. 52 Abs. 2 GRCh kann demgegenüber nicht den Zweck haben, spezifischen Schrankenregelungen für Einzelgewährleistungen der GRCh jede Bedeutung zu nehmen, wenn eine Gewährleistung an anderer Stelle ohne derart differenzierte Bedingungen normiert ist. Die Schrankenregelung des Art. 8 GRCh wird daher durch Art. 16 AEUV nicht aufgehoben. Das **Datenschutzgrundrecht** ist demzufolge **schrankenbewehrt**.[55] Damit folgt die Auslegung des Art. 16 Abs. 1 AEUV in grundrechtlicher Hinsicht im Ergebnis derjenigen des Art. 8 GRCh.[56]

51 EuGH 20.5.2003 – C-465/00, ECLI:EU:C:2003:294 Rn. 68 – Österreichischer Rundfunk ua.

52 EuGH 17.10.2013 – C-291/12, ECLI:EU:C:2013:670 Rn. 55 – Schwarz; EuGH 8.4.2012 – C-293/12 und C-594/12, ECLI:EU:C:2014:238 Rn. 35, 47, 55 – Digital Rights Ireland und Seitlinger ua; zur umstrittenen Frage, ob für das Verhältnis von Art. 8 Abs. 1 EMRK zu Art. 8 GRCh der Mechanismus des Art. 52 Abs. 3 GRCh greift Calliess/Ruffert/*Kingreen* GRCh Art. 8 Rn. 4, zudem → Art. 1 Rn. 10 ff., insbes. 13.

53 Dagegen Calliess/Ruffert/*Kingreen* GRCh Art. 8 Rn. 3; von der Groeben/Schwarze/Hatje/*Brühann* AEUV Art. 16 Rn. 31; dafür Meyer/Hölscheidt/*Bernsdorff* GRCh Art. 8 Rn. 24; *Frenz* EuropaR-HdB IV, 2009, Rn. 1363, 1430.

54 Streinz/*Streinz* GRCh Art. 8 Rn. 4.

55 *Frenz* EuropaR-HdB IV, 2009, Rn. 1363; von der Groeben/Schwarze/Hatje/*Brühann* AEUV Art. 16 Rn. 31; Streinz/*Hermann* AEUV Art. 16 Rn. 4; aA wohl Jarass GRCh Art. 8 Rn. 1.

56 In diese Richtung von der Groeben/Schwarze/Hatje/*Brühann* AEUV Art. 16 Rn. 31 und Streinz/*Hermann* AEUV Art. 16 Rn. 4 f.

bb) Schutzgehalt und Schutzniveau

27 Der auslegungsbedürftige **Begriff der personenbezogenen Daten** war bereits vor Erlass der DS-GVO durch die Judikatur des EuGH[57] und durch Sekundärrecht konkretisiert, unter anderem durch Art. 2 lit. a RL 95/46/EG und Art. 2 lit. a VO (EG) Nr. 45/2001:[58] Personenbezogene Daten sind alle Informationen über eine bestimmte oder jedenfalls bestimmbare Person. Für die Eröffnung des Schutzbereichs ist unbeachtlich, ob eine solche Information als vertraulich einzustufen ist;[59] sie kann sogar öffentlich zugänglich sein.[60] Vielmehr unterfallen alle denkbaren Informationen dem Schutzbereich, sofern sie einen personalen Bezug aufweisen.[61] Dies entspricht der auch in Deutschland vollzogenen Abkehr vom starren Stufenmodell von drei Schutzsphären, anhand dessen ursprünglich die Schutzbedürftigkeit von Daten beurteilt worden war. Richtigerweise kommt es stets auf die **Wirkung und die Verwendung der Daten im Einzelfall** an.[62] Diesem Konzept trägt eine extensive Auslegung des Schutzbereichs des Art. 8 Abs. 1 GRCh Rechnung.

28 Im Unterschied zu den primärrechtlichen Regelungen verschiedener anderer Bereiche – insbesondere zur Rechtsangleichung in den Bereichen Gesundheit, Umwelt- und Verbraucherschutz[63] – verpflichtet Art. 16 AEUV nicht ausdrücklich auf ein hohes Schutzniveau im Bereich des Datenschutzes. Eine solche **Schutzniveauklausel** dürfte bei der Formulierung des Art. 16 AEUV für entbehrlich gehalten worden sein, weil Art. 16 AEUV der Kompetenznorm eine Grundrechtsgewährleistung voranstellt, die das Datenschutzgrundrecht aus Art. 8 GRCh aufnimmt. Die Datenschutzgesetzgebung nach Art. 16 AEUV ist bereits durch dessen ersten Absatz grundrechtlich gebunden. Es besteht daher kein Bedarf, die Datenschutzgesetzgebung über eine (analoge) Heranziehung des Art. 114 Abs. 3 AEUV auf ein hohes Datenschutzniveau zu verpflichten.[64]

cc) Grundrechtsberechtigte und -verpflichtete

29 Durch Art. 16 Abs. 1 AEUV, Art. 8 Abs. 1 GRCh wird „jede Person" berechtigt. Hierunter fallen zunächst alle natürlichen Personen. Uneinheitlich wird hingegen beantwortet, ob auch **juristische Personen** zu den Grundrechtsberechtigten zählen. Der EuGH vertritt als vermittelnden Stand-

57 EuGH 9.11.2010 – C-92/09 und C-93/09, ECLI:EU:C:2010:662 Rn. 52 – Volker und Markus Schecke und Eifert.

58 Der Inhalt dieser Bestimmungen ist überdies leicht modifiziert in Art. 4 Nr. 1 DS-GVO übernommen worden; zur Auslegung ferner *Frenz* EuropaR-HdB IV, 2009, Rn. 1361, 1364, 1368.

59 EuGH 20.5.2003 – C-465/00, ECLI:EU:C:2003:294 Rn. 75 – Österreichischer Rundfunk ua.

60 Jarass GRCh Art. 8 Rn. 7; Frenz EuropaR-HdB IV, 2009, Rn. 1375.

61 Jarass GRCh Art. 8 Rn. 7; Meyer/Hölscheidt/*Bernsdorff* GRCh Art. 8 Rn. 20; Calliess/Ruffert/*Kingreen* GRCh Art. 8 Rn. 9; von der Groeben/Schwarze/Hatje/*Augsberg* GRCh Art. 8 Rn. 6.

62 Hierzu *Nebel* ZD 2015, 517 (519).

63 Vgl. Art. 114 Abs. 3 AEUV, der ein hohes Schutzniveau für vier andere Bereiche festschreibt und dabei das Datenschutzrecht gerade nicht aufnimmt; zudem Art. 191 Abs. 2 AEUV.

64 So aber wohl das Konzept von von der Groeben/Schwarze/Hatje/*Brühann* AEUV Art. 16 Rn. 13, 34 ff.

punkt, dass der persönliche Schutzbereich des Art. 8 Abs. 1 GRCh nur dann eröffnet sei, wenn der „Name" der juristischen Person einen Rückschluss auf die Namen natürlicher Personen zulässt.[65] Insbesondere in der deutschen Literatur hält eine Mehrheit juristische Personen im Rahmen des Art. 8 Abs. 1 GRCh jedoch für unbeschränkt grundrechtsberechtigt.[66]

30 Hinsichtlich der Grundrechtsverpflichtung ergibt sich für das Datenschutzgrundrecht keine Abweichung von der allgemeinen Regel des Art. 51 Abs. 1 S. 1 GRCh: Grundrechtsverpflichtet sind alle **unionalen Stellen** und zudem die **Mitgliedstaaten**, sofern sie Unionsrecht durchführen.[67]

dd) Schutzdimensionen

31 Art. 16 Abs. 1 AEUV, Art. 8 Abs. 1 GRCh ist als **Abwehrrecht** gegenüber hoheitlichem – unionalem oder mitgliedstaatlichem – Handeln konzipiert. Hierunter fallen alle denkbaren Eingriffshandlungen, insbesondere Datenerhebung und -verarbeitung sowie ihre Speicherung. Gleichwohl sind solche Eingriffe nicht prinzipiell ausgeschlossen: Eine Einwilligung des Betroffenen gemäß Art. 8 Abs. 2 S. 1 Alt. 1 GRCh kann bereits dem hoheitlichen Handeln die Eingriffsqualität nehmen.[68] Ferner ist ein Eingriff gerechtfertigt, der auf Grundlage eines Gesetzes erfolgt, das der üblichen Verhältnismäßigkeitsprüfung standhält, indem es insbesondere einen legitimen Zweck verfolgt.[69]

32 Weiterhin ist Art. 16 Abs. 1 AEUV, Art. 8 Abs. 1 GRCh als **Leistungsgrundrecht** konzipiert, das dem Betroffenen einen Anspruch auf staatlichen Schutz vermittelt.[70] Eine eigenständige Bedeutung erlangt dieser zusätzliche Gehalt vor allem im Verhältnis zu privaten Dritten, deren Umgang mit Daten unionaler bzw. staatlicher Regulierung bedarf, um der Schutzpflicht nachzukommen. Zwar werden Private hierdurch nicht zu Grundrechtsverpflichteten,[71] der Datenschutz wird jedoch so auf nicht-hoheitliche Datenverarbeitung erstreckt,[72] so dass jedenfalls von einer mittelbaren Drittwirkung des Grundrechts auf Private zu sprechen ist.[73] Schließlich können Art. 16 Abs. 1 AEUV, Art. 8 Abs. 1 GRCh **Auskunfts- und Berichtigungsansprüche** des Betroffenen entnommen werden.[74]

65 EuGH – C-92/09 und C-93/09, ECLI:EU:C:2010:662 Rn. 53 – Volker und Markus Schecke und Eifert; zust. Meyer/Hölscheidt/*Bernsdorff* GRCh Art. 8 Rn. 25.
66 von der Groeben/Schwarze/Hatje/*Brühann* AEUV Art. 16 Rn. 47; Streinz/*Streinz* GRCh Art. 8 Rn. 6; ablehnend *Frenz* EuropaR-HdB IV, 2009, Rn. 1374.
67 Weiterführend Jarass GRCh Art. 51 Rn. 23.
68 Zum Rechtscharakter der Einwilligung *Frenz* EuropaR-HdB IV, 2009, Rn. 1417.
69 Art. 8 Abs. 2 S. 1 Alt. 2 GRCh, hierzu Calliess/Ruffert/*Kingreen* GRCh Art. 8 Rn. 14 ff.
70 *Frenz* EuropaR-HdB IV, 2009, Rn. 1386; von der Groeben/Schwarze/Hatje/*Augsberg* GRCh Art. 8 Rn. 8; Jarass GRCh Art. 8 Rn. 12.
71 Jarass GRCh Art. 8 Rn. 3.
72 *Frenz* EuropaR-HdB IV, 2009, Rn. 1388.
73 von der Groeben/Schwarze/Hatje/*Augsberg* GRCh Art. 8 Rn. 10; Streinz/*Streinz* GRCh Art. 8 Rn. 6; Grabitz/Hilf/Nettesheim/*Sobotta* AEUV Art. 16 Rn. 11.
74 Hierzu *Frenz* EuropaR-HdB IV, 2009, Rn. 1392 ff., 1401 ff.

b) Unabhängigkeit der Aufsichtsbehörden, Art. 16 Abs. 2 S. 2 AEUV

33 Die Kompetenztitel des Europarechts dienen vielfach nicht nur der Begründung einer Verbandskompetenz der EU und der Bestimmung von Organkompetenzen und Handlungsformen für die Sekundärrechtsetzung, sondern auch der Normierung einzelner inhaltlicher Vorgaben für das Sekundärrecht. So bestimmt Art. 16 Abs. 2 S. 2 AEUV, dass die Einhaltung der Datenschutzbestimmungen von **unabhängigen Behörden** überwacht werden müsse.

34 Die DS-GVO setzt diese Vorgabe, die bereits vor Erlass der DS-GVO durch die Rechtsprechung des EuGH[75] nähere Konturen gewonnen hatte, durch Art. 52 DS-GVO um. Die Norm enthält Bestimmungen zur Unabhängigkeit und Weisungsfreiheit der Mitglieder der Aufsichtsbehörde, Inkompatibilitätsregelungen und Bestimmungen über die personellen, technischen und finanziellen Ressourcen der nationalen Aufsichtsbehörden.

III. Strukturfragen der DS-GVO

1. Heterogenität der Regelungsgehalte und Verbindlichkeitsgrade der DS-GVO

35 Die Kompetenzgrundlage der DS-GVO, Art. 16 Abs. 2 S. 1 AEUV, ermöglicht den Erlass nicht näher spezifizierter „Vorschriften", nimmt also keine Festlegung auf eine der Handlungsformen des Art. 288 AEUV vor. Art. 16 Abs. 2 AEUV entspricht in dieser Hinsicht der großen Mehrzahl der Kompetenztitel der Verträge, die nicht mehr – wie in der Anfangszeit der europäischen Integration – bereits primärrechtlich eine Festlegung auf den Erlass einer Verordnung oder einer Richtlinie vorsehen. Der europäische Gesetzgeber war daher grundsätzlich frei, die europäische Datenschutz-Richtlinie durch eine **Verordnung mit unmittelbar anwendbaren Regelungen** abzulösen. Dementsprechend behauptet der Schlusssatz der DS-GVO in Übereinstimmung mit Art. 288 Abs. 2 AEUV, dass die DS-GVO „in allen ihren Teilen verbindlich" sei und „unmittelbar in jedem Mitgliedstaat" gelte.[76] Für zahlreiche Bestimmungen der DS-GVO ist aber genau dies nicht der Fall.

36 Die einzelnen Normen der DS-GVO sind vielmehr in ihren Regelungsgehalten und Verbindlichkeitsgraden von ausgesprochener **Heterogenität.** Diese durchzieht die gesamte Verordnung:

37 Neben unmittelbar anwendbaren Normen finden sich zahlreiche explizite und implizite, an die Mitgliedstaaten gerichtete **Gesetzgebungs-, Umsetzungs- und Konkretisierungsaufträge** für die DS-GVO.[77] Zahlreiche Normen des Kapitels VIII (Rechtsbehelfe, Haftung und Sanktionen) und des

75 EuGH 9.3.2010 – C-518/07, ECLI:EU:C:2010:125 – Kommission/Deutschland; EuGH 16.10.2012 – C-614/10, ECLI:EU:C:2012:631 – Kommission/Österreich; EuGH 8.4.2014 – C-293/12 und C-594/12, ECLI:EU:C:2014:238 – Digital Rights Ireland und Seitlinger ua; dazu auch von der Groeben/Schwarze/Hatje/*Brühann* AEUV Art. 16 Rn. 76 ff.; *von Lewinski* ZG 2015, 228 ff.

76 Zu den Voraussetzungen unmittelbarer Wirkung von Unionsrecht von der Groeben/Schwarze/Hatje/*Geismann* AEUV Art. 288 Rn. 11 f.

77 Umfassende Typologie der verschiedenen Öffnungsklauseln bei *Kühling/Martini ua* DS-GVO, 2016, S. 9 ff.

Kapitels IX (Vorschriften für besondere Datenverarbeitungssituationen) sind aus sich heraus nicht vollzugsfähig, sondern zwingend auf eine ausgestaltende Umsetzung durch nationales Recht angewiesen. Materiell haben die entsprechenden Normen der DS-GVO Richtliniencharakter.

Diese verpflichtenden Gesetzgebungs-, Umsetzungs- und Konkretisierungsaufträge werden ergänzt durch **optionale Öffnungs- oder Abweichungsklauseln** zugunsten staatlicher (und nicht-staatlicher) Gesetzgebung, und zwar sowohl im materiellen Datenschutzrecht wie auch in den akzessorischen Haftungs-, Sanktions- oder Rechtsschutzregelungen. 38

Manche Artikel der DS-GVO entbehren schließlich jedes normativen Gehalts: Sie formulieren nichts weiter als **politische Absichtserklärungen** zur späteren Änderung des bestehenden Sekundärrechts.[78] 39

Als Konsequenz aus diesen Öffnungsklauseln enthält die DS-GVO eine Reihe von **Notifizierungspflichten**, nach denen die Mitgliedstaaten der Kommission ihre nationalen Umsetzungs- oder Abweichungsnormen zur DS-GVO mitzuteilen hatten, in der Regel bis zum 25.5.2018. Die umsetzungsbedürftigen Normen bestimmter Kapitel der DS-GVO (Kapitel VIII und IX) sind dabei konsequent mit Notifizierungspflichten verbunden worden,[79] während dies in den anderen Kapiteln der DS-GVO nicht der Fall ist[80] – ein kaum überzeugendes Differenzierungskriterium. 40

Der Frage nach der primärrechtlichen Zulässigkeit eines derart kreativen Umgangs mit Art. 288 AEUV soll hier nicht nachgegangen werden; letztlich wird sie zu bejahen sein.[81] Das Problem dieser heterogenen Normstruktur liegt eher darin, dass unterschiedlichste Mechanismen zur Konkretisierung der DS-GVO nebeneinander bestehen und deshalb ein nur schwer überschaubares, in jeder Einzelfrage differenziertes Nebeneinander von europäischem und nationalem Recht entsteht. 41

2. Instrumentenmix zur Konkretisierung der Bestimmungen der DS-GVO

Das hohe Abstraktionsniveau vieler Regelungen der DS-GVO erfordert eine Konkretisierung. Aus dieser Notwendigkeit heraus erklärt sich die **Bezeichnung als Grund-Verordnung** (englisch „general regulation", französisch „règlement général") statt als einfache Verordnung, ohne dass mit diesem Hinweis auf Konkretisierungsbedarf im Gesetzestitel weitergehende normative Konsequenzen verbunden wären. Um die Kompetenzen zu dieser Konkretisierung ist im Gesetzgebungsverfahren intensiv gerungen worden. Man kann dies auf EU-Ebene als institutionelle Auseinandersetzung 42

78 Art. 2 Abs. 3 S. 2, Art. 98 DS-GVO.

79 Art. 83 Abs. 9 S. 3, Art. 84 Abs. 2, Art. 85 Abs. 3, Art. 88 Abs. 3, Art. 90 Abs. 2 DS-GVO.

80 Bspw. Art. 6 Abs. 2, Abs. 3, Art. 8 Abs. 1, Art. 9 Abs. 4 DS-GVO.

81 von der Groeben/Schwarze/Hatje/*Geismann* AEUV Art. 288 Rn. 22 (kein numerus clausus – Zulässigkeit atypischer Handlungsformen); ebenso Grabitz/Hilf/Nettesheim/*Nettesheim* AEUV Art. 288 Rn. 209 ff.; auch *Glaser*, Die Entwicklung des Europäischen Verwaltungsrechts aus der Perspektive der Handlungsformenlehre, 2013, S. 342, nach dessen Auffassung die Verordnung nur grundsätzlich keiner Umsetzung in nationales Recht bedarf.

Zu Absatz 4 – Weiterverarbeitung nach Zweckänderung:

Culik/Döpke, Zweckbindungsgrundsatz gegen unkontrollierten Einsatz von Big Data-Anwendungen – Analyse möglicher Auswirkungen der DS-GVO, ZD 2017, 226; *Eichenhofer*, Vom Zweckbindungsgrundsatz zur Interessenabwägung? PinG 2017, 135; *Monreal,* Weiterverarbeitung nach einer Zweckänderung in der DS-GVO. Chancen nicht nur für das europäische Verständnis des Zweckbindungsgrundsatzes, ZD 2016, 507. Siehe außerdem die zu Art. 5 DS-GVO angegebene Literatur.

A. Grundlagen

I. Umfassendes präventives Verbot

1 Die Bestimmung regelt **das „Ob" der Verarbeitung** (zB einer Datenübermittlung), während Art. 5 DS-GVO wesentliche Aspekte des „Wie" betrifft[1] (zB die Notwendigkeit verschlüsselter Übermittlung[2]). Entgegen der weit gefassten Überschrift von Art. 6 DS-GVO entscheiden Art. 5 DS-GVO und andere Bestimmungen der Verordnung mit über die Rechtmäßigkeit einzelner Verarbeitungen.[3] Gegenstand der Regelung ist dabei die objektive Rechtmäßigkeit, während subjektive Rechte nach der systematischen Anlage der DS-GVO aus diesem Kapitel nicht folgen (→ Rn. 107).

2 Kernelement des Art. 6 ist, wie sich aus dem Wort „nur" im Einleitungssatz des Abs. 1 ergibt, ein **umfassendes präventives Verbot**[4] mit unmittelbar geltenden Ausnahmen und ergänzenden Vorbehalten legislativer Erlaubnis („Verbotsprinzip"[5]):[6] Die Verarbeitung personenbezogener Daten ist generell verboten und nur im Einzelfall erlaubt, soweit einer der sechs Erlaubnistatbestände des Abs. 1 gegeben ist.[7] Gegenüber privaten Verarbeitern ist das grundrechtlich problematisch.[8]

3 **Anwendbar** ist die Bestimmung auf alle personenbezogenen Daten mit Ausnahme der in Art. 9 DS-GVO geregelten „besonderen Kategorien", wofür dort ein eigenes präventives Verbot aufgestellt ist (→ Art. 9 Rn. 4, 62), und auf alle Verarbeitungsarten (→ Art. 4 Rn. 42 ff.) mit Ausnahme der

1 Darüber hinaus schreibt Art. 5 Abs. 1 DS-GVO auch einige Verarbeitungen positiv vor, vgl. → Art. 5 Rn. 11.

2 Entgegen *Lorenz* DuD 2017, 757 (759) sollte dieser Aspekt daher grds. von der Rechtmäßigkeit der Übermittlung getrennt werden. Allenfalls im Rahmen der Interessenabwägung nach Abs. 1 lit. f könnte er auch für das „Ob" eine Rolle spielen, vgl. → Rn. 84.

3 EuGH 16.1.2019 – C-496/17, Rn. 57 – Deutsche Post. Aus der Fachjudikatur vgl. LG Wiesbaden ZD 2019, 512 Rn. 10; aus dem Schrifttum Paal/Pauly/*Frenzel* DS-GVO Art. 6 Rn. 7; *Ziegenhorn/von Heckel* NVwZ 2016, 1585 (1586); *Hamann* BB 2017, 1090 (1091).

4 Zur Kritik dieser Regelungstechnik siehe statt vieler *Härting/Schneider* CR 2015, 819 (822 f.); *Giesen* PinG 2013, 62; befürwortend dagegen etwa *Weichert* DuD 2013, 246; *Karg* DuD 2013, 75. S. a. → Einleitung Rn. 71 ff. – Selbstverständlich enthält Art. 6 Abs. 1 DS-GVO keine Pflicht zur Verarbeitung, siehe EuGH 4.5.2017 – C-13/16, Rn. 26 – Rīgas satiksme (noch zu Art. 7 DSRL).

5 Der eingeführte Begriff bereits bei *Bühnemann*, Datenschutz im nicht-öffentlichen Bereich, 1974, 103ff.

6 Wenn Roßnagel Neues DatenschutzR/*Roßnagel*, 2018, § 3 Rn. 50, meint, es gebe „kein Verbotsprinzip" und die Verarbeitung sei „nicht grundsätzlich verboten", so ist dem zu widersprechen. Nach Art. 6 Abs. 1 UAbs. 1 DS-GVO ist die Verarbeitung „nur rechtmäßig" in Fällen, wo ein Erlaubnistatbestand einschlägt. Wie anders denn als „verboten" soll die Konsequenz für die verbleibenden Fälle bezeichnet werden?

7 Vgl. Erwägungsgrund 40.

8 Vgl. *Giesen* NVwZ 2019, 1711 (1713: „a priori freiheitswidrig"); *Veil* NVwZ 2018, 686 (688 f., 695); entsprechend zum TMG *Buchheim* JZ 2021, 539 (545).

Übermittlung in datenschutzrechtlich problematisches Ausland, wofür Art. 44, 49 DS-GVO ebenfalls ein eigenes präventives Verbot mit ähnlichen Erlaubnistatbeständen aufstellen (→ Art. 49 Rn. 4 ff.).[9]

Abs. 4 ist im Zusammenhang mit dem Verbot der Weiterverarbeitung zu unvereinbaren Zwecken in Art. 5 Abs. 1 lit. b Hs. 1 Var. 2 DS-GVO zu lesen (vgl. → Art. 5 Rn. 25 ff.). Dieses Verbot wird hier durch eine prozedurale Pflicht zur Berücksichtigung bestimmter Belange vor einer solchen Verarbeitung ergänzt (→ Rn. 92 ff.). 4

II. Bisherige Rechtslage

Abs. 1 der Bestimmung entspricht Art. 7 DSRL, dessen Struktur – Verbot und sechs Erlaubnistatbestände – genau und dessen Wortlaut im Wesentlichen übernommen wurden.[10] Die weiteren Absätze sind im Zuge des Übergangs zur Verordnungsform neu hinzugekommen; der mitgliedstaatliche Spielraum in Abs. 2, 3 musste nunmehr ausdrücklich eingeräumt werden. 5

Im Vergleich zu § 4 Abs. 1 BDSG aF reduziert Art. 6 DS-GVO die Reichweite des datenschutzrechtlichen Vorbehalts des Gesetzes in gewissem Umfang, indem es über die Einwilligung (Abs. 1 lit. a) hinaus eine Reihe stets geltender Erlaubnistatbestände unmittelbar vorsieht. Insbes. die Vertragserfüllung erfordert damit keine eigene gestattende Rechtsvorschrift mehr wie noch § 28 Abs. 1 S. 1 Nr. 1 BDSG aF, sondern stellt gemäß Abs. 1 lit. b unmittelbar eine rechtmäßige Verarbeitung dar. Dagegen bleibt es außerhalb von lit. a, b, d, f insofern bei einem Vorbehalt des Gesetzes, als hier gesonderte Rechtsgrundlagen vonnöten bleiben (→ Rn. 14). 6

III. Entstehung der Norm

Entgegen aller dagegen vorgebrachten Kritik[11] hat der Verordnungsgeber am generellen präventiven Verarbeitungsverbot festgehalten und Vorschläge für einen konsequent risikobasierten Ansatz nicht aufgenommen.[12] Angesichts des extrem weiten Verarbeitungsbegriffs der DS-GVO werden damit auch in vermeintlich einfachen Fällen komplexe Begründungen erforderlich,[13] was tendenziell eine weite Auslegung der Erlaubnistatbestände nahelegt. 7

Die Grundelemente der Vorschrift – Erlaubnistatbestände in Abs. 1 und Rechtsgrundlagenerfordernis in Abs. 3 S. 1 – standen fast wörtlich bereits im Kommissionsentwurf.[14] Korrigiert wurde insbes., dass nach dem Entwurf für den Erlaubnistatbestand nach lit. f das berechtigte Interesse eines

9 Teilweise werden Art. 6 Abs. 1 und 44 DS-GVO auch kumulativ angewandt (→ Art. 44 Rn. 23), wogegen allerdings die inhaltliche Spezialität der Erlaubnistatbestände von Art. 49 DS-GVO spricht, die grundsätzlich einen Erlaubnistatbestand von Art. 6 Abs. 1 DS-GVO als miterfüllt erscheinen lassen; vgl. *Reimer* VerwDatenschutzR-HdB, 2019, Rn. 119.

10 *Härting* BB 2012, 459 (462 f.).

11 Etwa von *Giesen* PinG 2013, 62; *Härting/Schneider* CR 2015, 819 (822 f.). Siehe jetzt auch *Schmidt-Jortzig* DVBl 2018, 10 (14); *Veil* NVwZ 2018, 686 (bes. 688f.).

12 Vgl. zur punktuellen Risikoorientierung *Veil* ZD 2015, 347; *de Jong* PinG 2020, 173.

13 *Wolff/Kosmider* ZD 2021, 13 (13).

14 KOM(2012) 11 endg., 50 f.

Dritten nicht genügen sollte;[15] das hätte womöglich die Auskunfteien existenziell gefährdet.[16] Nicht durchsetzen konnte sich die Kommission auch

- mit der generellen Zulassung der Weiterverarbeitung auch zu unvereinbaren Zwecken (entgegen Art. 5 Abs. 1 lit. b Var. 2 DS-GVO), sofern nur ein Erlaubnistatbestand nach Abs. 1 lit. a–e gegeben wäre[17] (der Rat hätte die Regelung auch noch auf lit. f ausgedehnt[18]),
- mit einem zusätzlichen Erlaubnistatbestand für wissenschaftliche und ähnliche Zwecke,[19]
- mit dem (in Art. 7 verorteten) Ausschluss der Einwilligung nach lit. a bei erheblichem Ungleichgewicht[20] sowie
- mit ihrer eigenen Ermächtigung zur tertiärrechtlichen Konkretisierung der Interessenabwägung nach lit. f.[21] Zur Konkretisierung desselben Erlaubnistatbestands hatte das Parlament vorgeschlagen, stattdessen einige Beispiele in die Erwägungsgründe aufzunehmen.[22] Auch dies wurde letztlich nicht aufgenommen, ebensowenig der Vorschlag der Artikel-29-Datenschutzgruppe, für die Abwägung nähere Kriterien zu bestimmen,[23] so dass insgesamt eine nur noch judikativ zu konkretisierende Generalklausel übriggeblieben ist (vgl. → Rn. 82).

8 Dass Verarbeitungen nach Abs. 1 lit. c und e einer zusätzlichen Rechtsgrundlage bedürfen sollten (vgl. → Rn. 14 f., 37 ff., 64 ff.), stand während des ganzen Gesetzgebungsverfahrens fest. Die jetzt in Abs. 2 vorgenommene weitgehende Öffnung dieser beiden Erlaubnistatbestände für mitgliedstaatliche Spezifizierungen und Präzisierungen verdankt sich dem Rat, der sie ursprünglich sogar programmatisch im ersten Artikel der Verordnung hatte unterbringen wollen.[24]

15 Nur punktuelle Erweiterung durch das Parlament: P7_TA(2014)0212, 12.3.2014, 110 (Änderungsantrag 100).
16 Vgl. *Gola/Schulz* RDV 2013, 1 (6); *Breinlinger/Scheuing* RDV 2012, 64 (70 f.); *Dehmel/Hullen* ZD 2013, 147 (149). Zu Auskunfteien jetzt *von Lewinski/Pohl* ZD 2018, 17; *Buchner* FS Taeger, 2020, 95.
17 Dagegen schon *Europäischer Datenschutzbeauftragter*, Stellungnahme zum Datenschutzreformpaket, 7.3.2012, Tz 66 f., 121; *Artikel-29-Datenschutzgruppe*, Stellungnahme 03/2013, 569/13/EN, 36 f.; zur Kritik auch *Gola/Schulz* RDV 2013, 1 (7).
18 Ratsdok. 9565/15, 11.6.2015, 85.
19 Dagegen insbes. *Artikel-29-Datenschutzgruppe*, Stellungnahme 03/2013, 569/13/EN, 33.
20 Kritisch bezüglich des Arbeitsverhältnisses *Wybitul/Rauer* ZD 2012, 160 (162), bezüglich des Verbraucher-Unternehmer-Verhältnisses *Buchner* DuD 2016, 155 (158). Siehe jetzt aber Erwägungsgrund 43 und etwa *Laue/Nink/Kremer* DatenschutzR § 2 Rn. 17.
21 Kritisch aus Gründen der demokratischen Legitimation etwa *Beyvers* PinG 2015, 60 (64); aus Gründen der Bestimmtheit der Vorschrift selbst Simitis/*Simitis*, 6. Aufl. 2006, Einleitung Rn. 256 f.; im Ergebnis auch *Roßnagel* DuD 2017, 277 (278); vgl. → Einleitung Rn. 30 f.
22 Parlamentsdok. P7_TA(2014)0212, 12.3.2014, 16 f. (Änderungsanträge 17, 18). Zustimmend *Beyvers* PinG 2015, 60 (64); kritisch *Dehmel/Hullen* ZD 2013, 147 (149).
23 *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014, 844/14/EN, 66.
24 Ratsdok. 9565/15, 11.6.2015, 75.

B. Kommentierung

I. System der Erlaubnistatbestände

Die sechs Erlaubnistatbestände des Abs. 1 stehen **alternativ** nebeneinander, ohne dass einer davon besonders herausgehoben wäre. Weder lit. a[25] noch lit. f[26] genießen Vorrang. 9

Die Vorschrift erwähnt dabei auch ausdrücklich den Fall, dass mehrere Erlaubnistatbestände **kumulativ** verwirklicht sein können. So wird die Erfüllung einer Rechtspflicht (lit. c) gewiss oft zugleich einer öffentlichen Aufgabe (lit. e) oder einem berechtigten Interesse (lit. f) dienen. Zur Begründung der Rechtmäßigkeit einer Verarbeitung genügt aber bereits eines davon; darauf kann es ankommen, sollte einer von mehreren angenommenen Erlaubnistatbeständen doch ausfallen,[27] wie Art. 17 Abs. 1 lit. b DS-GVO deutlich zeigt (für den Wegfall von lit. a).[28] Auch wenn die Verarbeitung danach rechtmäßig ist, muss der Verantwortliche aber auf die Transparenz der genutzten Erlaubnistatbestände, also seine Pflichten aus Art. 5 Abs. 1 lit. a Var. 3 und Art. 12 ff. DS-GVO, achten (vgl. → Art. 5 Rn. 16 ff., Art. 13 Rn. 18).[29]

Auch kann ein Erlaubnistatbestand grds. zugleich eine **Weiterverarbeitung derselben Daten** tragen, dies jedoch nur, wenn seine Voraussetzungen dafür ebenfalls vorliegen.[30] Ansonsten müsste ein neuer Erlaubnistatbestand bemüht werden (ergänzend ist Art. 5 Abs. 1 lit. b Hs. 1 Var. 2 DS-GVO zu beachten, wobei das Verhältnis noch nicht ganz geklärt ist, vgl. → Art. 5 Rn. 26). 10

1. Persönlicher Anwendungsbereich

Alle Erlaubnistatbestände stehen grds. jedermann, insbes. öffentlichen und nichtöffentlichen Stellen gleichermaßen zur Verfügung. Die Ausnahme bil- 11

25 Das gilt es angesichts des „‚Einwilligungswahn[s]'" – so *Uecker* ZD 2019, 248 (248) – zu betonen. Entgegen BSG 28.11.2019 – B 8 SO 55/17 B, juris, Rn. 12 kommt es für Abs. 1 lit. c auf eine Einwilligung überhaupt nicht an. Wie hier etwa *Veil* NJW 2018, 3337 (3344). Vorrang hatte die Einwilligung noch nach § 4 Abs. 1 BDSG aF, vgl. *Laue/Nink/Kremer* DatenschutzR § 2 Rn. 4. Dagegen auch weiterhin für ein Verbot des Rückgriffs auf andere Tatbestände neben einer unwirksamen Einwilligung *Schneider* CR 2017, 568 (573); zur Kritik *Härting/Gössling/Dimov* ITRB 2017, 169 (171). Besser lässt sich das Problem nach neuem Recht als Transparenzfrage einordnen, dazu bei und in Fn. 35.

26 Für Vorrang hier (noch zur DSRL) *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014, 844/14/EN, 13, 62.

27 *Krusche* ZD 2020, 232 (234f.); *Veil* NJW 2018, 3337 (3342). Mit Blick auf die Wirksamkeit von Einwilligungen gegenüber Dritten raten zur Kumulation auch *Kollmar/El-Auwad* K&R 2021, 73 (77).

28 Vgl. Plath/*Plath* Art. 6 Rn. 6; *Waldkirch* VersR 2020, 1141 (1147).

29 Vgl. *Ruschemeier* ZD 2020, 618 (618f.); an „Treu und Glauben", also Art. 5 Abs. 1 lit. a Var. 2 DS-GVO, machen das Gleiche fest *Breyer* DuD 2018, 311 (312); *Uecker* ZD 2019, 248 (249). Zwischen Transparenz- und Rechtsgrundlagenfehler unentschieden *Krusche* ZD 2020, 232 (236).

30 Vgl. Erwägungsgrund 50 Abs. 1 S. 2, 5. Eine großzügigere Lesart von S. 2 („keine andere gesonderte Rechtsgrundlage erforderlich") dahin, es brauche für die Weiterverarbeitung kein Erlaubnistatbestand vorzuliegen, ist abzulehnen, vgl. *Schantz* NJW 2016, 1841 (1844); aA mN Roßnagel Neues DatenschutzR/*Roßnagel*, 2018, § 3 Rn. 68.

det das Paar von „berechtigtem Interesse“ (lit. f: grundsätzlich keine Hoheitsträger, vgl. → Rn. 90 f.) einerseits, „öffentlicher Gewalt“ (lit. e Var. 2: nur Hoheitsträger, vgl. → Rn. 62 f.) andererseits. Eine in ihrer Tragweite noch nicht zu beurteilende Einschränkung erfährt der Erlaubnistatbestand der Einwilligung (lit. a) durch den Hinweis im Erwägungsgrund 43 S. 1, wonach Verarbeitungsverantwortliche bei „klarem Ungleichgewicht“ sich darauf nicht berufen können sollen (vgl. → Art. 7 Rn. 27 ff.).

12 Für die Datenverarbeitung der mitgliedstaatlichen Sicherheitsbehörden regelt die Rechtmäßigkeit Art. 8 RL (EU) 2016/680 (bundesrechtlich nicht ausdrücklich umgesetzt, vgl. → BDSG § 3 Rn. 20), für die der Unionsorgane Art. 5 VO (EU) 2018/1725.

2. Tatbestandsmerkmal Erforderlichkeit

13 Alle Erlaubnistatbestände außer dem der Einwilligung (lit. a) setzen voraus, dass die Verarbeitung im Hinblick auf ein gewisses Ziel „**erforderlich**“ ist:[31]

- für die Erfüllung einer Vertrags- oder sonstigen Rechtspflicht (lit. b Var. 1, lit. c),
- für die Durchführung vorvertraglicher Maßnahmen (lit. b Var. 2),
- für den Schutz eines lebenswichtigen oder doch zumindest berechtigten Interesses (lit. d, f) oder
- für die Wahrnehmung einer öffentlichen Aufgabe (lit. e).

Die im deutschen Verhältnismäßigkeitsdenken eng mit der Erforderlichkeit verbundene Angemessenheit nach **Abwägung** wird dagegen **nur bei lit. f** vorausgesetzt (vgl. → Rn. 82 ff.).[32] Man mag das so ausdrücken, dass die Verordnung für die lit. b–e „die Abwägung vorweggenommen hat“.[33]

3. Tatbestandsmerkmal Rechtsgrundlage

14 Zwei Erlaubnistatbestände, lit. c und e, wirken nicht aus sich heraus, sondern gemäß Abs. 3 nur iVm einer besonderen unionalen oder mitgliedstaatlichen Rechtsgrundlage außerhalb der DS-GVO (vgl. → Rn. 37 ff. bzw. 64 ff.); die Verordnung baut insofern teilweise auf dem einzelstaatlichen Recht auf.[34] Das bringt einige Besonderheiten mit sich, weshalb die Verordnung mehrfach tatbestandlich an diese beiden Regelungen anknüpft (Art. 6 Abs. 2, Art. 35 Abs. 10, Art. 55 Abs. 2 DS-GVO). Insbesondere steht es den Mitgliedstaaten nach Abs. 2 (nur[35]) insoweit frei, zusätzliche **nationale Anforderungen** an das Gebrauchmachen von diesen beiden Erlaubnistatbeständen zu stellen.

31 Vgl. ausführlich *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 165–170, sowie Paal/Pauly/*Frenzel* DS-GVO Art. 6 Rn. 9, der einen Zusammenhang zu Art. 5 Abs. 1 lit. c, e DS-GVO herstellt; s. a. *Samardzic/Becker* EuZW 2020, 646 (649).
32 Zu weit daher *Bull* JZ 2017, 797 (806).
33 *Klaas* CCZ 2020, 256 (261).
34 Vgl. Roßnagel Neues DatenschutzR/*Nebel*, 2018, § 3 Rn. 98: „Scharniernormen“.
35 *Roßnagel/Kroschwald* ZD 2014, 495 (497). Regeln für Einwilligungen sind ausgeschlossen; aA offenbar *Sackmann* PinG 2019, 277 (278).

Soweit eine Verarbeitung nur auf lit. c oder e gestützt werden kann, bewirkt Abs. 3 für die Verantwortlichen insoweit einen **Vorbehalt des Gesetzes**. Für die mitgliedstaatliche Staatsgewalt in Durchführung des Unionsrechts konkretisiert es damit den von Art. 8 Abs. 2 S. 1 EUGRCh aufgestellten oder verlangten Vorbehalt des Gesetzes.[36] Für nicht grundrechtsgebundene, private Stellen stellt es ihn dagegen erst selbst auf[37] (soweit diese sich nicht auf Abs. 1 lit. a, d, f berufen können) und macht sich damit grds. rechtfertigungsbedürftig nach Art. 11, 16 EUGRCh, die hier als „Grundrecht auf Datenverarbeitung" fungieren.[38] 15

4. Weitere Gruppierungen

Zwei Erlaubnistatbestände, lit. e und f., lösen das **Widerspruchsrecht** nach Art. 21 Abs. 1 DS-GVO aus, dessen Ausübung uU auch einer an sich rechtmäßigen Verarbeitung entgegensteht. Hintergrund ist ein „potenziell sehr breit gefächertes Anwendungsspektrum" dieser beiden Erlaubnistatbestände.[39] Zusammen mit der Einwilligung nach lit. a, wo die Widerrufsmöglichkeit des Art. 7 Abs. 4 DS-GVO besteht, sind dies die drei Erlaubnistatbestände, auf deren Bestand die betroffene Person Einfluss nehmen kann.[40] 16

An die beiden Erlaubnistatbestände lit. a und lit. b ist die **Datenübertragbarkeit** nach Art. 20 Abs. 1 DS-GVO geknüpft; die Gemeinsamkeit liegt hier in der Freiwilligkeit der betroffenen Person (vgl. → Rn. 21). Schlägt zugleich lit. e ein, wird die Datenübertragbarkeit aber wieder ausgeschlossen (Art. 20 Abs. 3 S. 2 DS-GVO; vgl. → Art. 20 Rn. 16 f.).

36 Vgl. dazu ausführlich *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 153–157. – Für die Unionsorgane gilt gemäß Art. 2 Abs. 3 DS-GVO Sonderrecht (siehe auch Erwägungsgrund 17); die Rechtmäßigkeit regelt hier Art. 5 VO (EG) Nr. 45/2001.

37 Die aus grundrechtsdogmatischer Sicht fernliegende Behauptung einer unmittelbaren Bindung Privater an das Datenschutzgrundrecht wird durch ihre Wiederholung nicht überzeugender, doch siehe – im Anschluss an eine These von *Simitis* NJW 1984, 398 (401) – *Roßnagel* ZD 2013, 562 (563); *Roßnagel* ZD 2018, 339 (340); Roßnagel Neues DatenschutzR/*Roßnagel* , 2018, § 3 Rn. 51; *Roßnagel* NJW 2019, 1 (3). Die zu weit geratene Äußerung von EuGH 17.10.2013 – C-291/12, Rn. 25 – Schwarz – steht selbst im Kontext nur staatlicher Maßnahmen; in EuGH 6.11.2003 – C-101/01, Rn. 80 – Lindqvist – sowie EuGH 13.5.2014 – C-131/12, Rn. 68 – Google Spain – geht es um die grundrechtsorientierte Auslegung einer Richtlinie. Zur nur mittelbaren Grundrechtsbindung Privater auch nach Art. 8 EUGRCh vgl. *Reinhardt* AöR 142 (2017), 528 (544–553); *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 247–269; allgemein und je mwN etwa FK-EUV/GRC/AEUV/*Pache*, 2017, Art. 51 Rn. 38; Schwarze/*Hatje*, 4. Aufl. 2019, Art. 51 Rn. 22.

38 Begriff: *Giesen* PinG 2013, 62 (64). Den Unterschied zwischen öffentlichem und privatem Bereich betont namentlich *Masing* NJW 2012, 2305 (2306 f.); zur DS-GVO vgl. *Blume* EDPL 2015, 32 (38); *Stentzel* PinG 2016, 45 (47, 49); *Reimer* BRJ 2018, 6 (9 f.).

39 *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014, 844/14/EN, 28.

40 Das macht insbes. Abs. 1 lit. b attraktiv: *Gausling* ZD 2019, 335 (336).

II. Die einzelnen Erlaubnistatbestände (Abs. 1–3)

1. Einwilligung (Abs. 1 lit. a)

17 Erlaubt ist die Verarbeitung, wenn die betroffene Person ihre Einwilligung iSv Art. 4 Nr. 11 DS-GVO gegeben hat.[41] Nähere Voraussetzungen enthalten Art. 7 sowie für Kinder Art. 8 DS-GVO. Für sensible Daten korrespondiert Abs. 1 lit. a der Erlaubnistatbestand des Art. 9 Abs. 2 lit. a DS-GVO (→ Art. 9 Rn. 12 ff.), für die Übermittlung in datenschutzrechtlich problematisches Ausland derjenige des Art. 49 Abs. 1 S. 1 lit. a DS-GVO (→ Art. 49 Rn. 5 ff.); beide sind etwas enger gefasst. Hat die Einwilligung die Gestalt der Zustimmung zu einem Vertrag, so gilt Abs. 1 lit. b (→ Rn. 21 ff.).[42] Auch sonst sollte der Rückgriff auf eine Einwilligung vermieden werden, wenn ein anderer Erlaubnistatbestand zur Verfügung steht, damit nicht durch Vorspiegeln einer tatsächlich nicht bestehenden Wahlmöglichkeit ein Transparenzverstoß in Bezug auf Art. 5 Abs. 1 lit. a Var. 3 DS-GVO riskiert wird (→ Rn. 9).

Die Klausel schreibt Art. 7 lit. a DSRL fort; das Erfordernis der Erklärung „ohne jeden Zweifel" ist nur in die Legaldefinition der Einwilligung übergegangen und lautet dort jetzt „unmissverständlich" (englisch „unambiguous").

18 Die Einwilligung muss

- der betroffenen Person als Erklärung zuzurechnen sein (eine bloße Opt-out-Möglichkeit genügt nicht[43]), wenn auch nicht unbedingt ausdrücklich erfolgen,[44] wie der Umkehrschluss aus Art. 9 Abs. 2 lit. a DS-GVO ergibt;
- sich auf konkrete Daten und konkrete („bestimmte") Verarbeitungszwecke beziehen (eine Datenschutzerklärung des Verantwortlichen kann dafür den Auslegungshintergrund bilden[45]);
- freiwillig sein (vgl. Erwägungsgrund 43 und Art. 7 Abs. 4 DS-GVO),[46] was besonders das Arbeitnehmer- und das Verwaltungsdatenschutzrecht herausfordert (zu letzterem sogleich → Rn. 20). Im Übrigen dürfte die Freiwilligkeit gegenüber anderen Privaten höchstens dann anzuzweifeln sein, wenn diese eine Monopolstellung auf eine unverzichtbare Leistung innehaben (Energie, Wasser, eher nicht Messengerdienste[47]). Erfolgt die Einwilligung im Hinblick auf eine im Übrigen kostenlose Leistung, wird die Freiwilligkeit jedenfalls durch das Alternativan-

41 Vgl. dazu insgesamt *Europäischer Datenschutzausschuss*, Leitlinien 05/2020 zur Einwilligung gemäß Verordnung 2016/679, Version 1.1, 4.5.2020.
42 Dennoch auf Abs. 1 lit. a rekurrierend OLG Dresden NJW-RR 2020, 1370 (1373 Rn. 21).
43 EuGH 1.10.2019 – C-673/17, Rn. 60–63 – Planet49.
44 Beispiel für konkludente Einwilligung nach *Ehmann* ZD 2020, 65 (68): „Posing für die Kamera".
45 Vgl. dazu mit Blick auf die empirische Seite *Gerpott* MMR 2020, 739.
46 Dazu Erwägungsgrund 43, → Art. 7 Rn. 25 ff. sowie *Ruschemeier* ZD 2020, 618.
47 Diesbezüglich wohl zu weit *Bretthauer* VerfBlog, 2021/5/14, https://verfassungsblog.de/hamburg-schreitet-ein/.

gebot einer entgeltlichen Leistung ohne entsprechende Einwilligung („Pur-Abonnement" oä) sichergestellt.[48]

- zum Zeitpunkt der Verarbeitung noch gelten.[49] Neben dem von selbst eintretenden Erlöschen einer ausdrücklich oder konkludent befristeten Einwilligung ist nach Art. 7 Abs. 3 S. 1 DS-GVO auch ein ausdrücklicher Widerruf möglich, der weiteren Verarbeitungen nach Abs. 1 lit. a ex nunc entgegensteht (→ Art. 7 Rn. 45 ff.). Die bis dahin erfolgten Verarbeitungen macht der Widerruf aber nicht rechtswidrig (Art. 7 Abs. 3 S. 2 DS-GVO), sondern verpflichtet – bei Fehlen eines alternativen Erlaubnistatbestands – nur zur Löschung der gespeicherten Daten (Art. 17 Abs. 1 lit. b DS-GVO).[50] Umgekehrt sollte auch eine rückwirkende Einwilligung möglich sein.[51]

Dagegen muss die Einwilligung nicht gerade gegenüber dem Verantwortlichen erteilt worden sein. Möglich ist damit sowohl die gewillkürte Einholung von Einwilligungen durch Dritte als auch die Anwendung von Einwilligungen, die noch dem Vermögensträger erteilt wurden, etwa durch einen Insolvenz- oder Nachlassverwalter. Freilich trägt der Verantwortliche wie stets das Risiko, dass die Einwilligung unwirksam sein könnte, und hat darauf in diesen Dreiecksfällen geringen Einfluss. 19

Auch Fragen der Erforderlichkeit der Verarbeitung oder einer Interessenabwägung stellen sich bei der Einwilligung nicht (vgl. → Rn. 13).[52]

Für den **öffentlichen Bereich** bildet die Regelung die grundrechtliche Situation ab, dass bei Vorliegen einer Einwilligung schon der Schutzbereich von Art. 8 Abs. 2 S. 1 EUGRCh nicht berührt ist (wie auch ein Eingriff in das deutsche Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 GG dann nicht gegeben ist). Allerdings kann angesichts von Machtasymmetrien und Monopolstellungen[53] die Freiwilligkeit der Einwilligung gegenüber einer staatlichen Stelle zu verneinen sein. Sie kommt aber überall dort in Frage, wo der betroffenen Person eine echte Wahl bleibt (zB zwischen Online- und Präsenzprüfung hinsichtlich des Mehrs an Verarbeitun- 20

48 *Golland* MMR 2018, 130 (134 f.). Sozialpolitische Kritik hieran übt *Engeler* PinG 2019, 149 (152); freilich geht es in solchen Fällen um den Zugang zu einer Leistung, auf die kein Anspruch besteht, und hat jeder Nutzer die Möglichkeit zu entscheiden, was ihm das Unterbleiben der Datenverarbeitung wert ist (mitnichten dürfte es so sein, dass Reiche stets „Pur-Abonnements" abschlössen).

49 Hierzu *Rolfs* FS Taeger, 2020, 373. Zum Sonderproblem der Fortgeltung vor Inkrafttreten der DS-GVO erteilter Einwilligungen *Freiherr von Ulmenstein* ZD 2019, 117.

50 Vgl. *Laue/Nink/Kremer* DatenschutzR § 2 Rn. 14.

51 *Piltz/Zwerschke* DSB 2020, 148.

52 *Samardzic/Becker* EuZW 2020, 646 (649, 653).

53 *Ruschemeier* ZD 2020, 618 (620), zum öffentlichen Personennahverkehr.

gen[54] oder zwischen Installation oder Nichtinstallation einer Smartphone-App[55]).

2. Vertragserfüllung oder -vorbereitung (Abs. 1 lit. b)

21 Erlaubt ist die Verarbeitung, wenn die **betroffene Person Partei eines Vertrages** ist (Var. 1) oder erkennbar („auf Anfrage") werden will (Var. 2) und die Verarbeitung in diesem Zusammenhang erforderlich ist.[56] Dieser Erlaubnistatbestand verlängert gewissermaßen den der Einwilligung (Abs. 1 lit. a): zwar wird hier nicht unbedingt ausdrücklich der Verarbeitung als solcher zugestimmt, doch wird diese als notwendiges Zwischenziel gewissermaßen von der Freiwilligkeit des Vertragsschlusses mitumfasst.[57] Daten unbeteiligter Dritter dürfen dementsprechend nicht nach Abs. 1 lit. b verarbeitet werden.[58] In Anbetracht der Bindungswirkung eines Vertrags gibt es anders als bei der Einwilligung (Art. 7 Abs. 3 DS-GVO) keinen freien datenschutzrechtlichen Widerruf und auch kein Widerspruchsrecht (Art. 21 DS-GVO),[59] sondern nur die etwaigen vertragsrechtlichen Widerrufs- oder Kündigungsrechte.

Für die Übermittlung in datenschutzrechtlich problematisches Ausland korrespondiert Abs. 1 lit. b der Erlaubnistatbestand des Art. 49 Abs. 1 S. 1 lit. b DS-GVO (→ Art. 49 Rn. 10). Für sensible Daten gilt eine entsprechende Regelung nur punktuell nach Art. 9 Abs. 2 lit. b und h DS-GVO (→ Art. 9 Rn. 15 ff., 41 ff.).[60]

Die Veränderung gegenüber Art. 7 lit. b DSRL ist nur einer veränderten Übersetzung geschuldet; die englischen Sprachfassungen sind identisch.

54 SchlHOVG NJW 2021, 1407 Rn. 59; *Albrecht/Mc Grath/Uphues* ZD 2021, 80 (82 f.).

55 *Ruschemeier* ZD 2020, 618 (621 f.); s. a. *Samardzic/Becker* EuZW 2020, 646. Überraschend ausführlich behandelt die Frage *Robert Koch-Institut*, Bericht zur Datenschutz-Folgenabschätzung für die Corona-Warn-App der Bundesrepublik Deutschland, Öffentliche Version, Version 1.15, 12.7.2021, 146–150; deutliche Worte dazu bei *Giesen* PinG 2021, 96. Zu Corona-bezogenen Apps vgl. außerdem ausführlich *Dochow* GuP 2020, 129; *Blaeser/dos Santos Firnhaber* RDG 2020, 182.

56 Einschlägig, aber nichtssagend Erwägungsgrund 44. – Vgl. insgesamt *Europäischer Datenschutzausschuss*, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DS-GVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, Version 2.0, 8.10.2019.

57 Ähnlich *Heinzke/Engel* ZD 2020, 189 (189); *Traung* CRi 2012, 33 (41).

58 Vgl. *Wolff/Kosmider* ZD 2021, 13 (14) mwN AA, ohne das Problem zu sehen, KG ZD 2019, 272 Rn. 22. Möglich ist freilich, dass mit dem Dritten ein eigener Vertrag besteht; so für das Dreieck Plattformbetreiber–Nutzer–Kommunikationspartner BGHZ 219, 243 (268 f. Rn. 72), für das Dreieck Gesellschaft–Gesellschafter–Mitgesellschafter OLG München ZD 2019, 171 Rn. 30.

59 Vgl. *Gausling* ZD 2019, 335 (336).

60 Vgl. *Reimer* VerwDatenschutzR-HdB, 2019, Rn. 142.

a) Vertrag

„**Vertrag**" dürfte nur ein – im Falle des Abschlusses[61] – materiellrechtlich wirksamer sein,[62] was sich dann nach dem jeweils anwendbaren mitgliedstaatlichen Recht bestimmt (ggf. begrenzt durch den autonomen Gehalt des Verweises in Abs. 1 lit. b). Bürgerlichrechtliche Verträge (insbes. über Arbeits-, aber auch zB Mitgliedschaftsverhältnisse[63]) kommen ebenso in Betracht wie öffentlich-rechtliche. 22

Ausscheiden dürften aber Kollektivverträge (wie Betriebsvereinbarungen und Tarifverträge) in Bezug auf die Daten der an die vertraglichen Normen gebundenen natürlichen Personen (Arbeitnehmer und ggf. Arbeitgeber), die nicht selbst Vertragsparteien sind;[64] denn die Bindung ist hier nicht in gleichem Sinne freiwillig wie bei einem eigenen Vertragsschluss,[65] sondern für die Betroffenen eher mit einer gesetzlichen Pflicht vergleichbar und fällt daher höchstens unter Abs. 1 lit. c (vgl. → Rn. 35 ff.). Auch hoheitlich begründete Rechtsverhältnisse wie dasjenige zwischen Gericht und Sachverständigem, den nach Vorschriften wie § 407 ZPO eine Rechtspflicht im Sinne von Abs. 1 lit. c trifft, passen kaum hierher.[66]

Typischerweise ist der Verantwortliche zugleich der – ursprüngliche oder durch Gesamt- oder Einzelrechtsnachfolge (Zession) eingetretene – **Vertragspartner** der betroffenen Person; dann erscheint Var. 1 zugleich als Spezialfall des Erlaubnistatbestands der Pflichterfüllung (Abs. 1 lit. c), aus dem auf diese Weise die vertraglichen Pflichten herausgeschnitten und von dem Erfordernis einer besonderen Rechtsgrundlage (Abs. 3) freigestellt werden; durch den impliziten Verweis auf das (mitgliedstaatliche) Vertragsrecht wird dieses freilich der Sache nach als Rechtsgrundlage aktiviert, auch wenn eine autonome Auslegung des Erlaubnistatbestands angemahnt wird.[67] 23

Soweit dagegen der Verantwortliche selbst **am Vertrag nicht beteiligt** ist, muss er normalerweise entweder vom Vertragspartner in die Vertragsanbahnung oder -durchführung eingeschaltet[68] (etwa als Rechtsberater, Auskunftei[69] oder Inkassodienstleister[70]) oder hoheitlich dem Vertragspartner 24

61 Während vorvertraglicher Maßnahmen iSd Var. 2 kann der Vertrag natürlich noch nicht wirksam sein, und er muss auch im Ergebnis nicht zustande kommen (siehe BeckOK DatenschutzR/*Albers/Veit* Art. 6 Rn. 33), sondern nur rechtlich überhaupt möglich sein.
62 Vgl. *Heinzke/Engel* ZD 2020, 189 (190 f.); zu nichtigen Verträgen Kühling/Buchner/*Buchner/Petri* Art. 6 Rn. 31. Jedenfalls *reine* Gefälligkeitsverhältnisse scheiden aus: ebd., Rn. 30 mit Fn. 60; BeckOK DatenschutzR/*Albers/Veit* Art. 6 Rn. 30.
63 BGH NZG 2020, 381 Rn. 30; *Uecker* ZD 2019, 248 (250).
64 AA *Wybitul/Fladung* BB 2012, 509 (515).
65 *Klaas* CCZ 2020, 256 (259); vgl. mit Hinweis zur Entstehungsgeschichte Kühling/Buchner/*Buchner/Petri* Art. 6 Rn. 32.
66 So aber *Erkelenz/Leopold* NZS 2019, 926 (929).
67 *Golland* MMR 2018, 130 (132).
68 *Laue/Nink/Kremer* DatenschutzR § 2 Rn. 26; s. a. VG Mainz ZD 2020, 376 Rn. 29.
69 *Krämer* NJW 2020, 497 (498); aA *Buchner* FS Taeger, 2020, 95 (101): nur Abs. 1 lit. f. Fraglich ist in jedem Fall aber die Erforderlichkeit.
70 *Raji* ZD 2020, 279 (280).

beigegeben worden sein (etwa als Insolvenzverwalter[71]),[72] damit die Verarbeitung als zur Vertragserfüllung erforderlich gelten kann. Freilich trägt der nichtbeteiligte Verantwortliche das Risiko, dass der Vertrag unwirksam sein könnte.[73]

Eine vorangehende Datenübermittlung vom Vertragspartner der betroffenen Person an den nunmehrigen Verantwortlichen wird sich – sofern nicht vereinbart – normalerweise nicht als zur Erfüllung des Vertrags erforderlich auf Abs. 1 lit. b stützen können,[74] sondern nur auf Einwilligung oder berechtigte (Vermögens-)Interessen.

b) Erforderlichkeit

25 Einer Interessenabwägung bedarf es für Abs. 1 lit. b nicht.[75] Auch wird der Vertrags*inhalt* als solcher nicht datenschutzrechtlich kontrolliert.[76] Allein auf die Erforderlichkeit der Verarbeitung kommt es an, die zwei verschiedene Bezugspunkte hat.[77]

aa) Erfüllung eines Vertrags

26 Nach Var. 1 bezieht sich die Erforderlichkeit auf die **Erfüllung** des Vertrags. Auch wenn das erkennbar über die bloße Leistungserbringung iSv § 362 BGB hinausgeht, umfasst dieses Merkmal nicht jegliches vertragsbezogenes Handeln. Die Existenz des Vertrags selbst wird vorausgesetzt, so dass dessen Abschluss[78] ebensowenig wie dessen Abänderung durch einen weiteren Vertrag zur Erfüllung gehört;[79] für beides wäre systematisch Var. 2 zu bemühen (→ Rn. 33 f.). Auch die Beendigung[80] (Kündigung, Rücktritt) oder Übertragung[81] (Abtretung) vertraglicher Schuldverhältnisse verändern nur die Existenz bzw. die Personenkonstellation; da sie grundsätzlich im berechtigten Interesse des Beendigenden bzw. des Zedenten er-

71 Zu dessen Stellung als Verantwortlicher vgl. nur *Theurich/Degenhardt* NZI 2018, 870 (871 f.).
72 Dies mögen die wesentlichen weiteren Fälle sein, die Plath/*Plath* Art. 6 Rn. 15 antizipiert.
73 *Wolfff/Kosmider* ZD 2021, 13 (14) mit Hinweis auf §§ 15, 53 HGB, die dem Verantwortlichen hier nützen können.
74 So aber *Krämer* NJW 2018, 347 (347).
75 *Ziegenhorn/von Heckel* NVwZ 2016, 1585 (1588).
76 Vgl. *Bock* CR 2020, 173; *Engeler* PinG 2019, 149 (151 f.); *Heinzke/Engel* ZD 2020, 189 (190, mit Hinweis auf Art. 16 GRCh 192); *Indenhuck/Britz* BB 2019, 1091.
77 Vgl. mit vielen Beispielen zu beiden Varianten Schaffland/Wiltfang/*Schaffland/Holthaus* Art. 6 (Lfg. 7/21) Rn. 6–108.
78 Wenn BeckOK DatenschutzR/*Albers/Veit* Art. 6 Rn. 31 hierfür auf Erwägungsgrund 44 verweisen, geht das fehl; dort wird Abs. 1 lit. b insgesamt paraphrasiert, so dass die Wendung vom „geplanten Abschluss" offenbar auf dessen Var. 2 („Durchführung vorvertraglicher Maßnahmen") zu beziehen ist.
79 So aber etwa *Abel* ZD 2018, 103 (106, unter ungenauer Zitierung der Vorauflage); Plath/*Plath* Art. 6 Rn. 11. Zum Änderungsvertrag wie hier BeckOK DatenschutzR/*Albers/Veit* Art. 6 Rn. 31.
80 Für Abs. 1 lit. b hier aber *Gola/Wronka* RDV 2018, 309 (312).
81 Für Abs. 1 lit. b hier aber *Abel/Djagani* ZD 2017, 114 (117 zum Verkauf, 119 zur Due Diligence); *Härting* CR 2017, 724 (727); *Klausch/Mentzel* BB 2020, 1610 (1611).

folgen, lassen sich dafür erforderliche Datenverarbeitungen auf Abs. 1 lit. f stützen.

27 Erforderlichkeit zur Erfüllung heißt bei unbefangener Lesart: eine vertragliche (Primär-, Sekundär-,[82] Neben-[83] oder Rückabwicklungs-[84])**Pflicht kann nicht** auf zumutbare und rechtmäßige Weise **erfüllt werden, ohne dass das Datum verarbeitet würde.**[85]

Eine verarbeitungsfreundlichere Lesart, die „erforderlich" mit „objektiv sinnvoll im Vertragskontext" gleichsetzt,[86] stimmt dagegen nicht recht mit der Datenminimierungspflicht aus Art. 5 Abs. 1 lit. c DS-GVO zusammen, die eine Verarbeitung ohnehin der strengeren Erforderlichkeitsprüfung unterwirft (→ Art. 5 Rn. 35); systematisch spricht das für ein einheitliches Verständnis. Der Vorschlag, die Erforderlichkeit im Sinne einer Interessenabwägung zu bestimmen,[87] verkennt die systematische Trennung zwischen Erforderlichkeitsprüfung und Abwägung in Abs. 1, wo letztere nur in lit. f erscheint (→ Rn. 13). Die Regelungsabsicht von Abs. 1 lit. b, eine Art verbindlicher Einwilligung zu schaffen (→ Rn. 21), weist jedenfalls darauf, dass die Grenze dieses Erlaubnistatbestands wohl in dem von der betroffenen Person zumindest implizit Gebilligten liegt;[88] auch dies spricht für eine Begrenzung auf das, was verbindlicher Vertragsinhalt geworden ist. Das nötigt im Ergebnis zur Ausgrenzung sonstiger Verarbeitungen im Vertragskontext (→ Rn. 31).

28 **Adressat der Pflicht**, die den Bezugspunkt der Var. 1 bildet, wird in systematischer Parallele zu Abs. 1 lit. c regelmäßig der am Vertrag beteiligte Verantwortliche (→ Rn. 23) bzw. allgemeiner der Vertragspartner der betroffenen Person (→ Rn. 24) sein.[89]

Die insoweit offene Formulierung von Var. 1 schließt es aber nicht aus, auch die vertraglichen Pflichten der betroffenen Person selbst einzubeziehen, also den Fall, dass eine Verarbeitung durch den Verantwortlichen für die Vertragserfüllung durch die *Gegenseite* erforderlich sein sollte. Dabei würde es also um ggf. notwendig werdende Mitwirkungshandlungen des Verantwortlichen gehen.

82 Vgl. Kühling/Buchner/*Buchner/Petri* Art. 6 Rn. 33; Plath/*Plath* Art. 6 Rn. 11.
83 Vgl. BeckOK DatenschutzR/*Albers/Veit* Art. 6 Rn. 31.
84 Vgl. *Europäischer Datenschutzausschuss*, Leitlinien 2/2019, Tz. 42. Anders als die Kündigung selbst, die eine Vertragspartei im eigenen Interesse erklärt, stellen sich die Pflichten des Rückgewährschuldverhältnisses als von vornherein mitzudenkende Umgestaltung des Vertragsinhalts dar.
85 Gleichsinnig *Europäischer Datenschutzausschuss*, Leitlinien 2/2019, Tz. 25 (statt „zumutbar" heißt es dort „realistisch"). Von Zumutbarkeit sprechen auch Kühling/Buchner/*Buchner/Petri* Art. 6 Rn. 45.
86 So Gola/*Schulz* DS-GVO Art. 6 Rn. 38; dem folgend OLG München ZD 2019, 171 Rn. 30 (zustimmend *Wehmeyer* PinG 2019, 182, kritisch *Paul* GWR 2019, 413).
87 BeckOK DatenschutzR/*Albers/Veit* Art. 6 Rn. 32.
88 *Wehmeyer* PinG 2019, 182 (184).
89 Davon scheinen die meisten Kommentierungen implizit auszugehen, vgl. etwa Kühling/Buchner/*Buchner/Petri* Art. 6 Rn. 33.

29 Erforderlichkeit für die Erfüllung des Vertrags ist zum einen dann gegeben, wenn die **Pflicht selbst auf eine Datenverarbeitung gerichtet** ist.[90] Der Verantwortliche kann etwa im Sinne einer Nebenpflicht zur ordnungsgemäßen Dokumentation der Kundenbeziehung verpflichtet sein.[91]

Sieht man Pflichten der betroffenen Person als von Var. 1 erfasst (→ Rn. 28), so könnte man hier an eine Datenüberlassungspflicht (zB von Fotoaufnahmen[92] oder anstelle eines Entgelts[93]) als Grundlage der Speicherung und Verwendung durch den Verantwortlichen denken. Das ginge jedoch fehl. Denn zur Erfüllung einer solchen Pflicht ist eine Mitwirkung des Verantwortlichen gerade nicht erforderlich (sondern im Beispiel nur die Duldung der Ablichtung bzw. die Mitteilung der Daten). Der Sache nach geht es in dieser Konstellation daher vielmehr um eine Gestattung der Datenverarbeitung, die ein separates Problem aufwirft (→ Rn. 32).

30 Zum anderen und praktisch wohl wichtiger besteht Erforderlichkeit im Sinne von Var. 1 aber auch dann, wenn nur die **Pflichterfüllung von der Datenverarbeitung abhängt**.[94] Das gilt etwa, wenn eine Lieferung geschuldet ist, die nur unter Verwendung von Adressdaten (Verarbeitung iSv Art. 4 Nr. 2 Var. 9 DS-GVO) erfolgen kann,[95] oder ein „digitaler Assistent", der auf die Auswertung von Nutzungsdaten angewiesen ist.[96] Generell dürfte es für die Vertragsdurchführung insbes. erforderlich sein, Kontaktdaten der betroffenen Person zu erheben, zu erfassen, zu speichern, zu ordnen und im Bedarfsfall zu verwenden.[97] Bezieht man eine etwaige gerichtliche Durchsetzung der vertraglichen Ansprüche ein, gehören auch bürgerlicher Name und ladungsfähige Anschrift hierher; andernfalls ist deren Verarbeitung auf Abs. 1 lit. f zu stützen (→ Rn. 78, 85).[98]

Abgrenzungsfragen können sich dort stellen, wo eine höhere Qualität der Leistungserbringung die Verarbeitung zusätzlicher Daten erforderlich macht;[99] da nach deutschem Recht nur mittlere Art und Güte geschuldet

90 Der Beitrittsvertrag zu einem Verein kann auch dessen Pflicht zur Weitergabe der Mitgliedsdaten an *andere* Mitglieder umfassen, vgl. allgemein *Uecker* ZD 2019, 248 (250) und zu politischen Parteien *Härting/Gössling* PinG 2021, 54 (56). Einfacher erscheint die Konstruktion über Abs. 1 lit. c, vgl. → Rn. 42.

91 Siehe nur BeckOGK BGB/*Maties* BGB Rn. 316–318 zum Dienstvertrag. Zum Anwendungsbereich von Art. 9 DS-GVO gehört die Patientenakte nach § 630f BGB.

92 *Ehmann* ZD 2020, 65 (68).

93 In diese Richtung Tinnefeld/Buchner/Petri/Hof DatenschutzR/*Buchner* , 2020, Kap. 4 Rn. 114; *Heinzke/Engel* ZD 2020, 189 (191); dagegen etwa Kühling/Buchner/*Buchner/Petri* Art. 6 Rn. 41; *Dünkel* PinG 2020, 41; s. a. *Czajkowski/Müllerter Jung* CR 2018, 157 (161). Alternativ funktioniert die entgeltersetzende Datenüberlassung wohl nur über Abs. 1 lit. a oder f.

94 Dammann/Simitis EG-DatenschutzRL/*Dammann*, 1997, Art. 7 Rn. 5.

95 Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014, 844/14/EN, 21; s. a. *Zehelein* NJW 2020, 1572 (1574): Datenweitergabe an Handwerker zur Erfüllung von Vermieterpflichten.

96 *Gausling* ZD 2019, 335 (36).

97 Zurückhaltender *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014, 844/14/EN, 22 f.; s. a. OLG München 8.12.2020 – 18 U 5493/19 Pre, juris, Rn. 75.

98 Für Einschlägigkeit von Abs. 1 lit. f, freilich unter grundsätzlicher Verneinung von dessen Voraussetzungen, *Nebel* K&R 2019, 148 (150–152).

99 Vgl. anschaulich *Bock* CR 2020, 173 (176).

ist (§ 243 Abs. 1 BGB), muss hier für Abs. 1 lit. b der höhere Standard wohl vereinbart sein.

Nicht erforderlich ist dagegen eine Verarbeitung für vertragsfremde Zwecke, die nur in derselben Personenkonstellation stehen und bloß **durch den Vertrag ermöglicht** werden.[100] Das betrifft nicht zuletzt Big-Data-Auswertungen vertraglich erlangter Arbeitnehmer- oder Kundendaten.[101] Hier kann ggf. auf Abs. 1 lit. f ausgewichen werden;[102] auch können die vertragsfremden Zwecke ihrerseits Gegenstand eines weiteren Vertrags zwischen denselben Parteien sein (etwa: Kaufvertrag neben Arbeitsvertrag) und dann darüber auf Abs. 1 lit. b gestützt werden.[103] 31

Auch nicht erforderlich ist eine Verarbeitung, die nur **im Vertrag gestattet**, nicht aber aufgegeben wird; Vertragsinhalt ist hier eine Erlaubnis und keine Verpflichtung.[104] Außer der Konstellation des „Bezahlens mit Daten"[105] betrifft das zB die Verwendung der Daten bei Gewinnspielen und Kundenbindungsprogrammen,[106] aber auch etwa die Veröffentlichung in der Sportschiedsgerichtsbarkeit.[107] Hier kann mit der Zustimmung zum Vertrag ggf. zugleich eine Einwilligung nach Abs. 1 lit. a erteilt worden sein (die dann freilich widerrufen werden kann, → Rn. 18, Art. 7 Rn. 45 ff., was jetzt § 327q Abs. 2, 3 BGB aufnimmt); auch kann sich die betroffene Person mit dem Vertrag zur Erteilung der Einwilligung im Sinne eines Verfügungsgeschäfts verpflichtet haben (vgl. jetzt § 327 Abs. 3 Var. 2 BGB). Im Übrigen kommen Abs. 1 lit. e oder f in Frage. 32

bb) Durchführung vorvertraglicher Maßnahmen

Nach Var. 2 genügt alternativ auch die Erforderlichkeit der Verarbeitung zur Durchführung **vorvertraglicher Maßnahmen**, die die Bestimmung nicht 33

100 Speziell bei Arbeitsverträgen für „beschäftigungsfremde Zwecke": *Gola/Thüsing/Schmidt* DuD 2017, 244 (245). Zu weit dürfte es aber formuliert sein, „jede erforderliche Datenverarbeitung, die in Zusammenhang mit einem Vertragsverhältnis und seinen Haupt-und Nebenpflichten steht", auf lit. b zu stützen, so KG MDR 2020, 1070 (juris-Rn. 23).

101 Vgl. *Maschmann* BB 2019, 628 (629); Plath/*Plath* Art. 6 Rn. 35; *Niemann/Kevekordes* CR 2020, 17 Rn. 41.

102 *Mertens* PinG 2021, 115 (120), zum Newslettervertrag.

103 Hier ist außerdem die Zweckbindung der jeweils erhobenen Daten nach Art. 5 Abs. 1 lit. b DS-GVO zu beachten, vgl. → Art. 5 Rn. 25 und *Weichert* NZA 2020, 1597 (1601, 1604).

104 *Martini/Botta* VerwArch 110 (2019), 235 (258). Diese hier entscheidende rechtstheoretische Unterscheidung geht verloren, wenn man wie *Engeler* PinG 2019, 149 (152) nur auf die „valid terms" des Vertrags abstellt. Nicht ganz fern liegt es anzunehmen, dass der ebd. kritisierte *Europäischer Datenschutzausschuss*, Leitlinien 2/2019, Tz. 33, bei den „Grundgedanke[n]" und „wesentlichen Elemente[n]" im Ausgangspunkt eigentlich den Verpflichtungscharakter im Sinn hatte und dies nicht besser ausdrücken konnte.

105 Zu dessen neuer privatrechtlicher Seite etwa *Klink-Straub* NJW 2021, 3217. Die dahinter stehende RL (EU) 2019/770 soll ausweislich ihrer Erwägungsgründe 37, 38 an den Rechtmäßigkeitsvoraussetzungen der DS-GVO nichts ändern.

106 Gleichwohl für Abs. 1 lit. b hier *Gierschmann* MMR 2018, 7 (8); zwei Verständnisse des Vertragszwecks unterscheidet Tinnefeld/Buchner/Petri/Hof DatenschutzR/*Buchner*, 2020, Kap. 4 Rn. 117.

107 Vgl. zu dieser Problematik *Vieweg* SpuRt 2020, 163 (167).

konkretisiert. Nahe liegt die Deutung, dass die Verarbeitung zu solchen erforderlich ist, wenn

- der Vertragsschluss selbst,
- vorgezogene Schritte zur Erfüllung der erst zu begründenden Leistungspflicht – etwa die Erteilung einer Auskunft,[108] die Erstellung eines Angebots oder die Vormerkung einer Leistung[109] – oder
- die Leistungshandlung im Falle des Vertragschlusses[110]

nicht vorgenommen werden können oder dürfen[111], ohne dass das Datum verarbeitet würde.

34 Hierunter fallen namentlich die Erhebung, Erfassung, Speicherung und Verwendung von Kontaktdaten des potenziellen Vertragspartners, ohne die der Vertragsschluss faktisch unmöglich ist.[112] Soweit ein Vertrag ohne vorvertragliche Bonitätsanfrage bei einer Auskunftei gemäß §§ 505a BGB, 18a KWG oder ähnlichen Vorschriften nicht geschlossen werden darf, ist die entsprechende Übermittlung ebenfalls erforderlich;[113] im Übrigen müsste sie auf Abs. 1 lit. f gestützt werden (→ Rn. 78).[114]

3. Pflichterfüllung (Abs. 1 lit. c iVm Abs. 2, 3)

35 Erlaubt ist die Verarbeitung grds., wenn der Verantwortliche[115] einer Rechtspflicht unterliegt und die Verarbeitung in diesem Zusammenhang erforderlich ist. Dieser Erlaubnistatbestand begründet die **Subsidiarität des Datenschutzrechts**: das präventive Datenverarbeitungsverbot entbindet nicht von anderen Pflichten; vielmehr entbinden diese über Abs. 1 lit. c vom Datenverarbeitungsverbot. Die Verarbeitung in Gestalt der Löschung, soweit sie zur Erfüllung einer Rechtspflicht erforderlich ist, wird in Art. 17 Abs. 1 lit. e DS-GVO sogar pflichtig gestellt.

36 Die Veränderung gegenüber Art. 7 lit. c DSRL (entsprechend Art. 5 lit. b VO (EG) Nr. 45/2001) ist nur einer veränderten Übersetzung geschuldet; die englischen Sprachfassungen sind identisch. Doch können die Mitglied-

108 *Uecker* ZD 2019, 248 (249).
109 Beispiele nach Dammann/Simitis EG-DatenschutzRL/*Dammann*, 1997, Art. 7 Rn. 6.
110 *Gola/Wronka* RDV 2018, 309 (311): vor Vertragsschluss Abgleich mit Sanktionslisten erforderlich, weil später ggf. Leistung gegenüber Gelisteten rechtlich unmöglich.
111 Dafür implizit *Europäischer Datenschutzausschuss*, Leitlinien 2/2019, Tz. 47 (Beispiel 6). Ein derartiges Nicht-Dürfen kann sich aus Rechtspflichten zu vorvertraglichen Maßnahmen ergeben, etwa nach §§ 505a BGB, 18a KWG. Bezieht man diese Fälle nicht in Abs. 1 lit. b mit ein, so würde Abs. 1 lit. c die Verarbeitung gestatten (→ Rn. 35 ff.).
112 *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014, 844/14/EN, 23.
113 Darüber hinaus kann man mit *Abel* ZD 2018, 103 (106) an Abs. 1 lit. c denken. Dagegen spricht aber, dass nicht zur Prüfung eine Pflicht besteht, sondern zur Unterlassung von Vertragsschlüssen ohne Prüfung, die Prüfung also nur eine Obliegenheit darstellt; vgl. → Rn. 37.
114 *Buchner* FS Taeger, 2020, 95 (99); *Eichler* RDV 2017, 10 (10 f.); *Heintz* jM 2018, 184 (187, ganz ohne Abs. 1 lit. b). AA *Abel* ZD 2018, 103 (106); *Krämer* NJW 2018, 347 (349: bei kreditorischem Risiko stets); *von Lewinski/Pohl* ZD 2018, 17 (19 f.).
115 Nicht: ein Dritter, etwa ein Auftragsverarbeiter; vgl. Kühling/Buchner/*Buchner/Petri* Art. 6 Rn. 80, 80a.

staaten jetzt nach Abs. 2 zusätzliche Anforderungen stellen (vgl. → Rn. 48).

a) Rechtspflicht und Rechtsgrundlage (Abs. 3)

37 Rechtspflicht ist die subjektive Seite einer **gebietenden oder verbietenden Rechtsnorm**.[116] Eine erlaubende Rechtsnorm kann deshalb nicht Rechtsgrundlage für Abs. 1 lit. c,[117] sondern höchstens für lit. e sein; eine erlaubende Sekundärrechtsnorm wie Art. 12 Abs. 6 DS-GVO kommt im Übrigen – qua Gleichrangigkeit und nur bei Fehlen einer Nachrangklausel[118] – auch noch als lex specialis gegenüber Art. 6 Abs. 1 DS-GVO in Frage.[119] Auch eine bloße Obliegenheit (ohne Verarbeitung ist *h* verboten – geboten ist *h* dagegen nicht) passt nicht zu Abs. 1 lit. c (die Erfinderbenennung nach § 37 Abs. 1 S. 1 PatG kann deshalb nicht hierauf gestützt werden,[120] weil die Patentanmeldung als solche nicht geboten ist; auch nicht die Bonitätsanfrage nach §§ 505a BGB, 18a KWG,[121] weil der Vertragsschluss als solcher nicht geboten ist).

Die erforderliche Rechtsnorm nennt Abs. 3 die „Rechtsgrundlage für die Verarbeitung" und stellt dafür zugleich vier zwingende Anforderungen auf, damit der Erlaubnistatbestand wirkt (weitgehend zugleich für Abs. 1 lit. e, vgl. → Rn. 64).[122]

38 Die Rechtsgrundlage muss enthalten sein im **Recht der Union oder eines Mitgliedstaats** (nicht: eines Drittstaats[123]), dessen Recht der Verantwortliche unterliegt[124] (Abs. 3 S. 1). Da eine Rechtspflicht begründet werden muss (vgl. → Rn. 65),[125] können dies nur Rechtsvorschriften sein, die für den Verantwortlichen unmittelbar anwendbar sind.[126] Dagegen ergibt sich aus dem Wort „Rechtsvorschriften" nicht, dass individuelle Rechtsakte ausgeschlossen wären;[127] schließlich hat auch die englische Fassung nur ganz allgemein „law" und wirkt die individuell begründete Rechtspflicht nicht minder zwingend als ihr generelles Pendant, so dass auch die Interes-

116 *Kelsen*, Hauptprobleme der Staatsrechtslehre, 1911, 311 f.
117 Ebenso Auernhammer/*Kramer* Art. 6 Rn. 53; BeckOK DatenschutzR/*Albers/Veit* Art. 6 Rn. 35. Vgl. im Kontext der Rechtmäßigkeitspflicht aus Art. 5 Abs. 1 lit. a Var. 1 DS-GVO auch Mortensen/*Næsborg-Andersen*, Dansk persondataret, 2020, 55 (59).
118 Wie etwa in Art. 40 Abs. 4 RL (EU) 2018/1972 (Kodex für die elektronische Kommunikation, dort „unberührt"), Art. 1 Abs. 1 VO (EU) 2021/1232 (Bekämpfung des sexuellen Missbrauchs von Kindern im Internet, dort „unbeschadet") oder Art. 148 Abs. 1 VO (EU) 2019/6 (Tierarzneimittel, dort als „wenden [die DSGVO] an").
119 In diese Richtung Paal/Pauly/*Paal/Hennemann* Art. 12 Rn. 72. AA offenbar *Raji* ZD 2020, 279 (281).
120 So aber *Vierkötter/Heine* IPRB 2019, 114 (118); *Woger* Mitt. 2019, 438 (439).
121 So aber *Abel* ZD 2018, 103 (106).
122 Vgl. auch *Kühling/Martini* ua DS-GVO, 2016, 34 f.
123 Kuner/Bygrave/Docksey/*Kotschy* GDPR, 2020, Article 6, 326, 340. Insoweit hilft nur Abs. 1 lit. f; vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014, 844/14/EN, 24 f.
124 Zu der hierin liegenden Kollisionsrechtsproblematik vgl. *Gömann*, Das öffentlich-rechtliche Binnenkollisionsrecht der DS-GVO, 2021, S. 143–147.
125 Vgl. *Laue/Nink/Kremer* DatenschutzR § 2 Rn. 28.
126 Vgl. *Laue/Nink/Kremer* DatenschutzR § 2 Rn. 31.
127 So aber wohl *Piltz* FS Taeger, 2020, 351 (352).

senlage identisch ist. Erwägungsgrund 41 S. 1 Hs. 1 macht deutlich, dass auch aus Sicht des Verordnungsgebers ein parlamentarischer Gesetzgebungsakt nicht erforderlich ist.

39 Für **nichtöffentliche Stellen** kommen aus dem Unionsrecht nur Verordnungen und Beschlüsse (Art. 288 Abs. 2, 4 AEUV) sowie ausnahmsweise an sie ergangene Urteile unionaler Gerichte, aus dem deutschen Recht als generelle Rechtsakte Gesetze, Rechtsverordnungen und Satzungen sowie als individuelle Rechtsakte Verwaltungsakte[128] und Urteile in Frage.

Individuelle Verträge, wiewohl sie ebenfalls Rechtspflichten begründen, unterfallen in der Systematik der Vorschrift der Spezialregelung der lit. b (→ Rn. 21 ff.).[129] Zwei Private können einander dementsprechend nicht vertraglich die Verarbeitung von Daten über Dritte erlauben, wie man sonst etwa über § 402 BGB (als unmittelbare Verarbeitungspflicht, → Rn. 46) oder § 89b HGB (als mittelbare Verarbeitungspflicht, → Rn. 47)[130] konstruieren könnte.

Normenverträge (insbes. Tarifverträge oder Betriebsvereinbarungen) könnten zwar ebenfalls als „Recht der Mitgliedstaaten" angesehen werden,[131] da jenes seine Geltung von diesem herleitet, sind aber wohl nicht gemeint,[132] wie etwa die Nebeneinanderstellung in Art. 9 Abs. 2 lit. b DS-GVO zeigt. Verneint man außerdem die Einordnung der Kollektivverträge bei Abs. 1 lit. b (→ Rn. 22), so helfen nur noch die Öffnungsklausel in Art. 88 Abs. 1 DS-GVO (→ BDSG § 26 Rn. 53–56)[133] oder aber das berechtigte Interesse des Abs. 1 lit. f (→ Rn. 73 ff.).

128 Wie hier VG München BeckRS 2018, 32756 Rn. 41 (insoweit von der Berufungsinstanz nicht in Frage gestellt); *Klaas* CCZ 2020, 256 (260). AA jedoch Paal/Pauly/*Frenzel* DS-GVO Art. 6 Rn. 36 (mit dem Argument, Verwaltungsakte hätten „ihren Rechtsgrund selbst in einer materiellen Rechtsnorm"; das ist richtig, doch geht es hier gerade nicht um die Rechtmäßigkeit, sondern um die Wirksamkeit des befehlenden Verwaltungsakts); Kühling/Buchner/*Buchner/Petri* Art. 6 Rn. 78 (die ebenfalls auf die Rechtsgrundlage des *Behörden*handelns abheben).

129 Ebenso Kühling/Buchner/*Buchner/Petri* Art. 6 Rn. 77; Paal/Pauly/*Frenzel* DS-GVO Art. 6 Rn. 16. AA AG Schöneberg ZD 2019, 177 Rn. 32; dagegen *Chatard/Horn* ZIP 2019, 2242 (2246).

130 Hierzu *Beck/Kirschhöfer* ZVertriebsR 2019, 3, die Einwilligungen der Kunden verlangen.

131 Bejahend für Betriebsvereinbarungen *Wurzberger* ZD 2017, 258 (260); in Bezug auf die entsprechende Formulierung in Art. 4 Nr. 7 Hs. 2 DS-GVO *Kleinebrink* DB 2018, 2566 (2571).

132 *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014, 844/14/EN, 24 (zu Verträgen allgemein); *Gola* EuZW 2012, 332 (336, zu Betriebsvereinbarungen); *Kühling/Martini ua* DS-GVO,2016, 30 Fn. 49 (zu Tarifverträgen); *Laue/Nink/Kremer* DatenschutzR § 2 Rn. 31 (zu beidem). Für die Einbeziehung von Tarifverträgen und Betriebsvereinbarungen dagegen Paal/Pauly/*Frenzel* DS-GVO Art. 6 Rn. 16 f.; Auernhammer/*Kramer* Art. 6 Rn. 52; Kühling/Buchner/*Buchner/Petri* Art. 6 Rn. 85, 197.

133 § 26 BDSG übernimmt dann die Funktion von Abs. 1 lit. c, vgl. *Wybitul* NZA 2017, 1488 (1490); s. a. Specht/Mantz DatenschutzR-HdB/*Ströbel/Wybitul*, 2019, § 10 Rn. 14 f., 98–100.

Für **staatliche Stellen**[134] kann sich die Situation anders darstellen, soweit diese zusätzlichen Bindungen unterworfen sind. Aus dem deutschen Recht sind dies insbes. die Verwaltungsvorschriften; soweit diese wirksam verpflichten, sollten auch die erforderlichen Verarbeitungen nach Abs. 1 lit. c erlaubt sein;[135] zu beachten bleiben freilich die aus Art. 2 Abs. 1 GG und, soweit einschlägig, Art. 8 Abs. 2 S. 1 EUGRCh folgenden und innerhalb der mitgliedstaatlichen Spielräume weiterhin anwendbaren Vorbehalte des Gesetzes.[136] Aus dem Unionsrecht wäre noch an die Urteile der unionalen Gerichte sowie an die Richtlinien (Art. 288 Abs. 3 AEUV) zu denken, die zumindest nach der Rspr. für alle innerstaatlichen Stellen verbindlich sind;[137] dementsprechend läge auch in der (namentlich applikativen,[138] also administrativen und judikativen) Richtlinienumsetzung eine Rechtsgrundlage für dazu etwa erforderliche Datenverarbeitungen. 40

Die Rechtsgrundlage muss den **Zweck der Verarbeitung** selbst festlegen (Abs. 3 S. 2 Var. 1[139]). Die Festlegung hat selbst keinen gebietenden oder verbietenden Charakter. Sie wird deshalb nicht immer ausdrücklich im Normtext enthalten, sondern häufig aus dem Zusammenhang zu erschließen sein. 41

Die Rechtsgrundlage muss ein **im öffentlichen Interesse liegendes Ziel** verfolgen (Abs. 3 S. 4 Var. 1).[140]

Die Rechtsgrundlage muss **verhältnismäßig** in Bezug auf den verfolgten Zweck sein (Abs. 3 S. 4 Var. 2).

Als **unionsrechtliche Rechtsgrundlagen** kommen beispielhaft die im Datenschutzrecht selbst verankerten positiven Verarbeitungsverpflichtungen in Betracht, etwa zur Löschung personenbezogener Daten aus Art. 5 Abs. 1 lit. e, Art. 17 DS-GVO oder zur Sicherheit der Verarbeitung aus Art. 32 DS-GVO.[141] 42

134 Für deren Einbeziehung auch Paal/Pauly/*Frenzel* DS-GVO Art. 6 Rn. 18; sogar „vornehmlich" sehen BeckOK DatenschutzR/*Albers/Veit* Art. 6 Rn. 35 diese angesprochen.
135 AA Paal/Pauly/*Frenzel* DS-GVO Art. 6 Rn. 36.
136 Vgl. Erwägungsgrund 41 S. 1 Hs. 2; *Kühling/Martini ua* DS-GVO,2016, 28; *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 347 f. Art. 20 GG mobilisiert *Bieresborn* NZS 2017, 926 (927).
137 Ständige Rspr. seit EuGH 10.4.1984 – 14/83, Slg. 1984, 1891 Rn. 26 – von Colson; EuGH 10.4.1984 – 79/83, Slg. 1984, 1921 Rn. 26 – Harz. Zur Kritik vgl. *Reimer* JZ 2015, 910 (911 f., 919).
138 Begriff: *Burger*, Verantwortung und Verantwortlichkeit für die Umsetzung supranationalen Rechts im Bundesstaat, 2010, 198; *ders.* DVBl 2013, 1431 (1432).
139 Die Var. 2 gilt nur für Abs. 1 lit. e, nicht c, vgl. → Rn. 66.
140 Vgl. Kühling/Buchner/*Buchner/Petri* Art. 6 Rn. 87 ff.
141 Dazu *Piltz* FS Taeger, 2020, 351.

Aus dem deutschen Recht seien als **gesetzliche Rechtsgrundlagen** genannt

- die organisationsrechtlichen Verpflichtungen zur Sitzungsöffentlichkeit (wie § 35 GemO BW[142]) und zur Gewährung von Einsicht in Mitgliederlisten von Vereinen[143]
- die verfahrensrechtlichen Verpflichtungen zur Sachverhaltsermittlung (zB §§ 86 VwGO,[144] 5 InsO,[145] 24 VwVfG, 88 AO, 20 SGB X[146]), zur Mitteilung von Schriftsätzen (zB § 86 Abs. 4 S. 3 VwGO[147]), zur Zeugenaussage (zB § 161a StPO[148]), zum Sachverständigengutachten (wie § 407 ZPO)[149] und zur Gewährung von Akteneinsicht (zB § 29 VwVfG[150])
- die informationsrechtlichen Verpflichtungen zur Übermittlung von Verwaltungsinformationen (wie §§ 1, 5 Abs. 1 S. 1 IFG), sofern sie für personenbezogene Daten nicht ihrerseits gerade die datenschutzrechtliche Zulässigkeit voraussetzen (wie Art. 39 Abs. 1 S. 1 Nr. 1 BayDSG)
- die fachrechtlichen Verpflichtungen zur Erhebung (wie nach Infektionsschutzverordnungen für Gaststättenbesucherdaten,[151] nach Hochschulrecht für Evaluationsdaten[152] oder nach Energierecht für Smart Meters[153]), Speicherung (wie § 83 WpHG,[154] § 87 WpHG[155]), Aufbewahrung (wie nach § 257 Abs. 1 Nr. 2 HGB für Handelsbriefe[156]) oder Übermittlung (wie nach Jagdrecht für Daten der anderen Jagdgenossen,[157] nach Betriebsverfassungsrecht für gebotene Unterrichtungen des Betriebsrats[158] oder nach § 43 GwG für Geldwäscheverdachtsfälle[159]).

Statt aus Gesetz können entsprechende Rechtspflichten auch aus **individuellen Anordnungen** folgen, etwa zur Herausgabe von Unterlagen (zB zivil-

142 Mangels „Aufgabe" nicht lit. e zuzuordnen; so aber etwa *Katz* NVwZ 2020, 1076 (1080).
143 BGH NZG 2010, 1430. Auf Abs. 1 lit. f kommt es daher nicht mehr an, ergänzend kann auf Abs. 1 lit. b abgestellt werden, soweit die Übermittlung auch mit anderen Mitgliedern vereinbart ist; vgl. OLG München ZD 2019, 171 Rn. 30; *Härting/Gössling* PinG 2021, 54 (56).
144 VGH BW VBlBW 2019, 325 (juris-Rn. 20); *Bieresborn* DRiZ 2019, 18 (19).
145 *Theurich/Degenhardt* NZI 2018, 870 (871).
146 HessLSG RDV 2020, 95 (juris-Rn. 14 f.).
147 Zu § 108 S. 2 SGG *Erkelenz/Leopold* NZS 2019, 926 (929).
148 Einschränkend zur Erforderlichkeit *Raji* ZD 2020, 279 (283).
149 Vgl. BSG 28.11.2019 – B 8 SO 55/17 B, juris, Rn. 11 (wo allerdings noch § 3 BDSG zitiert wird, vgl. → BDSG § 3 Rn. 17 f.); s. a. *Nugel* ZD 2019, 341 (344 f.): Sachverständiger muss Fahrzeugdaten auslesen (→ Art. 4 Rn. 63).
150 BayVGH 7.1.2020 – 8 ZB 18.1652, juris, Rn. 28. Bei der Einsichtgewährung soll ggf. pseudonymisiert werden müssen: *Joos* NVwZ 2021, 1335 (1338 f.).
151 VGH BW ZD 2020, 655 Rn. 87f.
152 VGH BW DVBl 2020, 1600.
153 Zu § 29 MsbG *Bretthauer* EnWZ 2017, 56 (58); Abs. 1 lit. c dürfte zumindest dort einschlägig sein, wo ein Vertrag nach § 9 Abs. 3 MsbG nur fingiert wird.
154 *Buck-Heeb* FS Taeger, 2020, 111 (117–121).
155 HessVGH ZD 2019, 92 (93 Rn. 28).
156 *Geiser* ZInsO 2017, 1185 (1192).
157 OVG MV ZD 2021, 117 (117 Rn. 17). Für Mitgliederdaten einer Berufskammer verneint von NdsOVG GewArch 2020, 325 (juris-Rn. 29 f., dort lit. e zugeordnet). Zur privatvertragsrechtlichen Parallele → Rn. 29 mit Fn. 90.
158 *Lücke* NZA 2019, 658 (662) – sofern der Betriebsrat als eigener Verantwortlicher und damit als Dritter begriffen wird (dazu nur ebd., 659–661 mwN).
159 Vgl. *Klaas* CCZ 2020, 256 (259).

prozessual gemäß §§ 142, 144 ZPO[160] oder gewerberechtlich gemäß § 4 Abs. 3 S. 1 Nr. 1 FPersG[161]).

Dabei kann eine Rechtsgrundlage ohne Weiteres für **mehrere Verarbeitungen sowie Weiterverarbeitungen** gelten, wie die Erwägungsgründe 45 S. 2, 3 und 50 Abs. 1 S. 5 ausdrücklich klarstellen. Nicht in den verfügenden Teil der Verordnung einbezogen worden und damit bloße Hoffnungen des Verordnungsgebers geblieben sind die Erwartungen in Erwägungsgrund 41 S. 2, dass die Rechtsgrundlage klar, präzise und vorhersehbar sein sollte. Entsprechende rechtsstaatliche Anforderungen können sich freilich aus dem Primärrecht oder dem mitgliedstaatlichen Verfassungsrecht ergeben. 43

Eine Rechtsgrundlage kann sich auf eine **reduzierte Erlaubniswirkung**, die sie über Abs. 1 lit. c vermittelt, explizit beschränken, indem sie „spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung" aufnimmt (Abs. 3 S. 3). Für unionsrechtliche Rechtsgrundlagen ist diese Generalklausel überflüssig, weil spätere Unionsrechtsakte die DS-GVO ohne Weiteres verdrängen können. Für das mitgliedstaatliche Recht tritt ihre Bedeutung aber durch die im Verordnungstext enthaltenen Beispiele etwas klarer hervor, die den Umfang der Generalklausel weitgehend erschöpfen dürften. Danach kann die Rechtsgrundlage – außer der Statuierung der Rechtspflicht des Verantwortlichen – zugleich bestimmen: 44

- allgemeine Bedingungen für die Rechtmäßigkeit der Datenverarbeitung, wozu nach Erwägungsgrund 45 S. 5 insbes. die Bestimmung des Verantwortlichen gehören soll (s. a. → Art. 4 Rn. 141);
- die Art der erlaubterweise zu verarbeitenden Daten;
- den Kreis der erlaubterweise zu erfassenden Personen;
- Empfänger und Zwecke erlaubter Offenlegung;
- erlaubte und verbotene Zwecke (insbes. in Bezug auf eine Weiterverarbeitung);[162]
- zeitliche Grenzen für die Aufbewahrung, dh eine über Art. 5 Abs. 1 lit. e DS-GVO hinausgehende Löschungspflicht (vgl. → Art. 5 Rn. 42 ff.);
- die Art der erlaubterweise anzuwendenden Verarbeitungsvorgänge und -verfahren. Insbesondere können hier Vorkehrungen zur Sicherung der Rechtmäßigkeit und Fairness der Verarbeitung (Art. 5 Abs. 1 lit. a Var. 1, 2 DS-GVO; vgl. → Art. 5 Rn. 12 ff.) getroffen werden. Ausdrücklich soll dieser Mechanismus auch für die Erfüllung der mitgliedstaatlichen Regelungsaufträge und -befugnisse aus Kapitel IX zur Verfügung stehen (dazu → Einleitung Rn. 46).

160 Vgl. *Nugel* ZD 2019, 341 (345).
161 Vgl. BayVGH ZD 2019, 87 (88 f. Rn. 37), wo es um den Verwaltungsakt selbst als behördliche Datenerhebung nach Abs. 1 lit. e (Rechtsgrundlage: Gesetz) ging; für den Adressaten kommt es dann zu einer pflichtigen Datenübermittlung nach Abs. 1 lit. c (Rechtsgrundlage: Verwaltungsakt).
162 Vgl. Erwägungsgrund 50 Abs. 1 S. 3.

Als Anwendungsfälle im mitgliedstaatlichen Recht werden etwa §§ 49 ff. MsbG[163] und §§ 67a ff. SGB X[164] angesehen. Da es nur um eine Spezifizierung geht, sollte auch im Falle einer mitgliedstaatlichen Regelung weiterhin Abs. 1 lit. c und nicht die „spezifische Bestimmung" als Erlaubnistatbestand angesehen werden.[165]

45 Eine bereits für die Rechtsgrundlage vorgenommene **Folgenabschätzung** kann den Verantwortlichen von einer Folgenabschätzung im Einzelfall entlasten, Art. 35 Abs. 10 DS-GVO.

b) Erforderlichkeit

46 Die Verarbeitung muss zur Erfüllung der Rechtspflicht erforderlich sein, dh diese kann nicht erfüllt werden, ohne dass das Datum verarbeitet würde. Wie bei Abs. 1 lit. b Var. 1 (vgl. → Rn. 25 ff.) ist das zum einen der Fall, wenn der Verantwortliche **unmittelbar**[166] zu einer Verarbeitung rechtlich verpflichtet ist – namentlich zur Speicherung (Aufzeichnungs-, Aufbewahrungspflichten) oder Offenlegung (Melde-,[167] Vorlage-, Aussage-, Transparenzpflichten[168]). Der gegenständliche Umfang dieser Pflichten muss genau bestimmt werden, steht der Verantwortliche hier doch stets ungünstig zwischen der Gefahr eines Datenschutzrechts- und eines Fachrechtsverstoßes, die möglicherweise beide sanktionsbewehrt sind.[169]

47 Erforderlichkeit ist zum anderen aber auch dann gegeben, wenn die Pflichterfüllung die Verarbeitung nur als **Zwischenschritt** voraussetzt.[170] Besonders deutlich ist das bei Pflichten, die selbst eine Informationsbeschaffung erfordern und nur deren Modalitäten offenlassen. Der EuGH hat hier die Erforderlichkeit schon dann bejaht, wenn der Verantwortliche das Vorliegen der personenbezogenen Voraussetzungen einer gebundenen (Genehmigungs-)Entscheidung prüft.[171]

c) Zusätzliche mitgliedstaatliche Anforderungen (Abs. 2)

48 Gemäß Abs. 2 behalten die Mitgliedstaaten eine Rechtsetzungskompetenz, soweit es um Rechtsvorschriften geht, die ergänzend zu Art. 6 Abs. 1 lit. c,

163 *Bretthauer* EnWZ 2017, 56 (60).
164 *Roßnagel/Hoidn* DuD 2018, 487 (491), die zugleich Abs. 2 zitieren; dazu → Rn. 48.
165 Dafür aber *Roßnagel/Hoidn* DuD 2018, 487 (491), die dem Sozialdatenschutz nach wie vor die Eigenschaft eines „Vollregimes" zuschreiben.
166 Was sich selbstverständlich auch aus der Zusammenschau zweier Bestimmungen ergeben kann: *Piltz* FS Taeger, 2020, 351 (355).
167 Vgl. *Artikel-29-Datenschutzgruppe*, Stellungnahme 06/2014, 844/14/EN, 24.
168 Vgl. EuG 8.11.2007 – T-194/04, Slg. 2007, II-4523 Rn. 106 – Bavarian Lager (zu Art. 5 lit. b VO (EG) Nr. 45/2001; insoweit nicht betroffen durch die Rechtsmittelentscheidung).
169 *Buck-Heeb* FS Taeger, 2020, 111 (119 f., zu § 83 WpHG).
170 Ebenso *Hoffmann/Schulte* EuZW 2019, 733 (737); *Piltz* FS Taeger, 2020, 351 (352–355); implizit auch *Roßnagel/Geminn/Johannes* ZD 2019, 435 (436). Zu eng dagegen *Buchner* FS Taeger, 2020, 95 (99), der nur den Fall der „spezifischen Verpflichtung zu einer bestimmten Datenverarbeitung" einbeziehen will und deshalb Fälle wie § 18a KWG ausschließt (hierzu bereits bei lit. b → Rn. 34); ähnlich *Zehelein* NJW 2019, 3047 (3048).
171 EuGH 16.1.2019 – C-496/17, Rn. 61 f. – Deutsche Post; darauf dann FG Düsseldorf 6.2.2019 – 4 K 1404/17 Z, juris, Rn. 21.

benzuweisung stützen. Systematisch besser hätte die Vorschrift deshalb in den BDSG-Teilen 3 und 4 zum Richtlinien- und zum unionsrechtsfreien Restbereich platziert werden können. Angesichts Art. 8 Abs. 1 RL (EU) 2016/680 ist sie selbst insoweit freilich noch überschießend formuliert (→ Rn. 29).

§ 4 Videoüberwachung öffentlich zugänglicher Räume

(1) [1]Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke
erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. [2]Bei der Videoüberwachung von
1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder
2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs
gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.

(2) Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

(3) [1]Die Speicherung oder Verwendung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. [2]Absatz 1 Satz 2 gilt entsprechend. [3]Für einen anderen Zweck dürfen sie nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) [1]Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, so besteht die Pflicht zur Information der betroffenen Person über die Verarbeitung gemäß den Artikeln 13 und 14 der Verordnung (EU) 2016/679. [2]§ 32 gilt entsprechend.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der betroffenen Personen einer weiteren Speicherung entgegenstehen.

Literatur:

Ahrens, Dashcam-Aufzeichnungen als Beweismittel nach Verkehrsunfällen, NJW 2018, 2837; *Bier/Spiecker gen. Döhmann*, Intelligente Videoüberwachungstechnik – Schreckensszenario oder Gewinn für den Datenschutz?, CR 2012, 610; *Bischof*, Drohnen im rechtlichen Praxistext, DuD 2017, 142; *Bretthauer*, Intelligente Videoüberwachung, 2017; *Bull*, Fehlentwicklungen im Datenschutzrecht am Beispiel der Videoüberwa-

chung, JZ 2017, 797; *Datenschutzkonferenz*, Kurzpapier Nr. 15: Videoüberwachung nach der Datenschutzgrundverordnung, 8.1.2018; *dies.*, Positionspapier zur Nutzung von Kameradrohnen durch nicht-öffentliche Stellen, 16.1.2019; *dies.*, Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams), 28.1.2019; *dies.*, Orientierungshilfe der Datenschutzaufsichtsbehörden zu dem Einsatz von Bodycams durch private Sicherheitsunternehmen, 22.2.2019; *dies.*, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, 3.9.2020; *Desoi*, Intelligente Videoüberwachung – Rechtliche Bewertung und rechtsgemäße Gestaltung, 2018; *Dienstbühl*, Anforderungen an den Einsatz von „Wildkameras" durch Privatpersonen, CR 2019, 359; *Düsseldorfer Kreis*, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", 19.2.2014; *Europäischer Datenschutzausschuss*, Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte (Version 2.0), 29.1.2020; *Gola/Klug*, Videoüberwachung gem. § 6b BDSG, RDV 2004, 65; *Grages/Plath*, Black Box statt Big Brother: Datenschutzkonforme Videoüberwachung unter BDSG und DS-GVO, CR 2017, 791; *Heese*, Anmerkung zu BGH VI ZR 233/17 (Dashcam), JZ 2018, 942; *Griebel*, Schutz der Persönlichkeitsrechte vor Drohnenaufnahmen, InTeR 2019, 106; *Held*, Intelligente Videoüberwachung – Verfassungsrechtliche Vorgaben für den polizeilichen Einsatz, 2014; *Hornung/Schindler*, Das biometrische Auge der Polizei – Rechtsfragen des Einsatzes von Videoüberwachung mit biometrischer Gesichtserkennung, ZD 2017, 203; *Jandt*, Biometrische Videoüberwachung – was wäre wenn …, ZRP 2018, 16; *Klar*, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012; *Lachenmann*, Neue Anforderungen an die Videoüberwachung – Kritische Betrachtung der Neuregelungen zur Videoüberwachung in DS-GVO und BDSG-neu, ZD 2017, 407; *Roßnagel/Desoi/Hornung*, Noch einmal: Spannungsverhältnis zwischen Datenschutz und Ethik – Am Beispiel der smarten Videoüberwachung, ZD 2012, 459; *Schröder*, Datenschutz beim Kameraeinsatz im Automobil, ZD 2021, 302; *Schwenke*, Zulässigkeit der Nutzung von Smartcams und biometrischen Daten nach der DS-GVO, NJW 2018, 823; *Taeger (Hrsg.)*, Chancen und Risiken von Smart Cams im öffentlichen Raum, 2017; *Spiecker gen. Döhmann*, Big Data intelligent genutzt: Rechtskonforme Videoüberwachung im öffentlichen Raum, K&R 2014, 549; *Sydow/Kring*, Die Datenschutzgrundverordnung zwischen Technikneutralität und Technikbezug – Konkurrierende Leitbilder für den europäischen Rechtsrahmen, ZD 2014, 271; *Thiel*, Videoüberwachung unter Geltung der Datenschutz-Grundverordnung (DS-GVO) – alles neu?, NdsVBl. 2020, 136; *Wagner/Bretthauer/Birnstill/Krempel*, Auf dem Weg zu datenschutzfreundlichen Dashcams – Technische Maßnahmen zur Erhöhung des Datenschutzes, DuD 2017, 159; *Weichert*, Rechtsfragen der Videoüberwachung, DuD 2000, 662; *Wysk*, Tausche Freiheit gegen Sicherheit? Die polizeiliche Videoüberwachung im Visier des Datenschutzes, VerwArch 109 (2018), 141; *Ziebarth*, Verbesserte Videoüberwachung? Auswirkungen des Videoüberwachungsverbesserungsgesetzes vor und nach Wirksamwerden der DS-GVO, ZD 2017, 467.

A. Grundlagen

I. Gesamtverständnis und Zweck der Norm

1 Der deutsche Gesetzgeber hat mit § 4 eine 2001 (damals als § 6b) in das BDSG eingefügte Norm nahezu unverändert fortbestehen lassen, die im Gegensatz zum technologieneutralen Ansatz der DS-GVO und des übrigen BDSG die Verwendung einer spezifischen Technologie regelt. Da § 4 in der Folge in mehrerlei Hinsicht quer zum Datenschutzrecht liegt (→ Rn. 7 f.), kommt es über die Frage nach der dem deutschen Gesetzgeber verbleibenden Regelungsbefugnis (→ Rn. 12 ff.) hinaus zu Friktionen zwischen DS-GVO und BDSG, deren Auflösung sich teilweise als schwierig erweist (zB → Rn. 14, 32 f., 40). Zugleich hat § 4 durch den Erlass der DS-GVO weiter an Bedeutung verloren, da er nur noch auf Videoüberwachungen im öffentlichen Interesse Anwendung finden kann (→ Rn. 12 ff.) und er ohnehin im Gegensatz zum Wortlaut des Abs. 1 S. 1 („nur zulässig") nicht abschließend ist, weshalb ihm im Wesentlichen eine Auffang- und Ergänzungsfunktion zukommt (→ Rn. 15, 17, 19 f.). Nicht zu unterschätzen ist schließlich aber seine Funktion als Musterregelung, an der sich Bundes- und Landesgesetzgeber beim Erlass spezialgesetzlicher Regelungen orientieren.

2 § 4 regelt mit der Videoüberwachung eine Technologie, die aufgrund sinkender Kosten und des technologischen Fortschritts schnell Verbreitung gefunden hat und die als Bedrohung einer public privacy wahrgenommen wird. Soweit öffentlich zugängliche Räume überwacht werden, soll die Norm daher die berechtigten Überwachungsinteressen und die gegenläufigen Interessen der von der Videoüberwachung erfassten Personen in einen Ausgleich bringen, was wegen der geringen Regelungstiefe jedoch nur unzureichend gelingt (→ Rn. 17, 26, 47). Hinzu kommt, dass sich auch in rechtlichen Streits über die Zulässigkeit von Videoüberwachungsmaßnahmen vielfach emotional aufgeladene politische Positionen widerspiegeln,

was der Qualität der Diskussionen nicht zuträglich ist.[1] Die hohe Aufmerksamkeit, die der Videoüberwachung zuteilwird, kommt schließlich auch in einer ganzen Reihe von Orientierungshilfen und Kurzpapieren zum Ausdruck, die zunächst vom Düsseldorfer Kreis und nunmehr der Datenschutzkonferenz zum Thema veröffentlicht wurden.[2]

II. Verhältnis zur DS-GVO

Im Gegensatz zum BDSG enthält die DS-GVO entsprechend ihres technologieneutralen Ansatzes keine Regelung über die Zulässigkeit von Videoüberwachungsmaßnahmen und erwähnt sie nur mit Blick auf die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung in Art. 35 Abs. 3 lit. c DS-GVO. Soweit im Rahmen der Videoüberwachung öffentlich zugänglicher Räume personenbezogene Daten verarbeitet werden – was nicht zwingend immer der Fall ist (→ Rn. 7) – finden somit die allgemeinen Vorschriften der DS-GVO Anwendung, auch weil die Haushaltsausnahme (Art. 2 Abs. 2 lit. c) vom EuGH gerade in Bezug auf die Videoüberwachung eng ausgelegt wurde.[3] Da folglich § 4 die Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO nicht verdrängt, kann die Videoüberwachung – zumindest theoretisch – auch auf die Einwilligung der Betroffenen gestützt werden, was jedoch angesichts des von der DS-GVO verschärften Freiwilligkeitsmaßstabs[4] und der Tatsache, dass das bloße Betreten keine wirksame Einwilligung darstellt,[5] nur sehr selten praktisch relevant wird.[6] Darüber hinaus erweist sich § 4 in Teilen als unionsrechtswidrig, soweit er Videoüberwachungen im privaten Interesse regelt, bei denen personenbezogene Daten verarbeitet werden (→ Rn. 13). In diesen Fällen findet statt § 4 die Interessenabwägung des Art. 6 Abs. 1 lit. f DS-GVO Anwendung. Gleiches gilt für die nicht in den Anwendungsbereich des § 4 fallende Überwachung von nicht öffentlich zugänglichen Räumen durch Private, soweit diese nicht im Beschäftigungskontext erfolgt und daher der Regelung in § 26 unterfällt.[7] Schließlich geht mit der Videoüberwachung regelmäßig keine Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne des Art. 9 DS-GVO einher, weshalb dieser jedenfalls solange keine Anwen- 3

1 Wohltuend insoweit das Plädoyer aus richterlicher Perspektive für Nüchternheit und genaues Hinsehen von *Wysk* VerwArch 109 (2018), 141 (144).
2 Auch die Orientierungshilfen des Düsseldorfer Kreises können nunmehr über die Homepage https://www.datenschutzkonferenz-online.de abgerufen werden.
3 So zur gleichlautenden Vorgängernorm in der Datenschutzrichtlinie EuGH NJW 2015, 463 (Rn. 26 ff.) – Ryneš; kritisch hierzu Auernhammer/*Onstein* BDSG § 4 Rn. 10; ausführlich und mit Beispielen zur Haushaltsausnahme in Bezug auf den Einsatz von Videokameras *EDSA*, Leitlinien 3/2019 (Version 2.0), Rn. 11 ff.
4 Hierzu allgemein HK-EuDSchVO/*Ingold* DS-GVO Art. 7 Rn. 25 ff.; überzogen allerdings das Beispiel bei *EDSA*, Leitlinien 3/2019 (Version 2.0), Rn. 45, wonach es einem Sportverein nicht erlaubt sein soll, das Filmen einzelner Übungen einer Mannschaft zu Trainings- und Analysezwecken auf die Einwilligung zu stützen, da sich einzelne Teammitglieder in diesem Fall unter Druck gesetzt fühlen könnten, ihre Einwilligung zu erteilen.
5 BVerwG NJW 2019, 2556 (2559, Rn. 23).
6 *EDSA*, Leitlinien 3/2019 (Version 2.0), Rn. 44; Auernhammer/*Onstein* BDSG § 4 Rn. 3.
7 Auernhammer/*Onstein* BDSG § 4 Rn. 2; Plath/*Becker* BDSG § 4 Rn. 8.

dung findet, wie nicht eine Auswertung mittels biometrischer Gesichtserkennung[8] erfolgt.[9]

III. Verhältnis zu anderen Normen

4 Innerhalb des BDSG findet auf die praktisch besonders relevante Überwachung von Arbeitnehmern an ihrem Arbeitsplatz § 26 Anwendung.[10] Über das Datenschutzrecht hinaus wird das Phänomen der Videoüberwachung auch durch Normen des bürgerlichen Rechts und des Betriebsverfassungsrechts erfasst.[11] Schließlich sind bei der Auslegung von § 4 die Vorgaben des grundgesetzlichen Rechts auf informationelle Selbstbestimmung sowie des europäischen Datenschutzgrundrechts in Art. 8 GRC zu berücksichtigen, die insoweit nebeneinander Anwendung finden, wohingegen im Falle der auf Art. 6 Abs. 1 lit. f DS-GVO gestützten Videoüberwachung im privaten Interesse allein Art. 8 GRC in seiner Drittwirkungsdimension anwendbar ist.[12] Sowohl § 4 als auch Art. 6 Abs. 1 lit. f DS-GVO sind aber so offen formuliert (was aus anderen Gründen nicht unproblematisch ist, → Rn. 26, 47), dass sie die grundrechtlichen Wertungen unschwer aufnehmen können.

IV. Frühere Rechtslage und Entstehung der Norm

5 Die Vorgängervorschrift des § 4 wurde im Jahr 2001 als § 6b in das BDSG aF eingefügt und 2017 durch das Videoüberwachungsverbesserungsgesetz um die Regelungen des heutigen Abs. 1 S. 2 und Abs. 3 S. 2 ergänzt.[13] Eine im Rahmen des Gesetzgebungsverfahrens zum DSAnpUG vorgeschlagene Begrenzung des Anwendungsbereichs der Norm auf Überwachungen im öffentlichen Interesse[14] wurde verworfen, so dass sich die ursprüngliche Regelung § 6b BDSG aF bis auf redaktionelle Anpassungen nahezu unverändert in § 4 wiederfindet.

B. Kommentierung

I. Anwendungsbereich der Regelung und Vereinbarkeit mit dem Unionsrecht

1. Sachlicher Anwendungsbereich

a) Beobachtung: Keine Erhebung personenbezogener Daten erforderlich

6 Der sachliche Anwendungsbereich des § 4 wird zunächst durch den Begriff der Beobachtung beschrieben. Schon dem Wortlaut nach findet die Norm

8 Ausführlich zur Verwendung biometrischer Daten und insbesondere zur Gesichtserkennung *EDSA*, Leitlinien 3/2019 (Version 2.0), Rn. 73 ff.; s. auch Art. 5 Abs. 1 lit. d, Abs. 2–4 des Kommissionsvorschlags für eine KI-Verordnung, der eine „Verwendung biometrischer Echtzeit-Fernidentifizierungssysteme in öffentlich-zugänglichen Räumen" in engen Grenzen zulässt, hierzu *Spindler* CR 2021, 361 (365).

9 Ausführlich hierzu *EDSA*, Leitlinien 3/2019 (Version 2.0), Rn. 62 ff.; BeckOK DatenschutzR/*Wilhelm*, 37. Ed. 1.5.2021, BDSG § 4 Rn. 13 ff.; *Jandt* ZRP 2018, 16; *Schneider/Schindler* ZD 2018, 463; *Reuter* ZD 2018, 564.

10 BeckOK DatenschutzR/*Riesenhuber*, 37. Ed. 1.2.2021, BDSG § 26 Rn. 147 f.

11 S. den Überblick bei Plath/*Becker* BDSG § 4 Rn. 2.

12 Hierzu allgemein *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 344 ff.

13 BGBl. 2001 I 904; BGBl. 2017 I 968.

14 S. den zweiten Referentenentwurf des BMI vom 11.11.2016, S. 11 f., 72 f.

somit bereits auf die bloße **Videobeobachtung** Anwendung, also auch dann, wenn es nachfolgend nicht zu einer Aufzeichnung kommt.[15] Erfasst sind folglich Video-Monitor-Systeme, bei denen die Bilder in Echtzeit auf einem Monitor angezeigt und dort angesehen werden, ohne dass eine Speicherung der erhobenen Daten erfolgt.[16] Dass auch in diesen Fällen die in der Norm genannten Voraussetzungen zu beachten sind, ergibt sich zudem aus den Gesetzesbegründungen[17] sowie aus der Gesetzessystematik, da die ausdrückliche Regelung der Speicherung in Absatz 3 ansonsten überflüssig wäre.

Aufgrund seines technologiespezifischen Charakters, in dessen Folge der Gesetzgeber die Beobachtung von Räumen zum Anknüpfungspunkt gemacht hat, liegt § 4 was den Anwendungsbereich betrifft quer zum technologieneutralen Ansatz des europäischen und deutschen Datenschutzrechts.[18] Da bei der bloßen Videobeobachtung nur dann personenbezogenen Daten erhoben werden, wenn bereits identifizierte Personen iSd Art. 4 Nr. 1 DS-GVO gefilmt werden,[19] erstreckt sich entgegen der Rechtsprechung des Bundesverwaltungsgerichts zur Vorgängernorm der sachliche Anwendungsbereich von § 4 **über den Anwendungsbereich des übrigen BDSG hinaus** auch auf Sachverhalte, bei denen keine personenbezogenen Daten erhoben werden.[20] Weil parallel hierzu die bloße Videobeobachtung (nach allerdings umstrittener Ansicht) keinen Eingriff in das Recht auf in- 7

15 Terminologisch kann unter dem (auch im § 4 verwendeten) Oberbegriff der Video*überwachung*, also die Video*beobachtung* und die Video*aufzeichnung* unterschieden werden, *Siegel* NVwZ 2012, 738 (738); *Datenschutzkonferenz*, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, 3.9.2020, S. 5.

16 BVerwG NJW 2019, 2556 (2558, Rn. 15 f.); empirisch dürften bloße Beobachtungssysteme ohne Aufzeichnung die Ausnahme darstellen, s. *Bretthauer* Intelligente Videoüberwachung S. 98.

17 BT-Drs. 14/4329, 38; BT-Drs. 14/5793, 62.

18 Zu Recht kritisch zur Technologieneutralität als Leitbild *Sydow/Kring* ZD 2014, 271.

19 Eine Identifizierbarkeit iSd Art. 4 Nr. 1 DS-GVO kommt bei der bloßen Videobeobachtung wegen der Flüchtigkeit der Bilder regelmäßig nicht in Betracht (zweifelnd auch *Bretthauer* Intelligente Videoüberwachung S. 106); sollte die Beobachtung zur anschließenden Identifizierung führen, so ist das Datum zu diesem Zeitpunkt nicht mehr vorhanden. Aus der Entscheidung EuGH NJW 2015, 463 – Ryneš, ergibt sich nichts anderes, da der Gerichtshof ausdrücklich auf die Aufzeichnung der Bilder abstellt (Rn. 20 ff.); deutlicher noch EuGH ZD 2020, 148 (149 Rn. 35). Auch die vielfach aus technischen Gründen erfolgende kurzfristige Zwischenspeicherung führt nicht zu einem anderen Ergebnis, s. überzeugend *Schröder* ZD 2021, 302 (304).

20 Gola/*Gola* DS-GVO Art. 6 Rn. 145, 155, 161; Plath/*Becker* BDSG § 4 Rn. 1; aA zu § 6b BDSG aF BVerwG NJW 2019, 2556 (2558, Rn. 15), das eine zusätzliche Prüfung für erforderlich hält, ob personenbezogene Daten verarbeitet werden, dies im Ergebnis aber bejaht, wenn Gesichter erkennbar sind; in diesem Sinne auch NK-DS-GVO/BDSG/*Scholz* Anhang zu Artikel 6 DS-GVO (§ 4 BDSG) Rn. 38, kein Problem sieht hierin Auernhammer/*Onstein* BDSG § 4 Rn. 20, der davon ausgeht, dass die Beobachtung stets eine Erhebung personenbezogener Daten beinhaltet; in diesem Sinne auch *Datenschutzkonferenz*, Kurzpapier Nr. 15: Videoüberwachung nach der Datenschutzgrundverordnung, 8.1.2018, S. 3. Dass die Norm daher einen „Fremdkörper" im Datenschutzrecht darstellen soll, so Gola/*Gola* DS-GVO Art. 6 Rn. 155, scheint etwas überspitzt; richtig ist aber, dass die Norm aufgrund ihres technologiespezifischen Ansatzes ebenso quer zur sonstigen Konzeption des BDSG liegt wie zur DS-GVO (→ Rn. 1, 3).

formationelle Selbstbestimmung darstellt,[21] erfasst § 4 BDSG somit auch Tätigkeiten unterhalb der Schwelle zum Grundrechtseingriff.

8 Zugleich wird der Anwendungsbereich des § 4 durch den Begriff der Beobachtung begrenzt, was insbesondere angesichts der allgemeinen Verbreitung von Gegenständen, die als optisch-elektronische Einrichtung im Sinne der Norm einzustufen sind (→ Rn. 9), von Bedeutung ist. Da die genutzte Einrichtung zunächst **abstrakt zur Beobachtung geeignet** sein muss, werden Kameraattrappen und nicht-funktionsfähige Kameras nicht erfasst.[22] Darüber hinaus findet § 4 nur Anwendung, wenn die Einrichtung auch **konkret zur Beobachtung genutzt** wird.[23] Wann dies der Fall ist, muss in wertender Betrachtung des Einzelfalls festgestellt werden. Hierbei können als Kriterien insbesondere die Dauerhaftigkeit der Beobachtung und die Stärke des Beobachtungswillens herangezogen werden,[24] wobei eine besondere Ausprägung eines der beiden Kriterien eine schwächere Ausprägung des anderen Kriteriums ausgleicht.[25] So fallen aufgrund des starken Beobachtungswillens auch Wildkameras, die – ausgelöst durch einen Bewegungsmelder – nur einzelne Bilder anfertigen, in den Anwendungsbereich,[26] auch wenn eine Fotografie grundsätzlich nicht dem Beobachtungsbegriff unterfällt.[27] Beim Einsatz von Webcams, die nicht kontinuierlich filmen, sondern nur ein Foto übertragen, das in vorab bestimmten Zeitintervallen erneuert wird, kommt es für die Bewertung, ob eine Beobachtung vorliegt, zum einen auf die Länge des Intervalls, zum anderen auf den konkret gefilmten Raum an.[28] Der gelegentliche und nicht auf das Filmen eines konkreten Objekts oder einer konkreten Person abzielende Einsatz von Kameradrohnen stellt keine Beobachtung im Sinne der Norm dar, sofern

21 So überzeugend unter Rückgriff auf die bundesverfassungsgerichtliche Rechtsprechung *Wysk* VerwArch 109 (2018), 141 (146 f.); aA unter Verweis auf verwaltungsgerichtliche Rspr. *Siegel* NVwZ 2012, 738 (739), der allerdings auch in der Verwendung von Kameraattrappen einen Eingriff in das Recht auf informationelle Selbstbestimmung sieht und dabei auf die verhaltenslenke Wirkung abstellt; einen Grundrechtseingriff erkennen auch NK-DS-GVO/BDSG/*Scholz* Anhang zu Artikel 6 DS-GVO (§ 4 BDSG) Rn. 43; Auernhammer/*Onstein* BDSG § 4 Rn. 19.

22 Kühling/Buchner/*Buchner* BDSG § 4 Rn. 7; *Datenschutzkonferenz*, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, 3.9.2020, S. 6; die auf den von Attrappen möglicherweise ausgehenden „Überwachungsdruck" abstellende Gegenansicht (Gola/Schomerus/*Gola/Klug/Körffer* BDSG § 6b Rn. 7) ist mit dem Wortlaut der Norm nicht vereinbar. Unabhängig von der datenschutzrechtlichen Bewertung kann bei Attrappen ein zivilrechtlicher Abwehranspruch gegeben sein (s. nur LG Berlin ZD 2016, 189 mit Anm. *Widegreen*).

23 Zivilrechtliche Abwehransprüche können auch hier schon früher ansetzen.

24 Vgl. BVerwG NJW 2019, 2556 (2558, Rn. 15): „jede gewollte, auf einige Zeit angelegte Wahrnehmung äußerer Vorgänge."

25 So überzeugend Plath/*Becker* BDSG § 4 Rn. 11. Interpretationsansätze, die im Sinne einer grundrechtsgeleiteten Auslegung für eine weite Auslegung des Begriffs der Beobachtung plädieren und den Anwendungsbereich der Norm auch auf „flüchtige oder zufällige Kameraaufnahmen" erstrecken, so *Griebel* InTeR 2019, 106 (109), überspannen zum einen den Wortlaut der Norm, bemühen sich aber zum anderen auch um die Schließung von Schutzlücken, die angesichts des ohnehin weiten Anwendungsbereichs des Datenschutzrechts nicht wie behauptet bestehen.

26 *Dienstbühl* CR 2019, 359 (Rn. 2); Paal/Pauly/*Frenzel* BDSG § 4 Rn. 7; in diese Richtung auch Gola/*Gola* DS-GVO Art. 6 Rn. 162.

27 Auernhammer/*Onstein* BDSG § 4 Rn. 21.

28 Zu pauschal daher *Wrede* DuD 2010, 225 (226 ff.).

Menschen nur ungeplant und kurzfristig von den Aufnahmen erfasst werden.[29]

b) Optisch-elektronische Einrichtung

Der vom Gesetzgeber verwendete Begriff der Einrichtung lässt keine Beschränkung des Anwendungsbereichs auf ortsfeste Kameras erkennen; ein dahin gehender Wille des Gesetzgebers ist ebenfalls nicht feststellbar. Daher sind **sowohl stationäre als auch mobile Kameras** erfasst,[30] so dass beispielsweise auch Dash-Cams[31], Body-Cams[32], Kameradrohnen[33], digitale Fotoapparate sowie Smartphones mit integrierter Kamera in den Anwendungsbereich fallen.[34] Aus der Tatsache, dass die Transparenzverpflichtungen der Abs. 2 und 4 die Verwender mobiler Kameras regelmäßig vor Probleme stellt, ließe sich dagegen nur dann etwas ableiten, wenn dies im Einzelfall zur Verfassungswidrigkeit der gesetzgeberischen Ausgestaltung führen würde, was nicht ersichtlich ist. Durch die Beschränkung auf optisch-elektronische Einrichtungen fallen Ferngläser und optische Restlichtverstärker aus dem Anwendungsbereich heraus,[35] wohingegen Nachtsichtgeräte von § 4 erfasst werden.[36] Auch die rein akustische Überwachung wird nicht von § 4 geregelt. 9

c) Öffentlich zugänglicher Raum

§ 4 findet schließlich nur auf die Beobachtung öffentlich zugänglicher Räume Anwendung, wobei der Begriff des Raums nicht auf eine Begrenzung oder Überdachung verweist und somit weit als Bereich zu verstehen ist,[37] der innerhalb oder außerhalb eines Gebäudes liegen kann.[38] Für die Frage, ob dieser öffentlich zugänglich ist, kommt es nicht auf die Eigentumsverhältnisse an,[39] sondern darauf, ob ein Bereich **nach dem erkennbaren Willen des Berechtigten oder einer Zweckbestimmung von einem grundsätzlich offenen Personenkreis genutzt und betreten werden soll.**[40] Die grund- 10

29 AA *Griebel* InTeR 2019, 106 (109).
30 So die ganz hM, s. nur Auernhammer/*Onstein* BDSG § 4 Rn. 22; BeckOK DatenschutzR/*Wilhelm*, 37. Ed. 1.5.2021, BDSG § 4 Rn. 5; Kühling/Buchner/*Buchner* Rn. 7; Plath/*Becker* BDSG § 4 Rn. 12; Nachweise zur überkommenen Gegenansicht bei NK-DS-GVO/BDSG/*Scholz* Anhang 1 zu Artikel 6 DS-GVO (§ 4 BDSG) Rn. 35.
31 Hierzu *Datenschutzkonferenz*, Positionspapier zur Unzulässigkeit von Videoüberwachung aus Fahrzeugen (sog. Dashcams), 28.1.2019.
32 Hierzu *Datenschutzkonferenz*, Orientierungshilfe der Datenschutzaufsichtsbehörden zu dem Einsatz von Bodycams durch private Sicherheitsunternehmen, 22.2.2019.
33 Hierzu *Datenschutzkonferenz*, Positionspapier zur Nutzung von Kameradrohnen durch nicht-öffentliche Stellen, 16.1.2019.
34 *Düsseldorfer Kreis*, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", 19.2.2014, S. 5.
35 NK-DS-GVO/BDSG/*Scholz* Anhang 1 zu Artikel 6 DS-GVO (§ 4 BDSG) Rn. 37.
36 *Alich* DuD 2010, 44 (45).
37 BeckOK DatenschutzR/*Wilhelm*, 37. Ed. 1.5.2021, BDSG § 4 Rn. 7.
38 *Düsseldorfer Kreis*, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", 19.2.2014, S. 6.
39 *Düsseldorfer Kreis*, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", 19.2.2014, S. 6.
40 BVerwG NJW 2019, 2556 (2558, Rn. 14); BeckOK DatenschutzR/*Wilhelm*, 37. Ed. 1.5.2021, BDSG § 4 Rn. 8; Plath/*Becker* BDSG § 4 Rn. 9.

sätzliche Offenheit des potenziell zugangsberechtigten Personenkreises entfällt dabei nicht durch abstrakte Zugangsvoraussetzungen, wie ein Mindestalter oder die Zahlung eines Eintrittsgeldes.[41] Als öffentlich zugängliche Räume iSd § 4 sind somit unter anderem die für das allgemeine Publikum geöffneten Bereiche von Gaststätten, Hotels und Warenhäusern, sowie Kinosäle, die Ausstellungsräume eines Museums, Spielhallen und Casinos einzustufen.[42]

11 Nicht öffentlich zugänglich sind hingegen zum einen Bereiche, die nach dem Willen des Berechtigten oder ihrer Zweckbestimmung nach nur von einem bestimmten und abschließend definierten Personenkreis betreten werden dürfen.[43] Tritt dieser Wille nicht klar erkennbar zu Tage (wie zB durch ein Verbotsschild oder eine nur mit einem Schlüssel zu öffnende Tür), kommt es auf den Kontext und die Sozialanschauung an.[44] Daher kann im Einzelfall ein als solcher erkennbarer Vorgarten eines Hauses auch dann als nicht-öffentlicher Raum zu qualifizieren sein, wenn er nicht durch einen Zaun, eine Mauer oder eine Hecke als nicht zu betreten gekennzeichnet ist,[45] sofern sich der dem Zugang entgegenstehende Wille des Berechtigten aus der allgemeinen Lebenserfahrung ergibt. Auch Treppenhäuser von Mehrparteienhäusern, sind daher grundsätzlich als nicht-öffentlich anzusehen, selbst wenn die Eingangstür nicht verschlossen ist.[46] Anderes gilt nur für Häuser, in denen sich beispielsweise Arztpraxen oder Anwaltskanzleien mit einem offenen Publikumsverkehr befinden[47] und deren Treppenhäuser während der Öffnungszeiten als öffentlich zugänglich zu gelten haben.[48] Schließlich erfasst § 4 BDSG auch nicht die Videoüberwachung von Arbeitnehmern an ihren nicht öffentlich zugänglichen Arbeitsplätzen, auf die § 26 BDSG Anwendung findet (→ § 26 Rn. 26 ff., 33 ff.).[49]

41 *Düsseldorfer Kreis*, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", 19.2.2014, S. 6.
42 Ausführliche Aufzählungen bei Plath/*Becker* Rn. 9 sowie NK-DS-GVO/BDSG/*Scholz* Anhang 1 zu Artikel 6 DS-GVO (§ 4 BDSG) Rn. 58.
43 So *Düsseldorfer Kreis*, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", 19.2.2014, S. 6.
44 Diese laufen nicht notwendigerweise mit dem rechtlichen Dürfen parallel, hierzu anschaulich OVG Saarland ZD 2018, 97 (98 f.).
45 Hierauf abstellend BeckOK DatenschutzR/*Wilhelm*, 37. Ed. 1.5.2021, BDSG § 4 Rn. 10.
46 AA Paal/Pauly/*Frenzel* BDSG § 4 Rn. 9.
47 *Düsseldorfer Kreis*, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", 19.2.2014, S. 7.
48 VG Oldenburg ZD 2013, 296 (298 f.).
49 Ausführlich hierzu Weth/Herberger/Wächter/Sorge Arbeitnehmerdatenschutz-HdB/*Byers*, 2. Aufl. 2019, S. 475 ff.; *Datenschutzkonferenz*, Orientierungshilfe Videoüberwachung durch nicht-öffentliche Stellen, 3.9.2020, S. 24 ff.

2. Regelungsadressaten mit Blick auf die Zwecke des Abs. 1 (Unionsrechtskonformität)

a) Öffentliche Stellen des Bundes: Abs. 1 S. 1 Nr. 1 und 2

Die öffentlichen Stellen des Bundes als Regelungsadressaten (§ 1 Abs. 1 Nr. 1)[50] können Videoüberwachungsmaßnahmen allein auf die Zulässigkeitstatbestände des Abs. 1 S. 1 Nr. 1 („Aufgabenerfüllung öffentlicher Stellen") und Nr. 2 („Wahrnehmung des Hausrechts") stützen. Diese stellen eine mitgliedstaatliche Rechtsgrundlage im Sinne des Art. 6 Abs. 3 iVm Abs. 1 lit. e DS-GVO dar und sind somit unionsrechtlich unbedenklich.[51] Auf den Zulässigkeitstatbestand des Abs. 1 S. 1 Nr. 3 („Wahrnehmung berechtigter Interessen") können sich öffentliche Stellen seit jeher nicht berufen.[52] Dies ergibt sich nun auch aus Art. 6 Abs. 1 UAbs. 2 DS-GVO, der die unionsrechtliche Interessenabwägung als Erlaubnistatbestand für öffentliche Stellen explizit ausschließt, was durch das mitgliedstaatliche Recht nicht überspielt werden darf.[53] 12

b) Nichtöffentliche Stellen: Abs. 1 S. 2 iVm S. 1 Nr. 3

Was dagegen die Frage betrifft, inwieweit § 4 seit Geltungsbeginn der DS-GVO noch nichtöffentliche Stellen als Regelungsadressaten erfassen kann, ist danach zu unterscheiden, ob die Videoüberwachung allein im privaten Interesse des Verantwortlichen erfolgt oder ob primär öffentliche Zwecke bzw. die Interessen Dritter verfolgt werden. Denn für die **im privaten Interesse** erfolgende Verarbeitung personenbezogener Daten enthält Art. 6 DS-GVO keine Öffnungsklausel, sondern die Norm stellt insoweit eine abschließende Regelung dar. Da die Einwilligung als Erlaubnistatbestand für die Videoüberwachung kaum eine Rolle spielen dürfte (→ Rn. 3), ist somit die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO der alleinige Erlaubnisgrund für Video**aufzeichnungen** im privaten Interesse.[54] Soweit private Stellen bei der Videoüberwachung im privaten Interesse personenbezogene Daten verarbeiten, erweist sich § 4 Abs. 1 S. 1 Nr. 3 nach ganz herrschender Ansicht im Ergebnis als unionsrechtswidrig, da die Interessenabwägung leicht abweichend von der unionsrechtlichen Interessenabwägung formuliert ist („Anhaltspunkte") und zudem für bestimmte Fäl- 13

50 Die subsidiäre Anwendbarkeit des BDSG auf Landesbehörden (§ 1 Abs. 1 Nr. 2) ist praktisch von sehr untergeordneter Bedeutung, Auernhammer/*von Lewinski* BDSG § 1 Rn. 7; gerade für die Videoüberwachung gibt es Regelungen in den Landesdatenschutz- und den Landespolizeigesetzen, die dem BDSG insoweit vorgehen.

51 Auernhammer/*Onstein* BDSG § 4 Rn. 25 f. Kaum praktikabel erscheint dagegen die Ansicht, nach der die Wahrnehmung des Hausrechts durch öffentliche Stellen keine öffentliche Aufgabe darstellt, weshalb der Zulässigkeitstatbestand der Nr. 2 in Gänze unionsrechtswidrig sein soll und sich öffentliche Stellen insoweit auf die Interessenabwägung in Art. 6 Abs. 1 lit. f DS-GVO zu stützen hätten (so aber Roßnagel Neues DatenschutzR/*Nebel*, 2018, BDSG § 3 Rn. 119), da sich Aufgabenerfüllung und Wahrung des Hausrechts regelmäßig überschneiden (vgl. Plath/*Becker* BDSG § 4 Rn. 15).

52 NK-DS-GVO/BDSG/*Scholz* Anhang 1 zu Artikel 6 DS-GVO (§ 4 BDSG) Rn. 73.

53 Tinnefeld/Buchner/Petri/Hof DatenschutzR/*Buchner*, 7. Aufl. 2020, S. 258.

54 So auch die *Datenschutzkonferenz*, Kurzpapier Nr. 15: Videoüberwachung nach der Datenschutzgrundverordnung, 8.1.2018, S. 1; für die Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO können aber die mit Blick auf § 4 Abs. 1 BDSG angestellten Überlegungen (→ Rn. 24 ff.) als Richtschnur herangezogen werden.

le durch den Abs. 1 S. 2 vorstrukturiert wird.[55] Denn eine solche Konkretisierung der unionsrechtlichen Interessenabwägung durch einen mitgliedstaatlichen Gesetzgeber hat der EuGH bereits unter Anwendung der Datenschutz-Richtlinie 95/46/EG als unzulässig erachtet.[56] Mit Blick auf die im privaten Interesse erfolgende Videoüberwachung verbleibt § 4 Abs. 1 S. 1 Nr. 3 damit ein Restanwendungsbereich nur für jene Fälle der reinen Video**beobachtung**, auf die die DS-GVO mangels Verarbeitung personenbezogener Daten keine Anwendung findet (→ Rn. 7).[57] Auch der Zulässigkeitstatbestand des Abs. 1 S. 1 Nr. 2 („Wahrung des Hausrechts") kann auf nichtöffentliche Stellen wegen des Vorrangs von Art. 6 Abs. 1 lit. f DS-GVO nicht mehr angewandt werden.

14 Weiterer Diskussionen bedarf hingegen die vom BVerwG in einem obiter dictum und mit knapper Begründung[58] verneinte Frage, ob Abs. 1 S. 1 Nr. 3 in Fällen zur Anwendung kommen kann, in denen nichtöffentliche Stellen eine Videoüberwachung primär **im öffentlichen Interesse** vornehmen. Insoweit könnte der Zulässigkeitstatbestand der Öffnungsklausel des Art. 6 Abs. 3 iVm Abs. 1 lit. e DS-GVO greifen. Aus einem Referentenentwurf für DSAnpUG-EU vom November 2016, der sich in seiner Begründung ausdrücklich auf diese Öffnungsklausel und den Erwägungsgrund 45 stützte, ging dies deutlicher hervor, da nach diesem die Videoüberwachung durch nichtöffentliche Stellen nur dann unter das BDSG fallen sollte, wenn es zum Schutz „von Leben, Gesundheit oder Freiheit von Personen erforderlich ist, die sich in öffentlich zugänglichen großflächigen Anlagen (…) aufhalten."[59] Während in dieser Formulierung noch recht zwanglos die Übertragung einer im öffentlichen Interesse liegenden Aufgabe und damit eine Rechtsgrundlage im Sinne von Art. 6 Abs. 3 iVm Abs. 1 lit. e DS-GVO

55 BVerwG NJW 2019, 2556 (2562, Rn. 47); Ehmann/Selmayr/*Heberlein* DS-GVO Art. 6 Rn. 67; Kühling/Buchner/*Buchner* BDSG § 4 Rn. 2 ff.; HK-EuDSchVO/*Reimer* DS-GVO Art. 6 Rn. 83; *Lachenmann* ZD 2017, 407 (410); *Veil* NVwZ 2019, 1132 (1132 f.); *Ziebarth* ZD 2017, 467 (469); eine unionsrechtskonforme Auslegung scheitert letztlich am Widerholungsverbot (so im Ergebnis auch Paal/Pauly/*Frenzel* BDSG § 4 Rn. 5/6), da entgegen Erwägungsgrund 8 die Wiederholung einer DS-GVO-Norm durch eine erst im Wege der Konformauslegung inhaltsgleiche Norm des mitgliedstaatlichen Rechts nicht der Kohärenz und Verständlichkeit dient, aA Auernhammer/*Onstein* BDSG § 4 Rn. 30.

56 EuGH NVwZ 2017, 213 (Rn. 50 ff.) – Breyer, mit Anm. *Ziegenhorn*; s. in diese Richtung auch Schantz/Wolff Neues DatenschutzR/*Wolff*, 2017, Rn. 636.

57 AA *Datenschutzkonferenz*, Kurzpapier Nr. 15: Videoüberwachung nach der Datenschutzgrundverordnung, 8.1.2018, S. 3, die ohne weitere Begründung von einer Anwendbarkeit der DS-GVO auch auf die bloße Videobeobachtung ausgeht.

58 BVerwG NJW 2019, 2556 (2561 f., Rn. 46 f.).

59 Bemerkenswerterweise verweist der Entwurf in seiner Begründung für Videoüberwachungen im rein privaten Interesse auf Art. 6 Abs. 1 lit. f DS-GVO als Erlaubnistatbestand.

gesehen werden konnte,[60] lässt sich eine solche Aufgabenübertragung dem Abs. 1 S. 1 Nr. 3 isoliert betrachtet nicht mehr entnehmen. Anders stellt sich dies jedoch dar, bezieht man auch den Satz 2 mit ein, der für bestimmte Räume den Schutz von Leben, Gesundheit und Freiheit der sich dort aufhaltenden Personen als besonders wichtiges Interesse qualifiziert. Dass dieser Norm ein gefahrenabwehrrechtlicher Impetus innewohnt, da die Überwachenden ermächtigt werden, nicht nur eigene, sondern auch fremde Interessen (die sich zu einem öffentlichen Interesse aggregieren lassen) wahrzunehmen, steht außer Frage.[61] Auch wenn eine Aufgabenübertragung sicherlich gesetzestechnisch gelungener hätte formuliert werden können, ist es dennoch möglich, durch Auslegung unter Berücksichtigung des gesetzgeberischen Willens und des Regelungsziels in Abs. 1 S. 2 iVm S. 1 Nr. 3 eine solche Aufgabenübertragung iSv Art. 6 Abs. 1 lit. e DS-GVO zu sehen.[62] **§ 4 Abs. 1 S. 2 iVm S. 1 Nr. 3** kann also **als Zulässigkeitstatbestand für nichtöffentliche Stellen** herangezogen werden und kommt insoweit neben Art. 6 Abs. 1 lit. f DS-GVO zur Anwendung, sofern einer der in S. 2 genannten Räume überwacht wird.[63] Da die mitgliedstaatliche Rechtsgrundlage aber keine nach der Interessenabwägungsklausel des Art. 6 Abs. 1 lit. f DS-GVO zulässigen Datenverarbeitungen verbieten darf, behält § 4 Abs. 1 S. 2 iVm S. 1 Nr. 3 eine Bedeutung nur insoweit, als er Videoüberwachungsmaßnahmen rechtfertigt, die sich nach Art. 6 Abs. 1 lit. f

60 Das BVerwG NJW 2019, 2556 (2561 f., Rn. 45 f.) scheint Art. 6 Abs. 1 lit. e DS-GVO eng zu verstehen und als Erlaubnistatbestand für private Verarbeiter nur in Fällen einer Verantwortungsübertragung durch einen konkret-individuellen Hoheitsakt heranziehen zu wollen (da es sich nur um ein obiter dictum handelte, musste das Gericht diese Frage im Fall nicht dem EuGH vorlegen), s. kritisch *Veil* NVwZ 2019, 1132 (1134 f.). Wenn das Gericht seine Rechtsansicht im Wesentlichen damit begründet, dass bei der Übertragung einer im öffentlichen Interesse liegenden Aufgabe keine zusätzliche Abwägung mit den Interessen der Betroffenen vorgesehen ist, so vermag dies kaum zu überzeugen, da die die Aufgabe übertragende Rechtsgrundlage des nationalen Rechts nach der deklaratorischen Anordnung in Art. 6 Abs. 3 S. 4 DS-GVO verhältnismäßig sein muss und den Betroffenen zudem das Widerspruchsrecht nach Art. 21 DS-GVO zusteht.

61 In dieser Weise interpretiert erklären sich Private, die einen Raum iSd § 4 Abs. 1 S. 2 überwachen, nicht selbst zum Sachwalter des öffentlichen Interesses, wie es das Bundesverwaltungsgericht meint, sondern werden vom Gesetzgeber dazu ermächtigt; auch die vom Gericht zugrunde gelegte Trennung zwischen individuellen Sicherheitsinteressen und einem öffentlichen Interesse an der Gewährleistung von Sicherheit scheint zu scharf gezogen: dass „Semi-Öffentlichkeit" wie in Einkaufszentren ausreicht, damit die Polizei- und Ordnungsbehörden originär tätig werden dürfen (s. *Kingreen/Poscher* POR, 10. Aufl. 2018, Rn. 44 f.), heißt nicht zugleich auch, dass eine Überwachung durch die jeweiligen Eigentümer des Raums nicht auch im öffentlichen Interesse erfolgen kann und darf.

62 So auch Schantz/Wolff Neues DatenschutzR/*Wolff*, 2017, Rn. 637; Schwartmann/Jaspers/Thüsing/Kugelmann/*Schwartmann/Jacquemain* Anhang zu Art. 6 DS-GVO (§ 4 BDSG) Rn. 4 und 20; aA Tinnefeld/Buchner/Petri/Hof DatenschutzR/*Buchner*, 7. Aufl. 2020, S. 256; *Ziebarth* ZD 2017, 467 (469) und jetzt auch BVerwG Urt. v. 27.3.2019 – BeckRS 2019, 9874 (Rn. 44 ff.). Gegen eine solche Auslegung lässt sich auch nicht einwenden, dass § 4 Abs. 1 S. 1 Nr. 3 iVm S. 2 BDSG Private zur Videoüberwachung ermächtigt, aber nicht verpflichtet, denn eine Aufgabenübertragung an Private iSv Art. 6 Abs. 1 lit. e DS-GVO muss nicht mit einer rechtlichen Verpflichtung einhergehen, da lit. e sonst insoweit neben lit. c keine eigenständige Bedeutung hätte, s. HK-EuDSchVO/*Reimer* DS-GVO Art. 6 Rn. 41.

63 Ebenfalls davon ausgehend, dass eine solche parallele Anwendung möglich ist HK-EuDSchVO/*Reimer* DS-GVO Art. 6 Rn. 41, 57.

DS-GVO nicht rechtfertigen lassen. Dass eine solche Lösung aus Sicht des Unionsrechts akzeptabel sein und die Billigung des EuGH erfahren könnte,[64] dafür spricht zum einen, dass Videoüberwachungsmaßnahmen nahezu keine Binnenmarktrelevanz entfalten und dass zugleich ihre Akzeptanz in den Mitgliedstaaten stark divergiert.[65]

II. Zulässigkeit der Beobachtung (Abs. 1)

1. Zwecke der Beobachtung

15 § 4 Abs. 1 S. 1 erklärt Maßnahmen der Videoüberwachung „nur" in den Fällen der in den Nr. 1 bis 3 genannten Tatbestände für zulässig. Dies ist insofern irreführend, als der Zulässigkeitstatbestand in Nr. 1 (Aufgabenerfüllung öffentlicher Stellen) regelmäßig durch spezialgesetzliche Regelungen verdrängt wird (→ Rn. 17) und die Interessenabwägung in Nr. 3 nur noch in Verbindung mit Satz 2 als unionsrechtskonforme Regelung überdauern und auch nur *neben* Art. 6 Abs. 1 lit. f DS-GVO zur Anwendung kommen kann (→ Rn. 13 f., 19 f.). § 4 ist daher **nicht** als **abschließend**, sondern eher als **Auffang- und Ergänzungsregelung** zu verstehen.[66]

16 Innerhalb der relativ unbestimmten Grenzen der Zulässigkeitstatbestände des Abs. 1 können durch Maßnahmen der Videoüberwachung sowohl **präventive als auch repressive Zwecke** verfolgt werden, die regelmäßig verknüpft sind.[67] Sie sind im Einzelfall vor der Aufnahme von Überwachungsmaßnahmen von der verantwortlichen Stellen konkretisiert festzulegen und sollten möglichst schriftlich fixiert werden.[68] Dies gilt über den Zulässigkeitstatbestand in Nr. 3, der explizit die Festlegung konkreter Zwecke fordert, hinaus auch für die Tatbestände in Nr. 1 und 2. Denn eine möglichst präzise **Zweckfestlegung** ist nicht nur für die Prüfung erforderlich, ob die Videoüberwachung durch einen der Zulässigkeitstatbestände gedeckt ist, sondern sie ist – wie allgemein im Datenschutzrecht – als Dreh- und Angelpunkt der Erforderlichkeitsprüfung und der Interessenabwägung unverzichtbar. Auch kann ohne vorherige Zweckfestlegung nicht geprüft werden, ob eine Speicherung und Verwendung der erhobenen Daten nach Abs. 3 S. 1 zulässig ist (→ Rn. 38 f.) und wann eine Zweckänderung nach Abs. 3 S. 3 vorliegt (→ Rn. 40). Aus diesem Grund können Zwecke, die sich nur aus den Umständen ableiten lassen, ohne konkret festgelegt worden zu sein, bei der Überprüfung der Zulässigkeit nicht berücksichtigt wer-

64 Hiervon geht vorsichtig auch Schantz/Wolff Neues DatenschutzR/*Wolff*, 2017, Rn. 638, aus.

65 Ausführlich zu den Regelungs- und Rechtsprechungsreserven, die das europäische Datenschutzrecht den mitgliedstaatlichen Gesetzgebern und Gerichten belässt *Marsch*, Das europäische Datenschutzgrundrecht, 2018, S. 309 ff.

66 Im Gesetzgebungsverfahren war daher von *Piltz* vorgeschlagen worden, das „nur" durch ein „insbesondere" zu ersetzen, was die Auffang- und Ergänzungsfunktion aber auch nur unvollkommen widerspiegelt.

67 Auernhammer/*Onstein* BDSG § 4 Rn. 24.

68 *EDSA*, Leitlinien 3/2019 (Version 2.0), Rn. 15; *Düsseldorfer Kreis*, Orientierungshilfe „Videoüberwachung durch nicht-öffentliche Stellen", 19.2.2014, S. 8.

den,[69] da die Zweckfestlegung ansonsten unter anderem ihrer Hinweis- und Warnfunktion für den Verantwortlichen selbst[70] beraubt würde.[71]

a) Aufgabenerfüllung öffentlicher Stellen (S. 1 Nr. 1)

17 Regelungsadressat der Nr. 1 sind schon dem Wortlaut nach allein öffentliche Stellen (→ Rn. 12), die sich zur Erfüllung ihrer Aufgaben der Videoüberwachung bedienen dürfen. Dabei muss die Aufgabe, die anhand der Rechtsgrundlage über die Existenz und Tätigkeit der betreffenden Stellen zu ermitteln ist,[72] nicht durch die Videoüberwachung selbst (als Hauptzweck) erfüllt werden, sondern es genügt, wenn die Erfüllung einer Aufgabe gefördert wird.[73] Da die Norm darüber hinaus – von den Erfordernissen der Erforderlichkeit und des überwiegenden Interesses in Hs. 2 abgesehen – keine weiteren konkretisierenden Tatbestandsmerkmale enthält, fehlt es ihr an einer hinreichenden Bestimmtheit,[74] eingriffsintensive Videoüberwachungsmaßnahmen eines größeren räumlichen oder zeitlichen Ausmaßes zu tragen.[75] Der praktische Anwendungsbereich der Nr. 1 ist in der Folge auch eher schmal,[76] da die Norm regelmäßig durch spezialgesetzliche Regelungen des Bundesrechts (unter anderem §§ 12a, 19a VersG, § 100h StPO, §§ 26–28a BPolG, §§ 34 Abs. 1, 46 BKAG, § 8 Abs. 2 iVm § 9 BVerfSchG, § 5 BNDG, § 5 MADG, §§ 18–22a ZFdG) verdrängt wird, sofern nicht ohnehin landesrechtliche Regelungen (vor allem in den Landespolizeigesetzen und den Landesdatenschutzgesetzen) zur Anwendung kommen.

b) Wahrnehmung des Hausrechts (S. 1 Nr. 2)

18 Auch auf den Zulässigkeitstatbestand der Wahrnehmung des Hausrechts in Abs. 1 S. 1 Nr. 2 können sich in unionsrechtskonformer Auslegung (→ Rn. 12 f.) nur öffentliche Stellen berufen. Deren Hausrecht folgt als Annexkompetenz aus ihren jeweiligen Sachkompetenzen und hat dem **Schutz eines widmungsmäßigen Gebrauchs des Gebäudes oder Grundstücks** zu dienen.[77] Durch Maßnahmen der Videoüberwachung können insoweit präventiv ein unrechtmäßiger Zugang, Sachbeschädigungen und andere

69 So aber Plath/*Becker* BDSG § 4 Rn. 14, der allerdings auch einräumt, dass eine fehlende Dokumentation zulasten des Verantwortlichen geht (Rn. 18).
70 *Härting* NJW 2015, 3284 (3286).
71 Vgl. auch NK-DS-GVO/BDSG/*Scholz* Anhang 1 zu Artikel 6 DS-GVO (§ 4 BDSG) Rn. 81, der zu Recht betont, dass ein „Nachschieben an sich zulässiger Überwachungszwecke" nicht rückwirkend zur Rechtmäßigkeit der Überwachung führt, weshalb bereits vorhandene Aufzeichnungen zu löschen sind.
72 NK-DS-GVO/BDSG/*Scholz* Anhang 1 zu Artikel 6 DS-GVO (§ 4 BDSG) Rn. 68.
73 Auernhammer/*Onstein* BDSG § 4 Rn. 25, der als Beispiele den Schutz eigener Gebäude, Grundstücke und der Mitarbeiter sowie die Überwachung der Funktionsfähigkeit öffentlicher Anlagen nennt. Für ersteres ergeben sich Überschneidungen zur Wahrung des Hausrechts nach Nr. 2.
74 Ausführlich zur erforderlichen Bestimmtheit datenschutzrechtlicher Ermächtigungsgrundlagen für behördliches Handeln *Marsch*/*Rademacher* Die Verwaltung 54 (2021), 1.
75 Zur Kritik an der trotz des relativ grundrechtsintensiven Regelungsgehalts hohen Unbestimmtheit s. nur BeckOK DatenschutzR/*Wilhelm*, 37. Ed. 1.5.2021, BDSG § 4 Rn. 23.
76 Paal/Pauly/*Frenzel* BDSG § 4 Rn. 15.
77 *Ernst* NVwZ 2015, 333 (334, 336).

Störungen verhindert und repressiv Beweismittel mit dem Zweck der Aufklärung und Sanktionierung geschaffen werden.[78] Dabei kann die Wahrnehmung des Hausrechts, anders als in der Literatur vertreten, auch an einen privaten Sicherheitsdienst delegiert werden, ohne dass sich dieser in der Folge nicht mehr auf die Nr. 2 berufen könnte.[79]

c) Schutz von Leben, Gesundheit und Freiheit Dritter durch die Überwachung bestimmter Räume (S. 2 iVm S. 1 Nr. 3)

19 Der in Abs. 1 S. 1 Nr. 3 verankerte Zulässigkeitstatbestand der Wahrung berechtigter Interessen kann für sich genommen isoliert nicht mehr zur Anwendung kommen, da er von der insoweit vorrangigen unionsrechtlichen Interessenabwägung in Art. 6 Abs. 1 lit. f DS-GVO verdrängt wird (→ Rn. 13). Allein in Verbindung mit Satz 2 kann die Norm Maßnahmen der Videoüberwachung legitimieren, sofern diese zumindest auch dem Schutz der dort genannten Interessen Dritter dienen (→ Rn. 14). Diese unionsrechtskonforme Auslegung hat jedoch zur Folge, dass der auf eine gesetzgeberische Vorstrukturierung der Interessenabwägung abzielende **Satz 2** seinen Normcharakter wandelt und zum Teil eines **Zulässigkeitstatbestands** wird, wodurch dessen Tatbestandsmerkmale zu Zulässigkeitsvoraussetzungen erstarken.

20 Videoüberwachungsmaßnahmen können daher nur dann auf Abs. 1 S. 2 iVm S. 1 Nr. 3 gestützt werden, wenn sie dem Schutz von Leben, Gesundheit oder Freiheit anderer Personen dienen, die sich in den in Satz 2 genannten Räumen aufhalten. Entsprechend der unionsrechtlichen Qualifizierung als Aufgabe im öffentlichen Interesse muss es primär also um die Verfolgung dieser fremden Interessen gehen,[80] was nicht ausschließt, dass der Verantwortliche selbst auch ein eigenes (in der Regel wirtschaftliches) Interesse an der Verfolgung dieses Zweckes hat. Überwacht werden dürfen nur die hochfrequentierten Räume des Satzes 2, wodurch eine flächendeckende Überwachung des öffentlichen Raums verhindert wird.

2. Erforderlichkeit

21 In allen drei Fällen des Abs. 1 sowie auch im Rahmen einer bei Videoüberwachungen im privaten Interesse zur Anwendung kommenden Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO[81] ist die Erforderlichkeit der konkreten Maßnahme im Einzelfall zu prüfen. Unstreitig ist in diesem Zu-

78 NK-DS-GVO/BDSG/*Scholz* Anhang 1 zu Artikel 6 DS-GVO (§ 4 BDSG) Rn. 70.

79 So aber NK-DS-GVO/BDSG/*Scholz* Anhang 1 zu Artikel 6 DS-GVO (§ 4 BDSG) Rn. 71. Die Frage, ob eine Auftragsdatenverarbeitung vorliegt, spielt in diesem Zusammenhang keine Rolle, da schon der Wortlaut von Abs. 1 S. 1 Nr. 2 keine Identität von Hausrechtsinhaber und dem für die Beobachtung datenschutzrechtlich Verantwortlichen verlangt.

80 Damit (und dadurch, dass auch Art. 6 Abs. 1 lit. f DS-GVO die Interessen Dritter explizit nennt) ist einer zweifelhaften vormaligen Ansicht der deutschen Datenschutzaufsichtsbehörden der Boden entzogen, nach der das Interesse Dritter *an* einer Videoüberwachung nicht in die Abwägung einzustellen sei, s. nunmehr *Datenschutzkonferenz*, Kurzpapier Nr. 15: Videoüberwachung nach der Datenschutzgrundverordnung, 8.1.2018, S. 2; äußerst kritisch zur vormaligen Position *Bull* JZ 2017, 797 (802).

81 Hierzu HK-EuDSchVO/*Reimer* DS-GVO Art. 6 Rn. 58.