Typoskript im Sinne des § 38 Abs. 4 UrhG. Das Original ist abgedruckt in DVBl 2017, S. 749-758

„Once only“ versus „only once“: Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit

*von Prof. Dr. Mario Martini und wiss. Mit. Michael Wenzel, Speyer**

Formulare begleiten das Leben des Bürgers von der Wiege bis zur Bahre, heißt es im Volksmund. Dass die Verwaltung ihm Informationen abverlangt, die ihr bereits bekannt sind, nimmt der Citoyen ebenso mürrisch wie klaglos hin. Das sog. Once-only-Prinzip setzt dem einen regulatorischen Gegenentwurf entgegen: Die Verwaltung soll grundsätzlich alle ihr vorliegenden Daten nutzen, bevor sie diese dem Bürger erneut abringt. Die Implementierung des Prinzips hat sich gegenwärtig die Europäische Kommission auf die Fahnen geschrieben. So attraktiv der Grundgedanke auch ist: Er steht in einem Spannungsverhältnis zum datenschutzrechtlichen Zweckbindungsgrundsatz. Dieser ist von einem gegenläufigen Ansatz, dem Leitmotiv „only once“, getragen. Wie sich der Konflikt in dem Regime der DSGVO und des BDSG-neu sinnvoll auflösen lässt, analysieren die Autoren.

I. Once-only als Rationalitätsprinzip der Bürokratiekostenentlastung

„Einmal hin, alles drin“, mit diesem Slogan wirbt die Supermarktkette *real* für ihr Komplettpaket an Leistungen. Von einem „One-stop-government“ sind die Nutzer von Verwaltungsangeboten in Deutschland noch weit entfernt. Ihre Interaktion mit der Verwaltung ist eher von staatsbürgerlicher Demut geprägt: Behördliche Antragsmuster verlangen dem Bürger häufig Informationen ab, die der Verwaltung längst vorliegen. Effizient ist das nicht. Für den Behördenmitarbeiter ist es häufig gleichwohl einfacher, mehrfach Informationen anzufordern, als sich diese selbst „aus den Akten zu ziehen“ oder in Datenbanken danach zu recherchieren. Den Bürgern und der Wirtschaft entstehen dadurch vermeidbare Bürokratiekosten.

Dieser dysfunktionalen Anreizstruktur einer Kostenexternalisierung wirkt eine konsequente Umsetzung des Once-only-Prinzips entgegen. Es folgt einem einfachen Grundgedanken: Der Bürger speist seine Daten im Idealfall nur ein einziges Mal – typischerweise bei erstmaliger Nutzung eines digitalen Verwaltungsangebots – elektronisch ein. Die Verwaltung bündelt die – entweder zentral über eine allgemeine Eingabeseite [1] oder dezentral bei der jeweiligen

* *Mario Martini* ist Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer und Leiter des

Befassungsbehörde eingegebenen – Daten und eröffnet grundsätzlich allen staatlichen Stellen den Zugriff auf den Informationsbestand, soweit diese dazu autorisiert sind.[2]

Das Prinzip der einmaligen Erfassung ist ein elementarer Baustein einer modernen digitalen Verwaltung.[3] Seine Implementierung in die Architektur der staatlichen E-Government-Strategie erspart nicht nur Bürgern und Unternehmen lästige Doppeleingaben – und damit sowohl Zeit als auch Geld: Schätzungen zufolge ca. 5 Mrd. Euro jährlich im gesamten EU-Binnenmarkt.[4] Es fördert im Idealfall auch die Neigung zur Nutzung digitaler Angebote und trägt damit insgesamt zur Effizienzsteigerung der Verwaltung sowie zum Bürokratieabbau bei.[5]

II. Bestrebungen in der Europäischen Union

Einige Staaten der Europäischen Union richten ihre digitale Verwaltungstätigkeit bereits am Grundsatz einmaliger Erfassung aus. Insbesondere Österreich, Belgien, Tschechien, Dänemark,

---

Programmbereichs „Digitalisierung“ am Deutschen Forschungsinstitut für Öffentliche Verwaltung Speyer. *Michael Wenzel* ist Mitarbeiter am Lehrstuhl. Die Autoren danken insbesondere *Michael Kolain*, *Jan Mysegades* und *David Wagner* für ihre Unterstützung. Soweit nicht anders angegeben, wurden Internetquellen zuletzt am 20.3.2017 abgerufen. Der Aufsatz ist auch zur Veröffentlichung im Sammelband *Seckelmann*, Digitalisierte Verwaltung – Vernetztes E-Government, 2017, vorgesehen.

[1] Das Once-only-Prinzip kann seine Potenziale vor allem im Verbund mit einem allgemeinen Behörden(-service-)portal entfalten, welches dem Bürger die Möglichkeit eröffnet, die im Servicekonto gespeicherten personenbezogenen Daten auch in den Fachverfahren zu nutzen. Gegenwärtig existieren bereits mehrere derartige Portale (z. B. „Serviceportal Baden-Württemberg“, siehe https://www.service-bw.de/). Ihr Wirkradius beschränkt sich allerdings ihrem Wesen nach auf den Zuständigkeitsbereich der sie einrichtenden öffentlichen Stelle. Um dieser Parzellierung von Angeboten entgegenzuwirken, ist ein bundesweit einheitlicher Verwaltungszugang mit gemeinsamer Infrastruktur sinnvoll. Die Realisierung dieser Idee ist jüngst ein gutes Stück näher gerückt: Bund und Länder haben sich auf eine Änderung des Grundgesetzes verständigt, die dem Bund eine Kompetenz einräumt, den elektronischen Zugang zu allen Verwaltungsleistungen einheitlich zu regeln. Mittlerweile hat die Bundesregierung sowohl die Grundgesetzänderung (BT-Drucks. 18/11131) als auch das entsprechende Begleitgesetz (BT-Drucks. 18/11135) auf ihren parlamentarischen Weg gebracht.

[2] Fordert eine öffentliche Stelle die Daten bei der erhebenden Behörde bzw. bei dem allgemeinen Portal an, handelt es sich aus rechtsdogmatischer Sicht um eine Datenübermittlung i. S. d. § 3 Abs. 4 S. 2 Nr. 3 BDSG. Zugleich nimmt die abrufende Behörde eine (erneute) Datenerhebung (§ 3 Abs. 3 BDSG) vor, P. Gola/C. Klug/B. Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3, Rn. 24; vgl. auch BVerfG, Urt. v. 20.4.2016 – 1 BvR 966/09, 1 BvR 1140/09 – DVBl 2016, 770 = NJW 2016, 1781 (1803). Die Behörde, welche die Daten angefordert hat, speichert diese typischerweise ebenfalls (§ 3 Abs. 4 S. 2 Nr. 1 BDSG). Sinnvoll ist eine solche Potenzierung der Verarbeitung personenbezogener Daten indes nicht. Sie widerstrebt zum einen der mit dem Once-only-Prinzip verfolgten Zielsetzung der Entbürokratisierung der Verwaltung. Zum anderen erhöht die nochmalige Speicherung der Daten an anderer Stelle die Gefahr eines Missbrauchs oder eines unerlaubten Zugriffs auf den Datenbestand.

[3] Vgl. etwa Nationaler Normenkontrollrat, E-Government in Deutschland: Wie der Aufstieg gelingen kann – ein Arbeitsprogramm (Kurzfassung), 2016, S. 18.

[4] Europäische Kommission, Study on eGovernment and the Reduction of Administrative Burden, 2014, S. VI. Vgl. auch J. Fromm/C. Welzel/L. Nentwig, et al., Bürokratieabbau durch Digitalisierung: Kosten und Nutzen von E-Government für Bürger und Verwaltung, Version 1.0 vom 16.11.2015, S. 60. Hiervon sind auch die Betroffenen selbst überzeugt, wie Befragungen illustrieren: J. Cave/M. Botterman/S. Cavallini, et al., EU-wide digital Once-Only Principle for citizens and businesses, S. 132, 148 ff.

[5] Europäische Kommission (Fußn. 4), S. 4.

Estland, Finnland, die Niederlande, Portugal, Spanien sowie das Vereinigte Königreich verfolgen Once-only-Initiativen.[6] Österreich hat bspw. im Mai 2015 eine antragslose Familienbeihilfe eingeführt: Die Bewilligungsbehörde prüft die Anspruchsvoraussetzungen automatisiert und holt die erforderlichen Informationen (soweit verfügbar) via Datenaustausch mit anderen öffentlichen Stellen ein.[7] Ähnlich befüllt das Steuerformular in Estland seine Felder grundsätzlich mit allen vorhandenen Daten im Wege automatischen Datenabrufs.

Auch die Europäische Kommission unternimmt erste Anstrengungen, das Prinzip der einmaligen Erfassung auf unionaler Ebene normativ umzusetzen:[8] Sie hat es in ihren „EU-eGovernment-Aktionsplan 2016-2020“ aufgenommen.[9] Im Januar 2017 startete sie das „Once-Only“ Principle Project unter der Führung Estlands. Es lotet die Chancen für die Anwendung des Grundsatzes der einmaligen Erfassung auf Unternehmen aus.[10] Dessen Erfahrungswerte sollen die Grundlage für einen künftigen unionalen Gesetzgebungsakt legen.[11] Die Kommission hat auch eine zentrale europäische Anlaufstelle im Visier, welche das Once-only-Prinzip für Meldeverfahren im Seeverkehr fruchtbar machen soll.[12] Inwieweit sich das Prinzip der einmaligen Erfassung in der Interaktion zwischen Verwaltung und *Bürger* zu Leben erwecken lässt, will die Kommission bis zum Jahr 2019 prüfen.[13] Der großzügig bemessene Zeitrahmen ist ein Anzeichen dafür, dass die Kommission seine Anwendung auf den Bürger als persönlichkeitsrechtlich heikel einstuft. Jedenfalls wird sie nicht müde zu betonen, die durch das Datenschutzrecht gezogenen Grenzen stets achten zu wollen.[14]

III. Die gesetzliche Ausgangslage in der Bundesrepublik

Im deutschen Recht betritt das Once-only-Prinzip kein völliges Neuland*: § 38 BMeldeG* eröffnet schon heute der öffentlichen Verwaltung die Möglichkeit, personenbezogene Daten eines Bürgers

---

[6] Europäische Kommission (Fußn. 4), S. 4 mit Fußn. 17. Die Länder berichten von einer nennenswerten Entlastung der eigenen Verwaltung und nicht zu vernachlässigenden Kosteneinsparungen. Vgl. J. Cave/M. Botterman/S. Cavallini, et al. (Fußn. 4), S. 173.

[7] Siehe zu diesem Projekt: Österreichisches Bundesministerium für Familie und Jugend, Antragslose Familienbeihilfe ab Mai, https://www.bmfj.gv.at/ministerin/Aktuelles/Themen/Antragslose-FBH.html.

[8] Europäische Kommission, EU-eGovernment-Aktionsplan 2016-2020, COM(2016) 179 final, 19.4.2016, S. 7.

[9] Europäische Kommission (Fußn. 8), S. 3.

[10] Ausführlich über das Projekt informiert die Internetseite http://toop.eu/ Zu dem Rahmen des Projekts auch Krimmer/Kalvet/Toots et al., Das Projekt TOOP: Bürokratieabbau und Verwaltungsvereinfachung mittels des "Once-Only" Prinzips für Unternehmen, in: Schweighofer/Kummer/Hötzendorfer et al. (Hrsg.), Trends and Communities der Rechtsinformatik, 2017, S. 265 f.

[11] Eine Studie, welche die Kommission in Auftrag gegeben hat, empfiehlt insbesondere den Erlass einer Richtlinie, die den Datenaustausch zu Once-only-Zwecken regelt, J. Cave/M. Botterman/S. Cavallini, et al. (Fußn. 4), S. 46.

[12] Europäische Kommission (Fußn. 8), S. 9.

[13] Europäische Kommission (Fußn. 8), S. 12.

[14] Europäische Kommission (Fußn. 8), S. 12.

in beschränktem Maße, aber weitgehend voraussetzungslos[15] automatisiert bei der Meldebehörde abzurufen.[16] Darüber hinaus ebnet *§ 5 Abs. 2 S. 1 EGovG* der zuständigen Behörde den Weg, „erforderliche Nachweise" auf der Grundlage einer Einwilligung des Betroffenen[17] direkt bei einer anderen öffentlichen Stelle elektronisch einzuholen.[18] Das Gesetz dispensiert damit von dem dem nationalen Recht vertrauten [19] Direkterhebungsgrundsatz, also der Vorgabe, dass Daten grundsätzlich bei dem Betroffenen zu erheben sind (§ 4 Abs. 2 S. 1 BDSG [20]). [21] Einen bemerkenswerten Schritt in Richtung einer Verzahnung von Verwaltungsleistungen unternimmt auch die (jüngst durch das Asylverfahrensbeschleunigungsgesetz eingefügte) Regelung des *§ 8 Abs. 3 S. 3 AsylG*: Asylbehörden dürfen die auf der Grundlage des Asylgesetzes erhobenen Daten an die Bundesagentur für Arbeit übermitteln; diese darf die Daten zur Erfüllung von Aufgaben nach dem SGB III verwenden.

Mit der Speicherung personenbezogener Daten und einer (abstrakten) Zugriffsmöglichkeit für unterschiedliche Behörden geht ein Missbrauchsrisiko einher: Es besteht die Gefahr, dass der Staat die verfügbaren Daten zu einem umfassenden *Persönlichkeitsprofil* verquickt. Das Once-only-Prinzip setzt die Rechtsordnung daher einer persönlichkeitsrechtlichen Zerreißprobe aus. Es tritt –

---

[15] § 38 Abs. 2 S. 1 BMeldeG: „soweit diese Daten der abrufenden Stelle zur Erfüllung ihrer Aufgaben bekannt sein müssen".

[16] Vgl. dazu auch E. Ehmann, jurisPR-ITR 20/2014, Anm. 2.

[17] Diese kann auch elektronisch erklärt werden (§ 5 Abs. 3 S. 1 EGovG), ist aber zu protokollieren (§ 5 Abs. 3 S. 3 EGovG) und unterliegt den Garantien der Eindeutigkeit sowie Bewusstheit, der Abrufbarkeit und der jederzeitigen Widerruflichkeit (§ 5 Abs. 3 S. 2 EGovG). Eine Einwilligung ist nur entbehrlich, wenn eine besondere Verarbeitungsgrundlage die Datenübermittlung spezialgesetzlich gestattet.

[18] Das Informationsweiterverwendungsgesetz entbindet die Verwaltung dabei nicht von der Beachtung des Zweckbindungsgrundsatzes. Ausweislich des § 1 Abs. 3 IWG gelten weiterhin die entsprechenden Vorgaben des Datenschutzrechts.

[19] Die Datenschutzrichtlinie 95/46/EG hatte den deutschen Gesetzgeber nicht auf einen derartigen Grundsatz verpflichtet. Sie legte dem Verantwortlichen (wie nun auch die DSGVO) lediglich Informationspflichten auf, die sich danach unterschieden, ob die Datenerhebung beim Betroffenen selbst erfolgt (Art. 10, ErwGrd 39 und 40 DSRL) oder die Daten auf anderem Wege gewonnen werden (Art. 11 DSRL). Der deutsche Gesetzgeber konnte also bisher Datenverarbeitungen von der Geltung des Direkterhebungsgrundsatzes freistellen, solange er den durch die Datenschutzrichtlinie statuierten Informationspflichten anderweitig nachkam.

[20] Vgl. auch die entsprechenden Regelungen in den Ländern: § 13 Abs. 2-4 LDSG BW, Art. 16 Abs. 2 S. 1 BayDSG, § 10 Abs. 1, 3 BlnDSG, § 12 Abs. 2, 3 i. V. m. § 13 Abs. 2 S. 1 lit. a, c-f BbgDSG, § 10 Abs. 2 BremDSG, § 12 Abs. 2 i. V. m. § 13 Abs. 2 S. 1 HmbDSG, § 12 Abs. 1, 2 hessDSG, § 9 Abs. 2, 4 DSG M-V, § 9 Abs. 1 Satz 2 ndsDSG, § 12 Abs. 1 S. 2 i. V. m. § 13 Abs. 2 S. 1 lit. a, c-g, i DSG NRW, § 12 Abs. 2 LDSG R-P, § 12 Abs. 1 S. 2, Abs. 3 i. V. m. § 13 Abs. 1 lit. b-g saarlDSG, § 12 Abs. 2, 4 sächsDSG, § 9 Abs. 2 DSG LSA, § 13 Abs. 1 Sätze 1 und 2 i. V. m. Abs. 3 Nr. 1, 2, 4 LDSG S-H, § 19 Abs. 2 thürDSG.

[21] J. Keller-Harder/M. Schallbruch, in: Bauer/Heckmann/Ruge, et al., VwVfG, 2. Aufl. 2014, § 5 EGovG, Rn. 14. Mit dem Direkterhebungsgrundsatz konfligiert das Once-only-Prinzip zugleich nicht vollständig. Denn die erstmalige *Erhebung* der personenbezogenen Daten (§ 3 Abs. 3 BDSG) findet (unabhängig von der konkreten gesetzlichen Ausgestaltung des Once-only-Prinzips) beim Betroffenen selbst statt, sodass insoweit die Vorgabe des § 4 Abs. 2 BDSG eingehalten ist. Der anschließende behördliche Abruf der Daten ist aus der Perspektive der abgebenden Stelle eine Datenverarbeitung in Gestalt einer Daten*übermittlung* (vgl. § 3 Abs. 4 S. 2 Nr. 3 BDSG; vgl. auch Fußn. 2). Von der Warte der abrufenden Stelle aus handelt es sich jedoch um eine Daten*erhebung*, die somit die Rechtsfolge des § 4 Abs. 2 BDSG auslöst.

außer mit dem (nationalen) Direkterhebungsgrundsatz – mit dem Grundsatz der Zweckbindung in eine Spannungslage: Personenbezogene Daten dürfen die Behörden grundsätzlich nicht zu anderen Zwecken als jenen weiterverwenden, zu denen sie (erst-)erhoben worden sind (§ 14 Abs. 1 BDSG).[22] Statt „once only" gilt im Datenschutzrecht also im Grundsatz „only once".

Der Zweckbindungsgrundsatz ist ein „Kernelement des verfassungsrechtlichen Datenschutzes".[23] Ihn darf der Gesetzgeber auch bei der Implementierung des Once-only-Prinzips nicht aushöhlen. Ein umfangreiches Datenportfolio über den einzelnen Bürger anzulegen, auf das jede staatliche Stelle ungehindert zu eigenen Zwecken zugreifen kann, ist mit der verfassungsrechtlichen Wertentscheidung des Allgemeinen Persönlichkeitsrechts daher nicht vereinbar: Eine „umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger"[24] überschreitet – gerade mit Blick auf die Wesensgehaltsgarantie des Art. 19 Abs. 2 GG – die Grenzen des verfassungsrechtlich Zulässigen.[25]

Nicht jede Weiternutzung einmal erhobener Daten widerspricht aber dem Zweckbindungsprinzip: Deckt der ursprüngliche Erhebungszweck auch die Folgenutzung der Daten ab, löst die weitere Nutzung (jedenfalls nach Einschätzung des BVerfG) keinen neuen Grundrechtseingriff aus; einer neuen gesetzlichen Rechtfertigung bedarf es dann nicht.[26] Eine solche *zweckkonforme* Weiternutzung unterliegt jedoch engen Bindungen: Behörde, Aufgabe und Rechtsgüterschutz

---

[22] Diese Zweckfestlegung setzt das BDSG in seinem § 14 Abs. 1 voraus, P. Gola/C. Klug/B. Körffer, in: Gola/Schomerus, BDSG, 12. Aufl. 2015, § 14, Rn. 9. § 14 Abs. 2 BDSG zählt abschließend neun Fälle auf, in denen zweckänderndes Speichern, Verändern oder Nutzen der personenbezogenen Daten ausnahmsweise zulässig ist. In den Landesdatenschutzgesetzen ergibt sich der Zweckbindungsgrundsatz insbesondere aus § 15 Abs. 1 Nr. 2 LDSG BW, Art. 17 Abs. 1 Nr. 2 BayDSG, § 11 Abs. 1 BlnDSG, § 13 Abs. 1 S. 2, 3 BbgDSG, § 12 Abs. 1 S. 2 BremDSG, § 13 Abs. 1 HmbDSG, § 13 Abs. 1 hessDSG, §§ 10 Abs. 2, 11 Abs. 2 DSG M-V, § 10 Abs. 1 ndsDSG, § 13 Abs. 1 S. 2, 3 DSG NRW, § 13 Abs. 1 Nr. 2 LDSG R-P, § 13 Abs. 1 S. 2, 3 saarlDSG, § 13 Abs. 1 Nr. 2 sächsDSG, § 10 Abs. 1 DSG LSA, § 13 Abs. 2 LDSG S-H, § 20 Abs. 1 thürDSG.

[23] BVerfG (Fußn. 2), NJW 2016, 1781 (1802). Bereits im Volkszählungsurteil sah das BVerfG einen „Schutz gegen Zweckentfremdung durch Weitergabe- und Verwertungsverbote" als zentrales verfassungsrechtliches Prinzip in Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG eingeschrieben; BVerfG, Urt. v. 15. 12. 1983 – 1 BvR 209/83 – BVerfGE 65, 1 (46) = DVBl 1984, 128 (130).

[24] Zu dieser Gefahr bereits BVerfG, Urt. v. 15. 12. 1983 – 1 BvR 209/83 – BVerfGE 65, 1 (53) = DVBl 1984, 128 (132). Erst jüngst BVerfG (Fußn. 2), DVBl 2016, 770 (774).

[25] Ein solches Vorgehen wäre auch mit dem Grundgedanken des „Once-only-Prinzips" nicht vereinbar, dem *Bürger* einen Servicevorteil zukommen zu lassen. Der Befriedigung staatlichen Datenhungers und einem insbesondere polizei- und nachrichtendienstlichen Interesse an umfangreichen Informationen über die Bürger zwecks Gefahren- bzw. Terrorabwehr verleiht das Prinzip keine eigene Legitimation. Dazu auch IV. 1. b. cc.

[26] BVerfG (Fußn. 2), NJW 2016, 1781 (1800). Siehe dazu auch D. Müllmann, NVwZ 2016, 1692 ff., der darin eine Absenkung des Datenschutzniveaus sieht, a. a. O., 1693.

müssen bei der Weiternutzung identisch mit denjenigen der vorausgegangenen Datenerhebung sein.[27] Denn die Eingriffsgrundlage steckt auch die Grenzen der erlaubten Verwendung ab.

Sind Erhebungs- und Folgezweck demgegenüber *unvereinbar*, ist die Zweckänderung verfassungsrechtlich nur zulässig, wenn auch eine hypothetische Datenneuerhebung zulässig wäre[28], eine gesetzliche Verarbeitungsgrundlage diese also ebenso abdeckt.[29] Diese Norm muss strengen Verhältnismäßigkeitsanforderungen genügen[30] und darf nicht unspezifisch weit bemessen sein, sondern ist vielmehr „so konkret wie möglich“[31] zu fassen.[32] Für den Datenaustausch zwischen Polizei und Geheimdienst(en) gilt dabei – entsprechend dem getrennten Funktionsauftrag beider Einrichtungen – ergänzend ein „informationelles Trennungsprinzip“. Es verbietet grundsätzlich[33] einen Informationsaustausch zwischen ihnen.[34]

IV. Vorgaben der neuen Datenschutz-Grundverordnung und des BDSG-neu

Ab dem 25. Mai 2018 setzt die Datenschutz-Grundverordnung (DSGVO)[35] der Ausgestaltung des Once-only-Prinzips neue Rahmenbedingungen.

1. Ausgangslage nach der DSGVO

a) Direkterhebungsgrundsatz

Im Unterschied zum bisherigen deutschen Datenschutzrecht kennt die DSGVO keinen Direkterhebungsgrundsatz.[36] Sie enthält auch keine Öffnungsklausel, die es dem nationalen

---

[27] BVerfG (Fußn. 2), NJW 2016, 1781 (1800 f.).
[28] BVerfG (Fußn. 2), NJW 2016, 1781 (1801).
[29] BVerfG (Fußn. 2), NJW 2016, 1781 (1801) m. w. N. Mit diesem Urteil gleicht das BVerfG seine Rechtsprechung dem künftig geltenden Regelungsregime des Art. 6 Abs. 4 DSGVO zum Zweckbindungsgrundsatz an. So auch D. Müllmann (Fußn. 26), 1695.
[30] BVerfG (Fußn. 2), NJW 2016, 1781 (1801).
[31] P. Gola/C. Klug/B. Körffer (Fußn. 22), Rn. 9.
[32] Das BVerfG verlangt: „Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind.“ BVerfG (Fußn. 24), DVBl 1984, 128 (130). Ähnlich auch M. Albers, in: Wolff/Brink, BeckOK DatenschutzR, 19. Ed. 2017, § 14 BDSG, Rn. 17.
[33] Zulässig ist ein Informationsaustausch zwischen ihnen nur, wenn er „einem herausragenden öffentlichen Interesse dien[t], das den Zugriff auf Informationen unter den erleichterten Bedingungen, wie sie den Nachrichtendiensten zu Gebot stehen, rechtfertigt“. So für das Verhältnis zwischen Polizei und Geheimdiensten: BVerfG, Urt. v. 24. 4. 2013 – 1 BvR 1215/07 – BVerfGE 133, 277 (329) = DVBl 2013, 783 (785 f.).
[34] BVerfG (Fußn. 33), DVBl 2013, 783 (785).
[35] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. Nr. L 119 S. 1, ber. Nr. L 314 S. 72.
[36] So auch B. Buchner, DuD 2016, 155 (156).

Gesetzgeber gestattet, eine dem Vorbild des § 4 Abs. 2 BDSG entsprechende Regelung wie einen Springteufel erneut aus der Kiste der Gesetzgebung springen zu lassen.[37] Statt der Anordnung einer Direkterhebung bedient sich die DSGVO eines anderen Regelungsinstruments, um dem Betroffenen die Datenerhebung zur Kenntnis [38] zu bringen: Sie erlegt dem Verantwortlichen, der personenbezogene Daten nicht bei der betroffenen Person erhebt, die Pflicht auf, sie über die Datenerhebung (auch im Falle der Zweckänderung) zu informieren (Art. 14 Abs. 2 DSGVO).[39]

b) Zweckbindungsgrundsatz

An der Leitidee des Zweckbindungsgrundsatzes hält die DSGVO in konsequenter Fortführung des Art. 6 Abs. 1 lit. b der Datenschutzrichtlinie 95/46/EG fest. Art. 5 Abs. 1 lit. b DSGVO proklamiert ihn an prominenter Stelle als allgemeinen Grundsatz des unionalen Datenschutzrechts.

Er gilt aber weder vorbehaltlos noch ausnahmslos: Zum einen befreit der Unionsgesetzgeber im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder historische Forschungszwecke sowie statistische Weiterverarbeitungszwecke im Wege einer gesetzlichen Fiktion von der Zweckbindung. Für Once-only-Zwecke der Verwaltung sind diese Tatbestände im Regelfall freilich nicht einschlägig.[40]

Zum anderen lässt Art. 6 Abs. 4 DSGVO auch zweckändernde Verarbeitungen (aa) zu. Zulässig sind diese – ähnlich wie bereits nach bisherigem deutschem Recht –, wenn der Betroffene eingewilligt hat (bb) oder das Unions- bzw. mitgliedstaatliches Recht eine gesetzliche Erlaubnis ausspricht (cc).

aa) Kompatibilitätstest

Nicht jede Weiterverarbeitung eines bereits erhobenen Datums bedarf einer gesonderten Verarbeitungsgrundlage. Eine solche ist (ebenso wie im nationalen Recht)[41] nur dann erforderlich, wenn die neue Verarbeitung mit dem ursprünglichen Erhebungszweck *inkompatibel* ist (vgl. ErwGrd 50 S. 2 und S. 5). [42] Ob das der Fall ist, hat der Verantwortliche mit Hilfe eines

---

[37] J. Kühling/M. Martini/J. Heberlein, et al., Die DSGVO und das nationale Recht, 2016, S. 316.
[38] Hierin bestand auch die primäre Funktion des Direkterhebungsgrundsatzes, vgl. P. Scholz/B. Sokol, in: Simitis, BDSG, 8. Aufl. 2014, § 4, Rn. 4 m. w. N.
[39] Aus dieser Verpflichtung ergibt sich auch, dass die DSGVO die Direkterhebung nicht als zwingend ansieht.
[40] Für Archivzwecke ergibt sich das ausweislich der – in ErwGrd 158 S. 3 DSGVO zum Ausdruck kommenden – Vorstellung des Verordnungsgebers daraus, dass dieser Ausnahmetatbestand ausschließlich öffentlichen Interessen historischer Erinnerungskultur verschrieben ist.
[41] Dazu III. mit Fußn. 26.
[42] So auch bereits J. Kühling/M. Martini, EuZW 2016, 448 (451); M. Monreal, ZD 2016, 507 (510); a. A. P. Schantz, NJW 2016, 1841 (1844).

Kompatibilitätstests zu ermitteln (Art. 6 Abs. 4 DSGVO).[43] Nach dem Willen des Verordnungsgebers ist dabei nicht allein isoliert der Erhebungs- mit dem Weiterverarbeitungszweck abzugleichen. Vielmehr hat der Sache nach eine umfassende Interessenabwägung stattzufinden.[44] Die Prüfung erfolgt anhand fünf (enumerativ) in der Norm aufgezählter Kriterien.[45] Auch äußere Umstände des jeweiligen Verarbeitungsvorgangs – wie das Verhältnis zwischen den betroffenen Personen und dem Verantwortlichen (Buchst. b) – sind dabei von Relevanz.[46] Vor allem auf „die vernünftigen Erwartungen der betroffenen Person" (EG 50 S. 6 DSGVO) richtet die DSGVO den Fluchtpunkt der Zweckkompatibilitätsprüfung aus.[47]

Auf die Beurteilung, welche Zwecke als kompatibel anzusehen sind, hat nicht allein die Union, sondern auch der nationale Gesetzgeber Einfluss: Soweit die DSGVO ihm – wie für Verarbeitungen der öffentlichen Verwaltung[48] – die Möglichkeit eröffnet, die Voraussetzungen für die Zulässigkeit der Datenverarbeitung auf der Grundlage der Öffnungsklausel zu präzisieren (Art. 6 Abs. 1 UAbs. 1 S. 1 lit. c und e DSGVO i. V. m. Abs. 2 und 3 DSGVO; vgl. auch ErwGrd 50 S. 3 DSGVO), kann er zumindest partiell selbst festlegen, welche Verarbeitungszwecke kompatibel sind: Er darf „spezifischere Bestimmungen zur Anpassung der Anwendung dieser Vorschriften" erlassen, insbesondere regeln „für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen" sowie „welcher Zweckbindung sie unterliegen" (Art. 6 Abs. 3 UAbs. 2 S. 3 DSGVO). Auf diesem Weg kann er normativ absichern, dass die Weiterverarbeitung nicht zweckinkompatibel ist.

Die Mitgliedstaaten dürfen dadurch den Zweckbindungsgrundsatz jedoch nicht ad absurdum führen. Die Kompatibilitätskriterien des Art. 6 Abs. 4 DSGVO bilden deshalb die äußerste Grenze für die gesetzgeberische Beurteilung, welche weiteren Verarbeitungszwecke noch im Rahmen des Zulässigen liegen.[49] Im Grundsatz hat der Gesetzgeber also zunächst seinerseits eine abstrakte Kompatibilitätsprüfung nach Abs. 4 durchzuführen, bevor er die Öffnungsklauseln der Art. 6 Abs. 2 und 3 DSGVO ausschöpft.

---

[43] Ausführlich hierzu M. Monreal (Fußn. 42), 510 f. Die Zweckkompatibilitätsprüfung des Verantwortlichen anhand des Art. 6 Abs. 4 DSGVO ist gerichtlich voll überprüfbar, so auch U. Dammann, ZD 2016, 307 (312).

[44] So auch K.-U. Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 6 DSGVO, Rn. 38.

[45] Ergänzend kann der Verantwortliche aber auch andere Kriterien heranziehen („unter anderem").

[46] E. M. Frenzel, in: Paal/Pauly, DS-GVO, 2016, Art. 6, Rn. 51, will Hoheitsträger von der Kompatibilitätsprüfung vollständig ausnehmen. Der Normtext liefert dafür jedoch zum einen keine Anhaltspunkte. Zum anderen bestehen auch keine durchgreifenden inhaltlichen Argumente dagegen, dass eine öffentliche Stelle eine Weiterverarbeitung, welche der Kompatibilitätstest als zweckkompatibel ausweist, auf die ursprüngliche Verarbeitungsgrundlage stützt. Im Gegenteil: Ein solches Vorgehen entspricht unionsrechtlicher Tradition, vgl. auch M. Monreal (Fußn. 42), 510. Zum nationalen Verfassungsrecht auch die aktuelle Judikatur des BVerfG (Fußn. 23).

[47] T. Wybitul, BB 2016, 1077 (1081).

[48] Art. 6 Abs. 1 UAbs. 1 S. 1 lit. e DSGVO. Die Union zollt damit der Eigenstaatlichkeit der Mitgliedstaaten Respekt. Gerade für diese wirkt die DSGVO de facto wie eine Richtlinie, vgl. hierzu J. Kühling/M. Martini (Fußn. 42), 449.

[49] Vgl. die Beschreibung bei J. Kühling/M. Martini/J. Heberlein, et al. (Fußn. 37), S. 44.

bb) Einwilligung

Ist der Zweck der Weiterverarbeitung nicht mit dem ursprünglichen Erhebungszweck in Einklang zu bringen, ist die Einwilligung des Betroffenen der Königsweg, zweckverändernde bzw. zweckkompatible Verarbeitungen durch andere Behörden zu gestatten (Art. 6 Abs. 1 UAbs. 1 lit. a DSGVO). Allerdings knüpft die DSGVO die Zustimmung zu einer behördlichen Datenverarbeitung an hohe Anforderungen:[50] Sie muss freiwillig, für den bestimmten Fall, in informierter Weise und unmissverständlich in Gestalt einer eindeutigen bestätigenden Handlung erfolgen, die das Einverständnis der betroffenen Person mit der Verarbeitung zu verstehen gibt (Art. 4 Nr. 11 DSGVO).

(1) Freiwilligkeit von Einwilligungserklärungen gegenüber Behörden

Das Verhältnis zwischen Behörde und Bürger ist nach der Vorstellung des unionalen Gesetzgebers von einem strukturellen Ungleichgewicht geprägt. Vor diesem Hintergrund stellt ErwGrd 43 S. 1 DSGVO die Regelvermutung auf, dass der Bürger einer *behördlichen* Datenverarbeitung im Grundsatz nicht freiwillig zustimmt. Die DSGVO begegnet damit der Gefahr, dass die strukturelle Machtasymmetrie den Bürger oftmals nur mit Blick auf die Verengung der Handlungsalternativen auf zwei Übel unterschiedlichen Ausmaßes „in vorauseilendem Gehorsam“ zur Zustimmung veranlasst.[51]

Eine solche *coactus-volui*-Struktur[52] überschattet die Einwilligung des Bürgers in die Erfassung und anschließende Weiternutzung seiner Daten im Rahmen des Once-only-Prinzips jedoch typischerweise nicht. Eine E-Government-Strategie, die dem Bürger wiederholende Formulareinträge erspart, bietet ihm primär eine Entlastungsmaßnahme, die als zusätzlicher Servicekanal neben die analoge Bürger-Staat-Kommunikation tritt. Jedenfalls solange die Verwaltung dem Bürger die bisherigen analogen Kommunikationskanäle nicht versperrt, übt sie auch keinen, die Freiwilligkeit ausschließenden Druck auf den Bürger aus, das Angebot tatsächlich in Anspruch zu nehmen. Ein strukturelles Ungleichgewicht zwischen Bürger und Verwaltung äußert sich in der Erteilung einer Einwilligung zur Nutzung eigener Daten im Rahmen von „once only“ daher grundsätzlich nicht.

---

[50] So in der Bewertung auch M. Becker, JZ 2017, 170 (173), der in ErwGrd 32 DSGVO aber eine gewisse Aushöhlung der Vorgaben des Art. 4 Nr. 11 DSGVO sieht.
[51] Ausführlicher M. Peifer, PinG 2016, 222 (226).
[52] Dazu bspw. m. w. N. M. Martini, Der Markt als Instrument hoheitlicher Verteilungslenkung, 2008, S. 459 sowie N. Bethge, Die verfassungsrechtliche Zulässigkeit des Grundrechtsverzichts, 2014, S. 165 ff.

Anders kann sich die Situation dann darstellen, wenn die Verwaltung dem Bürger die Zustimmung unter dem Vorhalt abringt, dass sie sich anderenfalls die Daten selbst unmittelbar beschaffen werde. Ein solches Vorgehen liefe dem Grundgedanken des Freiwilligkeitsgebots sowie des Koppelungsverbots zuwider, welche die Verordnung in Art. 7 Abs. 4 DSGVO anlegt:[53] Eine Einwilligung unter Druck zu erwirken oder an inkonnexe Bedingungen zu knüpfen, schließt die Freiwilligkeit grundsätzlich aus.

Der bloße Hinweis auf eine – tatsächlich bestehende – gesetzliche Verarbeitungsmöglichkeit löst allerdings noch keinen unzulässigen Druck aus, der die Freiwilligkeit ausschließt. Ein strukturelles Ungleichgewicht schlägt erst (aber immerhin) dann auf die Freiwilligkeit der Einwilligung durch, wenn die Verwaltung dem Bürger fälschlich eine gesetzliche Verarbeitungserlaubnis vorspiegelt oder ihn im Unklaren darüber lässt, inwieweit eine gesetzliche Verarbeitungserlaubnis besteht. Weist die Behörde auf mögliche gesetzliche Verarbeitungserlaubnisse hin, die ihr im Falle fehlender Einwilligung zur Verfügung stünden, muss sie diese daher auch hinreichend konkret benennen, soll der Hinweis die Einwilligung nicht unwirksam machen.

(2) Entbündelungsgebot

Wer Daten auf der Grundlage einer Einwilligung verarbeiten will, muss „entbündelte" Einwilligungen zulassen. Das gilt in besonderer Weise für die Verwaltung als Hoheitsträger: Zu verschiedenen Verarbeitungsvorgängen muss sie dem Bürger auch verschiedene Erklärungen gestatten, statt ihm eine pauschale Einwilligung abzuringen (vgl. auch ErwGrd 43 S. 2 DSGVO). Das hindert den Bürger zwar nicht daran, auch eine generalisierte Einwilligung zu erteilen, wenn er diese Wahl unter mehreren verfügbaren Optionen autonom trifft, die Verwaltung seine verfügbaren Handlungsalternativen also nicht verengt.

Die Einwilligungserklärung darf dann aber keine Zweifel offen lassen: Sie muss eindeutig sein. Der Betroffene muss unmissverständlich erkennen können, welchen Verarbeitungsvorgängen er mit der Einwilligung zustimmt (vgl. Art. 4 Nr. 11, Art. 7 Abs. 2 S. 1 DSGVO). Bezugspunkt ist der konkrete behördliche Datenverarbeitungszweck (vgl. ErwGrd 32 S. 4 DSGVO). Dient die Verarbeitung mehreren Zwecken, muss die Einwilligung sich mithin zweifelsfrei auf jeden

[53] Es bezieht sich unmittelbar primär auf die Erfüllung von Verträgen. Seine normative Intention ist aber auf vergleichbare Konstellationen übertragbar („unter anderem"). Vgl. auch M. Becker (Fußn. 50), 174; U. Dammann (Fußn. 43), 311: „verkapptes Kopplungsverbot"; C. Krönke, Der Staat 2016, 319 (327); eher zurückhaltend aber E. M. Frenzel, in: Paal/Pauly, DS-GVO, 2016, Art. 7, Rn. 18; ablehnend (zumindest hinsichtlich eines strikten Kopplungsverbots) K.-U. Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 7 DSGVO, Rn. 14 ff.

einzelnen Zweck erstrecken (ErwGrd 32 S. 5 DSGVO: „für alle diese Verarbeitungszwecke“, „for all of them“, „pour l'ensemble d'entre elles“). Die Auswirkungen und Reichweite seiner Zustimmung wird der Bürger bei pauschalen Zustimmungserklärungen ex ante oftmals noch nicht erkennen und überblicken können. Eine pauschale Einwilligung des Bürgers in die spätere Nutzung personenbezogener Daten durch andere Behörden ist daher (wenngleich mit der DSGVO in Einklang zu bringen) höchsten Anforderungen an die Erkennbarkeit unterworfen. Grundrechtsschonender und im Lichte des unionsrechtlichen Kopplungsverbots angezeigt (Art. 7 Abs. 4, ErwGrd 43 S. 2 DSGVO) ist ein differenzierendes Modell, das den Bürger zu einer Aktualisierung der Einwilligung auffordert: Er muss grundsätzlich bei jeder Nutzung eines digitalen Verwaltungsangebots die Fortgeltung seiner Einwilligung bestätigen; nur dann dürfen die zu diesem Zweck bereits gespeicherten Daten Verwendung finden. Der Betroffene kann auf die erneute Bestätigung aber auch ausdrücklich auf eigenen Wunsch und unter klarem Hinweis auf die damit verbundenen Folgen verzichten.

(3) Opt-in-Gebot

Zusätzlich zu den allgemeinen Anforderungen schreibt ErwGrd 32 DSGVO der digital agierenden Verwaltung deutlich ins Stammbuch, wie sie eine rechtskonforme Online-Einwilligungserklärung zu gestalten hat:[54] Zulässig ist allein eine Opt-in-Lösung. Vorausgefüllte Kästchen, die der Betroffene bei mangelndem Einverständnis wieder abwählen kann (Opt-out), genügen den Anforderungen der Verordnung hingegen nicht.[55] Die digitale Verwaltung darf den Bürger zudem zur Abgabe einer Einwilligung auf elektronischem Weg nur „in klarer und knapper Form“ auffordern (EG 32 S. 6 DSGVO).

(4) Widerruflichkeit

Die Einwilligung kann der Betroffene jederzeit mit Ex-nunc-Wirkung widerrufen (Art. 7 Abs. 3 S. 1 und 2 DSGVO). Darüber muss die Verwaltung den Bürger vor seiner Zustimmung zur Nutzung von Once-only-Leistungen informieren (Art. 7 Abs. 3 S. 3 DSGVO). Die Ausübung des Widerrufsrechts darf die Verwaltung auch nicht unsachgemäß (z. B. durch die Pflicht zur Angabe von Gründen) erschweren, sondern muss sie „so einfach wie die Erteilung der Einwilligung“ ermöglichen (Art. 7 Abs. 3 S. 4 DSGVO).

---

[54] ErwGrd 32 S. 1-3 DSGVO.
[55] Dazu auch m. w. N. J. Kühling/M. Martini (Fußn. 42), 451.

cc) Gesetzliche Verarbeitungserlaubnis

Dem Informationshunger des Staates begegnen zahlreiche Bürger mit deutlich größerer Zurückhaltung als Big-Data-Kollektoren des Cyberspace, deren Geschäftsmodell auf dem offensiven Einsammeln aller abgreifbaren Daten fußt. Allein unter Rückgriff auf das Instrument der Einwilligung wird der Verwaltung eine flächendeckende Umsetzung des Once-only-Prinzips daher im Zweifel nicht gelingen.

Ein Datenzugriff ohne vorherige Zustimmung des Betroffenen entfernt sich allerdings zusehends von der ursprünglichen, den *Bürger* entlastenden Kernidee des Once-only-Prinzips. Es genießt zugleich als solches keinen eigenen verfassungsrechtlichen Schutz. Seine bürgerorientierte Philosophie alleine vermag den Gesetzgeber nicht daran zu hindern, es zu einem Instrument zustimmungsfreien Datenaustauschs auszubauen. Auf kurze oder lange Sicht wird das Prinzip der einmaligen Erfassung die Grundsatzfrage aufwerfen, in welchem Maße das Unionsrecht es dem nationalen Gesetzgeber erlaubt, eine zweckfremde Verarbeitung durch eigene Vorschriften zu gestatten.[56]

Die DSGVO öffnet den Mitgliedstaaten durchaus das Tor, im Rahmen ihrer Gestaltungsbefugnis Zweckänderungen zuzulassen (Art. 6 Abs. 4 DSGVO).[57] Sie knüpft diese jedoch implizit an die Voraussetzung, dass der Mitgliedstaat auch die Erstverarbeitung regeln dürfte. Die Befugnis zur Zweckänderung beschränkt sich also auf diejenigen Sachbereiche, in denen die Union den Mitgliedstaaten die Befugnis zur Erstverarbeitung zugesteht (mithin auf die Fälle des Art. 6 Abs. 1 UAbs. 1 lit. c bzw. lit. e DSGVO[58]); in allen anderen Konstellationen darf nur die Union selbst eine Zweckänderung zulassen. Anderenfalls hätten es die Mitgliedstaaten nämlich in der Hand, das System ihrer begrenzten Handlungsermächtigung nach Belieben zu unterlaufen, welches Art. 6 Abs. 1 DSGVO für die Erstverarbeitung anlegt. Insbesondere könnten sie unter Rückgriff auf die Befugnis zur Zweckänderung auch dort Regelungen treffen, wo die DSGVO ihnen schon eine Erstverarbeitung nicht gestattet. Soll die DSGVO systematisch kohärent sein, muss die Regelungsbefugnis für die Erst- und Zweitverarbeitung kompetenziell korrespondieren.

---

[56] Ausführlich hierzu J. Kühling/M. Martini/J. Heberlein, et al. (Fußn. 37), S. 38 ff.

[57] Bei Art. 6 Abs. 4 DSGVO handelt es sich um eine echte Öffnungsklausel, vgl. J. Kühling/M. Martini/J. Heberlein, et al. (Fußn. 37), S. 38 ff. Anders aber die BfDI in Bezug auf den Referentenentwurf des BMI: Die Bundesbeauftragte für Datenschutz und die Informationsfreiheit, Stellungnahme der BfDI zum Entwurf eines Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU, 31.8.2016, S. 15. Sie sieht in der Vorschrift lediglich eine unechte Öffnungsklausel, die eine mitgliedstaatliche Regelung nicht erlaubt, sondern voraussetzt; hierzu und zur Typik der Öffnungsklauseln allgemein J. Kühling/M. Martini/J. Heberlein, et al. (Fußn. 37), S. 9 ff.

[58] Art. 6 Abs. 1 UAbs. 1 S. 1 Buchst. c) und e) DSGVO legitimieren nicht selbst eine Datenverarbeitung. Es bedarf dafür vielmehr einer ergänzenden speziellen Rechtsgrundlage (Art. 6 Abs. 3 S. 1 DSGVO). Erst diese Normen definieren die öffentliche Aufgabe und dienen so als Verarbeitungsgrundlage.

(1) Die Gemeinwohlziele des Art. 23 Abs. 1 DSGVO

Auch soweit den Mitgliedstaaten eine Regelungsbefugnis für die Datenverarbeitung zukommt, legitimiert nicht jedes gesetzgeberische Ziel Ausnahmen vom Zweckbindungsgrundsatz der DSGVO. Die Zweckänderung muss vielmehr von dem Ansinnen getragen sein, jedenfalls eines der in Art. 23 Abs. 1 DSGVO genannten Gemeinwohlziele zu schützen (Art. 6 Abs. 4 DSGVO). Das Spektrum dieser Ziele legt die Verordnung insgesamt breit an,[59] gestaltet es aber auch abschließend aus.

Mit der größten Reichweite stattet die Verordnung – kraft seiner sprachlichen Offenheit – den Gemeinwohltatbestand des Art. 23 Abs. 1 lit. e DSGVO aus.[60] Er lässt Zweckänderungen zum „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses […]" zu. Als solcher setzt er an sich lediglich voraus, dass das verfolgte Ziel im allgemeinen öffentlichen Interesse liegt und die normative Waagschale mit hinreichendem Gewicht beschwert. Die Wirtschaftlichkeit und Sparsamkeit der öffentlichen Verwaltung sowie die Entbürokratisierung als die zentralen Once-Only-Ziele lassen sich bruchfrei unter diese Ziele des Buchst. e) rubrizieren.[61] Dies gilt umso mehr, je höher die durch den automatisierten Datenaustausch erzielten finanziellen Einsparungen sind.

Ein Vergleich mit den anderen hochrangigen Rechtsgütern, die Art. 23 Abs. 1 DSGVO nennt, gebietet – im Verbund mit dem normativen Ziel unionsweiter Harmonisierung (vgl. insbesondere ErwGrd Nr. 7 S. 1 DSGVO) – jedoch eine restriktive Interpretation des Buchst. e) Indem der europäische Gesetzgeber auf *sonstige* wichtige Ziele Bezug nimmt, stellt er eine innere Verbindung zu den übrigen Gemeinwohltatbeständen her: Die via Buchst. e) erfassten Gemeinwohlziele müssen den übrigen in Art. 23 Abs. 1 DSGVO genannten Zielen in ihrem normativen Gewicht

---

[59] Es reicht etwa von der „nationalen Sicherheit" (Buchst. a) über „die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe" (Buchst. g) und dem „Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats" (Buchst. e) bis hin zu dem „Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen" (Buchst. i).

[60] Vgl. auch die Bewertung von J. Stender-Vorwachs, in: Wolff/Brink, BeckOK DatenschutzR, 19. Ed. 2017, Art. 23 DSGVO, Rn. 26: „Mit diesem Ziel geht die Beschränkungsmöglichkeit der Union und der Mitgliedstaaten sehr weit".

[61] Ergänzend können Zulässigkeitstatbestände hinzutreten, die dem Bereich der Eingriffsverwaltung, insbesondere der öffentlichen Sicherheit zugehören. So ist es etwa denkbar, dass die Bauaufsicht für ein Erlass eines Verwaltungsaktes in Einzelfällen – bei entsprechender gesetzlicher Grundlage – zum Zwecke der Gefahrenabwehr auf Informationen zugreifen kann, die bei einer anderen Behörde bereits vorliegen.

nahekommen. Ein nachhaltiges Einsparpotenzial bei der Erfüllung von Verwaltungsaufgaben vermag diesem Anforderungsniveau jedoch gerecht zu werden.[62]

(2) Verhältnismäßigkeit in einer demokratischen Gesellschaft

Einspareffekte für Bürger und Verwaltung verleihen den Mitgliedstaaten keinen Freibrief, den Zweckbindungsgrundsatz nach Gutdünken zu zersetzen. Vielmehr knüpft das Unionsrecht (ähnlich wie das nationale Verfassungsrecht) Zweckänderungen an eine sachgerechte Abwägung zwischen dem Gemeinwohlziel und dem Persönlichkeitsinteresse des Betroffenen.[63] Jede mitgliedstaatliche Norm, die von der Geltung des Zweckbindungsgrundsatzes dispensiert, muss sich insbesondere daran messen lassen, inwieweit sie den Grundprinzipien der demokratischen Werte entspricht, zu denen sich die Union bekennt. Das Mehrheitsprinzip der Demokratie bürgt als solches zwar noch nicht notwendig für einen hinreichenden Grundrechtsschutz: Sub specie des Persönlichkeitsschutzes hat die Mehrheit keineswegs das Monopol der Wahrheit inne.[64] „In einer demokratischen Gesellschaft“ (Art. 6 Abs. 4 DSGVO) gelten die Grundrechte (mit Ausnahme der Menschenwürdeverbürgung) aber auch nicht vorbehaltlos: Die tatbestandliche Anknüpfung an die „demokratische Gesellschaft“ soll vielmehr ähnlich wie in der dogmatischen Blaupause des Art. 10 Abs. 2 EMRK betonen, dass sich eine Freistellung vom Zweckbindungsgrundsatz nur dann rechtfertigen lässt, wenn sie sich als in einer freiheitlich-demokratischen Gesellschaft tragfähige Beschränkung der Grundrechte darstellt. An diesem Staatsleitbild, nicht etwa an einer autoritären Verfassungsordnung, für die eine opake Überwachung des Individuums zur Normalität geworden ist, muss sich die beabsichtigte Maßnahme messen lassen.

In auffälligem Unterschied zu Art. 23 Abs. 1 DSGVO benennt Art. 6 Abs. 4 DSGVO nicht ausdrücklich auch den Wesensgehalt der Grundrechte und Grundfreiheiten als Schranke einer Zweckänderung. Er unterstreicht dafür jedoch das Gebot der Verhältnismäßigkeit umso deutlicher; insoweit scheint der sachlich verwandte Wesentlichkeitsgedanke in der Sache auch hier auf: Die Verfolgung mitgliedstaatlicher Ziele muss in einem angemessenen Verhältnis zu der Persönlichkeitseinschränkung stehen, die eine Maßnahme bewirkt. Der nationale Gesetzgeber muss seine Aufweichung des Zweckbindungsgrundsatzes auf das erforderliche Mindestmaß beschränken („notwendig“).[65] „Verhältnismäßig“ i. S. d Art. 6 Abs. 4 DSGVO ist die gesetzliche Auflösung der

---

[62] Die Erwägungsgründe der DSGVO benennen als sachnächstes Ziel lediglich explizit das „Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses“ (ErwGrd 73 S. 1 DSGVO).
[63] Vgl. auch allgemein B. P. Paal, in: Paal/Pauly, DS-GVO, 2016, Art. 23, Rn. 31.
[64] Dazu etwa G. Dworkin, Journal of Legal Studies 1980, 191 (207 f.); M. Martini (Fußn. 52), S. 252 ff.
[65] Vgl. auch Grages, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, Art. 23, Rn. 4. Ähnlich auch B. P. Paal (Fußn. 63), Rn. 10.

Zweckbindung insbesondere nur dann, wenn das Interesse der Allgemeinheit das Interesse des Einzelnen überwiegt. Eine kritische Grenze ist jedenfalls dann überschritten, wenn die Freistellung von der Einhaltung des Grundsatzes der Zweckbindung dazu dienen soll, Persönlichkeitsprofile der Bürger zu erstellen.[66]

dd) Zwischenfazit

Wie fest der Zweckbindungsgrundsatz die Daumenschrauben für eine spätere Zweckänderung anzieht – und damit die Bewegungsfreiheit des nationalen Gesetzgebers bei der Ausgestaltung des Once-only-Prinzips beschränkt –, bestimmen im Regime der DSGVO sowohl die Verarbeitungsermächtigung des Art. 6 Abs. 1 DSGVO[67] als auch die Gestaltungsmacht, die Art. 6 Abs. 2 und 3 DSGVO dem nationalen Gesetzgeber zugestehen.[68]

Sofern der Betroffene einer Zweckänderung zustimmt, können die Mitgliedstaaten das Once only-Prinzip grundsätzlich unschwer verwirklichen. Sie müssen lediglich sicherstellen, dass die Anforderungen gewahrt sind, welche die DSGVO an eine wirksame Einwilligung gegenüber Behörden stellt.

In allen anderen Fällen kann der nationale Gesetzgeber den Grundsatz der einmaligen Erfassung nur in eingeschränktem Maße in seine Rechtsordnung implementieren: Gesetzliche Regelungen, die eine zweckwidrige Weiterverarbeitung gestatten, sind an Art. 6 Abs. 4 i. V. m. Art. 23 DSGVO zu messen. Den Handlungsspielraum, der ihm dabei im Einzelfall zukommt, grenzt der Tatbestand des Art. 23 Abs. 1 lit. e DSGVO im regulatorischen Verbund mit dem Verhältnismäßigkeitsgrundsatz nachhaltig ein.

2. Umsetzung des Once-only-Prinzips durch das BDSG-neu

Den Regelungsspielraum, den die DSGVO den Mitgliedstaaten belässt, um Zweckänderungen zuzulassen, wird der Bund[69] durch das BDSG-Nachfolgegesetz (BDSG-neu) zu einem guten Teil ausschöpfen.[70] Die Bundesregierung hat einen Gesetzentwurf vorgelegt, der sich gegenwärtig der

---

[66] Insoweit lässt sich an die Prinzipien der verfassungsrechtlichen Rechtsprechung zum Allgemeinen Persönlichkeitsrecht anknüpfen; siehe dazu die Nachweise in Fußn. 24.
[67] P. Schantz (Fußn. 42), 1843.
[68] Vgl. auch B. Buchner (Fußn. 36), 157.
[69] Die *Länder* verharren im Hinblick auf ihre Datenschutzgesetze gegenwärtig noch abwartend wie das Kaninchen vor der Schlange. Sie werden nach Erlass des BDSG-neu mit Regelungen für ihre öffentliche Verwaltung nachziehen. Die Zeit dafür, bis die DSGVO gilt, wird allerdings knapp.
[70] Vgl. BT-Drucks. 18/11325, S. 94.

Beratung des Bundestages stellt.[71] Konkret gefasste Verarbeitungsgrundlagen für die öffentliche Verwaltung des Bundes sieht er in seinen §§ 4 und 23, 25, 27 f., 48 ff. vor. Das bereichsspezifische Datenschutzrecht, z. B. im Melde- oder Sozialrecht, mit seinen spezialgesetzlichen Verarbeitungsgrundlagen lässt er demgegenüber zunächst unangetastet.

Eine umfängliche „Rechts- und Verwaltungsvereinfachung" erklärt er zwar nicht zu seiner Agenda.[72] Die Grundkonstellation des Once-only-Prinzips – die Übermittlung personenbezogener Daten von einer öffentlichen Stelle an eine andere – führt der Regierungsentwurf des Bundes in § 25 Abs. 1 BDSG-neu jedoch einer Regelung zu. Die Zulässigkeit der Datenübermittlung knüpft er an zwei Voraussetzungen: Die Übermittlung muss zum einen zur Erfüllung der Aufgaben des Übermittlers oder des Empfängers erforderlich sein; zum anderen muss sie an die Tatbestände des § 23 BDSG-neu[73] rückgekoppelt sein, d. h. einen der sieben Erlaubnistatbestände erfüllen, die eine Ablösung vom ursprünglichen Verarbeitungszwecke gestatten.[74] Once-only-basiert kann die öffentliche Verwaltung deshalb auch auf Grundlage des § 25 Abs. 1 BDSG-neu nur in dem Rahmen handeln, den § 23 BDSG-neu inhaltlich absteckt. Die Vorschriften lehnen sich weitestgehend an das Vorbild des § 14 Abs. 2-5 bzw. § 15 Abs. 1 BDSG[75] an.[76]

a) Verarbeitung im Interesse des Betroffenen

Um eine Datenverarbeitung nach dem Once-only-Prinzip zu legitimieren, scheint prima facie der Tatbestand des § 23 Abs. 1 Nr. 1 BDSG-neu prädestiniert: Er gestattet Zweckänderungen, wenn die Verarbeitung „im Interesse der betroffenen Person liegt".[77] Es kann durchaus im Interesse des

---

[71] Art. 1 des Entwurfs eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680, BT-Drucks. 18/11325. Nur auf diese Entwurfsfassung beziehen sich die folgenden Ausführungen. Spätere Änderungen im Gesetzgebungsverfahren konnten keine Berücksichtigung mehr finden.
[72] BT-Drucks. 18/11325, S. 74.
[73] Die geltenden landesrechtlichen Regelungen knüpfen an einen jeweils ähnlichen Katalog an: § 15 Abs. 1-4 LDSG BW, Art. 17 Abs. 2-4 BayDSG, § 11 Abs. 2, § 6 Abs. 1 BlnDSG, § 13 Abs. 2 BbgDSG, § 12 Abs. 2 BremDSG, § 13 Abs. 2 HmbDSG, § 12 Abs. 2 hessDSG, § 10 DSG M-V, § 10 ndsDSG, § 13 Abs. 2 S. 1 DSG NRW, § 12 Abs. 4, § 13 Abs. 2 LDSG R-P, § 13 Abs. 2, 3 saarlDSG, § 13 Abs. 1-4 sächsDSG, § 10 DSG LSA, §§ 11, 13 Abs. 2-6 LDSG S-H, § 20 thürDSG.
[74] Die zweckändernde Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 Abs. 1 DSGVO) ist nur auf der Grundlage des § 23 Abs. 2 BDSG-neu zulässig.
[75] Ähnliche Regelungen enthalten die Landesdatenschutzgesetze in § 16 Abs. 1 LDSG BW, Art. 18 Abs. 1 BayDSG, § 11 Abs. 1 BlnDSG, § 14 Abs. 1 BbgDSG, § 13 Abs. 1 BremDSG, § 14 Abs. 1 HmbDSG, § 11 Abs. 1 S. 2 hessDSG, § 14 Abs. 1 DSG M-V, § 11 Abs. 1 ndsDSG, § 13 Abs. 1 DSG NRW, § 14 Abs. 1 LDSG R-P, § 14 Abs. 1 saarlDSG, § 14 Abs. 1 sächsDSG, § 11 Abs. 1 DSG LSA, §§ 14 Abs. 1 i. V. m. § 11 Abs. 1 Nr. 3 LDSG S-H, § 21 Abs. 1 thürDSG.
[76] BT-Drucks. 18/11325, S. 94.
[77] Die Vorschrift entspricht dem heutigen § 14 Abs. 2 Nr. 3 BDSG sowie im Wesentlichen auch § 15 Abs. 2 Nr. 2 LDSG BW, Art. 17 Abs. 2 Nr. 3 BayDSG, § 11 Abs. 2 Nr. 1 i. V. m. § 6 Abs. 1 S. 2 BlnDSG, § 13 Abs. 2 lit. e BbgDSG, § 12 Abs. 2 Nr. 5 BremDSG, § 13 Abs. 2 S. 1 Nr. 6 HmbDSG, § 12 Abs. 2 Nr. 5 hessDSG, § 10 Abs. 3 Nr. 3 DSG M-V,

Betroffenen liegen,[78] bereits erhobene und gespeicherte Daten an eine andere öffentliche Stelle weiterzugeben, mit der der Bürger digital in Kontakt tritt, mag er doch den angebotenen Servicevorteil nutzen wollen.

Das alleine genügt aber nicht. Die Verarbeitung muss nach dem Willen des Gesetzgebers auch „offensichtlich", d. h. in einer objektiv für jedermann erkennbaren Weise,[79] dem Interesse des Betroffenen entsprechen. Der (nach dem Vorbild des § 14 Abs. 2 Nr. 3 BDSG konzipierten) Vorschrift kommt eine Reservefunktion für solche Fälle zu, in denen die Einwilligung des Betroffenen faktisch nicht oder nur unter unverhältnismäßigem Aufwand zu erlangen gewesen wäre.[80] Besteht demgegenüber berechtigter Grund zu der Annahme, dass der Betroffene mit der Weitergabe der Daten nicht einverstanden ist, darf die öffentliche Stelle die Verarbeitung nicht auf § 23 Abs. 1 Nr. 1 BDSG-neu stützen.

An einem solchen hypothetischen Einverständnis mangelt es jedenfalls dann, wenn sich mit der Datenweitergabe unmittelbar negative Folgen für den Betroffenen verbinden. Ist es der Verwaltung – wie insbesondere im Rahmen digitaler Portalstrukturen – unkompliziert möglich, die Einwilligung des Betroffenen einzuholen, verweist der Gesetzgeber sie nach der Systematik seines Gesetzes auf diesen Weg.

b) Überprüfung von Angaben

Daten, welche die Verwaltung bereits für einen anderen Zweck erhoben hat, darf sie verwenden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Angaben des Betroffenen fehlerhaft sind (§ 23 Abs. 1 Nr. 2 BDSG-neu).[81] Dem liegt die normative Erwägung zugrunde, dass der datenschutzrechtliche Zweckbindungsgrundsatz den Behörden die Erledigung der ihnen

---

§ 10 Abs. 2 S. 1 Nr. 2 i. V. m. § 9 Abs. 1 S. 3 Nr. 4 ndsDSG, § 13 Abs. 2 S. 1 lit. e DSG NRW, § 13 Abs. 2 Nr. 1 i. V. m. § 12 Abs. 4 S. 1 Nr. 6 LDSG R-P, § 13 Abs. 2 lit. b saarlDSG, § 13 Abs. 2 Nr. 1 i. V. m. § 12 Abs. 4 Nr. 3 sächsDSG, § 10 Abs. 2 Nr. 3 DSG LSA, § 13 Abs. 3 Nr. 4 LDSG S-H, § 20 Abs. 2 Nr. 3 thürDSG.

[78] Instruktiv zur Frage, wann eine zweckändernde Verarbeitung nach § 14 Abs. 2 Nr. 3 BDSG im Interesse des Betroffenen liegt vgl. etwa J. Kühling/C. Seidel/A. Sivridis, Datenschutzrecht, 2015, S. 175.

[79] „Offensichtlich" meint in der Sache „ohne Weiteres und objektiv erkennbar", so zu § 14 Abs. 2 Nr. 3 BDSG M. Albers (Fußn. 32), Rn. 31. So auch M. Eßer, in: Auernhammer, BDSG, 4. Aufl. 2014, § 14 BDSG, Rn. 33 m. w. N.

[80] Vgl. U. Dammann, in: Simitis, BDSG, 8. Aufl. 2014, § 14, Rn. 61; P. Gola/C. Klug/B. Körffer (Fußn. 22), Rn. 17.

[81] U. Dammann (Fußn. 80), Rn. 62; vgl. auch die im Wesentlichen inhaltsgleichen § 15 Abs. 2 Nr. 4 LDSG BW, Art. 17 Abs. 2 Nr. 5 BayDSG, § 13 Abs. 2 lit. c BbgDSG, § 13 Abs. 2 S. 1 Nr. 4 HmbDSG, § 12 Abs. 2 Nr. 2 hessDSG, § 10 Abs. 3 Nr. 4 DSG M-V, § 10 Abs. 2 S. 1 Nr. 2 i. V. m. § 9 Abs. 1 S. 3 Nr. 3 ndsDSG, § 13 Abs. 2 S. 1 lit. c DSG NRW, § 13 Abs. 2 Nr. 1 i. V. m. § 12 Abs. 4 S. 1 Nr. 3 LDSG R-P, § 13 Abs. 2 lit. d saarlDSG, § 13 Abs. 2 Nr. 1 i. V. m. § 12 Abs. 4 Nr. 5 sächsDSG, § 10 Abs. 2 Nr. 4 DSG LSA, § 20 Abs. 2 Nr. 4 thürDSG. Lediglich Berlin, Bremen und Schleswig-Holstein kennen in ihrem geltenden Landesdatenschutzrecht keine ausdrückliche derartige Vorschrift.

übertragenen Aufgaben nicht in unangemessener Weise erschweren soll.[82] Der Anwendungsbereich der Vorschrift ist jedoch äußerst restriktiv: Sie verlangt (nach dem Paradigma des § 14 Abs. 2 Nr. 4 BDSG) „tatsächliche Anhaltspunkte" für die Unrichtigkeit von Angaben und einen entscheidungsrelevanten Fehler („überprüft werden müssen").[83] Einen präventiven Datenaustausch gestattet die Norm demgegenüber gerade nicht.[84] Sie errichtet daher keinen tragenden Pfeiler einer staatlichen Once-only-Architektur.

c) Wahrnehmung von Kontrollbefugnissen

A prima vista stützt immerhin § 23 Abs. 1 Nr. 7 BDSG-neu die Umsetzung des Once-only-Gedankens in breiterem Maße: Er lässt eine zweckwidrige Verarbeitung dann zu, wenn „sie für die Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient". Eine ähnliche Regelung enthalten bereits § 14 Abs. 3 BDSG[85] sowie sämtliche Landesdatenschutzgesetze.[86] Allerdings sind hier wie dort mit „Aufsichts- und Kontrollbefugnissen" nicht hoheitliche Maßnahmen des Staates im Verhältnis zum Bürger gemeint. Davon zeugen bereits die weiteren Begriffe „Rechnungsprüfung" und „Durchführung von Organisationsuntersuchungen", welche die Norm nennt. Regelungsobjekt des § 23 Abs. 1 Nr. 7 BDSG-neu ist vielmehr die rechts- und fachaufsichtliche Nachprüfung im verwaltungshierarchischen Binnenverhältnis.[87] Nur für diesen schmalen Bereich dispensiert die Vorschrift vom Grundsatz der Zweckbindung.

d) Zugriff auf allgemein zugängliche Daten

Allgemein zugängliche Daten, z. B. auf persönlichen Homepages oder in sozialen Netzwerken abgelegte öffentlich zugängliche Daten, befreit der Gesetzgeber grundsätzlich vollständig von einer

---

[82] P. Gola/C. Klug/B. Körffer (Fußn. 22), Rn. 18.
[83] U. Dammann (Fußn. 80), Rn. 64.
[84] U. Dammann (Fußn. 80), Rn. 66.
[85] Mit § 23 Abs. 1 Nr. 7 BDSG-neu beschreitet der Gesetzgeber regelungssystematisch einen neuen Weg: Er konzipiert den Tatbestand als zulässige Ausnahme vom Grundsatz der Zweckbindung. § 14 Abs. 3 BDSG beschreibt demgegenüber gegenwärtig eine Fallgruppe, in der schon keine Zweckänderung vorliegt, weil der Primärzweck die genannten Zwecke noch beinhaltet; vgl. auch P. Gola/C. Klug/B. Körffer (Fußn. 22), Rn. 24; J. D. Roggenkamp, in: Plath, BDSG/DSGVO, 2. Aufl. 2016, § 14 BDSG, Rn. 19; zum Streitstand hinsichtlich der genauen dogmatischen Einordnung des § 14 Abs. 3 BDSG, U. Dammann (Fußn. 80), Rn. 93 ff.
[86] § 15 Abs. 3 LDSG BW, Art. 17 Abs. 3 BayDSG, § 11 Abs. 4 BlnDSG, § 13 Abs. 3 BbgDSG, § 12 Abs. 3 BremDSG, § 13 Abs. 3 HmbDSG, § 13 Abs. 4 hessDSG, § 10 Abs. 4 DSG M-V, § 10 Abs. 3 ndsDSG, § 13 Abs. 3 DSG NRW, § 13 Abs. 4 S. 1 LDSG R-P, § 13 Abs. 4 saarlDSG, § 13 Abs. 3 sächsDSG, § 10 Abs. 3 DSG LSA, § 13 Abs. 5 LDSG S-H, § 20 Abs. 3 thürDSG.
[87] M. Albers (Fußn. 32), Rn. 53; U. Dammann (Fußn. 80), Rn. 97.

Zweckbindung (§ 23 Abs. 1 Nr. 3 BDSG-neu)[88]. Was kraft allgemeiner Wahrnehmbarkeit (unter dem Schutzmantel der grundrechtlich verbürgten Informationsfreiheit) jedermann nutzen kann, soll auch dem Nutzungsinteresse der öffentlichen Verwaltung nicht verschlossen sein.

Zu diesem Bestand zweckbindungsfrei erschließbarer personenbezogener Daten zählen bisher auch solche Daten, die nur nach vorheriger Anmeldung zu einem sozialen Netzwerk zugänglich, also durch ein Passwort gesichert sind. Das bringt de lege lata die Definition des § 10 Abs. 5 S. 2 BDSG zum Ausdruck („sei es ohne oder nach vorheriger Anmeldung […] nutzen kann“).[89] Der Verwaltung steht deshalb (vorbehaltlich überwiegenden schutzwürdigen Interesses des Betroffenen) ein vielgestaltiger Datenschatz zur Verwertung für „Once-only-Zwecke“ offen, der sich unterdessen auch technisch vergleichsweise leicht heben lässt (auch wenn er nicht immer valide ist, da nicht wenige Nutzer ihren Netzwerkprofilen bewusst falsche oder unbewusst veraltete Angaben unterlegen).

Ob dieses „Explorationsrecht“ auch unter dem BDSG-neu in seiner bisherigen Weite fortbesteht,[90] also auch (nach dem Vorbild des § 10 Abs. 5 S. 2 BDSG) passwortgesicherte Daten einschließt, lässt der Regierungsentwurf offen. Der Grundsatz der Direkterhebung, der einer Zusammenführung allgemein zugänglicher Informationen bisher normative Schranken setzte,[91] fällt mit Anwendbarkeit der DSGVO als Schutzelement jedenfalls weg. Gleiches gilt für die grundsätzliche Regelungsbefugnis des Mitgliedstaats für den Zugriff *nicht-öffentlicher* Stellen auf allgemein zugängliche Daten.[92]

Im Interesse zeitgemäßen Persönlichkeitsschutzes des *Homo digitalis* sollte der Gesetzgeber nur das, was für jedermann ohne weitere Einschränkung zugänglich, also über Suchmaschinen auffindbar ist, unter das Verarbeitungsprivileg der allgemeinen Zugänglichkeit stellen.[93] Nur ein solches restriktives Verständnis trägt der Rolle sozialer Netzwerke als Umschlagplatz der Meinungen und des unbefangenen demokratischen Austausches hinreichend Rechnung. Sonst

---

[88] Die Vorschrift entspricht im Wesentlichen den geltenden § 15 Abs. 2 Nr. 7 LDSG BW, Art. 17 Abs. 2 Nr. 8 BayDSG, § 13 Abs. 2 lit. f BbgDSG, § 12 Abs. 2 Nr. 6 BremDSG, § 13 Abs. 2 S. 1 Nr. 7 HmbDSG, § 10 Abs. 3 Nr. 5 DSG M-V, § 10 Abs. 2 S. 1 Nr. 2 i. V. m. § 9 Abs. 1 S. 3 Nr. 5 ndsDSG, § 13 Abs. 2 S. 1 lit. f DSG NRW, § 13 Abs. 2 Nr. 1 i. V. m. § 12 Abs. 4 S. 1 Nr. 9 LDSG R-P, § 13 Abs. 2 lit. f saarlDSG, § 13 Abs. 2 Nr. 2 sächsDSG, § 10 Abs. 2 Nr. 5 DSG LSA, § 11 Abs. 2 LDSG S-H § 20 Abs. 2 Nr. 5 thürDSG. Zu landesrechtlichen Ausnahmevorbehalten für allgemein zugängliche Daten siehe M. Martini, VerwArch. 2016, 307 (330 mit Fußn 97).

[89] Vergleichbare Definitionen in den geltenden Landesdatenschutzgesetzen finden sich lediglich in § 3 Abs. 10 LDSG R-P und § 2 Abs. 1 S. 3 DSG LSA. Dazu auch M. Martini (Fußn. 88), 337 f.

[90] Dazu auch M. Martini (Fußn. 88), 348 ff.

[91] M. Martini (Fußn. 88), 332 ff.

[92] Vgl. dazu M. Martini (Fußn. 88), 349 ff.

[93] M. Martini (Fußn. 88), 355.

erkauft die Verwaltung einen (vergleichsweise geringen) Effizienzgewinn der Verwendung auch anderweit beschaffbarer Daten mit dem hohen Preis eines – auch psychologisch – ungleich schwerer wiegenden Bruchs des bürgerlichen Vertrauens: nämlich des Glaubens daran, dass die Verwaltung personenbezogene Daten nicht ohne triftigen Grund unter Überwindung von Zugangshindernissen aus dem Zweckkontext herauslöst.

e) Sonstige Zwecke

Jenseits des Tatbestandes allgemein zugänglicher Daten legt das Gesetz die Hürden für einen Zugriff auf personenbezogene Daten zu anderen als den ursprünglichen Erhebungszwecken hoch. „Zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer (erheblichen) Gefahr für die öffentliche Sicherheit, die Landesverteidigung oder die nationale Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls“ (§ 23 Abs. 1 Nr. 4 BDSG-neu) wird ein Zugriff auf bereits vorhandene Daten ebenso nur selten eröffnet sein wie „zur Verfolgung von Straftaten oder Ordnungswidrigkeiten“ (§ 23 Abs. 1 Nr. 5 BDSG-neu). Selbiges gilt in Bezug auf den Legitimationstatbestand „zur Abwehr einer schwer wiegenden Beeinträchtigung der Rechte einer anderen Person“ (§ 23 Abs. 1 Nr. 6 BDSG-neu).[94] Die klassischen Anwendungsfälle des Once-only-Prinzips sind davon nicht umfasst.

f) Zwischenfazit

Der Entwurf für das neue BDSG und die geltenden Landesgesetze halten keine passgenaue Vorschrift vor, welche der Implementierung einer once-only-gestützten E-Government-Strategie in breitem Umfang den Boden bereitet. Auch unter dem den mitgliedstaatlichen Regelungsspielraum stark verengenden Regime der DSGVO wäre der nationale Gesetzgeber aber grundsätzlich befugt, eine Once-only-Verarbeitungsbefugnis selbst zu schaffen.

Sachgerecht kann de lege ferenda eine Norm sein, die speziell den Datenaustausch zwischen Behörden zu Once-only-Zwecken in eine rechtsstaatlich greifbare Eingriffsgrundlage gießt,[95] also regelt, welche Behörden welche Daten unter welchen Bedingungen zur Entlastung des Bürgers und der Verwaltung austauschen dürfen. Wenn auch in anderem Kontext, bestehen für einzelne Rechtsgebiete im bereichsspezifischen Datenschutzrecht bereits ausziselierte Vorschriften, die den zwischenbehördlichen Datenaustausch im Interesse übergeordneter Gemeinwohlgründe detailliert

[94] Gleiches gilt für die vergleichbaren Tatbestände in den Katalogen der Landesdatenschutzgesetze, vgl. Fußn. 75.
[95] Bereits vorgeschlagen in J. Kühling/M. Martini/J. Heberlein, et al. (Fußn. 37), S. 45 f.

regeln (etwa § 8 Abs. 1-3 BND-Gesetz sowie die umfänglichen Neuregelungen des Datenaustauschverbesserungsgesetzes[96]). Den verfügbaren nationalstaatlichen Handlungsrahmen für solche Vorschriften steckt Art. 6 Abs. 4 i. V. m. Art. 23 Abs. 1 DSGVO ab: Er formuliert spezifische Anforderungen an das den Zweckbindungsgrundsatz einschränkende Gesetz, insbesondere die Verhältnismäßigkeit der Maßnahme und die Beschränkung auf konkrete Gemeinwohlzwecke.

3. Datenschutz-Folgenabschätzung (Art. 35 DSGVO)

Setzt die öffentliche Verwaltung das Once-only-Prinzip gesetzlich um, kann das eine Datenschutz-Folgenabschätzung, also eine risikobasierte Selbsteinschätzung des anvisierten Verarbeitungsvorgangs, erforderlich machen.[97]

a) Erforderlichkeit einer Datenschutz-Folgenabschätzung auf der Grundlage der DSGVO

Nach dem Willen des Unionsgesetzgebers ist eine Datenschutz-Folgenabschätzung geboten, wenn die Verarbeitung „voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat (Art. 35 Abs. 1 S. 1 DSGVO).

Eine konsequente Umsetzung des Once-only-Prinzips ermöglicht immerhin die Sammlung und die Weitergabe zahlreicher personenbezogener Daten (mitunter besonders sensibler Daten i. S. d. Art. 9 DSGVO) einer großen Personenanzahl. Exakt solche Konstellationen sind es, welche nach der Vorstellung des Verordnungsgebers die Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung auslösen.[98] Das deutet auch ErwGrd 91 S. 1 DSGVO an („große Mengen personenbezogener Daten“, „eine große Zahl von Personen betreffen könnten“).

b) Anforderungen an die Durchführung

Dass eine Once-only-Strategie eine Datenschutz-Folgenabschätzung erforderlich macht, heißt nicht, dass die Verwaltung eine solche für jedwede once-only-basierte Verarbeitung im Einzelfall durchführen muss. Soweit die weitere Datennutzung sich auf die Verarbeitungsgrundlage des Art. 6 Abs. 1 UAbs. 1 lit. e DSGVO stützt (also insbesondere nicht bereits durch eine Einwilligung des

[96] Gesetz zur Verbesserung der Registrierung und des Datenaustausches zu aufenthalts- und asylrechtlichen Zwecken vom 2. 2. 2016, BGBl. I S. 130.
[97] Zum Wesen des Instruments vgl. M. Martini, in: Paal/Pauly, DS-GVO, 2016, Art. 35, Rn. 6.
[98] Zur Konkretisierung des Art. 35 Abs. 1 S. 1 DSGVO durch Positivlisten siehe Art. 35 Abs. 4 S. 1 DSGVO. Dazu M. Martini (Fußn. 97), Rn. 33 ff.

Betroffenen gedeckt ist), kann der nationale Gesetzgeber die Datenschutz-Folgenabschätzung auch in das Gesetzgebungsverfahren integrieren. Das gestattet ihm Art. 35 Abs. 10 DSGVO ausdrücklich.[99] Eine weitere Erleichterung des verfahrensrechtlichen Marschgepäcks verschafft Once-only-Modellen die Vorschrift des Art. 35 Abs. 1 S. 2 DSGVO: Errichten Mitgliedstaaten eine „gemeinsame Anwendung oder Verarbeitungsplattform" für ihre öffentlichen Stellen, können sie mehrere ähnliche Verarbeitungsvorgänge in *einer* Datenschutz-Folgenabschätzung bündeln (vgl. auch ErwGrd 92 DSGVO). Es bedarf dann nicht mehrerer, sondern nur einer einzigen Datenschutz-Folgenabschätzung.

V. Handlungsempfehlungen für Gesetzgeber und Verwaltung

Eine konsequente Once-only-Strategie kann die Bürger von Bürokratiekosten entlasten und die Verwaltung in eine benutzerfreundliche digitale Zukunft führen. Der Gesetzgeber ist dann aber gut beraten, die in der Bevölkerung verbreitete Sorge vor einer unbegrenzten und unkontrollierbaren staatlichen Datensammlung ernst zu nehmen. Am besten gelingt das, wenn der Bürger jederzeit Herr über die eigenen Daten bleibt und den Umfang der Datenweitergabe autonom bestimmen kann.

Dazu gehört auch und vor allem Transparenz über die Datenverwendung:[100] Eine (ungefragte) Offenlegung und Protokollierung, welche Behörden welche Daten wann und zu welchem Zweck abgerufen haben bzw. verwenden, stärkt das verfassungsrechtlich umhegte Bedürfnis, selbst über die Verwendung seiner Daten bestimmen zu können.[101] Eine automatische behördliche Benachrichtigung des Bürgers per E-Mail oder Push-Nachricht auf sein Endgerät ist ein guter Weg, ihm die Möglichkeit zur Steuerung des Datenflusses zu belassen. Sachgerecht ist mithin ein Datenmanagementsystem, mit dessen Hilfe ein Nutzer in concreto *für eine Vielzahl von Fällen ex ante* zu dekretieren in der Lage ist, welcher staatlichen Stelle welche Daten übermittelt werden sollen. Das versetzt ihn bei der Inanspruchnahme digitaler Verwaltungsleistungen in die Lage, selbst zu entscheiden, ob die Verwaltung seine Daten nie, zum Teil oder ggf. in bestimmten Kontexten weiterverwenden darf. Auf diese Weise kann er auch nach eigenem Gusto (präventiv) festlegen – und ggf. ändern, welche Behörden er vom Datenzugang ausschließt.

---

[99] Wie eine solche normative Datenschutz-Folgenabschätzung aussehen muss, um einer individuellen Datenschutz-Folgenabschätzung äquivalent zu sein, wirft zahlreiche Fragen auf. Kritisch zur Regelung des Art. 35 Abs. 10 DSGVO: M. Hansen, in: Wolff/Brink, BeckOK DatenschutzR, 19. Ed. 2017, Art. 35 DSGVO, Rn. 45.

[100] Der Transparenzgedanke ist auch der DSGVO insgesamt inhärent: Art. 5 Abs. 1 Buchst. a) DSGVO; vgl. dazu etwa M. Peifer (Fußn. 51), 225.

[101] Zur Information bzw. Auskunft auf Anfrage über die Verarbeitung personenbezogener Daten Betroffener verpflichten die Art. 13 ff. DSGVO den Verantwortlichen.

Alternativ (oder kumulativ) lässt sich das Once-only-Prinzip auch so ausgestalten, dass der Bürger nicht nur einmal vorab abstrakt einwilligt, sondern den jeweiligen Datenaustausch im Zeitpunkt der Datenanforderung *ad hoc* legitimiert. Er kann einem Datentransfer dann via Einwilligung im Einzelfall zustimmen. Setzt die Verwaltung demgegenüber (soweit unionsrechtlich zulässig) auf den Legitimationsweg einer abstrakten Einwilligung, so sollte sie den Bürger in jedem Einzelfall über die beabsichtigte Verarbeitung informieren. Die Benachrichtigung vermittelt ihm dann die Möglichkeit, innerhalb einer bestimmten Frist der Datenweitergabe durch Widerruf der zuvor pauschal erteilten Einwilligung die Grundlage zu entziehen.

Es braucht also zweierlei: ein Autorisierungsmanagement und Transparenz über die Datennutzung.

Auch an der psychologischen Wurzel der Amtsträger-Motivation, dem Bürger Informationen ein zweites Mal abzufordern, statt vorhandene Daten wiederholt zu nutzen, sollte der Gesetzgeber ansetzen. Verwaltungsmitarbeiter sollte er – z. B. im E-Government-Gesetz – darauf vergattern (in dem durch die Gesetze, insbesondere das Gebot der Zweckbindung gezogenen Rahmen) vorrangig auf bereits vorhandene Datenbestände zuzugreifen, statt sie beim Betroffenen ein zweites Mal zu erheben.

Setzt die digitale Verwaltung das Once-only-Prinzip konsequent um, häuft sie Berge sensibler Daten an. Den Staat trifft deshalb in besonderer Weise die verfassungsrechtliche Pflicht, die Sicherheit dieser Daten zu garantieren. Sowohl externe Cyberangriffe als auch interne Daten-Lecks gilt es dann, durch wirksame Abwehrmechanismen zu bekämpfen. Denn erst wenn der Bürger darauf vertrauen kann, dass weder der Staat noch Dritte seine persönlichen Daten gegen seinen Willen verwenden, wird er digitale Verwaltungsangebote wiederholt nutzen – und nicht „only once“.