Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)667 E

Hochschule der Akademie der Polizei Hamburg, Carl-Cohn-Straße 39,
22297 Hamburg

An den
Ausschuss für Inneres und Heimat
im Deutschen Bundestag
Platz der Republik 1
11011 Berlin

Prof. Eike Richter, ORR
Dekan
Professur für Öffentliches Recht,
insbesondere Recht der Digitalisierung
und IT-Sicherheitsrecht
Hochschule der Akademie der Polizei
Hamburg
Carl-Cohn-Straße 39, 22297 Hamburg
Tel.: +49(0)40-4286-24400
eike.richter@poladium.de

13. Dezember 2020

Gutachterliche Stellungnahme zum Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz – RegMoG; Drucksache 19/24226)

Sehr geehrte Frau Vorsitzende,
sehr geehrte Damen und Herren Abgeordnete,

ich danke für die Gelegenheit zur Stellungnahme zum genannten Gesetzentwurf.

Nach allgemeinen Erwägungen zum Gesetzentwurf (dazu A.), wird zunächst auf Regelungen eingegangen, die das vorgeschlagene, registerübergreifende Identitäts- und Datenmanagements kennzeichnen (dazu B.). Im Anschluss werden sonstige, einzelne Vorschriften thematisiert (dazu C.). Redaktionelle Hinweise zum Gesetzentwurf finden sich gesammelt zum Schluss der Stellungnahme (dazu D.).

Um in der vorliegenden Stellungnahme Vorschriften des vorliegenden Gesetzentwurfs von geltenden Vorschriften unterscheiden zu können, sind erstere mit einem „-E“ in der Gesetzesbezeichnung ergänzt (z.B. § 10 OZG-E). Seitenzahlen ohne Quellenangaben beziehen sich auf den Gesetzentwurf der Bundesregierung (Drucksache 19/24226).

Im Rahmen der Anhörung gehe ich gerne auf einzelne Punkte ein.

Akademie der POLIZEI Hamburg Fachhochschule

Überblick

A. Allgemeines ... 3

B. Zu Vorschriften, die das vorgeschlagene Modell eines registerübergreifenden Identitäts- und Datenmanagements kennzeichnen ... 5

I. Anpassungsbedarf am Maßstab der Datenschutz-Grundverordnung ... 5

1. Grundsatz der Datenminimierung ... 6

2. Grundsatz der Zweckbestimmung und -bindung ... 7

3. Grundsatz der Transparenz ... 8

4. Grundsatz der Datenqualität und -richtigkeit ... 8

II. Anpassungsbedarf am Maßstab des Grundrechts auf informationelle Selbstbestimmung ... 9

1. Absolute verfassungsrechtliche Unzulässigkeit einer einheitlichen registerübergreifenden Identifikationsnummer? ... 10

a. Maßstab ... 11

b. (Noch keine) Allgemeinheit des Personenkennzeichens ... 11

c. Prognose- und Einschätzungsprärogative des Gesetzgebers und die daran anzulegenden Sorgfalt ... 12

2. Zur Verhältnismäßigkeit des registerübergreifenden Identitäts- und Datenmanagements ... 14

a. Legitimität der Ziele ... 14

b. Geeignetheit und Erforderlichkeit ... 15

(1) Absehen von Maßnahmen? ... 16

(2) Verzicht auf die Verwendung einer gemeinsamen Identifikationsnummer? ... 16

(3) Verwendung bereichsspezifischer Personenkennzeichen? ... 17

(3) Verwendung eines anderen einheitlichen Personenkennzeichens als die Steuer-ID? ... 19

(4) Erneut: Sorgfältige Ausübung der Prognose- und Einschätzungsprärogative ... 19

c. Angemessenheit ... 20

(1) Ausweitung des 4-Corner-Modells ... 20

(2) Konkretisierung der Zweckbindung ... 20

(3) Reduzierung und Auswahl der einzubeziehenden Register ... 21

(4) Festlegung der Bereiche ... 22

(5) Ausbau technischer Schutzmechanismen ... 23

(6) Ausbau des Datencockpits ... 24

C. Weitere Einzelpunkte ... 25

I. Einwilligung in den Datenaustausch ... 25

II. Ausweitung der Evaluierungsvorgaben ... 26

III. Befristung des Gesetzes ... 27

D. Redaktionelle Hinweise ... 27

A. Allgemeines

Der vorgelegte Entwurf dient der Vereinfachung des Verwaltungskontakts zwischen Behörde und Bürger:innen. Hierzu soll die 2007 eingeführte Steueridentifikationsnummer (BGBl. 2006 S. 2726 ff.) als allgemeine Kennziffer in viele andere Verwaltungsbereiche übernommen werden. Die einzurichtende Registermodernisierungsbehörde würde zentral die Daten der natürlichen Personen verwalten und den Behörden bei Anfragen zur Verfügung stellen, um mehrfache Nachweise und Angaben persönlicher Informationen zur Identifizierung überflüssig zu machen.

Es besteht ein verbreitetes Einvernehmen, dass es einer schnelleren Umsetzung der Digitalisierung der Verwaltung bedarf und dass dabei der Registermodernisierung eine zentrale Bedeutung zukommt. Dem ist grundsätzlich zuzustimmen, wobei gerade der vorliegende Gesetzentwurf und die bislang geäußerten Einschätzungen daran erinnern, dass zugunsten der Schnelligkeit keine Abstriche in der fachlichen Qualität in Kauf genommen werden sollten. Eine ausführlichere parlamentarische und fachliche Befassung wäre insoweit wünschenswert gewesen. Der vorliegende Gesetzentwurf weitet zudem die „Parallelgesetzgebung“ und Regelungszersplitterung im Allgemeinen Verwaltungsverfahrensrecht weiter aus, wie sie mit den E-Government-Gesetzen von Bund und Ländern (EGovGe) und dem OZG ihren Anfang nahmen und einer sicheren und handhandbaren Rechtsanwendung nicht zuträglich sind. Die mit dem Gesetzentwurf vorgelegten Regelungsgegenstände der Digitalisierung betreffen, ebenso wie die meisten geltenden Regelungen der EGovGe des Bundes und der Länder und des OZG, das Verwaltungsverfahren im Allgemeinen und gehören damit in eine Reform der allgemeinen Verwaltungsverfahrensgesetze. Dies zeigt etwa der Vorschlag, mit der Steuer-ID ein Element aus dem allgemeinen (!) Steuerverfahrensrecht (§ 139b AO) in ein „spezielles“ Verwaltungsgesetz zu übernehmen, das aber die Verwaltung im Allgemeinen betrifft.

Die Wesentlichkeit vieler, im vorgelegten Entwurf aufgeworfener Regelungsgegenstände sprechen zudem für eine stärkere Regulierung unmittelbar auf Gesetzesebene. Dagegen

arbeitet der vorgelegte Gesetzentwurf wie auch schon das OZG in seiner geltenden Fassung mit einer Auslagerung der Regulierung auf die untergesetzliche Ebene, insbesondere auf die Verordnungsebene.

Weil es auf der anderen Seite – beinahe 30 Jahre nach der kommerziellen Öffnung des Internets – *wirklich* Zeit ist, die Chancen und Potenziale der Digitalisierung für die Verwaltung stärker als bisher nutzbar zu machen und die Reformgeschwindigkeit zu erhöhen, ist der vorgelegte Gesetzentwurf grundsätzlich zu begrüßen. Eine weitere Verzögerung – in Hinblick auf die vorangeschrittene Legislaturperiode dann womöglich um Jahre – ist aus reformerischer und innovationsbezogener Perspektive kaum hinnehmbar. Dies darf allerdings nicht dazu führen, dass verfassungsrechtliche Grenzen überschritten und sonstige Risiken nicht so gut wie möglich vorgebeugt werden. Diese Risiken und verfassungsrechtlichen Bedenken wurden seit Bekanntwerden des Gesetzentwurfs von vielen Seiten, teilweise auch sehr eindringlich formuliert (StN *Sorge* unter Verweis auf *Sorge/v. Lucke/Spiecker gen. Döhmann*, Registermodernisierung, Datenschutzkonforme und umsetzbare Alternativen; Stellungnahme des BfDI vom 21.10.2020; Wissenschaftliche Dienste des Bundestags, Ausarbeitung WD 3 – 3000 - 196/20).[1]

In diesem Sinne konzentriert sich die Stellungnahme darauf, Standpunkte und – nach Möglichkeit – Vorschläge zu unterbreiten, die den bislang aufgeworfenen Erwägungen, Bedenken und Risiken Rechnung tragen können. Diese knüpfen auf zwei Ebenen an: Zum einen an der Regulierung des vorgeschlagenen Modells eines registerübergreifenden Identitäts- und Datenmanagements selbst (dazu vor allem B.), zum anderen an der Methode und dem Vorgehen der gesetzlichen Steuerung, etwa im Hinblick auf Mechanismen zur Absicherung gesetzgeberischer Eigenkontrolle (dazu vor allem C.). Gerade mit dem zuletzt genannten Anknüpfungspunkt kann Unsicherheiten begegnet werden, die stets mit technischen Entwicklungen verbunden sind und insbesondere in derartig

[1] Bei der Erstellung dieser Stellungnahme konnten neben den Dokumenten der am Gesetzgebungsverfahren beteiligten Organe insbes. schon verschiedene Arbeitspapiere, Positionen, Gutachten und Stellungnahmen berücksichtigt werden, soweit sich konkret mit dem vorliegenden Gesetzentwurf befassen, so insbesondere *Martini/Wagner/Wenzel*, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, 2017; *Sorge/v. Lucke/Spiecker gen. Döhmann*, Registermodernisierung, Datenschutzkonforme und umsetzbare Alternativen; Stellungnahme des BfDI vom 21.10.2020; Wissenschaftliche Dienste des Bundestags, Ausarbeitung WD 3 – 3000 - 196/20StN; *Berger*, BV kommunale Spitzenverbände, 19(4)667A; StN *Sorge*, 19(4)667 C; StN Bundessteuerberaterkammer; ergänzende StN NKR, 19(4)670. Der Verfasser dankt seinen Mitarbeitern Jannes Matzen und Lennart Feix für die wertvolle Unterstützung.

innovationsdynamischen Bereichen wie der Digitalisierung unvermeidbar auf verfassungsrechtliche Bewertungen durchschlagen. Dies steht wiederum in einem unmittelbaren Zusammenhang mit der sorgfältigen Ausfüllung der gesetzgeberischen Einschätzungs- und Prognoseprärogative, die – wie die Stellungnahme zeigt – von besonderer Bedeutung für die verfassungsrechtliche Bewertung des vorgelegten Gesetzentwurfs ist.

B. Zu Vorschriften, die das vorgeschlagene Modell eines registerübergreifenden Identitäts- und Datenmanagements kennzeichnen

Der vorgelegte Gesetzentwurf statuiert durch das Zusammenspiel verschiedener Regelungen ein spezifisches Modell eines registerübergreifenden Identitäts- und Datenmanagements. Ob und in welcher Hinsicht der Gesetzentwurf in seinem Grundansatz oder auch nur in einzelnen Regelungen anpassungsbedürftig ist, richtet sich vor allem danach, ob und inwieweit dieser in der vorliegenden Fassung den Anforderungen höherrangigen Rechts, namentlich der Datenschutz-Grundverordnung (dazu I.) und des Grundrechts auf informationelle Selbstbestimmung (dazu II.) genügt.

I. Anpassungsbedarf am Maßstab der Datenschutz-Grundverordnung

Die Regelungen des RegMoG-E zur automatisierten Verarbeitung von personenbezogenen Daten wie der Steuer-ID in Registern öffentlicher Stellen müssen den Anforderungen der DSGVO genügen, vgl. Art. 2 Abs. 1 i.V.m. 4 Nr. 1 DSGVO. Besondere Anforderungen an nationale Kennziffern oder Kennzeichen von allgemeiner Bedeutung werden in Art. 87 DSGVO gestellt. Hiernach ist die Verarbeitung einer Kennziffer durch die Mitgliedstaaten mit der Verordnung vereinbar, sofern ein Mindestschutzniveau im Sinne des Art. 87 S. 2 DSGVO eingehalten wird. Die im RegMoG-E vorgesehene Identifikationsnummer ist als Kennzeichen von allgemeiner Bedeutung einzustufen, womit der Entwurf an den geforderten Schutzstandards in Bezug auf die Wahrung geeigneter Garantien für die „Rechte und Freiheiten der betroffenen Personen“ zu messen ist (vgl. *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 21). Ob diese materiellen Anforderungen an das Schutzniveau durch die im aktuellen Entwurf vorgesehenen Garantien eingehalten werden, erscheint jeden-

falls nicht zweifelsfrei. Derartige Garantien können gesetzlicher, technischer und organisatorischer Natur sein (*Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann, Art. 87 Rn. 23). Für eine Vereinbarkeit mit Art. 87 DSGVO sprechen im Ergebnis unter anderem die vorgesehene Zweckbindung, die Sanktionstatbestände und Schutzmaßnahmen wie das 4-Corner-Modell. Teilweise wird auch unter Hinweis auf die unkonkrete Norm lediglich ein Minimum an Garantien gefordert, was der Gesetzentwurf einhalten dürfte (vgl. *v. Lewinski*, S. 3). Dagegen wird jedoch angeführt, dass zum Einen die technischen Sicherungen noch zu konkretisieren sind (etwa durch Verordnungen des BMI, vgl. § 12 Abs. 2 IDNrG-E, siehe dazu II. 2. b. (3)) und zum Anderen die Zweckbindung durch die Verknüpfung der Vielzahl von Registern faktisch unterlaufen werden könne (vgl. *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 22).

Auch wenn der vorgelegte Gesetzentwurf bereits eine Reihe der gebotenen Sicherungen und Garantien enthält (so auch StN NKR, S. 1 f.; *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 22), sollten alle weiteren Möglichkeiten ergriffen werden, den datenschutzrechtlichen Prinzipien des Art. 87 S. 2 DSGVO und auch des – weiterhin zu berücksichtigenden (*Martini/Wagner/Wenzel*, S. 7) – Art. 5 DSGVO Rechnung zu tragen. Dies betrifft insbesondere die Datenminimierung, die Zweckbindung, die Transparenz und die Datenqualität bzw. -richtigkeit (ausführlich zum Folgenden auch *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 23 f.).

1. Grundsatz der Datenminimierung

In Hinblick auf den Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit. c DSGVO und den verfolgten Zwecken des Gesetzentwurfs erscheint die Erhebung des letzten Verwaltungskontakts nach § 4 Abs. 3 Nr. 2 IDNrG-E als ungerechtfertigt (vgl. Stellungnahme GI, S. 6). Auch die Begründung des Gesetzentwurfs (S. 77: „Lebenszeichen“) vermag insoweit nicht zu überzeugen.

§ 4 Abs. 3 Nr. 2 IDNrG-E sollte ersatzlos gestrichen werden.

Ebenfalls aus Gründen der Datenminimierung sollte geprüft werden, ob es nicht regelmäßig ausreicht, sich im Hinblick auf das Basisdatum „Staatsangehörigkeiten“ (§ 4 Abs. 2 Nr. 8 IDNrG-E) bei Abfragen bzw. „Abrufen“ auf die Mitteilung zu beschränken, ob es

sich um einen deutschen, einen EU- oder einen Nicht-EU-Staatsbürger handelt (vgl. *Martini/Wagner/Wenzel*, S. 10):

> *In § 6 IDNrG-E könnte unter Verschiebung der Folgeabsätze ein neuer Absatz 3 eingefügt werden:*
> *„Der Abruf und die Übermittlung des Datums nach Absatz 2 Nummer 8 ist auf eine Zuordnung zu den Kategorien der deutschen, der EU- und Nicht-EU-Staatbürgerschaft zu beschränken, soweit für die Aufgabenerfüllung nicht die Kenntnis der Staatsangehörigkeit erforderlich ist.*

Die Datenminimierung gebietet es schließlich, keine Register einzubinden, die bei der Erbringung von Verwaltungsleistungen nicht benötigt werden, wie dies etwa für das Gesamtverzeichnis bei der Bundesrechtsanwaltskammer (IDNrG-E Anlage Nr. 46) angemerkt wurde (vgl. Stellungnahme BRAK, S. 2 f.). Die in der Anlage zum IDNrG-E genannten Register sollten im Zweifel nochmal im Hinblick auf ihre Relevanz für Verwaltungsleistungen überprüft werden.

> *In Ziffer 46 der Anlage zum IDNrG-E sollten die Worte „und Gesamtverzeichnis der Bundesrechtsanwaltskammer nach § 31 der Bundesrechtsanwaltsordnung“ ersatzlos gestrichen werden.*

2. Grundsatz der Zweckbestimmung und -bindung

Personenbezogene Daten müssen gemäß Art. 5 Abs. 1 lit. b DSGVO für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden. In dieser Hinsicht wurden ernst zu nehmende Bedenken gegen den vorgelegten Gesetzentwurf erhoben (Art. 29 Working Party, S. 16; BfDI, S. 9; *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 23 f.), die letztlich bemängeln, dass die Eingrenzungsfunktion, die über die Zweckbestimmtheit erreicht werden soll, kaum gewahrt ist. Die einschlägigen Vorschriften wie §§ 1, 5 Abs. 1 Nr. 1 und 2 IDNrG-E sind zu unbestimmt, wenn man die Eingriffsintensität berücksichtigt. Vor diesem Hintergrund wird zu Recht vorgeschlagen, der Identifikationsnummer einen einzigen Zweck zuzuordnen, nämlich die Identifikation von natürlichen Personen gegenüber der Verwaltung (BfDI, S. 9), sowie ausdrücklich darauf hinzuweisen, dass die Identifikationsnummer auch nur zu diesem Zweck verarbeitet werden darf (vgl. DRV 2020, S. 10).

§ 5 Abs. 1 IDNrG-E sollte um einen folgenden Satz 2 ergänzt werden:
„Die Verarbeitung der Identifikationsnummer durch öffentliche und nicht-öffentliche Stellen zu anderen Zwecken ist außer in den gesetzlich oder der Verordnung (EU) 2016/679 vorgesehenen Fällen unzulässig.“

3. Grundsatz der Transparenz

Art. 5 Abs. 1 lit. a Alt. 3 DSGVO sieht vor, dass personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen. Das RegMoG-E reagiert hierauf mit der Einführung des Datencockpits (§§ 10, 11 OZG-E), worüber es für den Bürger möglich wird, die ihn betreffenden Datenverarbeitungen mit der Identifikationsnummer nachzuvollziehen. Es ist zu begrüßen, dass auf Hinweis des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI, S. 10) mit § 10 Abs. 2 S. 2, 2. HS und S. 3 OZG-E eine Regelung nachgeschoben wurde, welche die Aufbewahrung der Daten auf die Dauer der jeweiligen Nutzersession begrenzt. Allerdings sollten auch vor den Hintergrund des Grundrechts auf informationelle Selbstbestimmung ein weiterer funktionaler Ausbau des Datencockpits unbedingt erwogen werden (s. dazu noch II. 2. b (6) und den dortigen Vorschlag).

4. Grundsatz der Datenqualität und -richtigkeit

Gemäß Art. 5 Abs. 1 lit. d DSGVO müssen personenbezogene Daten sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. § 1 Nr. 2 INrG-E erklärt die Verbesserung der Datenqualität zum ausdrücklichen Ziel des Gesetzentwurfs. In der Konsequenz enthält der Gesetzentwurf mit § 10 IDNrG-E auch konkrete Festlegungen – etwa zu Zuständigkeiten für die Qualitätssicherung des Systems und der Daten oder zur Bereinigung von Mehrfach-, Über- und Unterdatenerfassungen, damit die Datenqualität auch tatsächlich gewährleistet werden kann (kritisch Databund 2020, S. 2; *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 24).

II. Anpassungsbedarf am Maßstab des Grundrechts auf informationelle Selbstbestimmung

Soweit – wie vorliegend im Fall des Art. 87 DSGVO – das Handeln der Mitgliedsstaaten nicht vollständig durch das Unionsrecht vorbestimmt ist, verbleibt dem deutschen Gesetzgeber ein Gestaltungsspielraum, ob und wie er Kennzeichen von allgemeiner Bedeutung reguliert. Selbstverständlich bleibt er dabei an das nationale Verfassungsrecht gebunden (vgl. BVerfG, NJW 2020, S. 314). Das mit dem Gesetzentwurf vorgelegte Modell eines registerübergreifenden Identitäts- und Datenmanagements samt Einführung einer registerübergreifenden einheitlichen Identifikationsnummer muss sich dabei vor allem am Maßstab des Allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG in seiner Ausprägung als Recht auf informationelle Selbstbestimmung messen lassen.

Das Recht auf informationelle Selbstbestimmung gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen (BVerfGE 65, 1 [43]). Es trägt Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich unter den Bedingungen moderner Datenverarbeitung aus informationsbezogenen Maßnahmen ergeben (vgl. BVerfGE 65, 1 [42 f.]; 118, 168 [184]; Beschl. v. 10.11.2020 – 1 BvR 3214/15, Rn. 71). Das mit dem vorgelegten Gesetzentwurf beabsichtige Modell eines registerübergreifenden Identitäts- und Datenmanagements greift sowohl in seinen einzelnen Elementen – insbesonder mit der Einführung einer Identifikationsnummer (§ 1 IDNrG-E), deren Speicherung in 56 Registern (§ 1 IDNrG-E i.V.m. Anlage) und dem Verfahren des Datenabrufs und -übermittlung (§§ 6 f. IDNrG-E) – als auch in seiner Gesamtfunktionalität in das Recht auf informationelle Selbstbestimmung ein (vgl. S. 62).

Das Recht auf informationelle Selbstbestimmung ist allerdings nicht schrankenlos gewährleistet. Der Einzelne muss Einschränkungen durch oder aufgrund eines Gesetzes hinnehmen, soweit dies durch überwiegendes Allgemeininteresse gerechtfertigt wird.

1. Absolute verfassungsrechtliche Unzulässigkeit einer einheitlichen registerübergreifenden Identifikationsnummer?

Eine solche Rechtfertigung durch überwiegendes Allgemeininteresse scheidet allerdings von vornherein aus, wenn die vom Gesetzentwurf vorgesehene Einführung und Verwendung einer einheitlichen registerübergreifenden Identifikationsnummer (vgl. insbesondere § 1 IDNrG-E) den Kernbereich des Allgemeinen Persönlichkeitsrechts dergestalt berührt, dass die Menschenwürde im Sinne von Art. 1 Abs. 1 GG tangiert ist.

Die Menschenwürde ist verletzt und damit der Kernbereich des Allgemeinen Persönlichkeitsrechts betroffen, wenn der Mensch zu einem bloßen Objekt des Staates gemacht würde. Mit der Menschenwürde wäre es nicht zu vereinbaren – so das Bundesverfassungsgericht im Mikrozensus-Urteil von 1969 (BVerfGE 27, 1 ff.) –, „wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist.“

Im Volkszählungsurteil von 1983 stellte das Gericht die Möglichkeit einer umfassenden Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten in den teleologischen Kontext der Gefahr der „Erstellung von Persönlichkeitsprofilen“ (BVerfGE 65, 1 [53]). Eine Abbildung der Persönlichkeit sei anzunehmen, „soweit eine unbeschränkte Verknüpfung der erhobenen Daten mit den bei den Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbeständen oder gar die Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal möglich wäre“ (BVerfGE 65, 1 [53]). In Maßnahmen wie „zum Beispiel [der] Einführung eines einheitlichen, für alle Register und Dateien geltenden Personenkennzeichens oder dessen Substituts,“ läge „ein entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren“ (BVerfGE 65, 1 [27]), weil „sie es erst erlauben, diese Daten, bezogen auf bestimmte Personen oder Institutionen, zusammenzuführen“ (BVerfGE 65, 1 [57]). Diese Aussagen des Gerichts werden verbreitet so verstanden, dass eine allgemeine Personenkennziffer generell unzulässig ist, während eine bereichsspezifische Ziffer wie die Steuer-ID in ihrer derzeitigen Verwendung nicht per se im Widerspruch zur

Verfassung steht (vgl. *Martini/Wagner/Wenzel*, S. 30 f.; BfDI, S. 4 u. 8; vgl. auch BFH, Urt. v. 18.1.2012 – II R 49/10).

Ob das Gericht vor diesem Hintergrund die mit dem vorgelegten Gesetzentwurf beabsichtigte Einführung der Steuer-ID als Identifikationsnummer für verfassungsrechtlich absolut – also ohne Abwägung – unzulässig ansehen würde, ist zwar denkbar, erscheint aber keinesfalls ausgemacht.

a. Maßstab

Zunächst lassen sich die Aussagen des Bundesverfassungsgerichts auch so verstehen, dass nicht die Einführung eines Personenkennzeichens an und für sich ausgeschlossen sein soll, sondern nur bestimmte Verknüpfungen von personenbezogenen Daten und damit einhergehende Profilbildungen, die mit der Einführung eines Personenkennzeichens zwar möglich, aber – weil es hierfür weitere Schritte bedürfte – nicht identisch sein würden (vgl. BVerfGE 65, 1 [27]: „ein entscheidender Schritt“). Möglicherweise ist dieses Verständnis angesichts der heute bestehenden technischen Möglichkeiten, auch ohne Personenkennzeichen Profile zu bilden, nochmal plausibler (vgl. *Martini/Wagner/Wenzel*, S. 31). In der Konsequenz muss es dann eher darum gehen, die technischen und organisatorischen Mittel zu erörtern, welche die Gefahren aus der Profilbildung reduzieren können (vgl. *Hornung*, Die digitale Identität, 2005, S. 161 f.; *Martini/Wagner/Wenzel*, S. 33). Gemessen an diesem Maßstab lässt sich vertreten, dass die mit dem vorgelegten Gesetzentwurf beabsichtigte Einführung der Steuer-ID als Identifikationsnummer in Hinblick auf die Breite der verknüpften Register und auf die Abrufmöglichkeiten der darüber erschließungsfähigen Daten in den Bereich der Profilbildung vordringt und das Risiko entsprechend erhöht (so *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 15), aber eben nicht mit einer solchen Profilbildung gleichbedeutend ist.

b. (Noch keine) Allgemeinheit des Personenkennzeichens

Doch selbst wenn man die Aussagen des Bundesverfassungsgerichts – entgegen der Überlegungen zu a) – so verstünde, dass es nicht auf die tatsächlichen Verknüpfungen von Daten oder auf konkrete Profilbildungen, sondern allein auf die Einordnung eines Kennzeichens als allgemeines Personenkennzeichen ankommt, wäre die Annahme einer

absoluten Verfassungswidrigkeit nicht zwingend. Denn der Gesetzentwurf sieht zwar vor, dass 56 Register mit der Steuer-ID ergänzt werden sollen, was aber nur ein gutes Viertel der vorhandenen 214 Register (Statistisches Bundesamt, Beistellung zum Gutachten des Nationalen Normenkontrollrats, 2017, S. 4) ausmacht. In dieser Hinsicht mag die Steuer-ID ein bereichsübergreifendes, aber noch kein allgemeines Personenkennzeichen sein.

c. Prognose- und Einschätzungsprärogative des Gesetzgebers und die daran anzulegenden Sorgfalt

Letztlich wird deutlich, dass sich die Fragen, ob, in welcher Form und mit welcher Reichweite Personenkennzeichen eingeführt werden dürfen, nicht eindeutig aus der Verfassung und der sie konkretisierenden Verfassungsrechtsprechung beantworten lassen, ohne hierfür Wirkungen, Nutzen, Risiken und Vor- und Nachteile einzuschätzen. Dies gilt nicht zuletzt vor dem Hintergrund des heute erreichten, technischen Entwicklungstandes der Digitalisierung, der vom Volkszählungsurteil im Jahr 1983 naturgemäß nicht berücksichtigt, möglicherweise noch nicht mal erahnt werden konnte. Soweit es aber einer solchen (Neu)Einschätzung bedarf, ist hierzu in erster Linie der demokratisch unmittelbar legitimierte Gesetzgeber berufen. Ihm steht ein verfassungsrechtlich fundierter Prognose- und Einschätzungsspielraum zu (vgl. etwa BVerfGE 90, 145 [173]; 110, 177 [194]; 113, 167 [234]) – freilich ungeachtet der Kontrollkompetenzen der Gerichte und deren Reichweiten.

Dabei ist allerdings zu bedenken, dass dem Gesetzgeber bei der Einschätzung der Auswirkungen einer neuen Regelung zwar ein beträchtlicher Spielraum zustehen kann (vgl. BVerfGE 110, 177 [194]), er aber bei der Ausübung seines Prognose- und Einschätzungsspielraums nicht völlig frei ist, sondern auch hier an die Verfassung gebunden bleibt (Art. 20 Abs. 3 GG) und auch insoweit der verfassungsgerichtlichen Kontrolle unterliegt. Dabei hängt der Spielraum von der Eigenart des in Rede stehenden Sachbereichs, den Möglichkeiten, sich ein hinreichend sicheres Urteil zu bilden und der Bedeutung der auf dem Spiel stehenden Rechtsgüter ab (BVerfGE 50, 290 [332 f]), 90, 145 [173]). Die Kontrolldichte durch das Bundesverfassungsgericht hängt vom Rang und der Bedeutung des „Grundrechtsguts und der Eigenart des betroffenen Sachbereiches“ ab (BVerfGE 76, 1, 51). Sachlich wird dabei auf die Beurteilung abgestellt, die dem Gesetzgeber „bei der

Vorbereitung des Gesetzes möglich war“ (BVerfGE 25, 1, [17]; 113, 167 [234]). Das Gericht bewertet, ob der Gesetzgeber „seinen Einschätzungsspielraum in vertretbarer Weise gehandhabt hat” (BVerfGE 88, 203 [262]) und wieweit er sich ein sicheres Urteil bilden konnte (BVerfGE 100, 59 [101]; 103, 242 [267]). Je gewichtiger das gefährdete Rechtsgut ist und je weitreichender es beeinträchtigt werden kann, desto höhere Anforderungen stellt das Gericht an den Grad der notwendigen Wahrscheinlichkeit bzw. die Sicherheit der gesetzgeberischen Prognose und Einschätzung (BVerfGE 113, 348 [286]).

Der vorgelegte Gesetzentwurf und insbesondere die Einführung der Steuer-ID als zusätzliches Ordnungsmerkmal nach § 1 IDNrG-E greift in die informationelle Selbstbestimmung mit einer Intensität ein, die – wie ausgeführt – an den von der Menschenwürde in Art. 1 Abs. 1 GG absolut geschützten Kernbereich jedenfalls heranreicht. Die mit der Digitalisierung der Verwaltung einhergehenden Komplexitäten und Unsicherheiten und die damit dem Gesetzgeber zufallende Prognose- und Einschätzungsprärogative sollte daher keinesfalls als „Freifahrtschein“ missverstanden werden. Das Gewicht der in Rede stehenden Rechtsgüter und die Eingriffsintensität machen es vielmehr besonders wichtig, im Gesetzgebungsprozess den möglichen Regulierungsalternativen nachzuspüren, sie abzuwägen und dies auch zu dokumentieren, um dem Eindruck entgegenzutreten, wegen Zeitdrucks oder anderen sachwidrigen Erwägungen die erstbeste Möglichkeit gewählt zu haben. So ist von parlamentarischer und auch fachlicher Seite wiederholt angemahnt worden, sich mit den vorgebrachten Einwänden, Bedenken und Alternativen substantiiert auseinanderzusetzen. Die Ausführungen zu möglichen Alternativen im Vorblatt (S. 3) wie auch an anderen Stellen der Gesetzesbegründung fallen weitgehend abstrakt und pauschal aus und erschöpfen sich häufig darin, auf mögliche Mehrkosten und die zeitliche Dringlichkeit hinzuweisen. Hier sollte geprüft werden, ob dies inhaltlich und dokumentarisch dem Sorgfaltsmaßstab genügt, den das Bundesverfassungsgericht vorliegend an die Ausfüllung des gesetzgeberischen Einschätzungs- und Prognosespielraums stellen würde.

Dieser Aspekt der sorgfältigen Ausübung der gesetzgeberischen Einschätzungsprärogative ist auch von zentraler Wichtigkeit, um die ihrerseits den vorliegenden Entwurf verfassungsrechtlich stützenden Instrumente gesetzgeberischer Eigenkontrolle – wie insbesondere Evaluation und Befristung (s. dazu unter C.) – nicht zu entwerten.

2. Zur Verhältnismäßigkeit des registerübergreifenden Identitäts- und Datenmanagements

Soweit die vom Gesetzentwurf vorgesehene Einführung einer einheitlichen registerübergreifenden Identifikationsnummer nicht als rechtfertigungsunfähig und damit als absolut unzulässig angesehen wird, muss sich das vorgelegte Modell eines registerübergreifenden Identitäts- und Datenmanagements vor allem am Maßstab der Verhältnismäßigkeit rechtfertigen lassen, d.h. es muss legitime Zwecke mit geeigneten, erforderlichen und angemessenen Mitteln verfolgen (vgl. BVerfGE 65, 1 [43 f.]; 109, 279 [335]).

a. Legitimität der Ziele

Der Gesetzentwurf nennt folgende Zwecke (vgl. S. 62 f.), die für sich betrachtet legitim sind:

- Hohes Bedürfnis für eine eindeutige Zuordnung von Datensätzen zu der jeweils richtigen Person, und zwar im Interesse der Funktionsfähigkeit und Effektivität der Verwaltung und im Interesse der betroffenen Person an der Richtigkeit der über sie gespeicherten Daten
- Steigerung der Leistungsgerechtigkeit staatlichen Handelns, weil Bürger:innen bei Inanspruchnahme von Verwaltungsleistungen von ihren Nachweispflichten entlastet werden könnten
- Vorbeugung von Leistungsmissbrauch durch Nutzung von Falschidentitäten
- Bedeutung insbesondere eines einheitlichen und bereichsübergreifenden Ordnungsmerkmals für die Durchführung des registerbasierten Zensus

Teilweise wird diesen Zielen kein sonderlich großes Gewicht zugesprochen und auf die fehlende verfassungsrechtliche Gebotenheit hingewiesen (*Sorge*, S. 3; *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 16). Daran ist richtig, dass sie anders als die hier gegenläufigen Grundrechte nicht explizit im Grundgesetz verankert sind, sich aber dennoch verfassungsrechtlich fundieren lassen. Dabei kann dahinstehen, ob die Digitalisierung an und für sich einen Zielwert darstellen kann und sollte. Ihre Potenziale sind jedenfalls einzusetzen, soweit sie dazu beitragen, die materiellen Grundsätze einer guten Verwaltung zu unterstützen, wie sie sich zum Teil aus der Verfassung ableiten lassen, einfachgesetzlich normiert sind und von Art. 41 der Charta der Grundrechte der Europäischen Union in

Bezug genommen werden. So weist etwa Art. 114 Abs. 2 S. 1 GG auf die Wirtschaftlichkeit hin. Auch Art. 108 Abs. 4 GG kann als Ausdruck eines Gebots einer effizienten Verwaltung angesehen werden. Mit Art. 91c GG hat die informationstechnische Zusammenarbeit von Bund und Ländern und insbesondere der übergreifende Zugang zu Verwaltungsleistungen eine grundgesetzliche Anerkennung erfahren. § 10 S. 2 der Verwaltungsverfahrensgesetze von Bund und Ländern normiert seit jeher als zentralen Gestaltungsgrundsatz des Verwaltungsverfahrens, dass dieses einfach, zweckmäßig und zügig durchzuführen ist. Dahinter steht die Vorstellung von einer leistungsfähigen, funktionalen, wirksamen und bürgerorientierten Verwaltung (vgl. Kopp/Ramsauer, VwVfG, 21. Aufl. 2020, § 9 Rn. 15a) – eine Vorstellung, wie sie auch dem Grundgesetz zugrunde liegen dürfte, das die Verwaltung nicht nur als eigenständige Gewalt (vgl. Art. 1 Abs. 3, 20 Abs. 3, 83 ff. GG), sondern auch als Teil eines Staates ansieht, dessen Ausgangspunkt die Grundrechte sind (Art. 1 GG ff.) und dessen Legitimität sich so gesehen maßgeblich daraus ableitet, sich in den Dienst seiner Menschen zu stellen. Diese prinzipiellen Anforderungen bzw. Erwartungen an eine „gute Verwaltung“ können natürlich nicht losgelöst von den sich verändernden gesellschaftlichen Realitäten und des technischen Fortschritts verstanden werden. Eine sich in vielen Bereichen stetig fortdigitalisierenden Gesellschaft verändert auch die Vorstellung, was unter einer leistungsfähigen und bürgerorientieren Verwaltung verstanden wird. Bürger:innen, die im wirtschaftlichen, kulturellen oder im privaten Leben tagtäglich die Innovationsdynamik der Digitalisierung erfahren, dürfen erwarten, dass auch Staat und Verwaltung die Potenziale der Digitalisierung nutzen, um ihre Leistungen effizient und nutzerorientiert zu erbringen. Neuere Verwaltungsgesetze wie die E-Government-Gesetze und das Online-Zugangsgesetz, aber auch die dem „Once-Only“-Prinzip zugrundeliegende Single Digital Gateway-VO (EU) 2018/1724 sind nicht zuletzt der gesetzgeberische Ausdruck dieser gewandelten Erwartung der Gesellschaft an ihre Verwaltung (vgl. dazu Denkhaus/Richter/Bostelmann, EGovG/OZG, Einl Rn 1 ff.).

b. Geeignetheit und Erforderlichkeit

Dass das mit dem Gesetzentwurf vorgelegte Modell eines registerübergreifenden Identitäts- und Datenmanagements, insbesondere die mit ihm verbundene Einführung eines numerischen Identifikationsmerkmals, förderlich und damit geeignet ist, die genannten

Zwecke zu erreichen, ist plausibel (s. dazu *Martini/Wagner/Wenzel*, S. 22 f.; speziell zum Zweck der Vorbeugung von Leistungsmissbrauch vgl. BFH, Urteil vom 18. Januar 2012, Az.: II R 49/10, juris, Rn. 48, 63).

In Hinblick auf die Erforderlichkeit erscheint das mit dem Gesetzentwurf vorgelegte Modell eines registerübergreifenden Identitäts- und Datenmanagements jedoch unter mehreren Gesichtspunkten fraglich. Die Erforderlichkeit ist nur gegeben, wenn es neben dem Modell, wie es durch die Regelungen des Gesetzentwurfs konkret ausgestaltet ist, keine anderen, gleichermaßen geeigneten, aber in das Recht auf informationelle Selbstbestimmung weniger eingreifende Möglichkeiten und Lösungen gibt, um die oben genannten Zwecke zu erreichen. Seit Bekanntwerden des vorliegenden Regelungsansatzes wurden verschiedene, die informationelle Selbstbestimmung schonendere Alternativen angeführt und die Erforderlichkeit der vorliegenden Lösung in Frage gestellt (s. *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 16 f. und 27 ff. m.w.N.).

(1) Absehen von Maßnahmen?

Dabei wird auch die Möglichkeit angeführt, den bisherigen Zustand so zu belassen (BfDI, S. 1 f.), also von jeder Veränderung des derzeitigen Verwaltungssystems abzusehen. Diese Option ist aber nicht geeignet, die dargelegten Ziele der Verwaltungsmodernisierung zu erreichen (*v. Lewinski*, S. 8).

(2) Verzicht auf die Verwendung einer gemeinsamen Identifikationsnummer?

Man könnte als eine weitere alternative Lösung daran denken, auf die Verwendung von Personenkennzeichnen gänzlich zu verzichten. So wird etwa vorgeschlagen, das im vorgelegten Gesetzentwurf vorgeschlagene Modell ohne die in § 1 IDNrG-E vorgesehene gemeinsame Identifikationsnummer einzuführen. Denn das Modell sehe bei der Datenübermittlung ohnehin Zwischenstellen (§ 7 IDNrG-E) vor, die anhand von Metadaten die Übermittlung vollzögen. Dementsprechend bräuchten die registerführenden Behörden keine gemeinsame Identifikationsnummer (s. *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 16). Die Herausforderung dieser Alternativlösung dürfte dann in der Wahrung der Datenrichtigkeit liegen (vgl. Art. 5 Abs. 1 lit. d DSGVO), also der Wahrung der Datenwahrheit, der Datenaktualität und der Datenvollständigkeit. Es spricht viel dafür, dass ein Verzicht

auf eine gemeinsame Identifikationsnummer eine höhere Anfälligkeit für Datenunrichtigkeiten und damit auch einen erheblich höheren Pflegebedarf begründen würden (S. 35; *v. Lewinski*, S. 8), zumal sich die Grundrechtsrelevanz des staatlichen Registersystems auch in den Anstrengungen zur Wahrung der Datenrichtigkeit wiederspiegeln müsste.

Auf der anderen Seite spezifiziert der vorgelegte Gesetzentwurf die Gründe nicht eingehender, welche Prüfungen und Erwägungen zu dem Ergebnis geführt haben, dass der Verzicht auf die Verwendung einer gemeinsamen Identifikationsnummer die Fehleranfälligkeit und den Pflegebedarf erhöhen würde. Dies wäre – auch angesichts der europarechtlichen Verankerung des sogenannten datenschutzfördernden Identitätsmanagement in Art. 11 DSGVO – zu erwarten gewesen.

(3) Verwendung bereichsspezifischer Personenkennzeichen?

In Betracht kommt die Einführung bereichsspezifischer Kennzeichen. Diese Möglichkeit nach österreichischem Vorbild wurde im Gesetzentwurf als Alternative angeführt, aber verworfen (S. 3; kritisch auch StN NKR, S. 4). In diesem Modell wird Bürger:innen eine für alle Verwaltungsbereiche geltende Stammzahl zugewiesen, die in Kombination mit generierten bereichsspezifischen Kennziffern eine eindeutige Identifikation gewährleistet. Dies führt dazu, dass diese zusammengesetzten Kennziffern nur für einen staatlichen Bereich eingesetzt werden (vgl. § 9 Abs. 1 S. 2 EGovG Österreich). Auch ist die Nummer immer nur denjenigen Behörden bekannt, die in dem jeweiligen Tätigkeitsfeld agieren. Zweck dieser Lösung ist es, die Erstellung umfassender Persönlichkeitsprofile durch die Verbindung von Informationen aus sachlich nicht zusammenhängenden Bereichen zu verhindern. Insbesondere unter dem Gesichtspunkt der Eingriffsintensität wurde von Beginn an auf verschiedene Aspekte hingewiesen, die dieses Modell in Hinblick auf mögliche Gefahren überlegen erscheinen lassen (vgl. BfDI, S. 4 f.; *Sorge/Leicht*, ZRP 2020, 242 [243 f.]).

Zugleich wurde repliziert, dass das vorgelegte Modell des RegMoG im Vergleich zum „österreichischen Modell“ allenfalls höhere Risiken des Missbrauchs und damit Risiken für die Datensicherheit begründe, sich beide Modelle im Übrigen aber nicht kategorial unterschieden, so dass es letztlich Sache des Gesetzgebers sei, sich im Rahmen seiner

Einschätzungsprärogative und des empirisch Nachgewiesenen zu entscheiden (*v. Lewinski*, S. 11). In beiden Modellen sei die Eingriffsintensität ähnlich, da jeweils dieselben Daten erhoben und automatisiert verknüpfbar gemacht würden (aaO, S. 9). Dagegen wird Missbrauchsrisiko allerdings als gewichtig eingeschätzt, weil die einer bereichsübergreifenden Identitätsnummer innewohnende Mächtigkeit im Zugriff auf die Register auch denjenigen zufalle, die eine solche Nummer unberechtigt verwenden. In der Folge sei das Schadenspotenzial – etwa eines „Identitätsdiebstahls" – höher und in der Folgesfolge der Anreiz für entsprechende Angreifer. Zwar wird im gleichen Zug zu Recht darauf hingewiesen, dass der Gesetzentwurf diesen Missbrauchsrisiken der Identitätsnummer durch eine Reihe von Maßnahmen – etwa das 4-Corner-Modell (§ 7 Abs. 2 IDNrG-E), die Protokollierung aller Zugriffe (§§ 7 Abs. 2, 9 IDNrG-E), die Verschlüsselung (§ 7 Abs. IDNrG-E), Löschpflichten (§ 11 IDNrG-E), die Datenschutzkontrolle (§ 13 IDNrG-E) und eine Strafbewehrung (§ 17 IDNrG-E) – entgegen zu wirken versucht und dass auch das „österreichische Modell" der bereichsspezifischen Kennzeichen keinen absoluten Schutz böte, sondern in einzelnen Punkten – etwa was unbemerkte Zugriffe oder die informationelle Gewaltenteilung betrifft – sogar hinter dem Gewährleistungsniveau des vorgelegten RegMoG zurückbliebe (ausführlich v. Lewinski, S. 10 f.; zur Bedeutung des Erhalts des dezentralen Registersystems s. auch *Berger*, S. 2). Letztlich bleibt es aber auch hier bei einem Spielraum der Einschätzung und Prognose, ob und wie sich verbleibende, unauflösbare Restrisiken verwirklichen könnten.

Vor diesem Hintergrund wäre es wünschenswert, die gesetzgeberische Entscheidung gegen bereichsspezifische Kennzeichen etwa im Wege eines Vergleichs der Modelle besser zu begründen (so auch BfDI, S. 5; *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 17) bzw. die diesbezüglichen Erwägungen offen zu legen. Möglicherweise wäre dies sogar verfassungsrechtlich geboten, da auch hier die Reichweite der gesetzgeberischen Einschätzungsprärogative und die damit einhergehenden Sorgfaltsanforderungen ein zentrales Moment in der verfassungsrechtlichen Bewertung darstellen (s. allein der dreifache Hinweis bei *v. Lewinski*, S. 10 u. 11). Die mit dem Gesetzentwurf vorgelegte Begründung, die sich hauptsächlich auf die größere Komplexität der Umsetzung und damit verbundene höhere Kosten sowie mangelnde Vergleichbarkeit bezieht, vermag die Erforderlichkeit auch im Hinblick auf die Alternative bereichsbezogener Kennzeichen nur in Teilaspekten

zu veranschaulichen und lässt insbesondere Aspekte des Grundrechtsschutzes zugunsten der genannten Argumente unterbelichtet.

(3) Verwendung eines anderen einheitlichen Personenkennzeichens als die Steuer-ID?

Unter dem Gesichtspunkt der Erforderlichkeit könnte zudem die Einführung eines anderen Personenkennzeichens in Erwägung gezogen werden (Sorge/v. Lucke/Spiecker gen. Döhmann, S. 34 ff.). Dies hätte den Vorteil, dass nicht die Steuer-ID, die ursprünglich als bereichsspezifische Nummer im Steuerbereich eingeführt und nur begrenzt hierauf verwendet werden sollte, zur bereichsübergreifenden Nummer ausgeweitet werden müsste. Auch eine andere (neue) Nummer wäre dazu geeignet, diese Funktion zu übernehmen. Allerdings würde die Einführung und Regelung des rechtlichen Rahmens für ein solches Verwaltungskennzeichen wohl einen erheblichen zeitlichen Mehraufwand bedeuten. Allerdings verbleiben auch bei diesem Modell Risiken und Gefahren, etwa das die Vergabe von bereichsspezifischen Personenkennzeichen weitgehend zentralisiert erfolgen müsste und die vermittelnden Stellen – wie im „österreichischen Model“ – ein attraktives Ziel für Angriffe von außen darstellen (vgl. Sorge/v. Lucke/Spiecker gen. Döhmann, S. 36; v. Lewinski, S. 11).

(4) Erneut: Sorgfältige Ausübung der Prognose- und Einschätzungsprärogative

Alle in Betracht zu ziehenden alternativen Lösungen bieten Argumente für eine stärkere Schonung der informationellen Selbstbestimmung als das mit dem Gesetzentwurf vorgelegte Modell. Ob dies jedoch tatsächlich anzunehmen ist und ob die alternativen Lösungen auch in Hinblick der Erreichung der legitimen Ziele gleich geeignet sind, lässt sich nicht abschließend beurteilen und fällt insoweit in die Prognose- und Einschätzungsprärogative des demokratisch unmittelbar legitimierten Gesetzgebers. Hinzuweisen bleibt allerdings auch an dieser Stelle darauf, dass der Gesetzentwurf in der Prüfung alternativer Lösungen möglicherweise nicht vermittelt, dass der Gesetzgeber die verfassungsrechtlich fundierten und verfassungsgerichtlich überprüfbaren Sorgfaltsanforderungen an die Ausübung der ihm zustehenden Einschätzungsprärogative nachgekommen ist. Auf die Ausführungen zu B. II. 1. c. kann insoweit verwiesen werden.

c. Angemessenheit

Soweit man die Erforderlichkeit des mit dem Gesetzentwurf vorgelegten Modells eines registerübergreifenden Identitäts- und Datenmanagements annimmt, dürften die mit dem Modell verfolgten Zwecke zum Eingriffsgewicht nicht außer Verhältnis stehen. Angezeigt hierfür ist es allerdings, verschiedene Mechanismen und Maßnahmen zum Schutz der informationellen Selbstbestimmung nachzuziehen.

(1) Ausweitung des 4-Corner-Modells

Um die Gefahr der Bildung von unzulässigen und umfangreichen Persönlichkeitsprofilen zu minimieren, sieht der Gesetzentwurf insbesondere in § 7 Abs. 2 IDNrG-E technische Absicherungen bei bereichsübergreifenden Datenübermittlungen im Sinne des sogenannten 4-Corner-Modell vor. Danach dürfen Daten nicht direkt zwischen den Kommunikationspartnern ausgetauscht werden, sondern nur unter Einschaltung von Vermittlungsstellen, die kontrollieren, ob eine Behörde grundsätzlich berechtigt ist, der anderen Behörde zu dem angegebenen Zweck die jeweiligen Daten zu übermitteln. Weil diese abstrakte, grundsätzliche Übermittlungsbefugnis von der Zulässigkeit der Übermittlung im konkreten Einzelfall zu unterscheiden ist, wäre es zur Reduzierung der Gefahr der Bildung von Persönlichkeitsprofilen wichtig, die Absicherungen des 4-Corner-Modells, insbesondere den Einsatz von Verschlüsselungen (StN des BfDI, S. 6 f.), nicht nur auf die bereichsübergreifenden Kommunikationen zu beschränken (vgl. § 7 Abs. 2 S. 1 IDNrG-E), sondern bei allen Übermittlungen vorzugeben. Die in der Gesetzesbegründung genannten (nicht näher spezifizierten) Umsetzungsaufwände sollten demgegenüber nicht ins Gewicht fallen (so auch *v. Lewinski*, S. 9).

> *In § 7 Abs. 2 S. 1 IDNrG-E sollten die Wörter „zwischen öffentlichen Stellen verschiedener Bereiche“ ersatzlos gestrichen werden.*

(2) Konkretisierung der Zweckbindung

Der verfassungsrechtlich fundierte Zweckbindungsgrundsatz kommt beim Schutz vor ungerechtfertigten Eingriffen in die informationelle Selbstbestimmung eine entscheidende Funktion zu. Dementsprechend ist der Gesetzeber gehalten, die Zwecke, zu denen personenbezogene Daten verarbeitet werden dürfen, selbst und genau zu bestimmen. Mit § 5 Abs. 1 IDNrG-E nimmt der Gesetzentwurf zwar eine solche Zweckbestimmung vor.

Sie bleibt aber insoweit unbestimmt, als dass sie nur (positiv) festlegt, welchen Zwecken die Identifikationsnummer dienen darf, nicht aber auch (negativ), inwieweit eine Verarbeitung unzulässig ist. So sollte zum einen ausdrücklich festgelegt werden, dass es unzulässig ist, die Steuer-ID für andere Datenverarbeitungen als die Identifikation von natürlichen Personen gegenüber der Verwaltung zu verwenden. In ähnlicher Weise sollte die Verarbeitung durch nicht-öffentliche Stellen außer in den gesetzlich und in den von der DSGVO vorgesehenen Fällen für grundsätzlich unzulässig erklärt werden (s. dazu bereits den Vorschlag oben unter B. I. 2.).

(3) Reduzierung und Auswahl der einzubeziehenden Register

Angesichts der jedenfalls nicht von der zu Hand weisenden Möglichkeit von Profilbildungen kommt der Art, der Anzahl und dem Umfang der einzubeziehenden Register eine entscheidende Bedeutung für Gefährdungen und Verletzungen der informationellen Selbstbestimmung zu. Die Anlage zu § 1 IDNrG-E sieht eine Einbindung von 56 Registern vor, ohne dass ein Kriterium für die Auswahl erkennbar wäre. So wird etwa gerade der Steuerbereich, aus dem die Steuer-ID stammt, nicht einbezogen, obwohl dies doch naheliegen würde. Damit geht einher, dass die Sicherungs- und Transparenzmaßnahmen, die für die genannten Register gelten, nicht auf die weiterhin bestehende Steuer-ID ausgeweitet werden, obwohl die Risiken sich durch die Ausweitung des Anwendungsbereichs des Kennzeichens erheblich vergrößern (StN des BfDI, S. 7). Um etwaige Risiken zu minimieren und um Zeit zu gewinnen, Erfahrungen im tatsächlichen Betrieb des vorgelegten registerübergreifenden Identitäts- und Datenmanagement sammeln zu können, erscheint eine deutliche Reduzierung und eine systematischere Auswahl der im ersten Angang einbezogenen Register sinnvoll (für eine Anpassung der Registerauswahl im Hinblick auf den kommunalen Bedarf *Berger*, S. 3).

So führt die Begründung zum Gesetzentwurf aus (S. 34), dass in (dem vorgelegten) ersten Schritt (nur) die für die Umsetzung des Onlinezugangsgesetzes relevanten Register modernisiert und Teil eines registerübergreifenden Identitätsmanagements werden sollen. Dies sollte sich dann aber auch im Gesetz widerspiegeln.

§ 1 IDNrG-E sollte um folgenden Satz 2 ergänzt werden:

> *„Die in der Anlage zu diesem Gesetz aufgeführten Register sind einzubeziehen, wenn und soweit dies zur Erbringung von Verwaltungsleistungen nach dem Onlinezugangsgesetzes notwendig ist.“*

Um die Auswahl in einem weiteren Schritt eng zu führen und die Wirkreichweite des Identitätsmanagements zu begrenzen, könnte man sich etwa daran orientieren, welche Register notwendig sind, um ausgewählte Verfahren vollständig basierend auf dem registerübergreifenden Identitäts- und Datenmanagement durchführen zu können. Auf Grundlage der Erfahrungen, die mit einem so in den einbezogenen Registern begrenztem Identitätsmanagement gewonnen würden, könnten dann später weitere Register einbezogen werden.

Widersprüchlich und im Hinblick auf den Vorbehalt des Gesetzes und Art. 80 GG wenig überzeugend ist es, wenn § 12 Abs. 1 Nr. 1 IDNrG-E die künftige Erweiterung der einzubeziehenden Register dem Verordnungsgeber überlässt, während die ursprünglich einzubeziehenden Register durch das Gesetz selbst bestimmt werden.

> *§ 12 Abs. 1 Nr. 1 IDNrG-E sollte ersatzlos gestrichen werden.*

(4) Festlegung der Bereiche

Verfassungsrechtlich problematisch sind die Regelungen zur Festlegung der sogenannten Bereiche in § 7 Abs. 2 IDNrG-E. Dabei handelt es sich letztlich um eine Einteilung des Verwaltungsregisterraums in informationstechnisch zusammenhängende Bereiche. Dabei knüpft der Gesetzentwurf an die Einteilung der Bereiche erhebliche Folgen. Für innerhalb eines Bereichs stattfindende Datenübermittlungen gelten nicht die im IDNrG-E festgelegten Sicherungs-, Protokollierungs- und Überprüfungsvorschriften (s. dazu bereits vorstehend unter (1) sowie § 7 Abs. 2 S. 1 IDNrG-E), sondern nur die Sicherungs- und Zweckbestimmungsvorschriften des jeweils bestehenden Fachrechts, ungeachtet dessen, dass nun die Steuer-ID als Personenkennzeichen verwendet wird. Die nähere Ausregulierung eines Bereichs und der bereichsinternen Datenübermittlungen wird stattdessen der Zuständigkeit eines Bundesministeriums zugeordnet (vgl. § 12 Abs. 3 IDNrG-E).

Angesichts der Grundrechtsrelevanz erscheinen diese Regelungen in Hinblick auf den Parlamentsvorbehalt und den Anforderungen aus Art. 80 Abs. 1 S. 2 GG bedenklich.

Weder würde gesetzgeberisch vorgegeben, welche Kriterien zur Bestimmung von Bereichen herangezogen werden sollen, noch würde die Zahl bestimmt (lediglich die Untergrenze von sechs Bereichen ist benannt), noch festgelegt, welche Zielsetzung mit der Bereichsaufteilung einhergehen soll (ebenfalls kritisch sowie ausführlich *Sorge/v. Lucke/Spiecker gen. Döhmann*, S. 15; *v. Lewinski*, S. 5 f.).

> *Die Regulierung der Bereiche in §§ 7 Abs. 2 S. 2, 12 Abs. 1 Nr. 2, Abs. 3 IDNrG-E sollte entsprechend der Anforderungen des Parlamentsvorbehalts und von Art. 80 Abs. 1 S. 2 GG angepasst werden.*

(5) Ausbau technischer Schutzmechanismen

Das mit dem Gesetzentwurf vorgeschlagene registerübergreifenden Identitäts- und Datenmanagement schöpft nicht alle Möglichkeiten aus, den möglichen Gefährdungen der informationellen Selbstbestimmung mit technischen Schutzmechanismen spezifisch entgegenzuwirken. Der Gesetzentwurf beschränkt sich auf die allgemeine Vorgabe, dass der aktuelle Stand von Sicherheit und Technik eingehalten werden muss, bezieht diese Vorgabe aber nur auf die Datenübermittlung zwischen öffentlichen Stellen verschiedener Bereiche (§ 7 Abs. 2 S. 1 IDNrG-E) und überlässt die weitere Regulierung dem Verordnungsgeber (§ 12 Abs. 2 Nr. 4 IDNrG-E; kritisch zu der Norm in Bezug auf den geringen Einfluss der Länder und Kommunen *Berger*, S. 3). Diese und andere Absicherungen richten ihre Schutzwirkungen aber vor allem nach innen und nicht auch gegen Angriffe von außen. Es sind aber keine Gründe ersichtlich, warum etwa auf eine sichere Authentifizierung der beteiligten Behörden verzichtet werden sollte. Auch die technische Sicherung des übermittelbaren Datenkranzes oder eine die Vorgabe einer durchgehenden Ende-zu-Ende-Verschlüsselung wären Möglichkeiten, die technischen Schutzmechanismen zu verstärken und ggf. auch ausdrücklich im Gesetz zu normieren. So sollte angesichts des hohen Schutzniveaus der in Rede stehenden Daten etwa die Vorgabe einer Ende-zu-Ende-Verschlüsselung nicht der Auslegung des Merkmals „ohne Kenntnis der Nachrichteninhalte“ in § 7 Abs. 2 S. 4 Hs. 2 IDNrG-E sowie einem Hinweis in der Gesetzesbegründung (S. 65 f.) überlassen werden (vgl. v. Lewinski, S. 16).

Das vorgeschlagene registerübergreifende Identitäts- und Datenmanagement begründet besondere IT-sicherheitsrechtliche Herausforderungen, weil es alle staatlichen Ebenen – Bund, Länder, Landkreise und Gemeinden – betrifft und damit die Gefahr einhergeht,

dass Cyber-Angriff beispielsweise auf eine kommunale Behörde über die gemeinsam genutzte Anwendung an den Sicherheitsvorkehrungen vorbei auf eine Landes- oder gar Bundesbehörde „durchschlagen“ kann. Dabei ist auch zu berücksichtigen, dass die Sicherheit des Gesamtsystems auch vom Vermögen jedes einzelnen Akteurs abhängt, den Sicherheitsvorgaben auch nach zu kommen. Gerade kleinere Körperschaften stehen nicht selten vor der Herausforderung, die entsprechenden Ressourcen und Expertisen bereit zu stellen (vgl. Schardt, in: Hornung/Schallbruch, IT-Sicherheitsrecht, 2020, § 25 Rn. 63).

(6) Ausbau des Datencockpits

Art. 2 Ziffer 2 RegMoG-E sieht die Einfügung der §§ 10, 11 in das OZG vor. Sie normieren ein sogenanntes Datencockpit, in dem natürliche Personen sich registrieren und einsehen können, welche Datenabrufe auf Grundlage der Steuer-ID stattgefunden haben. Damit wird den Betroffenen die Möglichkeit eröffnet, jedenfalls im Nachhinein jederzeit Einblick in die stattgefundenen Datenverarbeitungen zu erhalten. Die damit hergestellte Transparenz dient der Kontrolle und unterstützt die Einholung nachträglichen Rechtsschutzes. Zugleich ist es datenschutzrechtlich zu begrüßen, dass nach § 10 Abs. 2 S. 1, Hs. 2 und S. 3 OZG-E die Daten nur für die Dauer des jeweiligen Nutzungsvorgangs gespeichert und nach dessen Beendigung unverzüglich zu löschen sind.

Das Recht auf informationelle Selbstbestimmung will insbesondere vor Gefährdungen schützen, die daraus resultieren, dass personenbezogene Informationen von staatlichen Behörden in einer Art und Weise genutzt und verknüpft werden, die Betroffene weder überschauen noch beherrschen können (vgl. BVerfGE 118, 168 [184]; Beschl. v. 27.5. 2020 – 1 BvR 1873/13 u. 1 BvR 2618/13, Rn. 92; v. 10.11.2020 – 1 BvR 3214/15, Rn. 71). Daher sollten etwaige Möglichkeiten genutzt werden, das Datencockpit weiter auszubauen und die Transparenz noch weiter zu stärken. So sollte es für den Nutzer leicht und einfach sein, die ihn betreffenden Datenübermittlungen zwischen allen öffentlichen Stellen, die die Identifikationsnummer nutzen, anzeigen zu lassen (vgl. auch § 9 EGovG und dazu *Denkhaus/Richter/Bostelmann*, EGovG/OZG, § 9 EGovG, Rn. 6).

In § 10 Abs. 4 OZG-E sollte als Satz 4 unter Verschiebung der nachfolgenden Sätze eingefügt werden:

„Das Datencockpit muss aus Sicht des Nutzers einfach und zweckmäßig zu bedienen sein.“

Es sollten Schutzmechanismen eingezogen werden, die verhindern, dass die Bauweise des Cockpits und sämtliche seiner Teile veränderbar sind. Die Anzeige sollte auf die Bestandsdaten und nicht nur auf die Protokolldaten erstreckt werden (vgl. § 10 Abs. 2 S. 1 Hs. 1 OZG-E, wobei ungeachtet der vorgeschlagenen Erweiterung das Wort „können“ im derzeitigen Wortlaut der Vorschrift missverständlich ist, weil es vom Rechtsanwender – entgegen der Gesetzesbegründung, S. 78 – als Einräumung von Ermessen und nicht als technische Möglichkeit verstanden werden könnte).

§ 10 Abs. 2 S. 1, Hs. 1 OZG-E sollte wie folgt gefasst werden:
„In einem Datencockpit werden ausschließlich die Protokolldaten nach § 9 des Identifikationsnummerngesetzes und die Bestandsdaten angezeigt.“

C. Weitere Einzelpunkte

I. Einwilligung in den Datenaustausch

Das RegMoG setzt an verschiedenen Stellen an den Zielen des OZG an, dass die Bürger:innen erforderliche Daten und Nachweise nicht in jedem Verwaltungsverfahren erneut beibringen müssen, sondern dass sich die verfahrensführenden Behörden sich diese Daten und Nachweise von anderen öffentlichen oder nicht-öffentlichen Stellen beschaffen. Wie auch das OZG setzt auch das RegMoG dazu nicht nur auf entsprechende gesetzliche Ermächtigungen, sondern zum Teil auch auf die Legitimation durch Einwilligung des Betroffenen (vgl. etwa § 6 Abs. 3 IDNrG-E und dazu S. 71). Das mag aus einer ersten, verbraucherschutzgeprägten Sicht plausibel wirken. In vielen Bereichen des Verwaltungshandelns – und so auch im vorliegenden – dürfte dadurch aber die Legitimation im Vergleich zu einer gesetzlichen Rechtsgrundlage, die dezidiert die Kriterien staatlichen Handelns (z.B. Voraussetzungen des Datenabrufs) benennt und parlamentarisch demokratisiert und so das Verwaltungshandeln diszipliniert, abgesenkt werden – dies zumal man für eine tragfähige Einwilligung stets verlangen muss, dass die Bürger:in die Bedeutung, die Tragweite und die Risiken erkennt, die sich etwa im vorliegenden Bereich mit einer Datenübermittlung innerhalb eines sehr komplexen und voraussetzungsvollen IT-

Registersystems verbinden. Dies impliziert einen kaum erfüllbaren Anspruch an Information und Aufgeklärtheit.

II. Ausweitung der Evaluierungsvorgaben

In Hinblick auf die Unsicherheiten und fehlenden Erfahrungswerte, die sich mit dem Einsatz des vorgeschlagenen registerübergreifenden Identitäts- und Datenmanagements verbinden, sieht § 16 Abs. 2 IDNrG-E zu Recht vor, dass die Wirksamkeit der im IDNrG-E enthaltenen Maßnahmen für die Erreichung der in § 1 IDNrG-E genannten Ziele zu evaluieren sind. Ebenfalls zu begrüßen ist, dass dies unter Einbeziehung von wissenschaftlichem Sachverstand zu erfolgen hat. Mit Blick auf die Eingriffsintensität erscheint jedoch die Evaluationsfrist zu lang bemessen. Sollte das Gesetz 2021 in Kraft treten und rechnet man das Jahr des Inkrafttretens nicht mit, dann wäre das Gesetz erst im Jahr 2027 („im sechsten Jahr nach Inkrafttreten“) zu evaluieren. Bezieht man die notwendige Zeit für ein sich anschließendes Gesetzgebungsverfahren ein, könnte es dazu kommen, dass das Gesetz faktisch erst in den Jahren 2028 bzw. 2029 gesetzgeberisch in den Blick genommen wird. Die Evaluation von Gesetzen zielt aber nicht nur auf eine Bewährungsprüfung von Gesetzen und damit allein auf eine Korrektur und Verbesserung. Sie dient auch einem Lernprozess und begründet – auch auf der Ebene gesetzlicher Regulierung – eine notwendige „Feedback-Kultur“ (vgl. Kommission, Weißbuch „Europäisches Regieren“ v. 25.7.2001, KOM (2001) 428 endg. S. 29). Ein solcher (organisationaler) Lernprozess ist wegen der hohen Innovationsdynamik und Entwicklungsgeschwindigkeit der Informationstechnologien gerade bei der regulativen Umhegung der Digitalisierung besonders wichtig. Angesichts der raschen Innovationszyklen erscheint dann aber ein Zeitraum von (faktisch mindestens) sieben Jahren zu groß bemessen. Andere Digitalisierungsgesetze legen dementsprechend wesentlich kürzere Evaluationsfristen von drei bis vier Jahren fest (z.B. NetzDG, BT-Drucks. 18/12356, S. 18; § 26 EGovG Bln; Art. 97 DSGVO).

In § 16 Abs. 2 IDNrG-E sollten die Worte „im sechsten Jahr“ durch die Worte “frühestens im dritten und spätestens im vierten Jahr” ersetzt werden.

III. Befristung des Gesetzes

Als weitere Maßnahme, um den Unsicherheiten zu begegnen, die mit dem RegMoG-E einhergehen, sollte eine Befristung des Gesetzes in Betracht gezogen werden – dies zumal die in § 16 IDNrG-E vorgeschriebene Evaluation des Gesetzes eine schwache Verbindlichkeit aufweist (*v. Lewinski*, S. 16). Durch die Befristung zwingt sich der Gesetzgeber faktisch durch die erneute Befassung mit der Materie, die Verlängerung von der Wirksamkeit des Gesetzes abhängig zu machen (vgl. *Höfling/Engels* in Gesetzgebung, S. 865 f.). Durch diese Selbstkontrolle des Gesetzgebers kann erreicht werden, dass Entwicklungen in den Blick genommen werden müssen und die anfangs bestehenden Unsicherheiten zu bewerten sind. Der Gesetzgeber kann nach dem festgesetzten Zeitraum das Gesetz verlängern, oder gegebenenfalls eine Alternative umsetzen. Dies erscheint in Hinblick auf die vorgebrachten Bedenken hinsichtlich der informationellen Selbstbestimmung und der Frage, welche Gefahren sich realisieren, durchaus sinnvoll. Dabei sollte eine Befristungsregel zeitlich angemessen (vgl. etwa § 17 Abs. 2 EGovG Hessen) und mit der Evaluationsbestimmung (s. vorstehend II.) korrespondieren.

> *Dem RegMoG-E sollte folgender Artikel 23 angefügt werden:*
> *Befristung*
> *Dieses Gesetz tritt mit Ablauf des 31. Dezember 2026 außer Kraft.*

D. Redaktionelle Hinweise

Abschließend werden folgende, redaktionelle Hinweise gegeben:

1. In § 10 IDNrG-E müsste es anstelle von „§ 4 Absatz 12 und 3" entweder „§ 4 Absatz 1, 2 und 3" oder – wohl sinnvoller – nur „§ 4 Absatz 2 und 3" heißen (vgl. auch Gesetzesbegründung, S. 74). Einen Absatz 12 gibt es in § 4 IDNrG-E nicht.

2. In § 4 Abs. 1 IDNrG-E heißt es „Die Daten nach Absätze 2 und 3 […]", was grammatikalisch nicht korrekt sein dürfte ("nach den Absätzen 2 und 3" oder "Die Daten nach Absatz 2 und 3").

3. Zu Artikel 2 Ziffer 1: § 2 Abs. 6 OZG würde nach der beabsichtigten Ergänzung lauten: „… sind IT-Anwendungen, Basisdienste digitale Werkzeuge und die elektronische Realisierung…“. Möglicherweise fehlt hier ein Komma nach „Basisdienste“. Eine Gesetzesbegründung zu dieser – bildsprachlich anmutenden – Ergänzung (Was sind „digitale Werkzeuge?“) fehlt.

Prof. Eike Richter, ORR