Der digitale Staat als gläserner Staat. Transparenz als Bedingung verfassungskonformer Registermodernisierung

Jonas Botta

A. Auf dem Weg zum digitalen Staat

Deutschland befindet sich bereits seit mehr als zwei Jahrzehnten auf dem Weg, ein digitaler Staat zu werden. Als E-Government-Vorreiter gilt die Bundesrepublik bis heute gleichwohl nicht.[1] Spätestens die globale COVID-19-Pandemie hat den politischen Verantwortungsträgern jedoch nachdrücklich vor Augen geführt, dass eine digitale Verwaltung entscheidend dafür ist, die Herausforderungen des 21. Jahrhunderts bewältigen zu können. Folgerichtig entschied sich die schwarz-rote Bundesregierung 2020 dafür, als „Digitalisierungsbooster" zusätzliche drei Milliarden Euro für die Umsetzung des Onlinezugangsgesetzes (OZG) in ihrem Corona-Konjunkturpaket vorzusehen.[2]

I. Elektronische Verwaltungsleistungen

Das OZG ist seit seinem Inkrafttreten 2017 das zentrale Gesetz für die Verwaltungsdigitalisierung in Deutschland. Sein verfassungsrechtliches Fundament ist der Art. 91c Abs. 5 GG, der den Bundesgesetzgeber ermächtigt, den übergreifenden informationstechnischen Zugang zu den Verwaltungsleistungen von Bund und Ländern zu regeln. Demgemäß verpflichtet § 1 OZG beide Staatsebenen, ihre Verwaltungsleistungen bis Ende 2022 auch elektronisch anzubieten und über eine Verknüpfung ihrer Verwaltungsportale (Portalverbund) zugänglich zu machen. Eine Frist, die Bund

1 In internationalen E-Government-Rankings belegte Deutschland bislang keine Spitzenplätze. Siehe EU-Kommission, Index für die digitale Wirtschaft und Gesellschaft 2022, Länderbericht Deutschland (englischsprachige Fassung), Brüssel 2022, S. 15; United Nations, Department of Economic and Social Affairs, E-Government Survey 2020, Digital Government in the Decade of Action for Sustainable Development, New York 2020, S. 51.

2 *S. E. Schulz*, Der elektronische Zugang zur Verwaltung, RDi 2021, 377 (378).

und Länder trotz der coronabedingten „Finanzspritze“ nicht einhalten konnten.[3] Nun soll das „OZG 2.0“ den bestehenden Rechtsrahmen weiterentwickeln und zum einen Antworten auf Fragen der föderalen Zusammenarbeit und der End-to-End-Digitalisierung finden und zum anderen das Once-Only-Prinzip endlich Wirklichkeit werden lassen.[4]

II. Once-Only-Prinzip

Das Once-Only-Prinzip verspricht eine erhebliche Entlastung für Bürger und Unternehmen. Perspektivisch soll ihnen nicht nur der „Gang aufs Amt“ erspart bleiben, sondern es soll ihnen auch offenstehen, der Verwaltung ihre Daten und Nachweise nur noch einmalig zu übermitteln.[5] Benötigt eine Behörde anschließend Informationen, die bereits (bei einer anderen Behörde) vorliegen, kann sie zukünftig auf diese elektronisch zugreifen, anstatt sie erneut erheben zu müssen. Dadurch sollen Bürger 84 Mio. und die Verwaltung 64 Mio. Zeitstunden jährlich einsparen können, was eine Aufwandsreduzierung um 47 % bzw. 60 % bedeutete.[6] Als Pilotprojekt lassen sich die Namensbestimmung, die Geburtsurkundenbestellung sowie das Kinder- und Elterngeld in Bremen seit dem 1.7.2022 gebündelt online beantragen („Einfach Leistungen für Eltern“, kurz ELFE).[7] Um Once-Only für alle (geeigneten) Verwaltungsleistungen bundesweit anbieten zu können, müssen jedoch noch erhebliche rechtliche und technische Hürden genommen werden. Der behördliche Datenaustausch setzt insbesondere eine Reform der Registerlandschaft voraus.

---

3 *O. Voß/L. Rusch*, Digitalisierung in der Warteschleife: „Ein bisschen Veränderung hier, ein wenig dort – so kommen wir nicht weiter“, Tagesspiegel.de v. 9.12.2022, https://www.tagesspiegel.de/politik/verheerende-bilanz-digitalgipfel-in-krisenzeiten-9003220.html (zuletzt abgerufen: 11.12.2022).

4 *M. Punz*, OZG: Was ein Folgegesetz bringen soll, Tagesspiegel Background v. 8.2.2022, abrufbar unter https://background.tagesspiegel.de/smart-city/ozg-was-ein-folgegesetz-bringen-soll (zuletzt abgerufen: 11.12.2022).

5 *H. P. Bull*, Die Nummerierung der Bürger und die Angst vor dem Überwachungsstaat, DÖV 2022, 261 (265); *M. Martini/M. Wenzel*, »Once only« versus »only once«: Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit, DVBl. 2017, 749.

6 Nationaler Normenkontrollrat, Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren., Berlin 2017, S. 55.

7 *M. Klein*, Per Once-Only zu Kinder- und Elterngeld, eGovernment Computing v. 25.3.2022, abrufbar unter https://www.egovernment-computing.de/per-once-only-zu-kinder-und-elterngeld-a-1105530/ (zuletzt abgerufen: 11.12.2022).

III. Registermodernisierung

Unter den (uneinheitlich definierten) Registerbegriff fallen in erster Linie alle (elektronischen) Datenbestände, die Informationen enthalten, die für ein Verwaltungsverfahren erforderlich sind, die als staatliche Entscheidungsgrundlage dienen oder die für die amtliche Statistik genutzt werden sollen.[8] Aktuell gibt es in Deutschland über 375 zentrale und dezentrale Registertypen.[9] Die Gesamtzahl der einzelnen Register ist zudem noch viel höher. So existieren bundesweit über 5000 kommunale Melderegister. Register sind somit die „Datenschätze" der öffentlichen Verwaltung. Sie zu „bergen", kann sich bislang als schwieriges bis unmögliches Unterfangen erweisen. Auf die Register können im Regelfall nur die registerführenden Stellen selbst zugreifen. Zwischenbehördliche Austauschmöglichkeiten sind die Ausnahme. Die Register beinhalten daher zumeist alle Daten, die für ihren Anwendungsbereich notwendig sind. Dies führt einerseits zu Mehrfacherhebungen derselben Datenkategorien (z.B. Name, Geburtsdatum und Anschrift) und andererseits aufgrund von unterschiedlichen Aktualisierungsfrequenzen sowie Transkriptionsfehlern zu uneinheitlichen Datenbeständen für dieselbe Person. Unter diesen Bedingungen lässt sich Once-Only nur sehr eingeschränkt umsetzen.

Mit dem Registermodernisierungsgesetz (RegMoG) verfolgt der Bundesgesetzgeber nunmehr das Ziel, zumindest die wichtigsten Register(typen) bis 2025 zu verknüpfen, um Informationen registerübergreifend übermitteln und medienbruchfreie E-Government-Angebote gewährleisten zu können. Außerdem sollen perspektivisch neue Register geschaffen (z.B. ein Gebäude- und Wohnungsregister) und analog geführte Register digitalisiert werden. Die föderale Registerarchitektur lässt der Gesetzgeber indes grundsätzlich unangetastet.[10]

---

8 Nationaler Normenkontrollrat, Mehr Leistung für Bürger und Unternehmen (Fn. 6), S. 13; *E. Peuker*, Registermodernisierung und Datenschutz, NVwZ 2021, 1167 (1168). Weiterführend zum Registerbegriff *F. Wollenschläger*, Register als Instrument der Wirtschaftsverwaltung, ZHR 186 (2022), 474 (477 ff.).

9 IT-Planungsrat, Registermodernisierung: Zielbild und Umsetzungsplanung, 2021, S. 12.

10 *A. Guckelberger/G. Starosta*, Die Fortentwicklung des Onlinezugangsgesetzes, NVwZ 2021, 1161 (1165).

B. Risiko der gläsernen Bürger

Kernstück des RegMoG ist das Identifikationsnummerngesetz (IDNrG). Es führt ein Identitätsmanagement ein, um bei den registerübergreifenden Datenübermittlungen Personenverwechselungen zu verhindern (§ 1 Nr. 1 IDNrG) und die unterschiedlichen Register miteinander zu synchronisieren. Dadurch soll die Datenqualität erhöht (§ 1 Nr. 2 IDNrG) und Once-Only ermöglicht (§ 1 Nr. 3 IDNrG) werden. Seine Vorschriften treten überwiegend erst an dem Tag in Kraft, an dem das Bundesministerium des Innern (BMI) im Bundesgesetzblatt bekannt gibt, dass die technischen Voraussetzungen für das IDNrG vorliegen (Art. 22 S. 2 RegMoG).

I. Einführung einer Identifikationsnummer

Für das registerübergreifende Identitätsmanagement soll ein zusätzliches Ordnungsmerkmal in die 51 Register(typen) eingefügt werden, die in der Anlage zu § 1 IDNrG aufgelistet sind. Der Bundesgesetzgeber hat darauf verzichtet, ein neues Ordnungsmerkmal zu schaffen und hat stattdessen bestimmt, dass die Identifikationsnummer nach § 139b Abgabenordnung als Ordnungsmerkmal fungieren soll (§ 1 IDNrG).

Durch das „Upgrade" der Steuer-ID erhält das Bundeszentralamt für Steuern eine Schlüsselposition im Rahmen der Registermodernisierung.[11] Es ist fortan dafür zuständig, die Qualität der sogenannten Basisdaten nach § 4 Abs. 2 und 3 IDNrG (neben der Steuer-ID insbesondere Name, Geburtsdatum und -ort, Geschlecht, Staatsangehörigkeit, Anschrift und Datum des letzten Verwaltungskontakts) zu überwachen (§ 10 Abs. 1 IDNrG). Die registerführenden Stellen des Bundes und der Länder fügen die Steuer-ID in ihre Datenbestände ein und passen die Informationen, die den Basisdaten entsprechen, an diese an (§ 2 Nr. 1 und 2 IDNrG). Die Übermittlung der Basisdaten erfolgt dabei nicht unmittelbar zwischen den Behörden, sondern über das Bundesverwaltungsamt als Registermodernisierungsbehörde i.S.d. § 3 IDNrG (§ 6 Abs. 1 S. 1 Hs. 1 IDNrG).[12] Die Behörden können die Basisdaten auch bei der Registermodernisierungsbehörde abrufen, wenn sie eine OZG-Leistung erbringen (§ 6 Abs. 2 S. 1 IDNrG). Nach dem Übermittlungsvorgang löscht die Registermodernisierungsbehörde die Daten unver-

11 *M. Knauff/L. Lehmann*, Das Registermodernisierungsgesetz, DÖV 2022, 159 (160).

12 Mit Ausnahme des Datenabrufs bei den Meldebehörden (§ 6 Abs. 1 S. 1 Hs. 2 IDNrG).

züglich (§ 11 IDNrG). Dadurch ist sichergestellt, dass kein zusätzliches Basisdatenregister entsteht.

Die Nutzung der Steuer-ID als Ordnungsmerkmal wird sich nicht auf die Basisdaten beschränken. Vielmehr können öffentliche (und nicht-öffentliche) Stellen auch weitergehende Informationen und Nachweise unter Verwendung der Steuer-ID miteinander austauschen. Dies setzt voraus, dass eine Einwilligung vorliegt (§ 5 Abs. 1 S. 2 Var. 2 IDNrG) oder die Datenverarbeitung einem der abschließend aufgezählten Zwecke dient. Zulässige Verarbeitungszwecke sind – abgesehen vom Abgleich der Basisdaten (§ 5 Abs. 1 S. 1 Nr. 2 IDNrG) – die Zuordnung der Datensätze zur richtigen Person (§ 5 Abs. 1 S. 1 Nr. 1 IDNrG), die Erbringung von OZG-Leistungen auf Grundlage von Rechtsvorschriften (§ 5 Abs. 1 S. 2 Var. 1 IDNrG) und ein registerbasierter Zensus (§ 5 Abs. 1 S. 2 Var. 3 IDNrG). Wenn die übermittelnden Behörden unterschiedlichen Bereichen[13] angehören, ist ihnen kein direkter Datenaustausch erlaubt, sondern nur eine verschlüsselte Übermittlung über sogenannte Vermittlungsstellen (§ 7 Abs. 2 S. 1 IDNrG). Dieser Übertragungsweg wird als 4-Corner-Modell (Behörde A ↔ Vermittlungsstelle 1 ↔ Vermittlungsstelle 2 ↔ Behörde B) bezeichnet.[14]

II. Unions- und verfassungsrechtliche Zulässigkeit

Die Einführung der Identifikationsnummer nach § 1 IDNrG ist äußerst umstritten. Ihre Kritiker fürchten, dass sie einer panoptischen Gesellschaftsordnung den Weg bereitet, in der der Staat immer umfassendere Einblicke in das Leben seiner Bürger erhält. Ob sie rechtlich zulässig ist, bemisst sich nach den Vorgaben des Unions- und Verfassungsrechts.

1. Öffnungsklausel für nationale Kennziffern (Art. 87 DSGVO)

Das Recht der digitalen Verwaltung ist keineswegs eine rein nationale Materie. Mit der „Single Digital Gateway"-Verordnung (EU) 2018/1724 verpflichtet die Union ihre Mitgliedstaaten, ausgewählte Verwaltungsleistun-

13 Die Behörden sollen bundesweit in mindestens sechs unterschiedliche Bereiche aufgeteilt werden (§ 7 Abs. 2 S. 2 IDNrG), z.B. in Inneres (1), Justiz (2), Wirtschaft und Finanzen (3), Arbeit und Soziales (4), Gesundheit (5) und Statistik (6). Siehe BT-Drs. 19/24226, S. 74.

14 *Knauff/Lehmann*, Registermodernisierungsgesetz (Fn. 11), 161; *Peuker*, Registermodernisierung (Fn. 8), 1171.

gen bis Ende 2023 online anzubieten und dabei das Once-Only-Prinzip zu beachten (Art. 6 i.V.m. Anhang II sowie Art. 13 und 14 SDG-VO).[15] Zur Verwendung einer Identifikationsnummer schweigt sich die SDG-VO indes aus.[16] Ihre Rechtmäßigkeit richtet sich vielmehr nach dem geltenden Datenschutzrecht. Denn die behördliche Verarbeitung personenbezogener Daten ruft grundsätzlich die Datenschutz-Grundverordnung auf den Plan (Art. 2 Abs. 1 DSGVO). Ihr weiter Anwendungsbereich und das Erfordernis, jeden Verarbeitungsvorgang auf einen Erlaubnistatbestand stützen zu können (Art. 6 Abs. 1 UAbs. 1 DSGVO), haben der Verordnung den Ruf eines „Digitalisierungsverhinderungsrechts" eingebracht.

Die DSGVO stellt es den nationalen Gesetzgebern indes frei, ob sie eine Identifikationsnummer für ihre Bürger verwenden wollen. Die Öffnungsklausel des Art. 87 S. 1 DSGVO erlaubt es ihnen, näher zu bestimmen, unter welchen spezifischen Bedingungen eine nationale Kennziffer oder ein Kennzeichen von allgemeiner Bedeutung Gegenstand einer Verarbeitung sein dürfen.[17] Voraussetzung ist, dass geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen die Verarbeitung flankieren (Art. 87 S. 2 DSGVO). Die Verordnung konkretisiert diese geeigneten Garantien zwar nicht, sie müssen aber jedenfalls das Schutzniveau der allgemeinen Datenschutzgrundsätze wahren (vgl. ErwGr. 156 DSGVO): in erster Linie die Grundsätze der Transparenz (Art. 5 Abs. 1 lit. a Var. 3 DSGVO), der Zweckbindung (Art. 5 Abs. 1 lit. b Hs. 1 DSGVO) und der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO).[18] Unter Beachtung

15 Dazu *M. Martini*, Digitalisierung der Verwaltung, in: W. Kahl/M. Ludwigs (Hrsg.), Handbuch des Verwaltungsrechts, Heidelberg 2021, Rn. 33 f.; *T. Siegel*, Der Europäische Portalverbund – Frischer Digitalisierungswind durch das einheitliche digitale Zugangstor („Single Digital Gateway"), NVwZ 2019, 905 ff.

16 Der EU-Kommissionsvorschlag einer Verordnung über die europäische digitale Identität (EUid) sieht hingegen eine eindeutige und dauerhafte Kennung zur Identifizierung vor (COM(2021) 281 final, S. 32). Von dieser Regelung ist die EU-Kommission jedoch zwischenzeitlich abgerückt (*S. Krempl*, EU-weite Online-Ausweise: Lebenslange Identifikationsnummer vorerst vom Tisch, heise online v. 12.7.2022, abrufbar unter https://www.heise.de/news/EU-weite-Online-Ausweise-Dauerhafte-Identifikationsnummer-vorerst-vom-Tisch-7177700.html [zuletzt abgerufen: 11.12.2022]).

17 Obwohl die Identifikationsnummer zunächst „nur" in 51 Register eingeführt werden soll, ist sie aufgrund ihres weiten Anwendungsbereichs als nationale Kennziffer anzusehen (a.A.: *E. Ehmann*, Registermodernisierung in Deutschland, ZD 2021, 509 (511); *K. von Lewinski*, in: H. A. Wolff/S. Brink (Hrsg.), BeckOK DatenschutzR, 40. Ed. (Stand: 1.5.2022), München, Art. 87 Rn. 28.1.

18 *M. Hansen*, in: S. Simitis/G. Hornung/I. Spiecker gen. Döhmann (Hrsg.), DSGVO, Baden-Baden 2019, Art. 87 Rn. 24; *M. Martini/D. Wagner/M. Wenzel*,

dieser Vorgaben lässt sich eine Identifikationsnummer somit unionskonform einführen.

2. *Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)*

Da der Unionsgesetzgeber die Verwendung einer nationalen Kennziffer nicht abschließend geregelt hat, ist ihre Zulässigkeit in Deutschland insbesondere anhand der Vorschriften des Grundgesetzes zu überprüfen.[19] Einschlägig ist das Recht auf informationelle Selbstbestimmung, das das BVerfG aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG abgeleitet hat. Es schützt die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.[20] In dieses Grundrecht greifen das Vorhaben der Registermodernisierung im Allgemeinen und das IDNrG im Besonderen ein. Bereits die bloße Verknüpfungsmöglichkeit personenbezogener Daten stellt eine Persönlichkeitsgefährdung dar, die als Eingriff zu werten ist.[21] Daher ist es unerheblich, dass der Einzelne grundsätzlich darauf verzichten kann, seine Daten nach dem Once-Only-Prinzip an den Staat zu übermitteln. Jedenfalls kann er sich nicht der anlasslosen Vergabe einer Identifikationsnummer und deren Implementierung in die Fachregister entziehen.

Die aus dem RegMoG erfolgenden Eingriffe könnten sogar derart intensiv sein, dass sie nicht mehr zu rechtfertigen sind. Denn nach der Rechtsprechung des BVerfG ist es grundrechtswidrig, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren.[22] „[D]ie Einführung eines einheitlichen, für alle Register und Dateien geltenden Personenkennzeichens […] wäre aber gerade ein entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren".[23] Bei der Identifikationsnummer nach § 1 IDNrG handelt es sich um ein solches einheitliches Personenkennzei-

---

Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, Speyer 2017, S. 7; vgl. auch *T. Weichert,* in: J. Kühling/B. Buchner (Hrsg.), DSGVO/BDSG, 3. Aufl., München 2020, Art. 87 Rn. 15.

19 Vgl. BVerfGE 152, 216 (229); *J. Botta*, „Digital First" und „Digital Only" in der öffentlichen Verwaltung, NVwZ 2022, 1247 (1249 f.).

20 BVerfGE 65, 1 (43).

21 BVerfGE 65, 1 (45).

22 BVerfGE 27, 1 (6).

23 BVerfGE 65, 1 (57).

chen[24] – ein Novum in der deutschen Rechtsordnung unter Geltung des Grundgesetzes.[25] Dem steht nicht entgegen, dass sie zunächst nicht in alle Register Einzug hält und das IDNrG sie (im Gegensatz zur Gesetzesbegründung)[26] als bereichsspezifisches Kennzeichen ausweist (vgl. § 16 Abs. 2 S. 2 Nr. 1 Alt. 1 IDNrG). Denn schon durch die *de lege lata* getroffene Registerauswahl ließen sich umfassende Persönlichkeitsprofile erstellen, da sie wesentliche Lebensbereiche abdeckt. Insoweit unterscheidet sich die Identifikationsnummer nach § 1 IDNrG von der bloßen Steuer-ID, die nur zu Besteuerungszwecken dient (auch wenn das Steuerrecht ebenfalls sehr tiefe Einblicke in das Leben der Steuerpflichtigen ermöglicht).[27] Zudem hat sich der Bundesgesetzgeber offengehalten, die Identifikationsnummer zukünftig in alle Register einzufügen (vgl. § 16 Abs. 2 S. 2 Nr. 1 Alt. 2 IDNrG). Während die Steuer-ID als verfassungsgemäß erachtet worden ist,[28] könnte ihre modifizierte Verwendung somit per se verfassungswidrig sein.

Aus dem zitierten Volkszählungsurteil das absolute Verbot einer einheitlichen Identifikationsnummer zu folgern, schösse jedoch über den Schutz des Rechts auf informationelle Selbstbestimmung hinaus.[29] Das Kennzeichen selbst ist – zumal als sogenannte nicht-sprechende Nummer[30] – ungefährlich.[31] Erst seine konkrete Verwendungsmöglichkeit zur Erstellung umfassender Datensätze über den Einzelnen lässt es bedroh-

24 *C. Sorge/J. von Lucke/I. Spiecker gen. Döhmann*, Registermodernisierung, Potsdam 2021, S. 14 f.; a.A.: *Ehmann*, Registermodernisierung (Fn. 17), 512; *Peuker*, Registermodernisierung (Fn. 8), 1170.

25 Die DDR führte ab 1970 schrittweise eine Personenkennzahl (PKZ) für ihre Bürger ein. Siehe *T. Weichert*, in: J. Kühling/B. Buchner (Hrsg.), DSGVO/BDSG, 3. Aufl., München 2020, Art. 87 Rn. 13.

26 BT-Drs. 19/24226, S. 6.

27 FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08, BeckRS 2010, 26030144, Rn. 136.

28 BFH, Urt. v. 18.1.2012 – II R 49/10, BeckRS 2012, 94274, Rn. 46; *Knauff/Lehmann*, Registermodernisierungsgesetz (Fn. 11), 162.

29 *Martini/Wagner/Wenzel*, Personen- bzw. Unternehmenskennziffer (Fn. 18), S. 31 f.; *Peuker*, Registermodernisierung (Fn. 8), 1170; a.A.: *M. Kleinert/M. Kuhn/C. Otte/R. Will*, Stellungnahme zum Referentenentwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz), vorgänge. Zeitschrift für Bürgerrechte und Gesellschaftspolitik 2020, Nr. 230, 125 (130 ff.).

30 Die Steuer-ID ist eine elfstellige Nummer, die zufällig erzeugt wird und keine Informationen über den Bürger enthält.

31 *K. von Lewinski/M. Gülker*, Europa-, verfassungs- und datenschutzrechtliche Grundfragen des Registermodernisierungsgesetzes (RegMoG), DVBl. 2021, 633 (634); *Peuker*, Registermodernisierung (Fn. 8), 1170.

lich werden. Für eine derartige Differenzierung spricht insbesondere, dass das BVerfG in seinem damaligen Urteil die Bedingungen der modernen Datenverarbeitung als die entscheidende Herausforderung benannt hat.[32] Schon 1983 stand damit das Gefährdungspotenzial neuer Verknüpfungsmöglichkeiten und nicht die Verarbeitung personenbezogener Daten schlechthin im Mittelpunkt der verfassungsrechtlichen Erwägungen. Angesichts der heute als modern geltenden Datenverarbeitung haben sich die Gefährdungslagen deutlich gegenüber dem Stand der Technik von vor 40 Jahren geändert. In Zeiten von Big-Data-Analysen und künstlicher Intelligenz bedarf es längst keines Personenkennzeichens mehr, um den Einzelnen zu durchleuchten. Ein derartiges Kennzeichen erleichtert eine Profilbildung lediglich.

Die Nutzung der Steuer-ID als registerübergreifendes Ordnungsmerkmal verstößt folglich nicht generell gegen geltendes Verfassungsrecht und ist damit rechtfertigungsfähig. Eingriffe in das Recht auf informationelle Selbstbestimmung sind indes nur im überwiegenden Allgemeininteresse gerechtfertigt.[33] Für das RegMoG ergibt sich ein derartiges Allgemeininteresse grundsätzlich aus der Sicherstellung einer zeitgemäßen und funktionierenden Verwaltung.[34] Denn ohne eine Reform der deutschen Registerlandschaft lassen sich die Effizienzpotenziale von Once-Only nicht entfalten.

Zudem muss das RegMoG den Grundsatz der Verhältnismäßigkeit wahren und der Bundesgesetzgeber Vorkehrungen getroffen haben, die der Gefahr einer Persönlichkeitsverletzung entgegenwirken.[35] Entscheidend für die Verfassungsmäßigkeit der einheitlichen Identifikationsnummer sind somit neben der Frage nach gleich geeigneten, aber milderen Mitteln,[36] bspw. der Kombination allgemeiner und bereichsspezifischer Perso-

---

32 BVerfGE 65, 1 (42, 43, 45, 46 und 48).

33 BVerfGE 65, 1 (44).

34 Vgl. *Botta*, „Digital First" und „Digital Only" in der Verwaltung (Fn. 19), 1250.

35 Vgl. BVerfGE 65, 1 (44).

36 Aufgrund der gesetzgeberischen Einschätzungsprärogative mehren sich im Schrifttum zwar die Stimmen, die die Identifikationsnummer als erforderlich ansehen (*Knauff/Lehmann*, Registermodernisierungsgesetz (Fn. 11), 162 f.; *von Lewinski/Gülker*, Registermodernisierungsgesetz (Fn. 31), 636 ff.; *Peuker*, Registermodernisierung (Fn. 8), 1171 f.), gegen diese Auffassung sind aber gewichtige Argumente vorgetragen worden (*Kleinert/Kuhn/Otte/Will*, Registermodernisierungsgesetz (Fn. 29), 129 f. und *Sorge/von Lucke/Spiecker gen. Döhmann*, Registermodernisierung (Fn. 24), S. 16 f.). Es kann daher zumindest als offen gelten, wie das BVerfG entscheiden wird, wenn es die Verfassungsmäßigkeit der einheitlichen Identifikationsnummer überprüfen muss.

nenkennzeichen („österreichisches Modell"),[37] die ergriffenen technischen, organisatorischen und rechtlichen Schutzmaßnahmen.[38]

C. Chance des gläsernen Staates

Das Unionsrecht und das deutsche Verfassungsrecht stehen einer einheitlichen Identifikationsnummer nicht unüberwindbar entgegen. Sowohl die Öffnungsklausel des Art. 87 DSGVO als auch das Recht auf informationelle Selbstbestimmung verlangen jedoch, dass der Staat den damit einhergehenden Datenschutzrisiken vorbeugt. Von Bedeutung sind dabei insbesondere die Transparenzmechanismen.[39] Dass der Staat grundsätzlich offen und nachvollziehbar handeln muss, war zwar bereits im analogen Zeitalter ein elementares Prinzip im demokratischen Rechtsstaat.[40] Aus der digitalen Transformation folgt nunmehr aber die Chance, dass der Staat für seine Bürger noch durchsichtiger wird.[41] Dieser Gewinn an Transparenz kann grundsätzlich einen (gewissen) Verlust an informationeller Selbstbe-

37 Dazu *Martini/Wagner/Wenzel*, Personen- bzw. Unternehmenskennziffer (Fn. 18), S. 36 ff.; *Sorge/von Lucke/Spiecker gen. Döhmann*, Registermodernisierung (Fn. 24), S. 16 f.

38 *Martini/Wagner/Wenzel*, Personen- bzw. Unternehmenskennziffer (Fn. 18), S. 33.

39 Vgl. *M. Martini*, Transformation der Verwaltung durch Digitalisierung, DÖV 2017, 443 (452); *I. Sommer*, Datenschutz – Betroffenenrechte: Transparenz als Werkzeug und Voraussetzung der informationellen Selbstbestimmung, in: H. Lühr/R. Jabkowski/S. Smentek (Hrsg.), Handbuch Digitale Verwaltung, Wiesbaden 2019, S. 233 (234).

40 Im Grundgesetz findet sich zwar im Gegensatz zum unionalen Primärrecht (z.B. in Art. 1 Abs. 2 EUV) kein ausdrückliches Transparenzprinzip, dieses lässt sich aber aus den Grundrechten (insbesondere der Informationsfreiheit nach Art. 5 Abs. 1 S. 1 Alt. 2 GG) sowie dem Demokratie- und Rechtsstaatsprinzip (Art. 20 Abs. 2 und 3 GG) ableiten (weiterführend *J. Bröhmer*, Transparenz als Verfassungsprinzip, Tübingen 2004, S. 33 ff.; *B. W. Wegener*, Der geheime Staat, Göttingen 2006, S. 394 ff.). Da die Transparenz staatlichen Handelns nicht unbeschränkt gilt, spricht *C. Gusy*, Der transparente Staat, DVBl. 2013, 941 (942) vom Grundsatz der limitierten Öffentlichkeit. Zur Bedeutung des staatlichen Geheimnisschutzes siehe *T. Wischmeyer*, Formen und Funktionen des exekutiven Geheimnisschutzes, Die Verwaltung 51 (2018), 393 ff. m.w.N.

41 *J. Fährmann*, Mehr Transparenz durch technische Innovationen?, MMR 2021, 775 ff.; *C. Fischer/S. Kraus*, Digitale Transparenz, in: T. Klenk/F. Nullmeier/G. Wewer (Hrsg.), Handbuch Digitalisierung in Staat und Verwaltung, Wiesbaden 2020, S. 159 ff.; *J. von Lucke*, Transparenz 2.0 – Transparenz durch E-Government, in: S. A. Jansen/E. Schröter/N. Stehr (Hrsg.), Transparenz, Wiesbaden 2010, S. 396 (398 ff.).

stimmung rechtfertigen, insoweit er es vermag, die informationellen Machtasymmetrien in der digitalen Verwaltung auszugleichen.

I. Verfassungsgerichtliche Transparenzanforderungen

Unter welchen Bedingungen die staatliche Datenverarbeitung als transparent anzusehen ist, hat das BVerfG in seiner Rechtsprechung niedergelegt.[42] Die Transparenzmechanismen des RegMoG müssen diesen Anforderungen genügen, um die angestrebte Reform tatsächlich verfassungsrechtlich absichern zu können.

Eine zentrale Transparenzanforderung ist der Grundsatz der Offenheit der Datenverarbeitung.[43] Zum einen muss der Person, die von der Datenverarbeitung betroffen ist, ein Auskunftsanspruch gegenüber den verarbeitenden Behörden zustehen.[44] Zum anderen müssen die verarbeitenden Behörden sie unabhängig von einem konkreten Auskunftsersuchen über die Datenverarbeitung informieren.[45] Dabei darf sich die Information nicht darauf beschränken, dass staatliche Stellen Daten verarbeiten, sondern muss insbesondere die konkreten Verarbeitungszwecke benennen.[46] Außerdem müssen die behördlichen Angaben hinreichend verständlich sein. Anderenfalls könnten die Bürger nicht wirklich wissen, wer was wann und bei welcher Gelegenheit über sie weiß.[47]

Dieses Wissen ist Voraussetzung dafür, dass die betroffene Person ihre Rechte – z.B. auf Löschung oder Berichtigung der personenbezogenen Daten – effektiv wahrnehmen kann.[48] Es ermöglicht ihr, die Datenverarbeitung in der Öffentlichkeit zu thematisieren und ihre etwaige Unrecht-

---

42 Das BVerfG entwickelt seine Transparenzanforderungen nicht nur aus dem Recht auf informationelle Selbstbestimmung, sondern auch aus dem Fernmeldegeheimnis (Art. 10 Abs. 1 Var. 3 GG) und dem Recht der Unverletzlichkeit der Wohnung (Art. 13 Abs. 1 GG). Sie stehen zudem in einem engen Zusammenhang zum Recht auf effektiven Rechtsschutz (Art. 19 Abs. 4 GG). Dazu ausführlich *B. Manthey*, Das datenschutzrechtliche Transparenzgebot, Baden-Baden 2020, S. 165 ff.

43 BVerfGE 125, 260 (335 f.).

44 BVerfGE 154, 152 (287).

45 BVerfGE 125, 260 (335); vgl. BVerfGE 100, 313 (361); 109, 279 (363 f.); 118, 168 (207 f.); 120, 351 (361 f.).

46 Vgl. BVerfGE 65, 1 (45).

47 Vgl. BVerfGE 65, 1 (43).

48 BVerfGE 125, 260 (335); vgl. BVerfGE 100, 313 (361); 109, 279 (363); 118, 168 (207 f.); 120, 351 (361).

mäßigkeit aufsichtsbehördlich oder gerichtlich überprüfen zu lassen.[49] Die Kenntnis von der Datenverarbeitung erlaubt der betroffenen Person darüber hinaus, ihr Verhalten anzupassen und z.B. bewusst auf Once-Only zu verzichten.[50] Das Erfordernis einer transparenten Datenverarbeitung verfolgt jedoch nicht nur einen individuellen, sondern auch einen gesamtgesellschaftlichen Zweck. Denn ist die Datenverarbeitung unter Nutzung der Identifikationsnummer hinreichend bekannt, beugt dies Spekulationen über eine heimliche Zusammenführung der Fachregister zu einer Art „Superregister" vor. So kann der Staat das Vertrauen seiner Bürger in den Prozess der Verwaltungsdigitalisierung stärken.[51]

Das Ausmaß der erforderlichen Transparenzmaßnahmen hängt vom Eingriffsgewicht der jeweiligen Verarbeitungsregelungen ab.[52] Auf den ersten Blick ließe sich annehmen, dass für die Registermodernisierung und die Einführung der Identifikationsnummer deutlich niedrigere Anforderungen als für die Antiterrordatei oder die Vorratsdatenspeicherung gelten, die den maßstabsetzenden Entscheidungen des BVerfG zugrunde lagen. Denn bislang stand mit der Leistungsverwaltung ein Bereich im Mittelpunkt der Verwaltungsdigitalisierung, in dem die Datenverarbeitung allgemein als nicht besonders grundrechtssensibel gilt, da sich Bürger ihr leichter entziehen können und aus ihr regelmäßig keine Eingriffe in die Freiheit der Person oder ihr Eigentum erfolgen.[53] Bei näherem Hinsehen erstreckt sich das RegMoG indes – im Gegensatz zum OZG[54] – auch auf die Eingriffsverwaltung. So soll die Identifikationsnummer bspw. in das Bundeszentralregister eingefügt werden (Nr. 27 Anlage zu § 1 IDNrG), aus dem u.a. strafrechtliche Verurteilungen oder gerichtliche Feststellungen zur Betäubungsmittelabhängigkeit hervorgehen. Die Verarbeitung und Verknüpfung derartig sensibler Daten gebietet ein hohes Transparenzniveau.

---

49 BVerfGE 125, 260 (335).

50 Vgl. BVerfGE 133, 277 (366).

51 Vgl. BVerfGE 133, 277 (366).

52 BVerfGE 156, 11 (46). Zur Eingriffsintensität staatlicher Datenverarbeitung siehe BVerfGE 115, 320 (347 ff.).

53 Vgl. *D. Caliebe*, Datenschutz – Allgemeines, in: H. Lühr/R. Jabkowski/S. Smentek (Hrsg.), Handbuch Digitale Verwaltung, Wiesbaden 2019, S. 226 (230 f.); *J. Masing*, Herausforderungen des Datenschutzes, NJW 2012, 2305 (2307); *M.-T. Tinnefeld/B. Buchner/T. Petri/H.-J. Hof*, Einführung in das Datenschutzrecht, 6. Aufl., Berlin 2018, S. 296 ff.

54 *M. Martini*, in: I. von Münch/P. Kunig (Hrsg.), GG, 7. Aufl., München 2021, Art. 91c Rn. 67.

II. Ausgestaltung des Datenschutzcockpits (§ 10 OZG)

Der zentrale Transparenzmechanismus des RegMoG ist das Datenschutzcockpit (zunächst Datencockpit genannt).[55] Seine Rechtsgrundlage wurde als § 10 neu in das OZG eingefügt[56] und tritt ebenfalls erst in Zukunft in Kraft (Art. 22 S. 2 RegMoG). In Bremen wird gleichwohl schon jetzt ein

---

55 BT-Drs. 19/24226, S. 2; *Knauff/Lehmann*, Registermodernisierungsgesetz (Fn. 11), 163.

56 Wortlaut der Vorschrift in ihrer Fassung nach Änderung durch das Gesetz v. 28.6.2021, BGBl. I S. 2250 (2261):
§ 10 Datenschutzcockpit
(1) [1]Ein „Datenschutzcockpit" ist eine IT-Komponente im Portalverbund, mit der sich natürliche Personen Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen anzeigen lassen können. [2]Erfasst werden diejenigen Datenübermittlungen, bei denen eine Identifikationsnummer nach § 5 des Identifikationsnummerngesetzes zum Einsatz kommt.
(2) [1]Im Datenschutzcockpit werden nach Maßgabe von Absatz 4 Satz 3 ausschließlich Protokolldaten nach § 9 des Identifikationsnummerngesetzes einschließlich der dazu übermittelten Inhaltsdaten sowie die Bestandsdaten der Register angezeigt. [2]Diese Daten werden im Datenschutzcockpit nur für die Dauer des jeweiligen Nutzungsvorgangs gespeichert; nach Beendigung des Nutzungsvorgangs sind sie unverzüglich zu löschen. [3]Der Auskunftsanspruch nach Artikel 15 der 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 (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1; L 314 vom 22.11.2016, S. 72; L 127 vom 23.5.2018, S. 2; L 74 vom 4.3.2021, S. 35) bleibt unberührt. [4]Das Datenschutzcockpit ist aus Sicht des Nutzers einfach und zweckmäßig auszugestalten. [5]Es sind technische und organisatorische Maßnahmen vorzusehen, damit staatliche Eingriffe zum Nachteil des Nutzers nicht möglich sind
(3) [1]Jede natürliche Person kann sich bei der öffentlichen Stelle, die das Datenschutzcockpit betreibt, für ein Datenschutzcockpit registrieren. [2]Sie hat sich bei der Registrierung und Nutzung des Datenschutzcockpits mit einem Identifizierungsmittel auf dem Vertrauensniveau hoch zu identifizieren. [3]Zur Feststellung der Identität darf bei Registrierung und Nutzung das dienste- und kartenspezifische Kennzeichen verarbeitet werden. [4]Im Übrigen kann sich der Nutzer auch mit einem Nutzerkonto des Portalverbundes beim Datenschutzcockpit registrieren.
(4) [1]Das Datenschutzcockpit darf die Identifikationsnummer nach § 139b der Abgabenordnung als Identifikator für die Anfrage zur Erhebung und Anzeige der Daten nach Absatz 2 verarbeiten. [2]Zur Anfrage nach § 6 des Identifikationsnummerngesetzes erhebt das Datenschutzcockpit bei der Registrierung des Nutzers folgende Daten:
1. Namen,
2. Vornamen,
3. Anschrift,
4. Geburtsname und
5. Tag der Geburt.

Pilot des Cockpits für ELFE entwickelt, dessen Erprobung sich auf § 11 OZG und Art. 21 RegMoG stützen kann. Wann der Pilot in der Hansestadt einsetzbar sein wird und wann er bundesweit Anwendung finden kann, ist noch offen.

1. De lege lata

Das Datenschutzcockpit ist eine IT-Komponente[57] im Portalverbund, mit der sich natürliche Personen Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen anzeigen lassen können (§ 10 Abs. 1 S. 1 OZG). Dies soll sicherstellen, dass die behördliche Datenverarbeitung nicht heimlich erfolgt. Das BMI bestimmt durch Rechtsverordnung die öffentliche Stelle,[58] die das Cockpit errichtet und betreibt (§ 10 Abs. 5 S. 1 OZG). Damit wird auf die regionale Erprobung ein zentrales Cockpit folgen.

a) Zugang zum Datenschutzcockpit

Es steht jeder natürlichen Person frei, sich für das Datenschutzcockpit zu registrieren (§ 10 Abs. 3 S. 1 OZG). Dabei muss sie ein Identifizierungsmittel auf dem Vertrauensniveau hoch verwenden (§ 10 Abs. 3 S. 2 OZG), z.B. das Nutzerkonto des Portalverbundes (§ 10 Abs. 3 S. 4 OZG), soweit dieses

---

[3]Der Nutzer legt fest, in welchem Umfang das Datenschutzcockpit Protokolldaten einschließlich der übermittelten Inhaltsdaten sowie die Bestandsdaten der Register nach Absatz 2 erheben und anzeigen darf. [4]Auf diese Daten hat nur der Nutzer Zugriff. [5]Der Nutzer muss sein Konto im Datenschutzcockpit jederzeit selbst löschen können. [6]Das Konto im Datenschutzcockpit wird automatisiert gelöscht, wenn es drei Jahre nicht verwendet wurde.

(5) [1]Das Datenschutzcockpit wird von einer öffentlichen Stelle errichtet und betrieben, die durch Rechtsverordnung des Bundesministeriums des Innern, für Bau und Heimat im Benehmen mit dem IT-Planungsrat mit Zustimmung des Bundesrates bestimmt wird. [2]Das Nähere zu den technischen Verfahren, den technischen Formaten der Datensätze und den Übertragungswegen legt das Bundesministerium des Innern, für Bau und Heimat im Benehmen mit dem IT-Planungsrat mit Zustimmung des Bundesrates durch Rechtsverordnung fest.

57 „IT-Komponenten" sind IT-Anwendungen, Basisdienste und die elektronische Realisierung von Standards, Schnittstellen und Sicherheitsvorgaben, die für die Anbindung an den Portalverbund, für den Betrieb des Portalverbundes und für die Abwicklung der Verwaltungsleistungen im Portalverbund erforderlich sind (§ 2 Abs. 6 OZG).

58 Im Benehmen mit dem IT-Planungsrat und mit Zustimmung des Bundesrates.

auf einem entsprechenden Niveau eingerichtet worden ist.[59] Die Verwendung des Cockpits ist folglich fakultativ und insbesondere keine Voraussetzung, um digitale Verwaltungsleistungen beantragen zu können. Staatliche Stellen haben keinen Zugang zum Cockpit (vgl. § 10 Abs. 4 S. 4 OZG). Es sind vielmehr technische und organisatorische Maßnahmen vorzusehen, damit staatliche Eingriffe zum Nachteil der betroffenen Personen ausgeschlossen sind (§ 10 Abs. 2 S. 5 OZG).

b) Angezeigte Daten im Datenschutzcockpit

Im Datenschutzcockpit erhält die betroffene Person eine Übersicht über diejenigen Datenübermittlungen, bei denen ihre Identifikationsnummer zum Einsatz gekommen ist (§ 10 Abs. 1 S. 2 OZG). Damit beschränkt sich das Transparenzkonzept des § 10 OZG auf eine Ex-post-Kontrolle. Die betroffene Person erhält keine Benachrichtigung vor oder zeitgleich zu der Datenverarbeitung, sondern muss sich selbständig einen Kenntnisstand verschaffen. In welchem Umfang sie die Daten angezeigt bekommen will, legt sie ebenfalls individuell fest (§ 10 Abs. 4 S. 3 OZG).

Konkret kann sich die betroffene Person die Protokolldaten nach § 9 IDNrG einschließlich der dazu übermittelten Inhaltsdaten sowie die Bestandsdaten der Register anzeigen lassen (§ 10 Abs. 2 S. 1 OZG).[60] Die Daten stammen einerseits von allen öffentlichen Stellen, zwischen denen Datenübermittlungen unter Nutzung der Identifikationsnummer stattgefunden haben (§ 9 Abs. 1 S. 1 IDNrG).[61] Andererseits stammen sie von der Registermodernisierungsbehörde, die sowohl die bei ihr erfolgten Datenabrufe als auch die Datenübermittlungen zwischen ihr und dem Bundeszentralamt für Steuern erfasst (§ 9 Abs. 1 S. 2 IDNrG). Da das Cockpit nutzerzentriert ausgestaltet sein soll (§ 10 Abs. 2 S. 4 OZG), müssen diese Informationen verständlich aufbereitet sein. Der Datenbestand soll zudem

59 Das Nutzerkonto lässt sich auf einem oder mehreren Vertrauensniveaus einrichten und nutzen (Basisregistrierung/substantielles Vertrauensniveau/hohes Vertrauensniveau).

60 Ursprünglich sollten sich die betroffenen Personen nur die Protokolldaten anzeigen lassen können (BT-Drs. 19/24226, S. 80 f.).

61 Damit beschränken sich die angezeigten Datenübermittlungen nicht auf bereichsübergreifende Datenübermittlungen i.S.v. § 7 Abs. 2 IDNrG, was während des Gesetzgebungsverfahrens noch unklar gewesen war (BfDI, Stellungnahme zum Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz), Bonn 26.8.2020, S. 4).

in Echtzeit einsehbar sein, was sich infolge der Vielzahl an zu verknüpfenden Registern als technisch herausfordernd darstellen dürfte.[62]

c) Speicherort der angezeigten Daten

Für die Speicherung der Daten, die sich im Datenschutzcockpit anzeigen lassen, hat der Bundesgesetzgeber das sogenannte „Quellenmodell" gewählt. Die Daten sind grundsätzlich nur in den „Quellregistern" bei den öffentlichen Stellen und der Registermodernisierungsbehörde gespeichert. Im Cockpit werden die Daten nur für die Dauer des jeweiligen Nutzungsvorgangs gespeichert und anschließend wieder gelöscht (§ 10 Abs. 2 S. 2 OZG). Das Cockpit fungiert somit nicht als eine Art „Datentresor", in dem alle personenbezogenen Daten dauerhaft zentral gespeichert wären.[63] Eine derartige Funktion würde eine Vorratsdatenspeicherung durch die Hintertür einführen.

2. De lege ferenda

Um als Garant einer verfassungskonformen Registermodernisierung dienen zu können, bedarf § 10 OZG noch deutlicher Nachschärfungen.

a) Erweiterung des Anwendungsbereichs (bei gleichzeitiger Verhinderung eines „information overload")

Bislang beschränkt sich der Anwendungsbereich des Datenschutzcockpits darauf, der betroffenen Person die Datenverarbeitung öffentlicher Stellen anzuzeigen (vgl. § 10 Abs. 1 S. 1 OZG). Wie sich jedoch aus § 5 Abs. 1 S. 2 IDNrG und der Gesetzesbegründung[64] ergibt, sollen auch nicht-öffentliche Stellen die Identifikationsnummer verarbeiten dürfen. Dies führt gegenwärtig zu einer Regelungslücke, die es zu schließen gilt. Die Registermodernisierung darf weder in einer Profilbildung durch den Staat noch

62 BT-Drs. 19/24226, S. 80 f.
63 *Guckelberger/Starosta*, Onlinezugangsgesetz (Fn. 10), 1166; vgl. *A. Berger*, Onlinezugangsgesetz und Digitalisierungsprogramm – Auf die Kommunen kommt es an!, KommJur 2018, 441 (443).
64 BT-Drs. 19/24226, S. 36.

durch die Privatwirtschaft münden. Der Transparenzmechanismus muss daher auf nicht-öffentliche Stellen erweitert werden. Dies erfordert zugleich, dass nicht-öffentliche Stellen zukünftig ebenfalls an die Protokollierungspflicht des § 9 Abs. 1 S. 1 IDNrG gebunden sind.

Des Weiteren sollten sich die betroffenen Personen auch grenzüberschreitende Datenübermittlungen im Cockpit anzeigen lassen können.[65] Denn mit der Umsetzung der SDG-VO umfasst der behördliche Datenaustausch nach dem Once-Only-Prinzip potenziell die gesamte Europäische Union. Dies kann der Bundesgesetzgeber zwar nicht einseitig im OZG festlegen, er sollte sich dafür aber auf Unionsebene einsetzen und die notwendigen technischen Voraussetzungen schaffen.

Je mehr Informationen sich im Cockpit abrufen lassen, umso wahrscheinlicher wird indes ein „information overload", d.h. eine intellektuelle Überforderung durch zu viele (ungefilterte) Informationen.[66] Entscheidend für den tatsächlichen Einblick in die behördliche Datenverarbeitung ist daher die Informationsdarstellung. Ausschließlich textbasierte, seitenlange Ausführungen erschweren regelmäßig das Verständnis, was dem Transparenzziel des § 10 OZG zuwiderliefe. „Icons" könnten hingegen ein niedrigschwelliger Lösungsansatz sein, um die Komplexität der Informationen zu reduzieren. Das Cockpit sollte der betroffenen Person sowohl derartige Vereinfachungen als auch umfassende Informationen anzeigen können.

b) Erweiterung der Anwendungsmöglichkeiten

Über das Datenschutzcockpit sollten sich neben dem Auskunftsanspruch aus § 10 OZG auch die allgemeinen datenschutzrechtlichen Betroffenenrechte (Art. 12 ff. DSGVO) ausüben lassen. Es erleichterte den Individualrechtsschutz nachhaltig, wenn die betroffenen Personen mithilfe derselben Anwendung zugleich den umfassenderen Auskunftsanspruch aus Art. 15 DSGVO, der von der nationalen Regelung unberührt bleibt (§ 10

65 *P. Parycek/V. Huber/S. S. Hunt/A.-S. Novak/B. E. P. Thapa*, Analyse der rechtlich-technischen Gesamtarchitektur des Entwurfs des Registermodernisierungsgesetzes, BT-Ausschuss-Drs. 19(4)667D, Berlin 2020, S. 21.

66 Zum Phänomen des „information overload" siehe bspw. *G. K. Ebner*, Information Overload 2.0?, ZD 2022, 364 (365 f.) und *D. M. Levy*, Information Overload, in: K. E. Himma/H. T. Tavani (Hrsg.), The Handbook of Information and Computer Ethics, New York 2008, S. 497 ff.

Abs. 2 S. 3 OZG)[67] und z.B. auch das Löschungs-, Berichtigungs- und Widerspruchsrecht geltend machen könnten.

Ein integrierter Informationskanal zu den Datenschutzbehörden würde zusätzlich eine niedrigschwellige Unterstützung bei der Rechtsdurchsetzung ermöglichen. Betroffene Personen könnten ihr Beschwerderecht aus Art. 77 DSGVO mit wenigen Klicks ausüben, sobald sie Datenschutzverstöße vermuten. Außerdem sollten sie Informationen nicht nur zu dem Zeitpunkt erlangen können, in dem sie das Cockpit aktiv nutzen. Vielmehr sollte das Cockpit über eine Benachrichtigungsfunktion verfügen, um die betroffene Person in Echtzeit über solche Datenübermittlungen zu informieren, die sie vorher entsprechend ausgewählt hat.[68]

c) Einheitlicher Datenaustauschstandard

Für ein hohes Transparenzniveau müssen die im Datenschutzcockpit angezeigten Daten richtig und vollständig sein. Daher muss das Cockpit alle Datensätze ordnungsgemäß verarbeiten können. Dies stellt eine erhebliche Herausforderung dar, da grundsätzlich alle registerführenden Stellen (d.h. tausende Behörden unterschiedlicher Hoheitsträger) in der Lage sein müssen, ihre Daten an das Cockpit übermitteln zu können. Einen einheitlichen Datenaustauschstandard gibt es indes noch nicht.[69] Es existieren zwar bereits verschiedene Austauschstandards auf Grundlage des textbasierten Datenformats „XML in der öffentlichen Verwaltung" (XÖV). Diese kommen bislang aber nur für spezifische Fachverfahren innerhalb geschlossener Informationsverbünde zur Anwendung, etwa „XMeld" im Meldewesen.

Infolgedessen drohen fehlerhafte oder unvollständige Auskünfte im Cockpit. Der Bundesgesetzgeber hat auf diese Problematik noch nicht ausreichend reagiert. Während Datenabrufe bei der Registermodernisierungsbehörde nach einem einheitlichen Datenaustauschstandard erfolgen sollen (§ 7 Abs. 1 S. 1 IDNrG), fehlt eine entsprechende Vorgabe für die sonstigen Datenübermittlungen unter Nutzung der Identifikationsnummer. Es ist in erster Linie dem BMI überlassen, mittels Rechtsverordnung das Nähere zu

---

67 Zur notwendigen Unterscheidung der beiden Auskunftsansprüche siehe BfDI, Einführung einer Identifikationsnummer (Fn. 61), S. 12.

68 Vgl. *Martini*, Transformation der Verwaltung (Fn. 39), 452.

69 *M. Klein*, Gesucht wird ein übergreifender Standard, eGovernment Computing v. 12.4.2022, abrufbar unter https://www.egovernment-computing.de/gesucht-wird-ein-uebergreifender-standard-a-1110389/ (zuletzt abgerufen: 11.12.2022).

den technischen Verfahren, Datenformaten und Übertragungswegen zu regeln (§ 10 Abs. 5 S. 2 OZG). Bis es einen Standard für alle Übermittlungen gibt, sollte diese Rechtsverordnung vorsehen, dass das Cockpit über eine Komponente verfügen muss, die abweichende Standards übersetzen kann.[70]

d) Speicherdauer der Daten

Derzeit ist offen, über welchen Zeitraum sich die Daten im Datenschutzcockpit anzeigen lassen. Denn die Protokolldaten sind grundsätzlich nur zwei Jahre aufzubewahren und danach unverzüglich zu löschen (§ 9 Abs. 3 S. 1 Hs. 1 IDNrG). Zwar können die Daten auch länger gespeichert bleiben, um die Nutzung des Cockpits zu ermöglichen (§ 9 Abs. 3 S. 1 Hs. 2 i.V.m. Abs. 2 IDNrG). Eine konkrete Speicherdauer ist aber gesetzlich nicht vorgesehen.[71]

Aus dieser Regelungslücke erwachsen zwei Risiken. Auf der einen Seite könnten der betroffenen Person Verarbeitungsvorgänge verborgen bleiben, wenn sie das Cockpit nur selten nutzt[72] und ältere Datensätze bereits gelöscht sind. Auf der anderen Seite führte eine unbegrenzte Speicherdauer dazu, dass Dritte im Falle unberechtigter Datenzugriffe wesentlich umfangreichere Datensätze erlangen könnten. Angesichts dieses Spannungsfeldes zwischen Transparenz und Datenschutz wäre es vorzugswürdig, gesetzlich zu verankern, dass grundsätzlich der betroffenen Person die Entscheidung über die Speicherdauer zukommt. Nur wenn sie keine Entscheidung trifft, sollte eine gesetzliche Aufbewahrungs- bzw. Löschungsfrist greifen. Diese sollte der Bundesgesetzgeber präzise bestimmen, um die Rechtssicherheit zu erhöhen.

e) Datenschutzrechtliche Verantwortlichkeit

Damit das Datenschutzcockpit den betroffenen Personen Auskunft zu staatlichen Verarbeitungsvorgängen gewähren kann, ist es erforderlich,

---

70 *Parycek/Huber/Hunt/Novak/Thapa*, Registermodernisierungsgesetz (Fn. 65), S. 20.

71 Auch in dieser Hinsicht könnte die Rechtsverordnung nach § 10 Abs. 5 S. 2 OZG mehr Rechtsklarheit ermöglichen.

72 Nutzt die betroffene Person das Cockpit länger als drei Jahre nicht, wird es gelöscht (§ 10 Abs. 4 S. 6 OZG).

dass erneut personenbezogene Daten verarbeitet werden. Es muss daher Klarheit darüber bestehen, wer für diese Datenverarbeitung nach Art. 4 Nr. 7 Hs. 1 DSGVO verantwortlich ist. Denn der bzw. die Verantwortlichen haben die Einhaltung der datenschutzrechtlichen Pflichten sicherzustellen, d.h. insbesondere die Betroffenenrechte zu wahren. Die Verantwortlichkeit richtet sich nach den tatsächlichen Einflussnahmemöglichkeiten auf die Zwecke und Mittel der Datenverarbeitung.[73] Ist nur eine Stelle an der Datenverarbeitung beteiligt, liegt es mithin auf der Hand, dass sie verantwortlich ist.

Die Datenverarbeitung für die Auskunft im Cockpit zeichnet sich jedoch durch eine besondere Akteursvielfalt aus: Neben der Registermodernisierungsbehörde sind potenziell tausende Bundes-, Landes- und Kommunalbehörden an der Verarbeitung beteiligt. Deshalb muss der Bundesgesetzgeber einem Transparenz- und Datenschutzdefizit vorbeugen. § 10 OZG lässt die Verantwortlichkeit indes noch unerwähnt und § 8 IDNrG findet keine Anwendung, da er nur die Verantwortlichkeit für Datenabrufe bei der Registermodernisierungsbehörde regelt.[74] Allein aus der Gesetzesbegründung ergibt sich (wenn auch unverbindlich), dass die übermittelnden Stellen für die Richtigkeit der Auskunft verantwortlich sein sollen.[75] Gänzlich unbeantwortet bleibt demgegenüber die Frage, wer für die weitere Datenverarbeitung – insbesondere im Rahmen der Registrierung (vgl. § 10 Abs. 4 OZG) – verantwortlich ist.

Verantwortlicher könnte die Stelle sein, die das Cockpit betreibt (§ 10 Abs. 5 S. 1 OZG). Diese könnte aber auch nur als Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO) derjenigen Stellen fungieren, die die Verwaltungsportale des Bundes und der Länder betreiben. Letztere wären dann allein verantwortlich. Denkbar wäre außerdem eine gemeinsame Verantwortlichkeit der genannten Stellen (Art. 26 Abs. 1 S. 1 DSGVO).[76] Ent-

73 *C. Böllhoff/J. Botta*, Das datenschutzrechtliche Verantwortlichkeitsprinzip als Herausforderung für die Verwaltungsdigitalisierung, NVwZ 2021, 425 (426); *K. Schreiber*, Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden, ZD 2019, 55 (56).

74 Ebenfalls keine definitive Klärung bietet § 9c Abs. 2 EGovG Bund, der die Verantwortlichkeit für die Datenverarbeitung im Bundesverwaltungsportal grundsätzlich der Stelle zuordnet, die es betreibt. Wie sich diese Regelung zur Datenverarbeitung im Zusammenhang mit dem Cockpit verhält, bleibt fraglich, solange offen ist, auf welche Weise die IT-Komponente in den Portalverbund eingebunden sein wird.

75 BT-Drs. 19/24226, S. 80.

76 Der EuGH hat diese Rechtsfigur bislang sehr extensiv auslegt. Siehe seine st. Rspr.: Urt. v. 5.6.2018, Rs. C-210/16 (Wirtschaftsakademie SH), ECLI:EU:C:

scheidend ist letztendlich, wie die IT-Komponente in den Portalverbund eingebunden sein wird.[77] Um bei der technischen Entwicklung des Cockpits von Anfang an klare Verantwortungssphären sicherzustellen, sollte der Bundesgesetzgeber den oder die Verantwortlichen vorab gesetzlich bestimmen (Art. 4 Nr. 7 Hs. 2 DSGVO).[78] Dadurch lässt sich verhindern, dass die später als verantwortlich ausgewiesene Stelle und die datenschutzrechtlich tatsächlich (mit-)verantwortliche Stelle nicht übereinstimmen.

III. Notwendigkeit weiterer Schutzmechanismen

Auch wenn der Bundesgesetzgeber die vorgeschlagenen Ergänzungen des Datenschutzcockpits umsetzen sollte, der Transparenzmechanismus allein vermag es nicht, die Datenschutzrisiken der Registermodernisierung auf ein angemessenes Maß zu reduzieren.[79] Die bloße Ex-post-Kontrolle im Cockpit kann nicht verhindern, dass unrechtmäßige Datenverknüpfungen erfolgen, sondern hilft lediglich dabei, diese aufzuklären.

Es braucht daher auch ex ante wirkende Schutzmechanismen. Als ein solcher soll vorrangig das 4-Corner-Modell dienen. Kritisch ist indes zu sehen, dass es nur bei bereichsübergreifenden Datenübermittlungen zur Anwendung kommen soll.[80] Die in der Gesetzesbegründung genannten Bereiche sind vergleichsweise weit gefasst und es obliegt der Exekutive, die Bereiche festzulegen (§ 12 Abs. 1 S. 1 IDNrG). Dies birgt das Risiko, dass sehr viele Datenübermittlungen als bereichsintern gelten werden. Bei bereichsinternen Datenübermittlungen schützt jedoch allein das Cockpit die betroffenen Personen. Das ist unzureichend, da sich in diesen Fällen der Grundrechtsschutz de facto auf die Bürger verlagert. Die Nutzerakzeptanz des Cockpits ist zudem noch ungewiss.

2018:388, Rn. 25 ff.; Urt. v. 10.7.2018, Rs. C-25/17 (Jehovan todistajat), ECLI:EU:C:2018:551, Rn. 63 ff.; Urt. v. 29.7.2019, Rs. C-40/17 (Fashion ID), ECLI:EU:C:2019:629, Rn. 64 ff. Kritisch dazu *Böllhoff/Botta*, Datenschutzrechtliches Verantwortlichkeitsprinzip (Fn. 73), 427.

77 BfDI, Einführung einer Identifikationsnummer (Fn. 61), S. 13.

78 Zu den Voraussetzungen einer mitgliedstaatlichen Festlegung der datenschutzrechtlichen Verantwortlichkeit siehe *Böllhoff/Botta*, Datenschutzrechtliches Verantwortlichkeitsprinzip (Fn. 73), 429 f.

79 *Sorge/von Lucke/Spiecker gen. Döhmann*, Registermodernisierung (Fn. 24), S. 24.

80 Darüber hinaus bietet das 4-Corner-Modell keinen Schutz vor unberechtigten Datenzugriffen. Siehe BfDI, Stellungnahme zum Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz), Bonn 21.10.2020, S. 5.

D. Fazit

Mit dem OZG und dem RegMoG hat der Bundesgesetzgeber die Weichen für die Zukunft der öffentlichen Verwaltung gestellt. Dafür greift er auch in die informationelle Selbstbestimmung ein. Die Registermodernisierung soll indes keine „gläsernen Bürger" hervorbringen, sondern vorrangig eine effizientere Verwaltungspraxis ermöglichen und zugleich den Staat selbst noch durchsichtiger werden lassen. Die Einlösung dieses Transparenzversprechens ist maßgebend für eine verfassungskonforme Registermodernisierung (wenn auch nicht ihre alleinige Garantie[81]).

Damit das Datenschutzcockpit aber seiner Bedeutung als zentraler Transparenzmechanismus gerecht werden kann, muss der Bundesgesetzgeber seine Potenziale voll ausschöpfen. Insbesondere ist sein Anwendungsbereich zu erweitern (ohne zugleich einen „information overload" zu bewirken). Außerdem bedarf es zusätzlicher Anwendungsmöglichkeiten, eines einheitlichen Datenaustauschstandards, einer grundsätzlichen Entscheidungsfreiheit über die Speicherdauer und der Klärung der datenschutzrechtlichen Verantwortlichkeit.

81 Siehe Fn. 36.