Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG

Gola / Heckmann

3. Auflage 2022
ISBN 978-3-406-78266-4
C.H.BECK

über 12 Millionen Bücher, eBooks, Loseblattwerke, Zeitschriften, DVDs, Online-Datenbanken und Seminare. Besonders geschätzt wird beck-shop.de für sein umfassendes Spezialsortiment im Bereich Recht, Steuern und Wirtschaft mit rund 700.000 lieferbaren Fachbuchtiteln.

Steuerdaten: *Frey/Schwarz/Exner,* Schutz des Steuergeheimnisses durch die DSGVO – Neuartige Auskunftsansprüche bei grenzüberschreitenden Kooperationen von Steuerbehörden, IstR 2019, 797; *Haupt,* Auskunftsrecht nach Art. 15 DSGVO iVm § 2a AO in der finanzgerichtlichen Praxis, DStR 2019, 2115; *Korts,* Die Auskunft nach der DSGVO und Akteneinsicht in die Steuerakte, SAM 2019, 123; *Norstedt/Paßberger,* Das Recht des Steuerpflichtigen auf Auskunft nach Art. 15 DSGVO – ein gebundener Anspruch auf Akteneinsicht?, SAM 2020, 99; *Poschenrieder,* Ein Recht auf Auskunft begründet kein Recht auf Akteneinsicht – Grenzen von Art. 15 DSGVO im Besteuerungsverfahren, DStR 2020, 21; *Schepers,* Der Umgang mit einem Auskunftsersuchen nach der DSGVO, DStR 2019, 1109; *Schober,* Keine Akteneinsicht in Akten der Finanzbehörden nach Art. 15 DSGVO, FR 2020, 558.

Versichertendaten: *Britz/Beyer,* Der datenschutzrechtliche Auskunftsanspruch in der Versicherungspraxis, VersR 2020, 65; *Waldkirch,* Der datenschutzrechtliche Auskunftsanspruch des Versicherten, r+s 2021, 317.

Übersicht

A. Allgemeines

I. Zweck und Bedeutung der Vorschrift

Das Auskunftsrecht gehört zu den basalen Betroffenenrechten und stellt faktisch (nicht rechtlich) eine unverzichtbare Voraussetzung für die Geltendmachung weiterer datenschutzrechtlicher Ansprüche dar.[1] Das Auskunftsrecht wird nicht ohne Grund als „Magna Charta" des Datenschutzrechts bezeichnet.[2] Dies bedeutet jedoch nicht, dass mittels der Auskunft nur datenschutzspezifische Ziele verfolgt werden dürften:[3] Art. 1 Abs. 2 schützt schlichtweg alle Grundrechte und Grundfreiheiten natürlicher Personen.[4] Pauschalen Vorwürfen der Rechtsmissbräuchlichkeit ist daher entschieden eine Absage zu erteilen.[5] Vielen Informationsansprüchen ist gemein, dass sie ein rechtliches Interesse voraussetzen. Demgegenüber einen voraussetzungslosen Anspruch zu verneinen, weil zugleich ein rechtliches Interesse besteht, ist kaum begründbar. Auch reine Neugieranfragen sind zulässig.[6] Der BGH hat die Frage der datenschutzfremd motivierten Auskunft dem EuGH vorgelegt.[7] Art. 15 gewährt einen Anspruch auf **umfassende Information** hinsichtlich der personenbezogenen Daten der betroffenen Person sowie **spezifischer Umstände** der Datenverarbeitung. Art. 15 ist abhängig vom Antrag der betroffenen Person, die Beantwortung kann erheblichen Aufwand beim Verantwortlichen erzeugen. Inzwischen gibt es empirische Studien zur Umsetzung des Auskunftsrechts in der Praxis.[8] **1**

[1] Vgl. nur Erwgr. 63 S. 1 DS-GVO; EuGH Urt. v. 7.5.2009 – C-553/07, BeckRS 2009, 70483 Rn. 52 f.

[2] BeckOK DatenschutzR/*Schmidt-Wudy* DS-GVO Art. 15 Rn. 2; *Korch/Chatard* CR 2020, 438 (441); LAG Hamm Urt. v. 11.5.2021 – 6 Sa 1260/20, BeckRS 2021, 21866 Rn. 43; LDA Brandenburg, 22. TB 2020, S. 47.

[3] So auch Kühling/Buchner/*Bäcker* DS-GVO Art. 15 Rn. 42a; LDA Brandenburg, 22. TB S. 49/51; AA BayLDA, 9. TB 2019, S. 27; vgl. insoweit ArbG Neumünster Urt. v. 11.8.2020 – 1 Ca 247 c/20, ZD 2021, 171; LG Köln Urt. v. 11.11.2020 – 23 O 172/19, ZD 2021, 213.

[4] Verkürzend insoweit Erwgr. 63 S. 1; so auch EDSA, Guidelines 01/2022 v. 18.1.2022, S. 9 f. Zum Auskunftsrecht als Pre-trial-discovery-Instrument insbes. *Riemer* ZD 2019, 413 (414); *Riemer* DSB 2019, 223 ff.

[5] In diese Richtung polemisierend *Suchan* ZD 2021, 198 ff. Vgl. OLG Dresden Urt. v. 29.3.2022 – 4 U 1905/21, BeckRS 2022, 8743; OLG Hamm Beschl. v. 15.11.2021 – 20 U 269/21, ZD 2021, 237; LAG Sachsen Urt. v. 17.2.2021 – 2 Sa 63/20, ZD 2022, 171 (172).

[6] So auch *Korch/Chatard* CR 2020, 438 (446).

[7] BGH Beschl. v. 29.3.2022 – VI ZR 1352/20, BeckRS 2022, 9584.

[8] *Ausloos/Dewitte* IDPL 2018, 4 ff.; *Buchmann/Eichhorn* DuD 2019, 65 ff.

II. Systematik, Verhältnis zu anderen Vorschriften

2 Das Recht auf Auskunft ergibt sich unmittelbar aus Art. 8 Abs. 2 S. 2 Alt. 1 GRCh. Art. 15 steht insoweit in der Tradition von Art. 12 lit. a DS-RL.[9] Der Anspruch reicht gewissermaßen vom **„Ob"** der Datenverarbeitung (Abs. 1 Hs. 1) über das **„Wie"** (Abs. 1 Hs. 2 lit. a–h, Abs. 2) bis zum **„Was"** (Abs. 1 Hs. 2, Abs. 3). Neben ein Recht auf Negativauskunft tritt die Angabe umfangreicher Metadaten, um schließlich in die inhaltlich-materielle Auskunft über die verarbeiteten Daten als solche zu münden.

3 Die formalen Informationsgehalte der Art. 13–15 (sog. **„Metadaten"**) sind weitgehend deckungsgleich. Art. 15 bleibt dabei freilich etwas hinter den Art. 13 und 14 zurück, gewährt aber stattdessen **materiell Einblick** in die verarbeiteten Daten beim Verantwortlichen (und seinem Auftragsverarbeiter). Die in den Art. 13 und 14 behauptete Unterscheidung zwischen allgemeinen Pflichtinhalten und besonderen Zusatzinhalten (→ Art. 13 Rn. 6) entfällt bei Art. 15 gänzlich. Die Metadaten ergeben sich zum Teil bereits aus dem Verarbeitungsverzeichnis gem. Art. 30 Abs. 1. Der Verantwortliche tut gut daran, anlässlich eines Auskunftsersuchens nicht einfach die einst erteilten Informationen nach den Art. 13 oder 14 bzw. die einschlägigen Inhalte aus dem Verarbeitungsverzeichnis in die Auskunft zu kopieren, sondern die Metadaten kritisch auf zwischenzeitliche Änderungen hin zu prüfen.[10] Die Auskunft über bestimmte Metadaten kann nicht durch pauschalen Verweis auf eine umfangreiche Datenschutzerklärung erfüllt werden.[11]

Kongruenzen	**Art. 13**	**Art. 14**	**Art. 15**
Verantwortlicher und Vertreter	Abs. 1 lit. a	Abs. 1 lit. a	–
Datenschutzbeauftragter	Abs. 1 lit. b	Abs. 1 lit. b	–
Zwecke und Rechtsgrundlage	Abs. 1 lit. c	Abs. 1 lit. c	Abs. 1 lit. a [abzügl. Rechtsgrundlage]
Datenkategorien	–	Abs. 1 lit. d	Abs. 1 lit. b
Berechtigte Interessen	Abs. 1 lit. d	Abs. 2 lit. b	–
Empfänger oder Kategorien von Empfängern	Abs. 1 lit. e	Abs. 1 lit. e	Abs. 1 lit. c
Drittstaatstransfer	Abs. 1 lit. f	Abs. 1 lit. f	Abs. 2 [abzügl. Angemessenheitsbeschluss und Garantien nach Art. 49 Abs. 1]
Speicherdauer	Abs. 2 lit. a	Abs. 2 lit. a	Abs. 1 lit. d
Auskunftsanspruch (Art. 15); Berichtigung (Art. 16); Löschung	Abs. 2 lit. b	Abs. 2 lit. c	Abs. 1 lit. e [abzügl. Auskunft (Art. 15) und

[9] Rspr. zu Art. 12 lit. a DS-RL: EuGH Urt. v. 7.5.2009 – C-553/07, EuZW 2009, 546; Urt. v. 12.12.2013 – C-486/12, ZD 2014, 248; Urt. v. 17.7.2014 – C-141/12, C-372/12, ZD 2014, 515; Urt. v. 20.12.2017 – C-434/16, ZD 2018, 113.

[10] So auch BayLfD, Das Recht auf Auskunft nach der Datenschutz-Grundverordnung. Orientierungshilfe, 2019, Rn. 97; Taeger/Gabel/*Mester* DS-GVO Art. 15 Rn. 4.

[11] KG Urt. v. 15.9.2021 – 5 U 35/20, GRUR-RS 2021, 45808.

Kongruenzen	Art. 13	Art. 14	Art. 15
(Art. 17 Abs. 1); Einschränkung der Verarbeitung (Art. 18); Widerspruch (Art. 21); Datenübertragbarkeit (Art. 20)			Datenportabilität (Art. 20)]
Widerruf der Einwilligung	Abs. 2 lit. c	Abs. 2 lit. d	–
Beschwerderecht	Abs. 2 lit. d	Abs. 2 lit. e	Abs. 1 lit. f
Pflicht zur Bereitstellung der Daten	Abs. 2 lit. e	–	–
Datenquelle	–	Abs. 2 lit. f	Abs. 1 lit. g
Automatisierte Entscheidungsfindung	Abs. 2 lit. f	Abs. 2 lit. g	Abs. 1 lit. h

Art. 15 Abs. 1 steht grundsätzlich neben anderen Auskunfts- und Einsichtsrechten **4**
wie beispielsweise dem Anspruch auf Einsichtnahme in die Patientenakte nach § 630g BGB,[12] der Einsichtnahme in die Personalakte nach § 83 Abs. 1 S. 1 BetrVG[13] bzw. § 110 Abs. 1 BBG.[14] Ob Ansprüche im Wege der **Spezialität** verdrängt werden, kann nicht pauschal festgelegt werden (Einzelheiten, → Art. 12 Rn. 61 ff.). Das Recht auf Datenübertragbarkeit nach Art. 20 ist insoweit spezieller[15] als das Auskunftsrecht, weil die betroffene Person Daten in einem strukturierten, gängigen und maschinenlesbaren Format herausverlangt und engere Tatbestandsvoraussetzungen gelten. Keine Betroffenenrechte stellen Ansprüche nach den Informationsfreiheitsgesetzen (IFG; VIG; UIG) oder sonstige Einsichtsansprüche (§ 29 VwVfG; § 100 VwGO; § 299 ZPO;[16] § 810 BGB etc) dar.[17] Dort niedergelegte Einschränkungen sind nicht im Anwendungsbereich des Art. 15 fruchtbar zu machen, auch nicht im Wege der Analogie.[18]

B. Einzelerläuterungen

I. Informationsgehalte

1. Negativauskunft (Abs. 1 Hs. 1). Die Bestätigung, ob Daten der betroffe- **5**
nen Person verarbeitet werden oder nicht, wurde schon nach Art. 12 lit. a Spiegelstrich 1 Var. 1 DS-RL gewährt. Dementsprechend bestand ein solcher Anspruch nach hM bereits gem. § 34 Abs. 1 S. 1 BDSG aF, obschon er dort nicht ausdrücklich

[12] Art. 15 umfasst laut Erwgr. 63 ausdrücklich auch gesundheitsbezogene Daten, etwa Patientenakten, Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen. Näher Ärztekammer Berlin, Auskunftsrecht und Einsichtnahme in Patientenunterlagen, Stand Oktober 2020.

[13] Hierzu *Franzen* NZA 2020, 1593 ff.; *Gola* RDV 2020, 169 (175 ff.); LfDI Baden-Württemberg, 35. TB 2019, S. 27; LAG Baden-Württemberg Urt. v. 20.12.2018 – 17 Sa 11/18, BeckRS 2018, 39584.

[14] Hierzu *Gola* RDV 2020, 169 (173 ff.).

[15] AA SächsDSB, 20. TB 2019, S. 77.

[16] Hierzu und § 13 FamFG *Deutschmann* ZD 2021, 414 ff.

[17] Überblick bei BayLfD, Das Recht auf Auskunft nach der Datenschutz-Grundverordnung. Orientierungshilfe, 2019, Rn. 14 ff.

[18] *Eßer/Franck*, Datenschutzrecht, 2022, Rn. 378 zu § 2 Abs. 3 Var. 3 IFG NRW.

A. Allgemeines

I. Zweck und Bedeutung der Vorschrift

1 Die DS-GVO sagt zur Verarbeitung von Beschäftigtendaten nichts bzw. nur wenig Spezielles und überlässt deren Regelung insbesondere im Rahmen der Öffnungsklausel des Art. 88 DS-GVO dem nationalen Gesetzgeber.[1]

2 Diese Möglichkeit hat der Bundesgesetzgeber auch genutzt, um die 2009 in das BDSG aF eingefügte Beschäftigtendatenschutznorm des § 32 BDSG aF in der etwas erweiterten Fassung des § 26 fortzuschreiben.[2] Den zahlreichen Aufrufen, die Möglichkeit des Art. 88 DS-GVO zur Schaffung umfassender und die fortschreitende Digitalisierung der Arbeitswelt[3] beachtender Normen zu nutzen, ist er allein schon im Hinblick auf den bestehenden Zeitdruck, unter dem der Erlass des DSAnpUG stand, nicht gefolgt.[4] Die Regelung des § 32 Abs. 1 S. 1 BDSG aF und seine Fortschreibung in § 26 Abs. 1 S. 1 sollen die bisherige Rechtsprechung zum Beschäftigtendatenschutz gesetzlich absichern[5] bzw. die Absicherung beibehalten.[6]

II. Systematik/Verhältnis zu anderen Vorschriften

3 **1. Konkretisierung des Verarbeitungsverbots mit Erlaubnisvorbehalt.** Die DS-GVO hält an dem bislang geltenden Grundprinzip fest, dass die automatisierte bzw. dateigebundene Verarbeitung personenbezogener Daten durch private und öffentliche Verarbeiter unter einem Verbot mit Erlaubnisvorbehalt steht. Die Verarbeitungserlaubnis kann sich aus Zulässigkeitstatbeständen der DS-GVO (ua Art. 6, 9) oder solchen in bereichsspezifischen Regelungen des Rechts der Union oder der Mitgliedstaaten ergeben, sofern die Verordnung hierauf verweist bzw. dem Mitgliedstaat die Möglichkeit zur Schaffung spezieller Erlaubnistatbestände eröffnet. Letzteres ist für den Beschäftigtendatenschutz der Fall.

4 **2. Verhältnis zur DS-GVO.** Soweit § 26 Rechtsgrundlagen enthält, treten die entsprechenden Regelungen der DS-GVO zurück. Insbesondere ist § 26 Abs. 1 S. 1 (Datenverarbeitung zur Begründung oder zur Durchführung eines Beschäftigungsverhältnisses) ***lex specialis*** zu Art. 6 Abs. 1 lit. b DS-GVO (Datenverarbeitung zur Vertragsdurchführung oder zur Durchführung vorvertraglicher Maßnahmen). Die Spezialität reicht aber nur so weit, wie die Zweckbestimmungen des § 26 einschlägig sind.[7] Für „**beschäftigungsfremde" Zwecke** kann hingegen ein Rückgriff auf Erlaubnistatbestände des Art. 6 Abs. 1 DS-GVO mög-

---

[1] *Franzen* EuZA 2017, 313; *Maier* DuD 2017, 169; *Sörup/Marquardt* ArbRAktuell 2016, 182; *Kort* DB 2016, 711; *Maschmann* DB 2016, 2480; *Rolf/Siewert* RDV 2017, 236; *Rose/Taeger* DFB 2016, 819; *Wybitul* NZA 2017, 413.

[2] *Gola* BB 2017, 1462.

[3] Vgl. BMAS (Hrsg.), Weißbuch „Arbeiten 4.0"; *Krause,* Digitalisierung und Beschäftigtendatenschutz; BMAS -Forschungsbericht 482.

[4] Eine Übersicht zu bisherigen gesetzgeberischen Initiativen gibt *Weichert* NZA 2020, 1597.

[5] BT-Drs. 16/13657, 35.

[6] Vgl. bei *Gola/Thüsing/Schmidt* DuD 2017, 244.

[7] Vgl. bei *Thüsing* NZA 2009, 865.

lich sein, insbesondere eine Verarbeitung auf Grundlage berechtigter Interessen gem. lit. f.[8]

Des Weiteren enthält § 26 klarstellende Hinweise[9] auf sich bereits aus der DS-GVO bzw. nationalem Recht ergebende Aspekte. So enthält § 26 Abs. 4 und 6 einen Hinweis auf die ohnehin gem. Art. 88 Abs. 1 DS-GVO bestehende Möglichkeit, im Rahmen des geltenden nationalen Kollektivrechts (TVG, BetrVG, BPersVG) die Verarbeitung personenbezogener Daten einschließlich besonderer Arten personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses zu regeln.[10] Die Basis für betriebsinterne kollektive Regelungen ergibt sich aus den **Mitbestimmungsrechten** der Mitarbeitervertretung, die nach § 26 Abs. 6 unberührt bleiben. **5**

3. Subsidiarität des § 26 gegenüber anderen nationalen Regelungen (§ 1 Abs. 2). Auch das neue BDSG ist als **Auffanggesetz** konzipiert; es tritt gegenüber spezifischen Rechtsvorschriften des Bundes zurück (§ 1 Abs. 2 S. 1). Durch § 1 Abs. 2 S. 2 wird jedoch ergänzend klargestellt, dass die jeweilige bereichsspezifische Spezialregelung nur vorrangig ist, wenn eine **Tatbestandskongruenz** vorliegt, dh, der Sachverhalt deckungsgleich ist. So wie auch zuvor nach § 4 Abs. 1 BDSG aF rechtfertigt eine Norm außerhalb des BDSG eine Datenverarbeitung nur, wenn sie eine konkrete Aussage bezüglich der Art der Daten und ihrer Zweckbestimmung macht. Es genügt nicht, dass lediglich „abstrakt" eine Aufgabe beschrieben wird, zu deren Erfüllung gegebenenfalls personenbezogene Daten benötigt werden.[11] Gegebenenfalls kann es aber im Einzelfall genügen, wenn sich diese Fragen durch Auslegung der Norm ermitteln lassen.[12] Zur Ausfüllung der eine Aufgabe abstrakt beschreibenden Norm ist andernfalls § 26 heranzuziehen. **6**

III. Adressaten des § 26

1. Arbeitgeber. Verantwortlicher und damit Adressat des Datenschutzrechts ist nach der Legaldefinition des Art. 4 Nr. 7 DS-GVO „die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Danach ist jedenfalls der **Arbeitgeber** Adressat des Datenschutzrechts für die im Unternehmen stattfindenden Verarbeitungen personenbezogener Daten. Nichts anderes gilt für § 26, der insofern keine von der DS-GVO abweichende Regelung trifft. **7**

Unklar ist hingegen, ob nur die jeweilige juristische Person Verantwortlicher ist oder ob daneben selbstständig agierende Einrichtungen oder **Stellen innerhalb der juristischen Person** ebenfalls Verantwortliche sind.[13] Die Wendung „juristische Person, Behörde *oder* andere Stelle" spricht eher für die Deutung, dass bei einer juristischen Person ausschließlich diese verantwortlich ist. Die Begriffe „Einrichtung" und „Stelle" sind andererseits offen und können zB nicht nur auf den **8**

---

[8] *Schmidt* RDV 2009, 193.

[9] Vgl. Gesetzesbegründung zu § 26 Abs. 4 S. 4 und zu Abs. 6; BT-Drs. 18/11325, 98 f.

[10] Zur Frage, ob diese Regelung als nationale Öffnungsklausel gleichwohl zwingend ist vgl. Schantz/Wolff Neues DatenschutzR/*Wolff* Rn. 1137 f.

[11] Vgl. zB *Kort* RDV 2012, 8 (9); Simitis/*Dix* BDSG § 1 Rn. 170; Simitis/*Sokol* BDSG § 4 Rn. 15.

[12] BeckOK DatenschutzR/*Brink/Wilhelm* BDSG § 4 Rn. 6.

[13] Vgl. bereits *Gola/Pötters* RDV 2017, 279.

öffentlich-rechtlichen Bereich beschränkt werden.[14] Der **Wortlaut** lässt also viele Lesarten zu – eine eigenständige Verantwortlichkeit von unabhängigen Stellen innerhalb eines Unternehmens, wie zB dem Betriebsrat, kann ihm sicherlich nicht zwingend entnommen werden.

9 Entscheidend sind damit **systematische und teleologische Argumente.** Ein systematischer Ansatzpunkt kann insofern der Begriff der Niederlassung sein. So macht Art. 3 Abs. 1, der die räumliche Anwendbarkeit der DS-GVO im internationalen Kontext regelt, deutlich, dass eine **Niederlassung** nur Teil der verantwortlichen juristischen Person, nicht aber selbst verantwortlich ist (siehe Wortlaut „Niederlassung eines Verantwortlichen"). Wenn also zB ein amerikanisches Unternehmen Standorte in London und Frankfurt hat, sind nicht diese Niederlassungen datenschutzrechtlich verantwortlich, sondern nur die amerikanische Gesellschaft. Auch Niederlassungen treffen natürlich häufig autonom Entscheidungen und verarbeiten dabei selbstständig personenbezogene Daten, etwa bei der Einstellung neuer Mitarbeiter oder beim Kauf von Arbeits- und Betriebsmitteln. Dies macht sie aber nicht automatisch zum Verantwortlichen, denn sonst wäre auch jede Einzelperson, die als Mitarbeiter einer juristischen Person Verarbeitungszwecke festlegen kann, selbst Verantwortlicher. Letzteres wird aber – früher wie heute – zu Recht von niemandem vertreten.

10 Die Erstreckung der datenschutzrechtlichen Verantwortlichkeit auf rechtlich unselbstständige Einheiten wie eine bloße Niederlassung wäre zudem in der Praxis kaum praktikabel und stünde im Widerspruch zur Systematik der **Sanktionen** bei Verstößen gegen die DS-GVO. Die Schadensersatzansprüche von Betroffenen (Art. 82 DS-GVO) und die behördlichen Befugnisse zur Verhängung von Bußgeldern (Art. 83 DS-GVO) setzen die Rechtsfähigkeit des Verantwortlichen voraus, schon um eine effektive Durchsetzung des Datenschutzes zu gewährleisten. Gleiches gilt für die Betroffenenrechte: Hier muss klar sein, an wen sich der Betroffene wenden kann.

11 Im Ergebnis ist also (nur) jede juristische Person Verantwortlicher,[15] das **Datenschutzrecht** ist sozusagen **gesellschaftsrechtsakzessorisch.** Spaltet sich eine juristische Person auf mehrere neue Rechtsträger auf oder werden diese umgekehrt zusammengelegt, verändert sich damit auch die datenschutzrechtliche Verantwortlichkeit. Selbstständig agierende Stellen innerhalb einer juristischen Person wie zB arbeitsrechtliche Betriebe, Abteilungen etc sind hingegen lediglich als Teil des Verantwortlichen Adressat des Datenschutzrechts, auch wenn sie selbst über Zwecke und Mittel der Datenverarbeitung entscheiden.

12 Es mag in der **Praxis** sinnvoll sein, zwischen selbstständig agierenden Standorten **Vereinbarungen** zum Datenschutz zu treffen, die sich an den Inhalten einer Vereinbarung zwischen gemeinsam Verantwortlichen nach Art. 26 orientieren. Zwingend ist dies aber nicht.

13 **2. Betriebsrat. a) Bindung des Betriebsrats an das Datenschutzrecht.** Schwierigkeiten hat lange Zeit die Einordnung des Betriebsrats bereitet.[16] Nach

---

[14] Vgl. auch die englische und französische Fassung: „agency or other body"; „le service ou un autre organisme".

[15] Schantz/Wolff Neues DatenschutzR/*Wolff* Rn. 359; vgl. auch BeckOK DatenschutzR/*Schild* DS-GVO Art. 4 Rn. 88.

[16] Vor Schaffung von § 79a BetrVG tendenziell für eine eigenständige Verantwortlichkeit *Wybitul* NZA 2017, 413 (414); *Kort* ZD 2017, 319 (323); aA Kühling/Buchner/*Hartung* DS-GVO Art. 4 Rn. 11; *Däubler* Gläserne Belegschaften Rn. 640; *Gola/Pötters* RDV 2017, 279; offengelassen *Düwell/Brink* NZA 2017, 1081.

bisherigem Recht ging das **BAG** in ständiger Rechtsprechung davon aus, dass der Betriebsrat – ähnlich wie andere Abteilungen oder Stellen innerhalb eines Unternehmens – nicht selbst Verantwortlicher ist, aber als Teil der verantwortlichen Stelle zur Einhaltung des Datenschutzrechts verpflichtet ist.[17] Er muss also die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch Betriebsratsmitglieder gewährleisten. Zu den Pflichten des Betriebsrats gehört nach dem BAG zB die Wahrung des Datengeheimnisses.[18] Vieles sprach dafür, dass sich daran **unter Geltung der DS-GVO** und dem neuen BDSG nichts geändert hat.[19] Wie vorstehend mit Blick auf andere selbstständige Stellen innerhalb eines Unternehmens dargelegt, weist die DS-GVO die datenschutzrechtliche Verantwortlichkeit einheitlich dem Unternehmen als juristischer Person zu (→ Rn. 8 ff.).

Mit dem Mitte Juni 2021 in Kraft getretenen „Gesetz zur Förderung der Betriebsratswahlen und der Betriebsratsarbeit in einer digitalen Arbeitswelt (Betriebsrätemodernisierungsgesetz)" und dem durch dieses Gesetz neu geschaffenen **§ 79a S. 2 BetrVG** hat der Gesetzgeber die bisherige Rechtsprechung gesetzlich normiert und damit die Streitfrage entschieden;[20] Gleiches gilt für die insofern parallel ausgestaltete Regelung des § 69 BPersVG.[21] Es bleibt also dabei: Der Arbeitgeber ist (allein) Verantwortlicher, der Betriebsrat muss aber bei seiner Tätigkeit die datenschutzrechtlichen Vorgaben ebenfalls beachten. Betroffene und Aufsichtsbehörden können sich somit nur an den Arbeitgeber wenden. Vor Schaffung des § 79a S. 2 BetrVG konnte die Frage der Verantwortlichkeit auch in einer **Kollektivvereinbarung** geregelt werden. Dies dürfte nun nicht mehr möglich sein, da § 79a S. 2 BetrVG kein Hinweis auf eine entsprechende Dispositivität enthält. **14**

Durch die Regelung des § 79a BetrVG wurde hingegen nicht geklärt, wie genau der Arbeitgeber eine hinreichende Datenschutz-Compliance mit Blick auf Datenverarbeitungen des Betriebsrats gewährleisten kann. Nach S. 3 der Norm „**unterstützen** [sie] **sich gegenseitig** bei der Einhaltung der datenschutzrechtlichen Vorschriften". Um dem fortbestehenden Konflikt zwischen der Eigenverantwortung der Mitarbeitervertretung und den Betroffenenrechten der Mitarbeiter gerecht zu werden, sollten klare innerbetriebliche Regelungen geschaffen werden. Für Auskunfts- und andere Betroffenenrechte sollten zB Prozesse vereinbart werden, die eine hinreichende Kooperation bei ihrer Umsetzung gewährleisten. Gleiches gilt für weitere Verpflichtungen des Arbeitgebers, bei denen er auf eine Mitwirkung des Betriebsrats angewiesen ist, wie etwa die Erstellung eines vollständigen Verarbeitungsverzeichnisses nach Art. 30 DS-GVO oder der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO. Entsprechende Regelungen sollten im Interesse klarer Verfahrensabläufe in einer Betriebsvereinbarung abgesichert werden.[22] **15**

[17] BAG Beschl. v. 14.1.2014 – 1 ABR 54/12, NZA 2014, 738 (739); Beschl. v. 7.2.2012 – 1 ABR 46/10, NZA 2012, 744 (747); Beschl. v. 12.8.2009 – 7 ABR 15/08, NZA 2009, 1218 (1221).

[18] BAG Beschl. v. 7.2.2012 – 1 ABR 46/10, NZA 2012, 744 (747); Beschl. v. 12.8.2009 – 7 ABR 15/08, NZA 2009, 1218 (1221); Beschl. v. 3.6.2003 – 1 ABR 19/02, BAGE 106, 188.

[19] S. bereits *Gola/Pötters* RDV 2017, 279.

[20] Zu einem anderen Ergebnis kann man nur kommen, wenn man wie *Maschmann* NZA 2021, 834 davon ausgeht, dass § 79a BetrVG unionsrechtswidrig sei.

[21] *Gola* RDV 2021, 181 (184).

[22] Ein Gestaltungsbeispiel findet sich bei *Gola* RDV 2021, 181 (183).

16 Verletzt der Betriebsrat datenschutzrechtliche Vorschriften, sind die Sanktionsmöglichkeiten begrenzt. Adressat von Betroffenenrechten, Schadensersatzansprüchen und Bußgeldern bleibt – wie dargelegt – der Arbeitgeber. Der Arbeitgeber kann jedoch bei (groben) Datenschutzverstößen die gerichtliche Auflösung des Betriebsrats nach § 23 Abs. 1 S. 1 BetrVG beantragen.[23]

17 **b) Der Betriebsrat als Wächter des Beschäftigtendatenschutzes.** Der Betriebsrat ist nicht nur als Teil des Verantwortlichen gem. § 79a S. 2 BetrVG zur Einhaltung des Datenschutzes verpflichtet, sondern er ist zugleich Wächter des Beschäftigtendatenschutzes und tritt insofern als **Kontrollinstanz** neben den betrieblichen Datenschutzbeauftragten.[24] Ebenso wie bislang § 32 Abs. 3 BDSG aF hält künftig § 26 Abs. 6 mit Blick auf das Verhältnis von BDSG und betrieblicher Mitbestimmung fest, dass die **Beteiligungsrechte** der Interessenvertretungen der Beschäftigten von den Regelungen des BDSG „unberührt" bleiben (→ Rn. 82). Der Betriebsrat bleibt somit auch künftig für den Beschäftigtendatenschutz zuständig und kann dem Arbeitgeber Schranken setzen.[25] Dies folgt aus seiner allgemeinen Befugnis zur Überwachung der Einhaltung der gesetzlichen Bestimmungen der DS-GVO gem. § 80 Abs. 1 Nr. 1 BetrVG[26] und dem Schutzauftrag für die Persönlichkeitsrechte der Arbeitnehmer gem. § 75 Abs. 2 S. 1 BetrVG. Bei § 26 handelt es sich um eine zugunsten der Arbeitnehmer geltende gesetzliche Vorschrift, deren Einhaltung durch den Arbeitgeber der Betriebsrat nach § 80 Abs. 1 Nr. 1 BetrVG überwachen kann.[27]

18 Außerdem kann sich der Betriebsrat – auch aktiv – im Rahmen der zwingenden Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG für datenschutzgerechte Regelungen im Unternehmen einsetzen. Durch das Betriebsrätemodernisierungsgesetz neu hinzugekommen ist das Mitbestimmungsrecht in § 87 Abs. 1 Nr. 14 BetrVG für die „Ausgestaltung von mobiler Arbeit, die mittels Informations- und Kommunikationstechnik erbracht wird".

19 **3. Betriebsärzte.** Auch für interne Betriebsärzte, die unabhängig und der Schweigepflicht unterliegend (§ 203 Abs. 1 Nr. 1 StGB, § 8 Abs. 1 S. 3 ASiG) im Betrieb arbeiten, wird – sofern das Thema problematisiert wird – die Stellung als Verantwortlicher iSd Art. 4 Nr. 7 DS-GVO überwiegend verneint.[28] Im Ausgangspunkt ist dies zutreffend, denn die internen Betriebsärzte agieren als Teil des Unternehmens, indem sie den Arbeitgeber gem. § 3 ASiG bei „Fragen des Gesundheitsschutzes unterstützen". Aufgrund der Schweigepflicht agieren sie allerdings innerhalb der datenverarbeitenden Stelle informationell abgeschottet und unterliegen innerhalb ihres geheimhaltungspflichtigen Wirkungsbereichs auch

---

[23] ArbG Iserlohn Beschl. v. 14.1.2020 – 2 BV 5/19, ZD 2020, 595 mAnm *Tiedeman*.

[24] Vgl. *Gola/Pötters* RDV 2017, 279.

[25] Forgó/Helfrich/Schneider Betr. Datenschutz-HdB/*Forgó/Helfrich/Schneider/Schoof* Teil II. Kap. 3. Rn. 61.

[26] *Kort* ZD 2017, 3 (5).

[27] BAG Beschl. v. 23.3.2021 – 1 ABR 31/19, NZA 2021, 959.

[28] BeckOK DatenschutzR/*Schild* DS-GVO Art. 4 Rn. 119; Bieresborn in Forgó/Helfrich/Schneider/ Betr.Datenschutz-HdB Teil X. Kap. 1 Rn. 64; *Schuler/Weichert*, Die Datenverarbeitung des Betriebsarztes Hinweise zum datenschutzgerechten Umgang mit Patientendaten durch Betriebsärzte und betriebsärztliche Dienste, Stand 22.9.2020 Version 1.0; vgl. zu Sozialdaten LSG Nordrhein-Westfalen Urt. v. 20.6.2007 – L 17 U 125/04, BeckRS 2007, 46657; SächsLfD, TB 2020, Abschn. 8; → DS-GVO Art. 4 Rn. 81.

dem Grundrechts- und Interessenschutz der betroffenen Personen herbeizuführen.[13]

§ 50 S. 2 nennt die **Anonymisierung** der personenbezogenen Daten (→ § 27 Rn. 40 ff.) als eine denkbare Garantie. Hiervon abgestuft kann auch die Pseudonymisierung als eine der Maßnahmen – gegebenenfalls in Verbindung mit weiteren Garantien – in Betracht gezogen werden. Die Bundesregierung selbst geht jedoch davon aus, dass in diesem Kontext die bloße Pseudonymisierung nicht ausreichen kann.[14] Letztendlich wird man dies jeweils im Einzelfall beurteilen müssen. **9**

Als **weitere geeignete Garantie** nennt § 50 S. 2 allgemein Vorkehrungen gegen die Möglichkeit der unbefugten Kenntnisnahme der personenbezogenen Daten durch Dritte und die räumlich und organisatorisch von den sonstigen Fachaufgaben getrennte Datenverarbeitung. Erforderlich kann damit in organisatorischer Hinsicht ein ausdifferenziertes Rollen- und Berechtigungskonzept sein. Technische Maßnahmen sind beispielsweise die Verschlüsselung und Separierung von Datenträgern. Darüber hinaus kann § 48 Abs. 2 als Orientierung für weitere erforderliche Maßnahmen herangezogen werden.[15] **10**

C. Parallelregelungen im Landesrecht

Die **Landesdatenschutzgesetze** enthalten nur zum Teil Parallelvorschriften für die Verarbeitung zu im öffentlichen Interesse liegenden archivarischen, wissenschaftlichen und statistischen Zwecke für Stellen, die der JI-RL unterstehen. Hervorzuheben sind die Vorschriften der Landesdatenschutzgesetze aus Berlin, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen, Schleswig-Holstein und Thüringen: § 35 BlnDSG, § 45 HDSIG, § 40 DSG NRW, § 31 LDSG RhPf, § 36 SächsDSDG, § 26 LDSG SchlH und § 33 Abs. 3 ThürDSG. **11**

§ 51 Einwilligung

(1) **Soweit die Verarbeitung personenbezogener Daten nach einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen kann, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.**

(2) **Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.**

(3) **[1]Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. [2]Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. [3]Die betroffene Person ist vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen.**

(4) **[1]Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. [2]Bei der Beurteilung, ob die Einwil-**

[13] Auernhammer/*Greve* BDSG § 50 Rn. 6.
[14] BT-Drs. 18/11655, 33.
[15] Paal/Pauly/*Frenzel* BDSG § 50 Rn. 5.

ligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. [3]Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. [4]Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

(5) **Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.**

Literatur: *Article 29 Data Protection Working Party,* Guidelines on Consent under Regulation 2016/679, 17/EN WP 259; *Bäcker,* Die Datenschutzrichtlinie für Polizei und Strafjustiz und das deutsche Eingriffsrecht, in Hill/Kugelmann/Martini (Hrsg.), Perspektiven der digitalen Lebenswelt, 2017; *El-Ghazi,* Die Einwilligung in strafprozessuale Zwangsmaßnahmen nach der Umsetzung der Richtlinie (EU) 2016/680 – das Ende der freiwilligen Atemalkoholkontrolle!, ZIS 2019, 110; *Golla/Skobel,* Sie haben doch nichts zu verbergen?, GSZ 2019, 140; *Greve,* Das neue Bundesdatenschutzgesetz, NVwZ 2017, 737; *Kühling/Klar/Sackmann,* Datenschutzrecht, 5. Aufl. 2021; *Radlanski,* Das Konzept der Einwilligung in der datenschutzrechtlichen Realität, 2016; *Roßnagel* (Hrsg.), Das neue Datenschutzrecht, 2017; *Schantz/Wolff,* Das neue Datenschutzrecht, 2017; *Schieder,* Zur datenschutzrechtlichen Einwilligung in polizeiliche Zwangsmaßnahmen, GSZ 2021, 16; *Schneider,* Das Rückgriffsverbot im Datenschutz – kein „best of both worlds"?, CR 2017, 568; *Schwichtenberg,* Die „kleine Schwester" der DSGVO: Die Richtlinie zur Datenverarbeitung bei Polizei und Justiz, DuD 2016, 605; *Singelnstein,* Folgen des neuen Datenschutzrechts für die Praxis des Strafverfahrens und die Beweisverbotslehre, NStZ 2020, 639; *Stief,* Die Richtlinie (EU) 2016/680 zum Datenschutz in der Strafjustiz und die Zukunft der datenschutzrechtlichen Einwilligung im Strafverfahren, StV 2017, 470; *Weinhold,* RL zum Datenschutz für Polizei und Justiz – Überblick und Umsetzung, ZD-Aktuell 2017, 05451.

Übersicht

A. Allgemeines

I. Zweck und Bedeutung der Vorschrift

§ 51 präzisiert die Voraussetzungen der Einwilligung im Kontext der Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Ordnungswidrigkeiten zuständigen öffentlichen Stellen. Hierdurch soll die Einwilligung weiterhin von zentraler Bedeutung für die **Legitimation der Verarbeitung personenbezogener Daten** in diesem Kontext sein. Diese Regulierung ist jedoch kritisch zu sehen, da es im genannten Anwendungsbereich umstritten ist, ob eine auf einer freiwilligen Entscheidung beruhende Einwilligung überhaupt möglich ist (→ Rn. 26).[1] Die JI-RL gibt zudem die Einwilligung als Handlungselement des Datenschutzrechts nicht unmittelbar vor.[2] Allerdings untersagt sie die Einwilligung als „Maßnahme der informationellen Selbstbestimmung" in diesem Zusammenhang auch nicht.[3] Der deutsche Gesetzgeber übernimmt daher für § 51 weitreichend die Vorgaben des Art. 7 DS-GVO. Ergänzend stellt § 51 Abs. 1 jedoch das Kriterium auf, dass es im vorliegenden Kontext einer Rechtsvorschrift bedarf, die die Einwilligung in einem bestimmten Bereich gestattet. Eine Einwilligung als Grundlage einer Datenverarbeitung bedarf somit einer weiteren gesetzlichen Gestattung. § 51 selbst nennt dabei lediglich die Kriterien, die in einem solchen Fall gelten, ohne selbst eine solche Rechtsvorschrift darzustellen.[4] Diese Einschränkung des Selbstbestimmungsrechts betroffener Personen im Rahmen von strafrechtlichen Verfahren führt dazu, dass die Einwilligung als Grundlage der Datenverarbeitung in der Praxis nur noch einen sehr eingegrenzten Anwendungsbereich besitzt.[5] **1**

Datenschutz ist in erster Linie Persönlichkeitsschutz oder in anderer Diktion **Schutz informationeller Selbstbestimmung,** vgl. Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG. Verfassungsrechtlich besitzt der Bürger somit auch das Recht, „unvernünftig" mit seinen personenbezogenen Daten umzugehen. Aufgrund der nur unvollständigen Vorgaben, die der Gesetzgeber zunächst in § 51 getroffen hat, sind bei der Auslegung der Norm die primär- bzw. verfassungsrechtlich geprägten **2**

[1] Kühling/Buchner/*Schwichtenberg* BDSG § 51 Rn. 1; vgl. auch Erwgr. 43 S. 1 der DS-GVO.
[2] So auch *Stief* StV 2017, 470 (473).
[3] *Stief* StV 2017, 470 (474).
[4] Kühling/Buchner/*Schwichtenberg* BDSG § 51 Rn. 1.
[5] So auch *Stief* StV 2017, 470 (476).

Grundprinzipien für eine wirksame Einwilligung zu berücksichtigen.[6] Danach sind folgende Grundprinzipien für die Einwilligung zu beachten: das Freiwilligkeitsprinzip (→ Rn. 24), der Zweckbindungsgrundsatz (→ Rn. 31) und der Grundsatz der freien Widerrufbarkeit (→ Rn. 32).[7]

3 Für die Geltung der vorstehenden Kriterien im Rahmen der BDSG-Normierung zeugt auch die **Begriffsdefinition** der Einwilligung **in § 46 Nr. 17.** Danach ist eine Einwilligung jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

4 § 51 selbst normiert hingegen nur folgende **(Wirksamkeits-)Voraussetzungen** im Kontext datenschutzrechtlicher Einwilligungen: die Beweislastregelung in § 51 Abs. 1 (→ Rn. 34), das Trennungs- und Transparenzgebot bei schriftlichen Einwilligungserklärungen (§ 51 Abs. 2, → Rn. 36), das Widerrufsrecht (§ 51 Abs. 3, → Rn. 40), eine Präzisierung des Freiwilligkeitsprinzips (§ 51 Abs. 4, → Rn. 43) und eine Präzisierung zur Einwilligung bei besonderen Kategorien personenbezogener Daten (§ 51 Abs. 5, → Rn. 45).

II. Systematik, Verhältnis zu anderen Vorschriften

5 **1. Allgemeines.** Die Einwilligung als Erlaubnis der Verarbeitung personenbezogener Daten ergibt sich bereits aus Art. 8 GRCh. Dieser schützt die **Herrschaft des Einzelnen über die eigenen Daten,** wozu auch die Entscheidung gehört, darüber bestimmen zu können, wer wie lange und zu welchem Zweck die eigenen personenbezogenen Daten verarbeiten darf.[8] Die dogmatische Einordnung der Einwilligung ist umstritten.[9] Unabhängig von der rechtlichen Einordnung wurde und wird die grundrechtlich gebotene Einwilligung in ihrer praktischen Umsetzung teilweise auch kritisch gesehen. Es ist nämlich davon auszugehen, dass der Betroffene vielfach keine bewusste, freie und informierte Entscheidung trifft, sondern die gegebenen Bedingungen blind akzeptiert, um einen (kurzfristigen) Vorteil in Anspruch zu nehmen, während die (Langzeit-)Risiken ausgeblendet werden. Gleichsam schwindet das Bewusstsein über den Wert und bestehende Risiken bei der unreflektierten Weitergabe personenbezogener Daten in der Bevölkerung.[10] Daher wird die Einwilligungsfähigkeit Betroffener in bestimmten Situationen infrage gestellt, da es für die Betroffenen oft kaum absehbar ist, welche zukünftige Wirkung ihre datenschutzrechtliche Einwilligung in bestimmten Situationen haben kann.[11]

6 **2. Europarechtlicher Kontext.** Die JI-RL regelt die datenschutzrechtliche Einwilligung nicht unmittelbar. Dies verwundert nicht, zumal sich bereits aus

[6] Gleiches gilt für die Regelung der Einwilligung in der DS-GVO, vgl. Ehmann/Selmayr/*Heckmann/Paschke* DS-GVO Art. 7 Rn. 1.

[7] Vgl. zu den Voraussetzungen → DS-GVO Art. 7 Rn. 21 ff.

[8] Ehmann/Selmayr/*Heckmann/Paschke* DS-GVO Art. 7 Rn. 16; Calliess/Ruffert/*Kingreen* EU-GRCh Art. 8 Rn. 9.

[9] BeckOK DatenschutzR/*Stemmer* DS-GVO Art. 7 Rn. 25 mwN; BeckOK Informations- und Medienrecht/*Gersdorf* EU-GRCh Art. 8 Rn. 20; Calliess/Ruffert/*Kingreen* EU-GRCh Art. 8 Rn. 13.

[10] Ehmann/Selmayr/*Heckmann/Paschke* DS-GVO Art. 7 Rn. 17.

[11] Ehmann/Selmayr/*Heckmann/Paschke* DS-GVO Art. 7 Rn. 17.

einem Rückgriff auf die GRCh ein datenschutzrechtliches Einwilligungskonzept ergibt (→ Rn. 2). Dieses geht bei verständiger Würdigung von den folgenden **Grundprinzipien** aus: das Freiwilligkeitsprinzip, der Zweckbindungsgrundsatz und der Grundsatz der freien Widerrufbarkeit, der die permanente Datenhoheit jedes Betroffenen sichert.[12] Das Freiwilligkeitsprinzip gliedert sich wiederum in die Unterprinzipien „Informiertheit" und „Freiheit von Zwang". Nur wenn die Einwilligung diese primärrechtlichen Vorgaben aus Art. 8 Abs. 2 GRCh beachtet, ist sie wirksam.

Wann eine Einwilligung als **freiwillig** angesehen wird, ist umstritten.[13] Im **7**
Rahmen der DS-GVO wird ua bei einem Machtungleichgewicht zwischen dem Einwilligenden und dem Einwilligungsempfänger nach der Maßgabe von Erwgr. 43 S. 1 die Freiwilligkeit und damit die Wirksamkeit der Einwilligung verneint, „insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde". Da im Anwendungsbereich der JI-RL lediglich öffentliche Stellen Daten verarbeiten, kann eine Einwilligung als untaugliches Legitimationsmittel angesehen werden.

In diesem Zusammenhang müssen auch die Erwägungsgründe der JI-RL **8**
Beachtung finden. In **Erwgr. 35 der JI-RL** heißt es, dass die zuständigen Behörden bei der Wahrnehmung von Zwecken der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit „natürliche Personen auffordern oder anweisen können, ihren Anordnungen nachzukommen. In einem solchen Fall sollte die Einwilligung der betroffenen Person im Sinne der Verordnung (EU) 2016/679 keine rechtliche Grundlage für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden darstellen. Wird die betroffene Person aufgefordert, einer rechtlichen Verpflichtung nachzukommen, so hat sie keine echte Wahlfreiheit, weshalb ihre Reaktion nicht als freiwillig abgegebene Willensbekundung betrachtet werden kann. Dies sollte die Mitgliedstaaten nicht daran hindern, durch Rechtsvorschriften vorzusehen, dass die betroffene Person der Verarbeitung ihrer personenbezogenen Daten für die Zwecke dieser Richtlinie zustimmen kann, beispielsweise im Falle von DNA-Tests in strafrechtlichen Ermittlungen oder zur Überwachung ihres Aufenthaltsorts mittels elektronischer Fußfessel zur Strafvollstreckung."[14] Letztgenannte Ausnahmefälle sind spezialgesetzlich normiert, vgl. ua § 81h StPO, § 56 BKAG, § 68b StGB.

Nichtsdestotrotz stehen die Regelungen der JI-RL nicht der grundsätzlichen **9**
Regelung der Einwilligung im Rahmen des BDSG entgegen.[15] Allerdings wird deren Anwendungsbereich dadurch stark eingeschränkt. Somit ist insbesondere im Zusammenhang mit **gesetzlichen Duldungs- und Mitwirkungspflichten** für Bürger die Einwilligung keine wirksame Grundlage für eine Datenverarbeitung.[16]

---

[12] Ehmann/Selmayr/*Heckmann/Paschke* DS-GVO Art. 7 Rn. 2.

[13] Ausf. hierzu *Radlanski,* Das Konzept der Einwilligung in der datenschutzrechtlichen Realität; *Sandfuchs,* Privatheit wider Willen?, S. 20 ff.; *Hermstrüwer,* Informationelle Selbstgefährdung.

[14] Erwgr. 35 der JI-RL. Daher gehen *Johannes/Weinhold* nicht davon aus, dass § 51 BDSG zur Umsetzung der JI-RL dient; HK-BDSG/*Johannes/Weinhold* § 51 Rn. 2.

[15] *Stief* StV 2017, 470 (473 f.); Kühling/Buchner/*Schwichtenberg* BDSG § 47 Rn. 7.

[16] Kühling/Buchner/*Schwichtenberg* BDSG § 47 Rn. 7.

10 Ferner sieht die JI-RL in Erwgr. 37 Einschränkungen im Umgang mit **besonderen Kategorien personenbezogener Daten** (zB Gesundheitsdaten) vor, da diese hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind und deshalb einen besonderen Schutz verdienen. „Die Verarbeitung solcher Daten [kann] ebenfalls durch Rechtsvorschriften erlaubt sein, wenn die betroffene Person der Datenverarbeitung, die besonders stark in ihre Privatsphäre eingreift, ausdrücklich zugestimmt hat. Die Einwilligung der betroffenen Person allein sollte jedoch noch keine rechtliche Grundlage für die Verarbeitung solch sensibler personenbezogener Daten durch die zuständigen Behörden liefern." Den Grundsatz, dass einer Einwilligung eine Rechtsvorschrift zugrunde liegen muss, damit diese als wirksam angesehen wird, hat der nationale Gesetzgeber für jede Form der Einwilligung im Anwendungsbereich von §§ 45 ff. übernommen, vgl. § 51 Abs. 1.

11 Die Parallelregelungen zur Einwilligung finden sich in Art. 4 Nr. 11, Art. 6 Abs. 1 lit. a, Art. 7 DS-GVO.[17] Ausweislich der Gesetzesbegründung beruht § 51 auf Elementen von Art. 7 DS-GVO und Elementen der Vorgängerregelung § 4a BDSG aF.[18] Die datenschutzrechtliche Legaldefinition in § 46 Nr. 17 entspricht der Begriffsbestimmung in § 4 Nr. 11 DS-GVO.

12 **3. Maßgebliche Vorschriften des BDSG aF.** Die Vorgaben der informierten Einwilligung des Betroffenen waren bereits in der Vergangenheit fester Bestandteil des Datenschutzrechts. Das bisher zur Anwendung gekommene nationale Datenschutzrecht beruhte auf der Richtlinie zum Datenschutz 95/46/EG vom 24.10.1995. In Deutschland war die Einwilligung in § 4a BDSG aF normiert. Diese bedurfte allerdings noch der Schriftform für ihre Wirksamkeit, sofern nicht eine andere Form angemessen war. § 51 tritt in Deutschland an die Stelle des bislang geltenden § 4a BDSG aF, der einerseits die in Art. 2 Abs. 1 iVm Art. 1 Abs. 1 GG normierte informationelle Selbstbestimmung konturierte und andererseits die europäischen Vorgaben aus Art. 7 lit. a DS-RL ausfüllte. Aufgrund der gesteigerten Verarbeitung personenbezogener Daten stieg auch das Risiko der Betroffenen. Den neuen Entwicklungen sollen die neuen europäischen Vorgaben Rechnung tragen.[19] Die oben genannten Grundprinzipien der Einwilligung galten bereits im Rahmen des früheren Regelungsregimes und finden trotz Reformierung des Datenschutzrechts weiterhin Anwendung.

III. Allgemeine Voraussetzungen der Einwilligung

13 Die Voraussetzungen der Einwilligung ergeben sich aus einer Gesamtschau der Regelungen von §§ 46 Nr. 17, 51 und den allgemeinen Prinzipien des Datenschutzrechts. Es ist zwischen formellen und materiellen Wirksamkeitsvoraussetzungen zu unterscheiden.[20] In den folgenden Ausführungen ist ein Rückgriff auf Erkenntnisse aus den Parallelnormen der DS-GVO zulässig, da der nationale Gesetzgeber in den Gesetzgebungsmaterialien ausdrücklich kennzeichnet, dass § 51 weitreichend von den Vorgaben der Art. 7 DS-GVO geprägt wurde.[21] Allerdings gilt § 51 nur, wenn in der Norm, die die Einwilligung als Rechtfertigungs-

[17] Vgl. ausf. Ehmann/Selmayr/*Heckmann/Paschke* DS-GVO Art. 7 Rn. 12 ff.
[18] BT-Drs. 18/11325, 112.
[19] Ehmann/Selmayr/*Heckmann/Paschke* DS-GVO Art. 7 Rn. 4.
[20] Ehmann/Selmayr/*Heckmann/Paschke* DS-GVO Art. 7 Rn. 31.
[21] BT-Drs. 18/11325, 112; vgl. zu den Voraussetzungen daher → DS-GVO Art. 7 Rn. 21 ff.