19. Wahlperiode

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Wortprotokoll
der 114. Sitzung

Ausschuss für Inneres und Heimat
Berlin, den 14. Dezember 2020, 14:00 Uhr
10117 Berlin, Adele-Schreiber-Krieger-Straße 1
Marie-Elisabeth-Lüders-Haus
3.101 (Anhörungssaal)

Vorsitz: Andrea Lindholz, MdB

Tagesordnung - Öffentliche Anhörung

Tagesordnungspunkt

a) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz – RegMoG)

BT-Drucksache 19/24226

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss Digitale Agenda
Ausschuss für Bau, Wohnen, Stadtentwicklung und Kommunen
Haushaltsausschuss (mb und § 96 GO)

Gutachtlich:
Parlamentarischer Beirat für nachhaltige Entwicklung

Berichterstatter/in:
Abg. Marc Henrichmann [CDU/CSU]
Abg. Elisabeth Kaiser [SPD]
Abg. Jochen Haug [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

b) Antrag der Abgeordneten Manuel Höferlin, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP

Verfassungskonforme Registermodernisierung - ohne steuerliche Identifikationsnummer

BT-Drucksache 19/24641

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss Digitale Agenda

Berichterstatter/in:
Abg. Marc Henrichmann [CDU/CSU]
Abg. Elisabeth Kaiser [SPD]
Abg. Jochen Haug [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

c) Antrag der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Britta Haßelmann, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

E-Government entschlossen vorantreiben - Registermodernisierung verfassungskonform umsetzen

BT-Drucksache 19/25029

Federführend:
Ausschuss für Inneres und Heimat

Mitberatend:
Ausschuss für Recht und Verbraucherschutz
Ausschuss Digitale Agenda

Berichterstatter/in:
Abg. Marc Henrichmann [CDU/CSU]
Abg. Elisabeth Kaiser [SPD]
Abg. Jochen Haug [AfD]
Abg. Manuel Höferlin [FDP]
Abg. Petra Pau [DIE LINKE.]
Abg. Dr. Konstantin von Notz [BÜNDNIS 90/DIE GRÜNEN]

Inhaltsverzeichnis

Mitglieder des Ausschusses

	Ordentliche Mitglieder	Stellvertretende Mitglieder
CDU/CSU	Henrichmann, Marc Lindholz, Andrea Müller, Axel Throm, Alexander	
SPD	Hitschler, Thomas Kaiser, Elisabeth	
AfD	Wirth, Dr. Christian	
FDP	Höferlin, Manuel	
DIE LINKE.	Jelpke, Ulla Pau, Petra	
BÜNDNIS 90/DIE GRÜNEN	Notz, Dr. Konstantin von	
fraktionslos		

Liste der Sachverständigen

Öffentliche Anhörung am Montag, 14. Dezember 2020, 14.00 Uhr
„Registermodernisierung“

Dr. Ariane Berger
Bundesvereinigung der kommunalen Spitzenverbände, Berlin

Ass. Jur. Kirsten Bock

Prof. Ulrich Kelber
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bonn

Prof. Dr. Kai von Lewinski
Universität Passau

Prof. Dr. Peter Parycek
Kompetenzzentrum Öffentliche IT am Fraunhofer FOKUS Institut
und Donau-Universität Krems

Prof. Eike Richter
Hochschule der Akademie der Polizei Hamburg

Prof. Dr.-Ing. Christoph Sorge
Universität des Saarlandes, Saarbrücken

Tagesordnungspunkt

a) Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz – RegMoG)

BT-Drucksache 19/24226

b) Antrag der Abgeordneten Manuel Höferlin, Stephan Thomae, Grigorios Aggelidis, weiterer Abgeordneter und der Fraktion der FDP

Verfassungskonforme Registermodernisierung - ohne steuerliche Identifikationsnummer

BT-Drucksache 19/24641

c) Antrag der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Britta Haßelmann, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

E-Government entschlossen vorantreiben - Registermodernisierung verfassungskonform umsetzen

BT-Drucksache 19/25029

Vors. **Andrea Lindholz** (CDU/CSU): Dann darf ich Sie alle ganz herzlich zu unserer 114. Sitzung des Ausschusses für Inneres und Heimat begrüßen. Wir haben von 14:00 bis 16:00 Uhr eine Anhörung zum Registermodernisierungsgesetz. Es liegt vor: Der Gesetzentwurf der Bundesregierung, der Antrag der Fraktion der FDP und der Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN. Ich darf ganz herzlich alle Kolleginnen und Kollegen begrüßen und sehe, die Fraktionen sind vollständig vertreten, und zwar real. Vielen Dank dafür. Ich darf auch ganz herzlich alle Sachverständigen begrüßen und gehe mal eben durch, wer wo anwesend ist. Wir haben zugeschaltet Herrn Professor Kelber. Herr Kelber.

SV **Prof. Ulrich Kelber** (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bonn): Guten Tag.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Dann haben wir Herrn Professor von Lewinski im Bild.

SV **Prof. Dr. Kai von Lewinski** (Universität Passau): Grüß Gott aus Passau.

Vors. **Andrea Lindholz** (CDU/CSU): Herrn Professor Parycek.

SV **Prof. Dr. Peter Parycek** (Kompetenzzentrum Öffentliche IT am Fraunhofer FOKUS Institut und Donau-Universität Krems): Liebe Grüße aus Krems.

Vors. **Andrea Lindholz** (CDU/CSU): Und Herr Professor Sorge müsste auch im Bild sein.

SV **Prof. Dr.-Ing. Christoph Sorge** (Universität des Saarlandes, Saarbrücken): Ja, ich grüße Sie aus dem Saarland.

Vors. **Andrea Lindholz** (CDU/CSU): Sehr schön. Vielen Dank. Dann haben wir anwesend bei uns hier vor Ort Frau Dr. Berger, Frau Bock und Herrn Professor Richter. Sehr schön. Ich darf mich auch für die Stellungnahmen bedanken, die bereits eingegangen sind. Unsere Anhörung wird wie immer übertragen, heute allerdings zeitversetzt um 18:30 Uhr auf Kanal 1 im Parlamentsfernsehen. Und später ist sie auch in der Mediathek bereitgestellt. Wir werden wie üblich ein Wortprotokoll anfertigen, das auch dann entsprechend zur Korrektur übersandt wird. Das Protokoll und die schriftlichen Stellungnahmen gehen hinterher in eine Gesamtdrucksache ein. Wir werden so verfahren, dass zunächst alle Sachverständigen ein kurzes Eingangsstatement machen. Wir beginnen das dann in alphabetischer Reihenfolge. Ich habe die Bitte, wenn es möglich ist, die fünf Minuten Eingangsstatement nicht zu überschreiten. Die Sachverständigen, die zugeschaltet sind, sehen immer die Uhrzeit nicht. Deswegen, wenn es Ihnen irgendwie möglich ist, selber ein bisschen mitzugucken, dass Sie so bei ungefähr fünf Minuten liegen. Wir kommen danach zur Fragerunde der Fraktionen. Die Fraktionen stellen zunächst alle gesammelt Fragen. Jeder Fragesteller hat zwei Fragen, die man entweder an einen Sachverständigen stellt oder eine gleiche Frage an zwei Sachverständige oder an zwei Sachverständige jeweils eine unterschiedliche Frage. Wie weit wir kommen, zu wie viel Runden, das werden wir dann je nach Zeitablauf sehen und auch entscheiden. Insofern habe ich jetzt glaube ich alles gesagt. Ich schaue noch in die Runde. Es gibt keine Rückfragen. Dann würden wir jetzt mit den Eingangsstatements beginnen und wir beginnen mit Frau Dr. Berger, bitte.

SV **Dr. Ariane Berger** (Bundesvereinigung der kommunalen Spitzenverbände, Berlin): Sehr geehrte Frau Vorsitzende, sehr geehrte Damen und Herren Abgeordnete, die kommunalen Spitzenverbände unterstützen das Koordinierungsprojekt Registermodernisierung des IT Planungsrates und tragen auch die von der Bundesregierung geplante Einführung der Steuer-ID als einheitliches Ordnungsmerkmal dem Grunde nach mit. Die geplante Registermodernisierung ermöglicht zwei zentrale Funktionalitäten, die aus kommunaler Sicht Voraussetzung für eine gelungene Digitalisierung der deutschen Verwaltung sind. Sie ermöglicht dem Bürger, digitale medienbruchfreie Anträge auf OZG-Verwaltungsleistungen zu stellen und seine Daten dabei nicht jedes Mal neu, sondern nur einmal, once only, abzugeben. Und sie ermöglicht der Verwaltung, ihre in den Registern vorhandenen digitalen Daten automatisiert, valide und datensicher zwischen den Behörden austauschen zu können. Die OZG-Verwaltungsleistungen basieren regelmäßig darauf, dass unterschiedlichste Informationen aus unterschiedlichsten Quellen zusammengeführt werden müssen. Zwar werden sowohl die kommunalen Personenstands- und die kommunalen Melderegister bereits jetzt vollständig elektronisch geführt und sind untereinander vernetzt. Aber das Ziel des Onlinezugangsgesetzes einer sehr viel stärkeren Vernetzung bestehender Register und eben auch kommunaler Datenbestände in den Fachverfahren kann bislang aufgrund von rechtlichen und auch technischen Hindernissen, Einschränkungen nicht umgesetzt werden. Voraussetzung hierfür sind standardisierte hochqualitative Daten. Datenerfassung, Datenverarbeitung und Datenaustausch in der öffentlichen Verwaltung müssen sehr viel stärker als bisher standardisiert werden.

Der vorliegende Gesetzentwurf nimmt als einen ersten Schritt in diese Richtung die Standardisierung der sogenannten Grunddaten natürlicher Personen in den Blick, also insbesondere Name, Anschrift, Geschlecht und Geburtsdatum. Auf diesen Basisdaten setzt jede Verwaltungsleistung auf. Diese Daten müssen stimmen und die eindeutige Zuordnung einer Person ermöglichen. Die Bundesregierung schlägt als Standard für diese Grunddaten die Steuer-ID vor. Aus kommunaler Sicht ist diese Form der Standardisierung keinesfalls zwingend, aber gut vertretbar. Sie setzt auf einer bestehenden kommunalen Praxis auf und lässt sich grundsätzlich verfassungskonform ausgestalten. Die Steuer-ID wird von den Kommunen bereits jetzt im Melde- und im Personalwesen verwendet, setzt also auf bestehenden kommunalen Kommunikationsstrukturen auf. Aber die Einführung eines einheitlichen Ordnungsmerkmals bei Personen erfordert freiheitssichernde Maßnahmen, um die Gefahr einer missbräuchlichen Profilbildung einzuhegen. Aus kommunaler Sicht kommt es dabei entscheidend auf die Beibehaltung der bestehenden dezentralen Datenhaltung in den kommunalen Fachverfahren und Registern an. Eine Zusammenführung der Grunddaten der Personen ist nur dann zulässig, wenn die Fachdaten weiterhin dezentral in den verschiedenen staatlichen und kommunalen Datenspeichern geführt werden. Nur so kann Profilbildung nachhaltig verhindert werden. Nur so kann Datensicherheit und Verfügbarkeit gewährleistet werden. Dezentral durch Kommunal- und Landesverwaltung verantwortete Datenspeicher können viel leichter wieder abgeschottet werden als zentrale Register und im Übrigen auch zentrale Fachverfahren auf Bundesebene, sollten tatsächlich einmal Missbrauch und rechtswidrige Überwachung festgestellt werden. Dezentrale getrennte Datenhaltung ist freiheitsschonend. Ein Grundsatz, den das Bundesverfassungsgericht in der Vergangenheit mehrfach und auch jüngst in seiner Entscheidung zur Verfassungswidrigkeit des Antiterrordateigesetzes ausgeführt hat. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Frau Dr. Berger, vielen Dank. Dann als nächstes Frau Bock, bitte.

SV **Kirsten Bock**: Vielen Dank. Sehr geehrte Frau Vorsitzende Lindholz, sehr geehrte Abgeordnete, meine Damen und Herren, die Bundesregierung plant mit dem Entwurf eines Registermodernisierungsgesetzes die Modernisierung der deutschen Verwaltung. Das ist legitim und überfällig. Wesentlicher Regelungsgegenstand ist das Identifikationsnummerngesetz zur Einführung einer lebenslangen registerübergreifenden Identifikationsnummer mit dem Ziel, die Effizienz der deutschen Verwaltung zu steigern. Im Zentrum der Registermodernisierung sollte aber nicht allein die Effizienz, sondern die Gewährleistung von moderner demokratiefester und grundrechtsverträglicher Verwaltung für die Bürger*innen unseres Landes stehen. Das lässt der

Entwurf noch nicht erkennen. Für die Steuer-ID wurde bei deren Einführung die alleinige Bindung zu Steuerzwecken versprochen. Jetzt soll sie zu einer lebenslangen bereichsübergreifenden Identifikationsnummer werden. Damit wird ein Damm gebrochen, den aller Voraussicht nach das Bundesverfassungsgericht wieder wird flicken müssen. In einer Reihe von Verfahren, maßgeblich im Volkszählungsurteil, hat das Bundesverfassungsgericht deutlich gemacht, dass bereits die Erschließung eines Datenverbundes durch ein einheitliches Personenkennzeichen (PKZ), das die Erstellung umfassender Persönlichkeitsprofile ermöglicht, verfassungswidrig ist. Die Schaffung einer registerübergreifenden Kennzahl und der Nutzung respektiert die verfassungsrechtlichen Anforderungen so noch nicht.

Auch das Datenschutzrecht stellt – und das betont insbesondere Artikel 87 der Datenschutz-Grundverordnung (DSGVO) – die Verarbeitung personenbezogener Daten auch und gerade mittels eines Identifizierungsmerkmals unter Bedingungen. Von einer generellen Vereinbarkeit einer Kennziffer mit dem europäischen Datenschutz und dem Verfassungsrecht kann daher nicht ausgegangen werden. Es kommt vielmehr auf die konkrete Ausgestaltung der Identifikationsnummer und der zur Nutzung verbundenen Verfahren an. Hier bedarf es noch erheblicher Anstrengungen, um die Eingriffsintensität einer lebenslangen Kennziffer auszugleichen. Wird – und dafür spricht die Lebenserfahrung – das Kennzeichen auch im Wirtschaftsleben aufgegriffen, wird ein allumfassendes Personenabbild nicht nur möglich, sondern Realität werden. Die Schnittstellen sind schon jetzt über die Krankenkassen, Arbeitgeber und Geldinstitute vorhanden. Zu einem Aufweichen der Zweckbindung darf es aber nicht kommen. Der für das Datenschutzrecht schlechthin konstituierende Zweckbindungsgedanke gilt auch und gerade für Personenkennzeichen. Zwar ist Zweck eines registerübergreifenden Identifikationsmerkmals die Verkettung von Informationen, doch das allein ist kein Grund, den Zweckbindungsgedanken aufzugeben, denn Sinn und Zweck der DSGVO ist gerade, Verkettung unter Bedingungen zu stellen. Der Umstand, dass eine Verkettung stattfindet, macht damit die Zweckbindung nicht obsolet. Im Gegenteil: Je höher das Verkettungspotenzial, desto höher sind auch die Anforderungen, die das Datenschutzrecht an die Verarbeitungsbedingungen stellt. Zudem ist eine einheitliche Identifizierungsnummer schon darum nicht erforderlich, weil mit bereichsspezifischen Kennzahlen weniger eingriffsintensive Alternativen bestehen, die zudem sicherstellen, dass das informationelle Trennungsprinzip nicht unterlaufen wird. Aber selbst wenn die Erforderlichkeit der ID bejaht würde, wären die vorgesehenen technischen und organisatorischen Schutzmaßnahmen nicht ausreichend. Auch nicht über das sogenannte 4-Corner-Modell, weil es die organisationsinternen Risiken nicht adressiert. Und machen wir uns nichts vor. Bei der Datenschutzaufsicht bestehen keine ausreichenden Ressourcen, um die ordnungsgemäße Nutzung der Identifikationsnummer zu kontrollieren. Und das wäre in einem hohen Maße erforderlich, denn allein die Verkettungsmöglichkeiten der Lebensbereiche der Bürger*innen führen in ihrer Gesamtheit zu einer außerordentlichen Eingriffsintensität. Verfassungsrechtlich ist das so nicht zu rechtfertigen. Auch die Ausgestaltung des Datencockpits als halbherziges Transparenztool ist noch nicht geeignet, die durch die Verkettungsmöglichkeiten intensivierte Machtasymmetrie zwischen Bürger*innen und staatlicher Verwaltung auszugleichen. Und was ich auch vermisse ist die Datenschutzfolgenabschätzung nach Artikel 35 DSGVO. Wenn sie Sinn machen soll, wird sie nicht – wie bei der CWA zum Beispiel – mit der heißen Nadel gestrickt, sondern betrachtet umfassend alle Risiken und Schutzmaßnahmen. Darauf bin ich sehr gespannt. Völlig außer Acht gelassen wird – und das wundert mich insbesondere bei der sonst auf Sicherheit so bedachten Bundesregierung schon – das Angriffspotenzial, das zentralisierte Systeme bieten. Die Möglichkeit von Cyberwars ist längst nicht mehr nur Science Fiction. Eine einheitliche Identifikationsnummer ist sicherlich praktisch, aber bei einer feindlichen Übernahme, etwa durch Identitätsdiebstahl oder Denial-of-Service-Attacken, die jetzt schon zum Alltag gehören, bietet eine föderierte Infrastruktur einen erheblichen Vorteil.

Meine Damen und Herren, der Verzicht auf die Steuer-ID als allgemeines Personenkennzeichen bei der Registermodernisierung ist aus verfassungs- und datenschutzrechtlichen Gründen geboten. Dadurch entginge die Bundesregierung der hohen Gefahr weiterer Verzögerungen, Kosten und Vertrauensverlusten, die bei einer höchstwahrscheinlichen Verfassungswidrigkeit der Verwen-

dung der Steuer-ID als allgemeines Personenkennzeichen entstünde. Der Verwaltungsaufbau der Bundesrepublik Deutschland steht einer bereichsspezifischen Lösung mit verbesserter Interoperabilität zwecks Gewährleistung moderner Verwaltung nicht entgegen, ja ist sogar dafür prädestiniert. Die Bundesregierung könnte aus der Not eine Tugend machen und richtungsweisend zeigen, dass moderne, zukunftsgerichtete Verwaltung Rechte und Freiheiten der Bürger*innen in einer digitalisierten Welt gewährleisten und schützen kann. Dieses staatliche Interesse besteht nicht nur im Hinblick auf die Gewährleistung der informationellen Selbstbestimmung der einzelnen Bürger*innen als Teil ihres Grundrechts auf Datenschutz, sondern setzt auch die informationelle Gewaltenteilung um, die einen wesentlichen Beitrag zur Demokratiefestigkeit des Staates leistet. Mit einem bereichsspezifischen Kennzeichen und einer föderierten Struktur wird nicht nur der leichte Aufbau eines Profilbildungs- und Überwachungssystems erschwert, sondern sie ermöglicht zudem auch einen verbesserten Schutz und eine Verringerung der Angriffsflächen gegenüber feindlichen Angriffen aus Drittstaaten. Allein die Zunahme von Cyberangriffen auf staatliche Verwaltung macht deutlich, dass bei der Modernisierung der Verwaltung die Digitalisierung nur einen Teilaspekt darstellt. E-Government muss demokratiefest sein. Das bedeutet, Digitalisierung nicht um der Digitalisierung Willen. Länder wie Dänemark machen es uns hier vor. Verwaltung und E-Government sollten so aufgebaut sein, dass sie nicht mit einem Federstrich für autokratische Bestrebungen genutzt werden können. Einfache normative Schutzvorkehrungen, die nicht auch technisch implementiert werden, bieten langfristig keinen Schutz. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Ich darf dann auch die Bundesregierung mit Herrn Professor Krings noch begrüßen, das hatte ich vorhin vergessen. Der nächste in der Runde ist Herr Professor Kelber.

SV **Prof. Ulrich Kelber** (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bonn): Vielen Dank, Frau Vorsitzende. „Ein Personenkennzeichen wäre aber gerade ein entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren.“ Wie Sie sich wahrscheinlich denken können, zitiere ich an dieser Stelle aus dem Urteil des Bundesverfassungsgerichts von 1983. Was aber vielleicht nicht alle wissen werden ist, dass ich damit nicht nur das Verfassungsgericht zitiere, sondern auch den Vortrag der damaligen Bundesregierung selbst. Beide Seiten waren sich einig, dass ein Personenkennzeichen an sich eine übergroße Gefahr für das Recht auf informationelle Selbstbestimmung darstellt. Beide haben sich damit übrigens auf ein weiteres Urteil des Bundesverfassungsgerichts aus dem Jahr 1969 berufen, das Mikrozensus-Urteil, in dem festgelegt war, dass es einen unabdingbaren geistigen Innenraum gibt, der auch schon durch technisch neutrale Maßnahmen gefährdet sein kann, so lange sie einen gewissen psychischen Druck ausüben. Beide Seiten wussten damals: Ein Personenkennzeichen ist eine solche Maßnahme. Es wäre ein mächtiges Werkzeug, das es dem Staat erstmals erlauben würde, Daten einer Person einfach, verlässlich und schnell zusammenzuführen, also sozusagen eine Bestandsaufnahme zu machen.

Wie kam man damals darauf? Personenkennzeichnen erzeugen ein Ungleichgewicht zwischen Staat und Bürgern. Der Staat verfügt in diesem Moment über eine niedrigschwellige Möglichkeit, Daten zusammenzuführen, ohne dass er noch eine Beteiligung des Bürgers bräuchte. Und weniger Selbstbestimmtheit im grundrechtlichen Sinne geht nicht. Die Bürger werden sich nicht darauf verlassen können, dass es nie zu einem Miss- oder Fehlgebrauch kommen wird, sondern es droht eine Schere im Kopf, der Verzicht auf eine öffentliche Beteiligung oder ein ungewöhnliches Ausleben der Freiheit oder des Anspruchs auf bestimmte Leistungen. Diese abstrakte Gefahr für die Freiheit ist zeitlos, deswegen gilt das Argument, es seien alte Entscheidungen, an dieser Stelle nicht. Die Gefahr ist nicht an die technische Entwicklung gekoppelt, sie ist nicht nur in einer verstaubten Papierwelt präsent. Alleine das Ungleichgewicht über die Informationszusammenführung ist das Risiko. Wenn überhaupt ist es durch die zunehmende Zahl von Registern und Datenbanken und die technologischen Möglichkeiten der Verknüpfung in dieser Zeit angestiegen. Dieses Ungleichgewicht zwischen Staat und Bürgern muss – und da sind es moderne Technologien, die helfen können – ausgeglichen werden, um so ein Werkzeug überhaupt verfassungsrechtlich nutzbar machen zu können.

Was braucht es, um dieses immanente Ungleichgewicht zu beseitigen, um den Bürger auf Augenhöhe zu bringen? Umfassende Transparenz, Beteiligung sowie systematische und architektonische Hemmnisse für die missbräuchliche, fehlgeleitete, niedrigschwellige Verknüpfung. Diese Punkte versucht der Entwurf der Bundesregierung anzugehen. Es bleibt aber hinter dem zurück, was notwendig wäre, um eine wirksame Gleichstellung von Staat und Bürgern zu erreichen. Erstens. Der Entwurf nutzt die Steuer-ID als einheitliches Personenkennzeichen. Das kann nicht architektonisch ausreichend eingefangen werden. Das dafür vorgesehene und zudem nur unzureichend umgesetzte 4-Corner-Modell schützt nicht vor einer Umgehung oder einem Fehlgebrauch des Systems. Auch vor Angriffen von außen schützt ein einheitliches Kennzeichen nicht. Mit bereichsspezifischen Kennzeichen gäbe es eine effektivere Alternative. Zweitens. Der Entwurf bindet das Personenkennzeichen nur unzureichend an den Zweck der Identitätsfeststellung zur Erbringung von digitalen Verwaltungsdienstleistungen. Ein zweckänderndes Ausbluten in andere Verwaltungs- oder sogar Gesellschaftsbereiche ist so nicht zu verhindern. Dieses Ausbluten kann bereits aktuell in einem Referentenentwurf des Gesundheitsministeriums beobachtet werden, bei dem die Sicherungen des Registermodernisierungsgesetzes, die unzureichend sind, sogar ganz fehlen. Drittens. Der Entwurf spart – übrigens entgegen dem Koalitionsbeschluss – viele Übermittlungen vom 4-Corner-Modell aus. Der Steuerbereich, der mit Verabschiedung des Registermodernisierungsgesetzes ja auch das einheitliche Personenkennzeichen einsetzt, wird komplett von allen Ausgleichsmaßnahmen ausgenommen. Und das, obwohl das 4-Corner-Modell die Angriffsflächen reduziert und einmal aufgesetzt auch nicht technisch komplexer im Verbindungsaufbau als herkömmliche Kommunikationsverbindungen ist. Deswegen glaube ich, dass der Gesetzgeber deutlich nachbessern muss, um das Vorhaben mit den verfassungsrechtlichen Anforderungen in Einklang bringen zu können. Man kann sogar bei der Fragestellung weitergehen und hinsichtlich der Transparenz, die mit dem Datencockpit berücksichtigt wurde, eine konsequente Weiterentwicklung, nämlich den Abruf von Bestandsdaten durch den Bürger, frühzeitig ermöglichen, zusammen mit echten architektonischen Sicherungen. Vielen Dank, Frau Vorsitzende.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Professor Kelber, vielen Dank. Herr Professor von Lewinski, bitte.

SV **Prof. Dr. Kai von Lewinski** (Universität Passau): Danke. Das Persönlichkeitsprofil ist der Gottseibeiuns des Datenschutzrechts. Und das Personenkennzeichen ist sein Gehilfe. So jedenfalls steht es in der Bergpredigt des Datenschutzrechts im Volkszählungsurteil, von dem wir eben schon gehört haben. Ein Datenschutzgeist, der stets verneint, wird das nun alles als Teufelei in einen Hexenkessel werfen. Die verfassungsrechtliche Analyse führt aber zu einem differenzierten Bild. In meiner Stellungnahme, die ich ja vorab gemacht habe, wurden deshalb die hiermit verbundenen verfassungsrechtlichen Fragen in einen ganz schulmäßigen Prüfungsaufbau gepackt. Damit will ich Sie, soweit Sie Juristen sind, nicht in Ihr erstes Semester zurückversetzen, sondern will das erreichen, wofür ein juristischer Prüfungsaufbau da ist, nämlich, dass Sie fachlich und konsentiert die jeweiligen Argumente und auch damit streitigen Argumente verorten können. Das ist insbesondere bei einem potenziell emotional so aufgeladenen Thema wie der Personenkennziffer sicherlich sinnvoll und hilfreich. Entlang der Prüfungsreihenfolge sind meine Ergebnisse kurzgefasst wie folgt: Das Europarecht macht keine relevanten Vorgaben für das hiesige Vorhaben, vor allem keine, die über die verfassungsrechtlichen Anforderungen des Grundgesetzes hinausgehen würden. Bei der verfassungsrechtlichen Analyse ist zwischen dem Personenkennzeichen und dem Persönlichkeitsprofil zu unterscheiden. Nur das Persönlichkeitsprofil bildet eine absolute Grenze für die Verdatung von Menschen. Ein Personenkennzeichen ist als solches datenschutzrechtlich, da es keinen semantischen Gehalt hat, sogar trivial. Für die Vorgabe der Registermodernisierung brauchen wir zunächst einmal eine gesetzliche Grundlage. Das ist hier unproblematisch. Ein Gesetz liegt vor. Ein solches Vorhaben muss ein legitimes Ziel verfolgen – das ist glaube ich hinsichtlich der Digitalisierung, Verwaltungseffekte unstreitig – und die Identifikationsnummer muss hierfür ein geeignetes Mittel sein. Auch das wird – soweit ersichtlich – nicht bestritten. Die Frage, um die es hier geht, ist wohl juristisch gesprochen auf der Stufe der Erforderlichkeit zu diskutieren, also die Frage, ob es ein gleich geeignetes, aber grundrechtschonenderes Mittel gibt. Diese Frage müssen vornehmlich

Verwaltungswissenschaftler und IT-Sicherheitsmenschen beurteilen; es sind einfach zum Großteil technische Fragen. Die Argumente scheinen mir sowohl bei der Durchmusterung der Literatur als auch der bisher eingegangenen Stellungnahmen für beide Fragen nicht eindeutig in eine Richtung zu weisen. Sowohl hinsichtlich der gleichen Eignung wie auch hinsichtlich womöglich zusätzlicher Datenschutz- und Datensicherheitsrisiken von Alternativmodellen ist im Vorfeld einiges vorgebracht worden, was aber Menschen aus der Praxis und Menschen aus den Serverräumen dieser Welt besser beurteilen können als ich.

Wozu ich wieder etwas mehr und originär etwas sagen kann als Verfassungsrechtler ist die Frage der Angemessenheit, die wir in den juristischen Hörsälen auch Verhältnismäßigkeit im engeren Sinne nennen. Hier geht es darum, die einschlägigen Verfassungsgüter zu identifizieren. Und wenn sie widerstreitend sind, müssen sie zu einem Ausgleich gebracht werden. Wir sprechen dann von praktischer Konkordanz. Praktische Konkordanz bedeutet, dass die Verfassungsgüter jeweils bestmöglich zur Geltung zu bringen sind. Die einschlägigen Verfassungsgüter hier sind natürlich die informationelle Selbstbestimmung auf der einen Seite, Effizienz der Verwaltung, Wirtschaftlichkeit, Rechtsstaatlichkeit, Sozialstaatlichkeit und Gleichheitsgebot auf der anderen Seite. Jetzt werden Grundrechte usw. natürlich nicht irgendwie abgewogen – nur eins auf der einen und fünf auf der anderen Seite, das wäre sicherlich zu simpel –, sondern es muss jetzt erst mal geschaut werden, welchen Rang haben diese Verfassungsgüter zueinander. Da wird man wohl sagen müssen, dass die Verwaltungseffektivität und die Wirtschaftlichkeit eher ein Hilfstopos ist. Ansonsten stehen Verfassungsgüter grundsätzlich – die Menschenwürde ausgenommen – alle auf derselben Stufe, also die informationelle Selbstbestimmung, Rechtsstaatlichkeit, Sozialstaatlichkeit und Gleichheit. Die sind nun zu praktischer Konkordanz zusammenzuführen, also man muss schauen, wie man eben die Gleichheit, Rechtsstaatlichkeit, informationelle Selbstbestimmung zueinander bringt, dass alle zur bestmöglichen Geltung kommen. Und hier sind sowohl im Gesetzesentwurf als auch in den begleitenden Vorschlägen eine Reihe von Vorschlägen gemacht worden. Das Datencockpit, was die Transparenz erhöht, dient sowohl der Rechtsstaatlichkeit als auch der Wirtschaftlichkeit als auch dem Datenschutz. Womöglich wird durch die Einführung dieses Systems dem Datenschutz jedenfalls an dem Ende entgegengekommen, als durch die Entbehrlichkeit von Stammdaten bei der Sachentscheidung pseudonyme Entscheidungen und Verarbeitungen im viel weiteren Maße möglich sind als bisher. Und die verbesserte Datenqualität durch einen engeren Abgleich der Register dient rechtsstaatlichen wie datenschutzrechtlichen Zielen gleichermaßen. Durch das Volkszählungsurteil und jetzt auch durch Artikel 87 Satz 2 DSGVO ist dem datenverarbeitenden Staat auch aufgegeben, technisch-organisatorische Maßnahmen zu treffen. Technischer Datenschutz, eine effektive Kontrolle, ein effektiver Rechtsschutz und effektive Sanktionierungen sind hier die Stichworte. Hierüber im Einzelnen kann in der Diskussion noch gesprochen werden.

Als letzten Punkt möchte ich noch etwas anmerken. Es geht ein klein bisschen über den engen Auftrag des Sachverständigen, zu diesem Gesetzesvorschlag Stellung zu nehmen, hinaus. Ich möchte nämlich noch auf eine Wechselwirkung hinweisen. Dass nämlich je mehr ein Staat regelt und deshalb je mehr er über den Einzelnen weiß, desto eher ist die kritische Masse erreicht, die dann zu einem Persönlichkeitsprofil führt. Es ist also nicht nur die Identifikationsnummer, die hier die datenschutzrechtliche Gefahr beschreibt, sondern der gewachsene Sozial- und Überwachungsstaat. Der Leistungsstaat überhaupt ist im Zusammenwirken mit der Identifikationsnummer das Problem. Wenn gesagt wird, dass der moderne Leistungsstaat eine PKZ oder eine Identifikationsnummer oder eine Registermodernisierung erfordert, ist es ein Argument, das man auch gegen den Leistungsstaat überhaupt wenden kann. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Dann Herr Professor Parycek.

SV **Prof. Dr. Peter Parycek** (Kompetenzzentrum Öffentliche IT am Fraunhofer FOKUS Institut und Donau-Universität Krems): Vielen Dank. Die datenschutzkonforme Registerlandschaft, die wir benötigen, steht glaube ich außer Streit. Das kann man aus der Stellungnahme glaube ich auch ganz gut herauslesen. Ich möchte trotzdem einen Punkt herausstreichen, und zwar, dass die höhere Datenqualität auch eine sehr inklusive Wirkung haben

kann, das heißt ein sozialpolitisches relevantes Faktum ist und daher von den Abwägungen berücksichtigt werden kann, weil wir wissen, dass gerade Transferleistungen in manchen Bereichen von weniger als 50 Prozent in Anspruch genommen werden. Und da gibt es natürlich auch eine Gewährleistungsverpflichtung des Staates, da Rahmenbedingungen zu setzen, dass es unter Umständen teilautomatisierte oder automatisierte Verfahren gibt, die solche Transferleistungen auch sicherstellen. Könnte man bis hin auch zur Frage stellen, ob das nicht auch das Grundrecht auf Eigentum mit umfasst, nach EMRK wären da Transferleistungen mit umfasst, also soziale Transferleistungen. Also das ist noch ein neuer Punkt, den man da in der Debatte glaube ich berücksichtigen kann. Das Weitere – es ist schon angesprochen worden, ich möchte es aber noch einmal herausstreichen: Die aktuelle Verwaltungspraxis ist aufgrund eines fehlenden Personenkennzeichens fast auf Datenmaximierung ausgelegt, weil man muss ja die Personen auch jeweils identifizieren können. Dazu werden jetzt über den eigentlichen Zweck des Verwaltungsverfahrens hinaus Datenpunkte gesammelt und auch gespeichert und verarbeitet. Und das widerspricht natürlich ganz massiv dem Datenschutzgrundsatz von Artikel 5 DSGVO und auch der informationellen Selbstbestimmung. Und des Weiteren wissen wir – und das ist auch mehrfach dargelegt worden –, dass die Datenqualität nicht ausreichend ist, also dass es daher auch zu Fehlauskünften kommen kann. Also, damit sind wir auch was die Datenintegrität betrifft, und da reden wir schon von maßgeblichen Datenschutzgrundsätzen, sind aktuell in der Verwaltungspraxis – das kann man auch jetzt nicht schönreden – nicht gegeben. Und das ist glaube ich daher ein ganz wesentlicher Punkt, den man in der Debatte mit berücksichtigen muss.

Das, was glaube ich nachvollziehbar ist, keiner will von uns ein digitales Persönlichkeitsprofil, das der Staat auch noch abrufen kann. Ich glaube, das ist die Horrorvorstellung von uns allen. Wir sehen, dass das in der Wirtschaft teilweise passiert ist. Und das ist natürlich die absolute Horrorvorstellung in einem demokratischen Rechtsstaat, dass ein digitales Persönlichkeitsprofil abrufbar ist. Die Frage, und da trennen sich glaube ich jetzt ein bisschen die Perspektiven, ich bin davon zutiefst überzeugt, dass eine Personennummer oder eine Identifikationsnummer, also die Verhinderung solch einer Nummer, keine Schutzwirkung heutzutage mehr hat, weil so viele Datenpunkte wiederum verspeichert sind, dass der Zugang, das ist das einzige, was entscheidend ist, ist der Zugang zu den Daten. Wenn ich den Zugang zu den Daten habe, dann kann ich über Datenanalysewerkzeuge sehr schnell eine hohe Deckung von weit über 50, 60, 70 Prozent erreichen, je nachdem wie viele Datenpunkte vorhanden sind. Und für Personen wie für mich ist das Verbot einer Personenidentifikationsnummer gar kein Schutz. Herr Parycek ist eindeutig. Also, so gesehen bleiben da wenige Prozent nur über am Ende eines Datenabgleichs, der tatsächlich nicht zu einem digitalen Persönlichkeitsprofil herausgearbeitet werden kann. Daher ist der Zugang das Entscheidende. Und ich glaube, da muss man bei der Debatte ganz, ganz intensiv draufschauen: Wie kann der Zugang zu den Datenbeständen möglichst gering gehalten werden? Und da – und das muss man jetzt wirklich sagen – ist das fast eine historische Chance, weil Deutschland eines der ganz wenigen Länder ist, das noch keine zentralen Register eingeführt haben. Alle führenden E-Government-Nationen haben zentrale Register auf Bundesebene eingeführt. In diesem Ansatz, der jetzt vorliegt, wird auf dezentrale Register gesetzt zur Verteiltheit. Das entspricht auch dem Separierungsprinzip, das man aus der DSGVO ableiten kann und die in dieser auch da sehr gut dargestellt hat. Und das ist eine einmalige Chance, jetzt wo es dieses Zeitfenster gibt, das zu nutzen, um diese Daten auf den jeweiligen lokalen Ebenen zu lassen, weil das den Zugang beschränkt, nämlich auf die, die auch lokal den Zugang haben. Und nur in Ausnahmefällen dürfen ja auch die Daten zwischen unterschiedlichen Kommunen, Ländern übermittelt werden. Und zusätzlich zu dieser lokalen Aufteilung kommt dann noch das 4-Corner-Prinzip, das den Staat noch mal in Bereiche aufteilt. Hier wird, bevor ein Datum übermittelt wird, geprüft, ob das überhaupt zulässig ist, das heißt, nicht im Anschluss, sondern vor einer Übermittlung. Also das ist ein sehr wirkmächtiges Werkzeug, das auf der europäischen Ebene entwickelt worden ist, wo EC – das ist glaube ich bekannt – dieses Prinzip mitentwickelt hat, das auch schon in der … zum Einsatz kommt und auch bei dem Single Digital Gateway zum Einsatz kommen wird, daher auch schon geprüft ist und man da eine gewisse Qualität und da schon viele Entwicklungsstunden hineingelaufen sind. Und

zusätzlich – ist auch schon genannt worden, ich möchte das auch wirklich noch einmal herausstreichen – ist die Möglichkeit, die vorgesehen ist, dass der Bürger und die Bürgerin, die Betroffenen also, hier Einsicht haben, wozu sind ihre Daten überhaupt verwendet worden über das Datencockpit, eine maßgebliche Qualitätsverbesserung, was den Datenschutz betrifft. Heute ist das eine Blackbox für viele Bürger und Bürgerinnen. Und so lange kein System etabliert ist, bleibt es eine Blackbox. Das muss man an der Stelle glaube ich auch ganz deutlich unterstreichen.

Und damit komme ich zum letzten Punkt. Natürlich kann man sich wünschen, Systeme beliebig zu kombinieren. Das ist in der Theorie auch gut machbar. Also, wenn wir uns als Informatiker zusammensetzen, in der Theorie ist das darstellbar. Aber in der Praxis brauchen Sie ja Elemente, die auch schon im Einsatz sind, die getestet sind, wo es Erfahrungswerte gibt. Und das ist das, was bei den vorgeschlagenen Konzepten, die ich bisher gesehen habe, absolut fehlt. Es gibt kein BBK-System in einem dezentral verteilten System. Also, mir ist keins bekannt. Daher beginnt man hier bei null und hat damit ein sehr hohes Risiko, auch bei dieser riesigen Anzahl von Beteiligten, dass diese Projekte scheitern werden. Das wissen wir auch aus der Historie, da gibt es Forschungen dazu, dass gerade im öffentlichen Sektor Großprojekte immer wieder auch gescheitert sind. Und wenn so ein Projekt scheitert, dann geht es jetzt nur darum, dass ein IT-Projekt scheitert, sondern dass man die Datenschutzgrundsätze, die ich gerade angesprochen habe, eben nicht einhalten kann, dem Bürger nicht den Einblick in seine Daten gewährt. Und damit steht wesentlich mehr auf dem Spiel als ein weiteres gescheitertes Einzelprojekt.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Jetzt Herr Professor Richter, bitte.

SV **Prof. Eike Richter** (Hochschule der Akademie der Polizei Hamburg): Sehr geehrte Frau Vorsitzende, sehr geehrte Abgeordnete, sehr geehrte Damen und Herren, um was geht es eigentlich? Es geht darum – das möchte ich an dieser Stelle erst mal am Startpunkt sagen – natürlich auch um die informationelle Selbstbestimmung, auch um die Grundrechte, keine Frage, und es ist nicht unterzubewerten. Allerdings ist der Ausgangspunkt, die Modernisierung der Verwaltung und dazu die Möglichkeiten der Digitalisierung auch zu nutzen. Und Herr Parycek hat gerade noch mal darauf hingewiesen: Lange Jahre und Jahrzehnte sind wirklich vergangen und die Digitalisierung der Verwaltung ist nicht richtig vorangekommen. Es sind immer wieder die ähnlichen Verwaltungsreformprojekte angelaufen, immer wieder über neue Reformüberschriften. Ich erinnere mal an BundOnline 2005, Deutschland-Online. Projekte sind dort immer wieder gestartet worden, die es eigentlich schon immer gab, und sind doch nicht zum Erfolg gekommen. Herr Parycek hat gerade auch noch mal darauf hingewiesen. Auch das OZG ist so ein neuer Anlauf, von dem es jetzt keinesfalls ausgemacht ist, ob das gelingt. Es steht auch in dieser Reform ja Entwicklung. Von daher ist der Gesetzesentwurf unter der dahinterliegenden Motivation erst mal grundsätzlich zu begrüßen. Und das ist der Ausgangspunkt. Die Frage ist natürlich: Ist das vorgelegte Gesetz dann die Lösung? Dazu haben wir jetzt schon einiges gehört. Ich würde sagen, grundsätzlich ja, weil die Verknüpfung der Register einen wichtigen Schritt darstellt, die Potenziale der Digitalisierung für die Verwaltung zu nutzen. Dies hat auch Frau Dr. Berger am Anfang ausgeführt. Aber natürlich darf das nicht dazu führen, dass die verfassungsrechtlichen Grenzen überschritten und sonstige Risiken nicht so gut wie möglich vorgebeugt werden. Auch das hat zum Beispiel eben Frau Bock ausführlich ausgeführt, wo dort die Risiken liegen. Ich habe mich in meiner Stellungnahme darauf konzentriert, die Standpunkte und Vorschläge zu unterbreiten, die den bislang aufgeworfenen Erwägungen, Bedenken und Risiken Rechnung tragen können, und zwar auf zwei Ebenen und die werde ich kurz skizzieren. Nämlich einmal die Regulierung des vorgeschlagenen Modells zur Registermodernisierung selbst, dann aber auch die Methode und das Vorgehen der gesetzlichen Steuerung, wie das Gesetz es angeht. Die verbindende Klammer – das wird auch in verschiedenen Stellungnahmen hier deutlich – auch für die verfassungsrechtliche Bewertung ist die Frage der gesetzgeberischen Einschätzungsprärogative an dieser Stelle. Dazu werde ich auch noch was kurz sagen.

Bestehen eigentlich Bedenken, die die Verfassungsmäßigkeit als absolut ausgeschlossen erscheinen lassen? Ich würde sagen, im Ergebnis nein. Es bestehen zwar zahlreiche zum Teil eindringliche

Bedenken, die aber eine Verfassungswidrigkeit nicht zwingend erscheinen lassen. Die wichtigsten Punkte dazu ist die Frage zum Beispiel: Verletzt die Einführung der Steuer-ID den Kernbereich der informationellen Selbstbestimmung? Und – Herr Professor Kelber hat es gerade vorhin schon zitiert – aus dem bundesverfassungsgerichtlichen Urteil der Volkszählung in Maßnahmen wie zum Beispiel der Einführung eines einheitlichen für alle Register und Dateien geltenden Personenkennzeichens läge „ein entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, weil sie es erst erlauben, diese Daten zusammenzuführen.“ Es gibt glaube ich kaum Seiten in den Urteilsbänden des Bundesverfassungsgerichts, die abgegriffener sind als die, habe ich jedenfalls das Gefühl, weil man mittlerweile alles Mögliche darin versucht zu interpretieren, jeden Artikel, jedes Komma, jeden Rechtschreibfehler – die es hoffentlich nicht gibt. Man kann jetzt darüber philosophieren und sagen, das Gericht spricht von einem Schritt. Ja, es spricht von einem Schritt. Aber ist das genau das, was tatsächlich unzulässig ist, oder ist das, was eigentlich danach folgt, eigentlich das, was unzulässig ist? Kann man sagen, dass es nicht nur eigentlich die Einführung eines Kennzeichens an sich gibt, was verboten ist oder was unzulässig ist, sondern eigentlich die dahinterliegende Profilbildung, wenn die stattfindet? Das wäre ja auch so möglich zu verstehen. Ich will mich da jetzt gar nicht festlegen, sondern eher sagen, es ist echt Kaffeesatzleserei, weil mittlerweile auch nicht nur vor dem Hintergrund der zurückliegenden Zeit des Urteils – das will ich gar nicht mal sagen, da stimme ich Herrn Professor Kelber zu – das hat natürlich auch eine gewisse abstrakte Richtigkeit weiterhin. Allerdings ist es eben so ein Urteil, das von einem anderen Kontext, von einem anderen technischen und von einer gesellschaftlichen Entwicklung entschieden worden ist. Und das Recht ist nicht in einem normativ absolut freien Raum, sondern bewegt sich in Rückwirkung mit dem Realitätsbereich. Aber selbst wenn man so ein darin explizites Verbot von einem allgemeinen Personenkennzeichen sehen würde, müsste man dann auch noch unterscheiden: Ist das jetzt ein allgemeines Personenkennzeichen, was hier geregelt ist? Ab wann ist denn etwas dann allgemein? Da kann man jetzt anfangen und sagen, es sind ja nur ein Viertel der Register betroffen und nicht alle. Ist ja gar nicht allgemein. Aber auf diese Spiele kann man sich jetzt einlassen. Ich finde, es führt nicht sehr viel weiter, sondern im Grunde bleibt da die Frage: Wie schätzt der Gesetzgeber die Situation dann ein vor diesem normativen Hintergrund und wie übt er das aus? Dazu will ich am Ende noch etwas sagen.

Dann ist natürlich der nächste Schritt bei der verfassungsrechtlichen Bewertung tatsächlich das, was auch Herr Professor von Lewinski schon angesprochen hat, die Frage der alternativen Mittel, die Frage der Erforderlichkeit. Gibt es eigentlich Alternativen, wirklich mildere Mittel als das hier im Gesetz vorgeschlagene Modell zum Beispiel das vom bereichsspezifischen Personenkennzeichen? Sicherlich werden wir von Herrn Professor Sorge gleich noch etwas dazu hören, aber was natürlich dann auch übrig bleibt, auch hier verbleiben nicht unerhebliche Unsicherheiten in der Entscheidungsgrundlage. Das muss dann auch genauso normativ bewertet werden. Die Frage ist: Wie hoch ist das Missbrauchsrisiko zum Beispiel bei dem hier vorgeschlagenen Modell bereichsübergreifender Kennzeichen? Wie ist die Missbrauchsgefahr bei einem anderen Modell? Wie sieht es aus mit der Wirtschaftlichkeit? Also auch dort gibt es im Grunde ja keine Hundertprozentlösung, sondern auch eine gewisse Unsicherheit. Auch hier – und das sieht man auch in den einen oder anderen Stellungnahmen – letztendlich kommt es wieder auf die Einschätzungsprärogative des Gesetzgebers an. Und das ist nicht etwas, was von ungefähr kommt. Allerdings muss man an dieser Stelle sagen, wenn man den bisherigen Gesetzgebungsverfahrensstand sieht einschließlich des Entwurfs der Bundesregierung, kann man als unvoreingenommener Leser das Gefühl haben, es ist hier und da wirklich etwas schmal. Man kann nicht genau sehen, warum der Gesetzgeber etwas genau gemacht hat. Am Beispiel der Erforderlichkeit wird das deutlich. Die Alternativen sind doch sehr kurz aufgeführt und es fehlt zum Beispiel ein eigenständiger Vergleich mit anderen Modellen. Das hätte man sich an der Stelle gewünscht, um zu sehen, wie der Gesetzgeber im Gesetzgebungsverfahren insgesamt seine Einschätzungsprärogative auch ausübt und dokumentiert.

Bei der Angemessenheit, wenn man also davon ausgeht, dass der vorliegende Entwurf so gesehen erforderlich wäre, wo ich mich an dieser Stelle aber nicht festlegen will, weil es mir um eine andere

Position geht, dann käme es aber natürlich darauf an, dass der vorliegende Entwurf auch angemessen ist, das heißt also, das verfolgte Ziel in einem angemessenen Verhältnis zur Betroffenheit der informationellen Selbstbestimmung steht. Und da möchte ich ein Wort vorab zum legitimen Ziel sagen, nämlich der Verwaltung zu ermöglichen, die digitalen Potenziale zu nutzen, um effizienter und zügiger zu arbeiten, aber auch, um die Erwartungen der Bürger zu erfüllen, die diese an die Verwaltung 30 Jahre nach Kommerzialisierung des Internets eigentlich stellen darf. Und da möchte ich auch Frau Dr. Berger an der Stelle schon mal zusprechen, dass – wie ich es teilweise gelesen habe – das als solches kein Wert sei. Es ist in der Tat in der Verfassung nicht direkt verankert und man kann es nicht lesen, aber das Internet kann man da drin auch nicht finden. Also in der Hinsicht muss man dann besser schauen, wie man die Verfassung vor dem Hintergrund heute liest. Und natürlich haben wir ein massives Interesse daran, dass eine Verwaltung in unserem Staat in der Lage ist, handlungsfähig ist, eigenständig bleibt und ausgestattet ist, tatsächlich diese Funktionen und diese Rolle zu übernehmen in der Eigenständigkeit, die sie hat. Und man kann auch tatsächlich dafür Anknüpfungspunkte finden. Ich sage mal einen, der noch etwas unbeleuchtet ist, weil er so fremd wirkt. Das ist Artikel 41 der Grundrechtecharta der EU – das Recht auf gute Verwaltung. Wir können ja mal überlegen, was das eigentlich heute genau bedeuten könnte. Man sollte finde ich also das verfassungsrechtliche Gewicht dieses Ziels, das dahinter steht, nicht so einfach abtun und auch nicht geringschätzen. Es ist tatsächlich etwas, was wichtig ist, gerade vor dem Hintergrund der Reformentwicklung der letzten Jahre. Dennoch ist es natürlich wichtig, das hilft nichts dabei, die Risiken, die bestehen für die informationelle Selbstbestimmung, so gut wie möglich zu minimieren. Und deswegen sozusagen habe ich auch in der Stellungnahme einige Vorschläge, auch konkrete Vorschläge, gemacht, die natürlich auch von anderen mitvertreten werden, tatsächlich die Risiken weiter zu minimieren. Und ich finde, die müssen auch ernsthaft erwogen und darüber entschieden werden eben im Sinne auch der Einschätzungsprärogative, wie zum Beispiel die Ausweitung des 4-Corner-Modells, die Schutzmechanismen auszuweiten, Ende-zu-Ende-Verschlüsselung und so weiter, auch zum Beispiel die Konkretisierung und Einführung der Zweckbindung. Herr Professor Kelber hat darauf bereits schon hingewiesen.

Jetzt ganz kurz zum Abschluss. Reicht es also demnach, sich jetzt einfach immer auf die Einschätzungsprärogative zu berufen? Und da geht noch mal ein ganz wichtiger Punkt: Ja, das ist ein wichtiger Punkt, weil dahinter steht letztendlich das Demokratieprinzip, nämlich Entscheidungen zu treffen in dem Moment, wenn sie unsicher sind oder unter Ungewissheit laufen, dass dann der demokratische Gesetzgeber nämlich hier unmittelbar demokratisch legitimiert die Entscheidungsmacht hat und auch die Verantwortung hat, jedenfalls zuerst zu entscheiden. Und das sollte man auch wahrnehmen. Nur, es wäre jetzt ein Irrtum, wenn man das als Freibrief verstehen würde, sondern das ist selbst in dem Moment wieder an die Verfassung rückangebunden, so wie es in Artikel 20 Absatz 3 steht und das Bundesverfassungsgericht hat sich auch vermehrt gerade in Bereichen der schnellen Innovationsentwicklung wie zum Beispiel Digitalisierung immer wieder auch darauf hingewiesen, dass man dort als Gesetzgeber einer Nachschau gewisser Sicherungsmechanismen sozusagen unterliegt. Und das würde ich hier auf jeden Fall anraten, gerade im Hinblick auf die verfassungsrechtliche Bewertung, nämlich dass erkennbar wird, dass der Gesetzgeber seinen Einschätzungsspielraum in vertretbarer Weise gehandhabt hat, sich ein sicheres Urteil bilden konnte und auch natürlich gerade, wenn es dann um besonders höherwertige Rechtsgüter geht oder besonders hohe Eingriffsintensitäten, so wie hier. Und da muss ich ganz ehrlich sagen, könnte oder sollte bei dem Entwurf hier noch etwas nachgebessert werden. Es muss klar erkennbar sein, dass die Auseinandersetzung mit der verfassungsrechtlichen Vereinbarkeit massiv und intensiv überdacht worden ist. Und dann als Ergänzung dazu habe ich auch in meiner Stellungnahme vorgeschlagen: Wenn eine Unsicherheitssituation entsteht, dann hat das Bundesverfassungsgericht auch häufig betont, dass es dann dem Gesetzgeber obliegt, auch entsprechende Eigenkontrollmechanismen und Nachschauen einzuräumen. Und wenn ich zum Beispiel die Evaluationsfristen lese, die beginnen im sechsten Jahr nach Inkrafttreten des Gesetzes. Das heißt also, wenn jetzt der BGB-Spezialist um die Ecke kommen würde und sagen, ja, dann rechnen wir das erste Jahr noch nicht mal

mit, dann sind es schon sieben Jahre. Das finde ich nicht passend. Digitalisierungsgesetze haben drei bis vier Jahre, um eben genau dort die Entwicklungen nachzuschauen. Und was natürlich auch fehlt, ist ein tatsächlicher Zwang, das Geschehen, das man jetzt vielleicht nicht abschließend beurteilen kann, wieder auf die Tagesordnung des Gesetzgebers zu heben. Das heißt, ich würde ernsthaft anraten, über eine Befristung des Gesetzes nachzudenken – die Argumentation, die Begründung dafür im Gesetzentwurf haben mich nicht überzeugt –, damit man auf jeden Fall zu späterer Zeit wieder das Thema aufrufen kann. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Den Schluss in der Runde macht Herr Professor Sorge.

SV **Prof. Dr.-Ing. Christoph Sorge** (Universität des Saarlandes, Saarbrücken): Jawohl, ich danke Ihnen, Frau Vorsitzende. Ich habe hier Folien freigegeben. Ich hoffe, Sie können die sehen. Ansonsten kann man glaube ich aber auch ohne die Folien folgen. Ich möchte zunächst betonen, die Ziele des Registermodernisierungsgesetzes sind ja absolut nachvollziehbar. Es bietet Chancen, Register zu verknüpfen, man kann Inkonsistenzen vermeiden, Doppeleingaben und kann unter Umständen sogar in einzelnen Registern die Datenspeicherung reduzieren, wenn man Daten aus anderen Register abrufen kann. Gleichzeitig ist natürlich die Zusammenführungsmöglichkeit schon gerade in der heutigen Zeit, wo man das sehr einfach, sehr schnell und mit über 50 Registern sehr umfangreich machen kann, ein Eingriff in das informationelle Selbstbestimmungsrecht. Eine Gefahr entsteht auch durch mögliche Cyberangriffe, mit denen wir ja alle leider mittlerweile vertraut sind. Das heißt, verfassungskonforme Registerverknüpfung benötigt jedenfalls einen wirksamen technischen und organisatorischen Schutz. Der Entwurf sieht vor, die Steuer-ID sehr breit zu verwenden. Schon jetzt ist im öffentlichen und im privaten Sektor verbreitet, beispielsweise bei Banken und Arbeitgebern. Auch das ist schon erwähnt worden. Ich denke, dass die Verwendung in zunächst mehr als 50 Registern, perspektivisch auch noch viel mehr Registern – die Möglichkeit steht ja offen – zu einem erhöhten Missbrauchsrisiko führt, zu erhöhten Gefahren durch Cyberangriffe und natürlich auch das Ganze aus meiner Sicht als allgemeines Personenkennzeichen einordnen lässt. Die Bezeichnung ist da an der Stelle natürlich nicht das relevante, sondern der Umfang der möglichen Datenzusammenführung. Eine so breite Verwendung der Steuer-ID ermöglicht die Umgehung von sinnvollen Schutzmaßnahmen, die ja im Regierungsentwurf durchaus vorgesehen sind. So ist das 4-Corner-Modell ja eine sehr sinnvolle Maßnahme. Eine dritte Stelle überprüft die Anfragen, bevor sie weitergegeben werden. Allerdings kann eine Datenzusammenführung anhand der Steuer-ID letztendlich auch ohne den intermediär funktionieren, gerade dann wenn die Steuer-ID zukünftig sehr weit verbreitet sein wird und sich eventuell gar als Authentifizierungsmerkmal etabliert, wenn also eine Bank oder eine Behörde davon ausgeht, wenn ich die Steuer-ID kenne, dann bin ich derjenige, der da behauptet es zu sein. Gerade in diesem Fall entstehen eben hohe Risiken. Es gibt mit bereichsspezifischen Kennzeichen eine datenschutzgerechtere Alternative ohne wesentliche Nachteile. Es gibt viele Möglichkeiten, wie man so etwas umsetzen kann. Ein Beispiel ist in meiner schriftlichen Stellungnahme auch erwähnt. Ich habe es hier auch noch mal auf der Folie dargestellt. Im Prinzip nimmt man die intermediäre, also Vermittlungsstelle oder Registermodernisierungsbehörde, die ohnehin schon vorgesehen sind, entwickelt sie weiter und gibt ihnen nur eine Zusatzfunktion, nämlich die Übersetzung von bereichsspezifischen Kennzeichen verschiedener Bereiche. Also eine registerführende Stelle schickt eine Anfrage mit ihren bereichsspezifischen Personenkennzeichen. Die Anfrage wird dann weitergeleitet mit dem bereichsspezifischen Personenkennzeichen eines anderen Bereichs, der intermediär dazwischen, übersetzt zwischen beiden bereichsspezifischen Personenkennzeichen ist. Keine Behörde muss jemals mit einem bereichsspezifischen Kennzeichen aus einem anderen Bereich umgehen. Das geht also alles in der bestehenden und vorgeschlagenen Registerstruktur, hat keine Einschränkung für das Datencockpit oder dergleichen zur Folge und es geht wie gesagt mit Intermediären, die man ohnehin braucht für das 4-Corner-Modell.

Wie auch schon richtig gesagt wurde in dieser Anhörung, führt dieses Alternativmodell noch nicht zu einem Schutz vor Missbrauch. Es verhindert auch keine Cyberangriffe. Es führt jedoch auch nicht zu neuen Risiken. Denn, wenn man in diesem Bild, was wir eben gesehen haben, die Tabelle bekommt, die die Zuordnung zwischen den bereichsspezifischen Kennzeichen verschiedener

Bereiche erlaubt, selbst dann ist man nicht weiter als jetzt schon mit der Steuer-ID, denn dann hat man eben die Kennzeichen, die in verschiedenen Bereichen verwendet werden. Bei der Verwendung der Steuer-ID als allgemeines Personenkennzeichen hat man das ohnehin. Insofern hat man kein neues Risiko. Man muss in der dargestellten Variante auch keine zusätzlichen Stammdaten bei den Intermediären speichern, sondern wirklich nur diese bereichsspezifischen Kennzeichen. Damit wird die Umgehung der Intermediäre erschwert. Man hat einen verbesserten Schutz beziehungsweise die Möglichkeit eines verbesserten Schutzes an dieser Stelle. Deshalb ist aus meiner Sicht auch zu bedenken, ob man die Intermediäre nicht weiter stärken kann, indem man sie einerseits bei unabhängigen Stellen ansiedelt wie der Datenschutzaufsicht. Das könnte das Vertrauen der Betroffenen stärken. Man kann diese Intermediäre auch in einer föderierten Umsetzung realisieren, das heißt, in einer verteilten Umsetzung. Man kann das ohne weiteres hinbekommen mit Intermediären pro Bundesland, was natürlich den Aufwand an dieser Stelle dann erhöhen würde, das muss ich hier einräumen. Die Intermediärsrolle kann in geeigneten Anwendungsfällen perspektivisch und nicht kurzfristig auch beim Betroffenen selbst liegen. Der kann eine App auf dem Handy haben oder er kann den Personalausweis benutzen, der ohnehin ja schon bereichsspezifische Kennzeichen vorsieht. Das ließe sich also problemlos erweitern in geeigneten Anwendungsfällen. Zugriffsbeschränkungen, wie sie auch der Regierungsentwurf schon vorsieht, wären strikt umzusetzen, insbesondere wäre der Schutz vor Innentätern mit Hardwaresicherheitsmodulen möglich, sicherlich nicht perfekt, aber man könnte damit, wenn man das jetzt schon gesetzlich regelt, glaube ich das Sicherheitsniveau deutlich erhöhen. Insgesamt lässt sich das aus meiner Sicht einfach umsetzen. Die Register speichern einfach das, was sie bisher speichern zusätzlich eines bereichsspezifischen Kennzeichens anstatt der Steuer-ID. Mehraufwand wäre nur bei den Intermediären. Auch der wäre aus meiner Sicht überschaubar. Und damit möchte ich schon enden, mich für die Aufmerksamkeit bedanken und freue mich auf die Fragerunde.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank für Ihre aller Stellungnahmen. Dann kommen wir jetzt zur Fragerunde und beginnen mit der Unionsfraktion und hier Herrn Henrichmann.

BE Abg. **Marc Henrichmann** (CDU/CSU): Vielen Dank. Ich glaube, in der Stellungnahme des Normenkontrollrates war die Aussage – und ich glaube, mit der können sich grundsätzlich alle hier versammeln –, dass es um den überragenden Nutzen der Registermodernisierung für die leistungsfähige digitale Verwaltung und den Bürokratieabbau geht. Und die Frage ist jetzt: Wie gestalten wir den Weg dahin? Und zwei Fragen. Die eine an Professor von Lewinski. Sie hatten sich ja dankenswerterweise auch mit dem sogenannten Volkszählungsurteil auseinandergesetzt und dann auch differenziert und vielleicht auch so ein bisschen der gelegentlich zu vernehmenden Legendenbildung entgegengewirkt, dass das Bundesverfassungsgericht sich gegen die einheitliche Kennziffer generell ausgesprochen habe. Und Sie hatten differenziert zwischen der Personenkennziffer und der Profilbildung als solche. Und die Frage dazu: Grundsätzlich ist der Gesetzgeber ja in der Wahl seiner Mittel frei, so lange es da eben adäquate Instrumente gibt, um dieser Profilbildung entgegenzuwirken. Wie bewerten Sie datenschutz-, aber auch verfassungsrechtlich die Instrumente im Gesetzentwurf, die jetzt gewählt wurden? Vielleicht das auch bitte in Abgrenzung zum österreichischen Modell, das ja immer genannt wird und da vielleicht insbesondere auch vor dem Hintergrund der Frage, dass die Österreicher ja bereichsspezifische Kennzahlen haben, aber eine zentrale Registerlandschaft und auch die ja ganz besonders anfällig unter Umständen sein kann. Also, wie bewerten Sie da die vorgenommenen Instrumente?

Und die zweite Frage an Professor Parycek. Auch Sie hatten sich ja auseinandergesetzt mit dem österreichischen Modell und seinen bereichsspezifischen Personenkennziffern. Jetzt ist bei uns die Registerlandschaft ja eine vollkommen andere. Und hier die Frage: Wie bewerten Sie die Übertragbarkeit des – ich sag mal – „zweiten Modells“, des österreichischen Modells vor dem Hintergrund, dass unsere Registerlandschaft anders ist und was würde das bedeuten, insbesondere auch für die, die damit arbeiten müssen? Und das ist jetzt so die Frage nach dem praktischen Nutzen oder vielleicht auch den praktischen Problemen. Ich habe vernommen, dass es in Österreich eine Debatte gab, dass die Bundesländer in Österreich tendenziell vielleicht manchmal sogar überfordert sind mit den

vielen bereichsspezifischen IDs oder Personenkennzahlen und dass ein entsprechend komplexes System hier und da auch erst recht Datenschutzverstöße provozieren kann, weil die Handhabbarkeit einfach nicht mehr gegeben ist. Wenn Sie da aus Ihrer praktischen Sicht oder der Kenntnis der österreichischen Materie für Aufhellung sorgen könnten, wäre ich Ihnen sehr dankbar. Danke schön.

Vors. **Andrea Lindholz** (CDU/CSU): Dann Herr Dr. Wirth.

Abg. **Dr. Christian Wirth** (AfD): Vielen Dank an die Sachverständigen. Schönen guten Tag. Besonderen Gruß nach Saarbrücken an meine Alma Mater. Meine erste Frage geht an Professor Kelber. Im Gesetzentwurf ist die Rede von Qualitätssicherungsprozessen, die die Aktualität, Konsistenz und Validität der personenidentifizierenden Basisdaten sicherstellen sollen. Können Sie bitte ausführen, wie solche Überprüfungsprozesse ablaufen sollen? Die zweite Frage an Professor Sorge ebenfalls zum österreichischen Modell: Könnten Sie bitte vielleicht nochmals ausführen, wie die Vor- und Nachteile dieses Modells sind und die Anwendbarkeit oder Nichtanwendbarkeit in Hinsicht auf die Bundesrepublik Deutschland? Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Dann für die SPD Frau Kaiser.

BE Abg. **Elisabeth Kaiser** (SPD): Vielen Dank, Frau Vorsitzende. Meine Frage, die etwas umfänglicher ist, richtet sich an Professor Eike Richter. Vielen Dank auch nochmal an Sie für die Ausführungen, wie auch an alle anderen Sachverständigen. Ich glaube, wir können darüber streiten, inwiefern eine Personenkennziffer jetzt an sich auch aufgrund des Volkszählungsurteils tatsächlich dem Verfassungsrecht entgegensteht. Wo wir uns aber denke ich einig sind ist, dass es durchaus verfassungsrechtliche Risiken zu bedenken gibt, wenn wir darüber nachdenken, inwiefern Daten verknüpft werden können über eine einheitliche Personenkennziffer. Deshalb richtet sich auch meine Frage in diese Richtung. Wie können wir denn diese Risiken minimieren, die wir jetzt in voller Größe und Umfänglichkeit an dieser Stelle denke ich noch nicht im vollen Maße abschätzen können? Zum Beispiel eben auch über eine engere Zweckbindung mit Blick auf die OZG-Relevanz, so wie das ja auch vorgegeben ist. Und genauso auch auf die bereichsspezifische Anwendung, aber auch die Sicherungsmechanismen, die jetzt im Gesetzentwurf vorliegen, wie eben auch das 4-Corner-Modell, das Datencockpit, das sind ja auch relevante Fragen. Wie kann man damit vielleicht noch besser umgehen? Was kann man dort noch schärfen oder diese Instrumente auch ausweiten, um eben eine missbräuchliche Nutzung der Personenkennziffer auszuschließen?

Vors. **Andrea Lindholz** (CDU/CSU): Frau Kaiser, Sie haben nur die eine Frage?

BE Abg. **Elisabeth Kaiser** (SPD): Ja.

Vors. **Andrea Lindholz** (CDU/CSU): Okay. Dann Herr Höferlin für die FDP, bitte.

BE Abg. **Manuel Höferlin** (FDP): Vielen Dank, Frau Vorsitzende. Ja, es ist schon beachtlich, dass der Großteil der Eingangsstatements der Sachverständigen – herzlichen Dank für alle Statements – sich entweder damit beschäftigen, zu erklären, warum der Entwurf verfassungswidrig ist oder sich damit beschäftigen, warum er nicht verfassungswidrig ist. Offensichtlich ist das aber ein starkes Thema, das uns zu denken geben sollte. Ich glaube, klar ist auch, dass die Einführung der zentralen Personenkennziffer oder die Verhinderung der Einführung nicht einen Schutz für die Bürger vermittelt. Hat Herr Professor Parycek ja gesagt, da haben Sie völlig Recht. Zu den Alternativen finde ich spannend, dass auch Sie, Herr Professor Richter, ja immerhin ein von der Koalitionsfraktion benannter Sachverständiger, auch keine wirkliche Nachvollziehbarkeit des Fehlens von Alternativen gesagt haben, außer der Aufwands- und Kostenargumente. Und ich will auch nicht verhehlen, dass wir als Freie Demokraten einige Dinge gut finden: Die Notwendigkeit der Registermodernisierung als vor allen Dingen auch das Datencockpit. Und sehr schön ist natürlich, dass es offensichtlich auch Alternativen gibt, wie Herr Professor Sorge am Ende ja dargestellt hat. Ich will mal sagen, das ist ja das Österreich-Plus-Modell, nicht das Österreich-Modell, um es mal so zu sagen.

An Sie, Herr Professor Sorge, würde ich auch gern zwei Fragen richten. Einmal zum Themenkomplex Kosten- und Aufwandsargumente wurde gesagt, dass man ja das machen könne, weil die Steuer-ID sei ja schon da und das sei auch praktisch und

könne man viel schneller und einfacher durchführen. Zwar wurde das jetzt nicht durchgerechnet, aber allein das darf es ja auch nicht sein. Man darf ja nicht, nur weil es kosten- und aufwandschonender ist, andere Güter vernachlässigen. Deswegen meine Frage zum Mehraufwand ist sozusagen die technische Frage. Ist es denn in der Struktur der vorhandenen Planung auch mit den entsprechenden Institutionen so kompliziert, ein solches Modell mit Intermediären aufzubauen? Oder anders: Ist die Umsetzung von Alternativen zur Steuer-ID eine unüberwindbare technische Hürde oder ist es eher vielleicht eine Frage, ob man auf Altbewährtes zurückgreifen will, weil es einfacher und schneller und günstiger ist? Und die zweite Frage auch an Sie, Professor Sorge, ist das alternative Modell zur Steuer-ID. Ich nenne es jetzt mal – Sie haben es in Ihrer Folie Neu-ID genannt, hier kann man ja dann einen schöneren Namen finden – irgendwie gute ID oder so. Durch das 4-Corner-Modell sind ja im Prinzip bereichsübergreifende Datenübermittlungen anskizziert in der Konzeption des Modells. Da drin wird sogar von Bereichen gesprochen in dem jetzigen Entwurfsformular. Und die Intermediäre haben auch jetzt ja schon Vermittlungsfunktionen, übermitteln aber sozusagen aber immer dieselbe Steuer-ID. Und jetzt ist die Frage: Wenn man eine Alternative nimmt, also ein Österreich-Plus-Modell mit bereichsspezifischen IDs, wie stellen sich die Autoren auch Ihrer Studie, die Sie gemacht haben, die Alternativen der ID denn vor, sodass man geeignete Maßnahmen zur Umsetzung der Registermodernisierung denn auch dann ergreifen kann und trotzdem zum Ergebnis kommt?

Vors. **Andrea Lindholz** (CDU/CSU): Dann für die Fraktion DIE LINKE. Frau Pau, bitte.

BE Abg. **Petra Pau** (DIE LINKE.): Danke. Ich kann da direkt anschließen. Allerdings richten sich meine Fragen erst einmal an Frau Bock. Sie haben ja in Ihrer mündlichen Stellungnahme Alternativen zur registerübergreifenden Identifikationsnummer genannt. Sie nannten Dänemark. Österreich ist hier jetzt schon nachgefragt worden. Können Sie uns noch mal erklären, wie das in Österreich einerseits funktioniert – die bereichsspezifische Identifikationsnummer – und was Sie dem Argument der Bundesregierung entgegensetzen, dass das für uns nicht in Betracht käme, weil eben die öffentliche Verwaltung in Österreich ganz anders funktioniere. Was müsste aus Ihrer Sicht dann im deutschen Verwaltungskontext angepasst werden, wenn man das übernehmen möchte? Und die zweite Frage: Im Gesetzentwurf ist ja auch vorgesehen, dass es ein Datencockpit geben soll. Auch dazu ist heute mehrfach schon gesprochen worden. Die Frage ist, was müsste aus Ihrer Sicht hier nachgebessert werden, um das Datencockpit eben nicht nur zur Steuerung zu nutzen, sondern auch hier die Möglichkeit zu schaffen, das Ungleichgewicht zwischen Verwaltung und Bürgern auszugleichen und Datenrechte wirksam zu schützen?

Vors. **Andrea Lindholz** (CDU/CSU): Frau Pau, vielen Dank. Und dann für die Fraktion BÜNDNIS 90/DIE GRÜNEN noch Herr Dr. von Notz.

BE Abg. **Dr. Konstantin von Notz** (BÜNDNIS 90/DIE GRÜNEN): Frau Vorsitzende, vielen Dank. Vielen Dank an die Sachverständigen für den Sachverstand und die Berichte. Es ist glaube ich ohne jeden Zweifel wichtig und richtig, dass man zu einer Modernisierung der Register kommt und das eint uns glaube ich alle hier. Die Frage ist nur: Wie? Und das Problem ist ja mit den IT-Großprojekten der Bundesregierung, ich will hier niemandes Gefühle verletzen, aber eigentlich hat kein einziges funktioniert. Seit elf Jahren beobachte ich das intensiv und bisher ist es noch immer gelungen, das Ding an die Wand zu knallen. Das einzige, was funktioniert hat, war die Corona-App, aber auch nur, weil man sich massiv auf die Opposition zubewegt hat und die datenschutzfreundliche Lösung gemacht hat. Das ist so. Ein Viertel der Leute vertrauen der. Das ist gar nicht so schlecht, wie jetzt alle tun. Und besser als die China-Lösung, sage ich gleich mal. Gut, das tut nichts zur Sache.

Ich habe zwei Fragen. Die erste geht an Herrn Professor Kelber. Herr Professor Kelber, vielleicht können Sie noch mal berichten, wie im Kreise der Datenschutzbeauftragten, auch der Länder, dieses Thema bewegt worden ist im Hinblick auf die Steuer-ID. Die Aufsichtsbehörden in den Ländern haben sich da ja auch sehr klar verhalten und sozusagen einen Weg vorgezeichnet, der geht und einen, der nicht geht. Und vielleicht können Sie das noch mal ausführen, wie Sie als bundesweite Aufsichtsbehörde, aber vor allen Dingen auch die Länder auf diese Frage der Steuer-ID draufgeguckt haben. Die andere Frage geht an Frau Dr. Berger. Frau Dr. Berger, ich habe Sie ja jetzt so verstanden,

dass Sie sagen, irgendwie mit der Steuer-ID, das geht schon, das kann man machen. Aber jetzt wissen wir ja beide, vor dem Bundesverfassungsgericht, man weiß es ja nicht so ganz genau, ja? Und das kann klappen oder es kann nicht klappen. Und jetzt mal für den Fall, dass es nicht klappt, also dass gesagt wird, die Steuer-ID, das ist einfach verfassungswidrig. Was würde das wohl so an Geld kosten? Haben Sie das mal bewegt sozusagen, auch für die kommunale Ebene, wenn man da jetzt ein System aufsetzt? Und vor allen Dingen, was würde es uns an Zeit kosten, wenn wir auf ein System setzen, das uns nachher in vier Jahren um die Ohren fliegt? Weil eins ist mal sicher: Beklagt werden wird das. Das ist sicher. Und wie es ausgeht, weiß man nicht genau. Und deswegen safety first. Ich würde ja immer für die sichere Lösung plädieren. Aber damit man so eine Risikoeinschätzung bekommt: Wie ist das denn auf kommunaler und vielleicht auch auf Landesebene mal bewegt worden? Kann vielleicht auch Herr Professor Kelber noch sagen. Was bedeutet es, wenn es nicht fliegt? Danke schön.

Vors. **Andrea Lindholz** (CDU/CSU): Dann kommen wir zur Antwortrunde und beginnen gleich mit Frau Dr. Berger, bitte.

SV **Dr. Ariane Berger** (Bundesvereinigung der kommunalen Spitzenverbände, Berlin): Herzlichen Dank. Vor Gericht und auf hoher See ist man in Gottes Hand. Wir haben als Kommunen immer – und da gebe ich Ihnen vollkommen Recht – das Damoklesschwert des scheiternden E-Governments über uns hängen. Das sehen wir mit dem Online-Zugangsgesetz und der misslichen Frist bis 2022. Das beschleunigt alles. Diese Frist hätte man möglicherweise streichen sollen. Und wir sehen jetzt das Registermodernisierungsgesetz, das aus unserer Sicht die echte Modernisierungsagenda dem Grunde nach ist und hoffen und warten darauf, dass es funktioniert. Ich kann Ihnen aus dem Online-Zugangsgesetzbereich berichten. Auch dort sind die Kommunen zum Warten verdammt, weil wir darauf angewiesen sind, dass der Bund über die Länder IT-Strukturen auskippt, die dann den Kommunen zur Verfügung gestellt werden müssen. Die Schnittstellen, die Standards, über die wir uns ja auch in diesem Kontext unterhalten, um die kommunalen Verfahren, die Hauptvollzugsebene in Deutschland anzubinden, fehlen. Darüber spricht man zu wenig.

Und auch in diesem Fall hier im Bereich Registermodernisierung hängt das Gelingen der Registermodernisierung davon ab, dass wir uns über Standards unterhalten, und zwar zügig. Und nicht nur über die Standards in Bezug auf die Grunddaten der Person – das kann die Steuer-ID sein, das kann auch eine Bereinigung der sprechenden Datensätze in den kommunalen Registern sein – aber das ist nur ein kleiner Teil. Es geht ja auch um die Standardisierung der Datenverarbeitungs-, der Datenaustauschstandards. Nur dann können wir die Daten laufen lassen zwischen den Registern. Und wir sehen natürlich als Kommunen die große Gefahr, dass das alles dauert. Hier ist Zügigkeit, Schnelligkeit geboten, sowohl beim OZG. Wir brauchen eine Standardisierungsagenda unter Beteiligung der Kommunen, unter Einbindung des kommunalen Wissens. Ich habe versucht, deutlich zu machen, dass das Registermodernisierungsgesetz aus unserer Sicht verfassungskonform ist, wenn wir eine Gesamtbetrachtung zugrunde legen, Datencockpit, Protokolle, 4-Corner-Ansätze nehmen und insbesondere auch die dezentrale Datenhaltung, also die Registerarchitektur jetzt festlegen und mit dem IT-Planungsrat die Austauschstandards schaffen, die noch fehlen. Das haben wir alles noch nicht. Wir können hier nur für Schnelligkeit plädieren.

Vors. **Andrea Lindholz** (CDU/CSU): Frau Bock, bitte.

SV **Kirsten Bock**: Vielen Dank. Ja, da kann ich eigentlich gleich anschließen. Also, es ist ja nicht so, als ob es noch gar keine Schnittstellen gäbe oder man sich nicht schon lange über Interoperabilität der Verfahren Gedanken macht. Also, das ist glaube ich aber auch tatsächlich ein Angelpunkt, an dem man ansetzen sollte, bevor man sich irgendwelche anderen Gedanken macht, wie – und das kann man auch ohne ein Personenkennzeichen – erhöhe ich die Interoperabilität und wie schaffe ich verbesserte Austauschstandards auch zwischen den Ländern? Ich komme jetzt zur Vergleichbarkeit mit Österreich, weil das meine Frage war. Hier wundert es mich tatsächlich, dass die Bundesrepublik nicht viel länger schon darüber nachgedacht hat. Ich kann mich sehr gut erinnern an die Zeit der Ratspräsidentschaft Österreichs. Das muss so um 2010 gewesen sein. Dort wurde sehr die Werbetrommel gerührt für dieses System. Aber ich glaube, in Deutschland war das noch die Zeit, als das Internet

noch ein Hype war und noch nicht mal Neuland. Und das erklärt vielleicht auch einiges, womit wir es hier zu tun haben.

Von der Struktur her denke ich ist das österreichische System sicherlich nicht eins zu eins übertragbar. Das wäre aber auch gar nicht sinnvoll. Also man könnte aus einigen Erfahrungen, die Österreich damit gemacht hat, auch lernen und das anpassen. Aber grundsätzlich ist die Struktur, die wir hier in der Bundesrepublik haben, durch unsere föderale Situation deutlich begünstigender und einfacher als es in Teilen für Österreich war. Andererseits muss man auch sagen, dass es nicht so ist, dass Österreich allein zentralistisch aufgebaut ist. Auch dort ist es so, dass viele Register in der Hand der Kommunen liegen und von diesen verwaltet werden. Ein gutes Beispiel ist das Melderecht in Österreich. Also insofern unterscheidet sich die Situation, dass in Deutschland die Ausgangsvoraussetzungen eigentlich einfacher sind vom Ursprung her als sie in Österreich waren. Insofern bietet sich das Verfahren an. Ich kann mich diesbezüglich den Ausführungen zur Intermediärslandschaft anschließen. Was sich aus meiner Sicht noch anbieten würde wäre, nicht nur über Zentralintermediäre nachzudenken, das klang auch schon an bei den Kollegen, sondern auch hier über eine föderale Infrastruktur nachzudenken. Auch das fordert die Struktur, die wir bisher haben, nämlich das kann man sehr gut an die Dienstleister der Länder angliedern, die das sehr gut auch föderal umsetzen könnten. Also eine föderale föderierte Intermediärslandschaft – das wäre innovativ tatsächlich, also auch weltweit innovativ. Und hier könnte sich Deutschland tatsächlich beweisen. Und wir haben schon gehört, der Mehraufwand ist gar nicht so hoch.

Vielleicht ein ganz kurzer Ausflug zum Verständnis, wie das in Österreich mit den bereichsspezifischen Kennzahlen funktioniert. Dort dürfen keine einheitlichen Personenkennzeichen verwendet werden, sondern eben nur die bereichsspezifischen Kennzeichen, die jeweils durch eine Ableitung aus einer Stammzahl gebildet werden. Also Kern des österreichischen Modells ist die Stammzahl, dafür gibt es auch ein Stammzahlregister, die den Personen zugewiesen wird und die sich auch jeweils auf den sogenannten Bürgerkarten befinden. Und dann werden kryptografische Verfahren angewendet, die nicht umkehrbar sind. Und das ist das Entscheidende. Das bedeutet, dass vom bereichsspezifischen Personenkennzeichen nicht mehr auf die Stammzahl zurückgerechnet werden kann. Das ist also ihr großer Vorteil. Und die Behörden dürfen diese Stammzahl natürlicher Personen nie als Identitätsmerkmal speichern. Benötigt nun eine Behörde zur Identifikation einer Person eine bereichsspezifische Personenkennzahl aus einem anderen Verfahrensbereich, also zum Austausch, wird es durch diese Stammzahlenregisterbehörde berechnet. Das ist die Funktion der Intermediäre. Und die Stammzahlregisterbehörde übermittelt dann das bereichsspezifische Kennzeichen ausschließlich verschlüsselt an die anfragende Behörde. Das verschlüsselte Personenkennzeichen also wird dort dann entschlüsselt und kann dann weiterverarbeitet werden. Das bedeutet, dass für Fremdverfahrensbereiche da kein Zugang mehr besteht.

Ja, die Berechnung dieses verschlüsselten bereichsspezifischen Personenkennzeichens muss so erfolgen, dass nicht auf die Personen zurückgeschlossen werden kann. Und das ist ein Verfahren, ja ein asymmetrisches, kryptografisches Verfahren, das eine sehr lange Schlüssellänge hat und auch schon deswegen aus Sicherheitsgesichtspunkten eben geeignet ist oder beziehungsweise das man sicher auch noch ausbauen könnte. In Österreich hat man zudem die Bürgerkarte damit verbunden, um die Akzeptanz des ganzen Verfahrens zu erhöhen. Also, die Bürger selbst können mit der Bürgerkarte und dieser Stammzahl signieren und elektronische Anträge abgeben. Und das erhöht natürlich den Nutzen dieses ganzen Verfahrens erheblich, weil diese Möglichkeit über die Portalverbünde, die wir bisher haben, eben immer noch nicht sicherstellen, dass Bürger tatsächlich sicher Anträge stellen können auf elektronischem Wege. Diese Verfahren insgesamt sind natürlich eingebettet in die historisch gewachsenen Verwaltungsstrukturen und schon deswegen ist es schwer, jetzt länderübergreifend hier Vergleiche anzustellen. Gern wird ja auch der Vergleich mit Skandinavien gewählt. Aber hier muss man eben bedenken, dass der ganze E-Government-Bereich dort für die Bürgerinnen und Bürger sehr viel einfacher zugänglich ist über Bürgerbüros und so weiter. Es wird also auch die IT-Infrastruktur den Bürgern kommunal zur Verfügung gestellt, sodass dort wirklich alle Bürger auch Zugang haben. Aber was wir in diesen

Ländern auch beobachten ist, zum Beispiel in Dänemark, dass dort wieder darüber nachgedacht wird, ganz von der elektronischen Akte zum Beispiel auch Abstand zu nehmen, also Digitalisierung nicht nur um jeden Preis zu betreiben im Hinblick darauf, dass es einfach Cybervorfälle gab und man sehr schnell festgestellt hat, was es eigentlich bedeutet, wenn so ein System, das zentral organisiert ist, runtergefahren wird. Und wir haben das gerade heute erlebt, offensichtlich gab es bei Google Probleme und zahlreiche Anwendungen standen nicht mehr zur Verfügung. Das ist schon krass, ja? Und das muss man sich hier sehr genau überlegen, inwieweit man die gesamte Infrastruktur eben von so einem System abhängig macht. Die Kommunen bestärken das hier sehr zu Recht, dass die dezentrale Struktur hier erhebliche Vorteile bringt, auch zum Schutz des gesamten Verfahrens und der gesamten Infrastruktur.

Ganz kurze Worte zum Datencockpit. Das ist in erster Linie geschaffen worden, um Transparenz zu gewährleisten, aber wenn man sich das mal im Detail anguckt, ist es ziemlich schwach. Also, da kann der Betroffene schauen, welche Datenzugriffe durch die Behörde erfolgt sind und dem zustimmen, aber was dort abgebildet wird, sollen wohl nur die Protokolle sein oder Protokolldaten. Also, eine echte Interaktion gibt es da gar nicht. Es ist auch die Frage, also wie komme ich als Bürger eigentlich da ran? Da gibt es sehr hohe Zugangshürden, auch zu Recht. Das ist aber auch für die Akzeptanz eine zusätzliche Hürde, wenn dieses Datencockpit nicht noch einen Mehrwert hat, außer jetzt ein bisschen Transparenz zu schaffen. Und in diesem Zusammenhang möchte ich auch noch mal kurz erwähnen, dass der Gesetzentwurf vorsieht, dass Protokolldaten sehr, sehr frühzeitig gelöscht werden. Also das ist ein absolut interessantes Verständnis von Datenschutz und auch der Datenminimierung. Protokolldaten bitte, ja, die sollen so lange wie erforderlich vorhanden sein. Also stellen Sie sich vor, wenn die Rentenversicherung Ihre Daten vorzeitig löscht, dann haben wir ein riesen Problem. Also, es geht nicht darum, möglichst schnell hier Protokolldaten zu löschen, sondern sie so lange zur Verfügung zu stellen, wie das erforderlich ist. Und im Zweifel sollte der Betroffene das entscheiden, wann dies der Fall sein soll. Und insofern denke ich bietet gerade das Datencockpit noch erhebliche Möglichkeiten, ausgebaut zu werden, aber einen wirklichen Mehrwert kann man da glaube ich nur erlangen, wenn man tatsächlich mit bereichsspezifischen Kennzeichen arbeitet. Die stellen dann sicher, dass es eben nicht zu Überschneidungen kommt oder zu Zweckbindungsaufweichungen. Und hier glaube ich könnte man noch erheblichen Mehrwert erreichen. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Professor Kelber, bitte.

SV **Prof. Ulrich Kelber** (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bonn): Vielen Dank, Frau Vorsitzende. Zur Frage vom Herrn Abgeordneten Dr. Wirth: Qualitätssicherungsprozesse sind natürlich fester Bestandteil jedes Datums von der Generierung bis hin zur Löschung und müssen auch Datenbanksysteme, Register immer begleiten. Es gibt zahlreiche Methoden, wie man das tun kann, übrigens auch eine Datenschutzanforderung. Organisatorisch Daten auf Korrektheit zu prüfen, ist eine der Anforderungen, die wir geben. Ein Beispiel ist sehr spezifisch für das jeweilige Register. Sie können Daten auf Widersprüchlichkeit prüfen. Nehmen Sie das Beispiel: Beim 106-jährigen Erstklässler ist eher zu vermuten, dass das Geburtsdatum falsch eingegeben wurde, als dass er einhundertmal von der Einschulung zurückgestellt wurde. Über sowas können Sie das finden. Über das Alter von unveränderten Daten bis hin zum Abgleich da, wo erlaubt ist zwischen unterschiedlichen Datenbeständen. Dafür brauchen Sie nicht unbedingt den bereichsübergreifenden Identifikator, auch nicht bereichsspezifisch. Auch das kann über Datenkranzabgleiche erfolgen, wo dann aber eben gefunden wird, wo ähneln sich Daten, wo unterscheiden sie sich? Und – und das war etwas, was ich vorhin ja Ihnen als Gesetzgeber empfohlen hatte – das Datencockpit als gute Idee dahingehend auszubauen, dass Bürgerinnen und Bürger darüber auch die Bestandsdaten, die sie betreffen, einsehen können. Damit hätten Sie die Bürgerinnen und Bürger selber als jemand, der darauf hinweisen kann, wenn falsche Daten über sie gespeichert sind.

Zur Frage vom Herrn Abgeordneten von Notz. Ja, die Datenschutzkonferenz der unabhängigen Datenschutzbeauftragten des Bundes und der Länder hat sich unisono geäußert. Es gab keine Abweichungen der Einschätzung. Das ist bei 18 Datenschutzbehörden nicht immer so, wie Sie ja öfters als Bundestag schon beklagt haben, aber an dieser Stelle alle. Und ich muss dazu sagen, bei der Einschätzung, was im

Datenschutzbereich verfassungswidrig ist oder nicht, haben wir eine sehr gute Bilanz. Also in der Bundesliga wären wir bestimmt Herbstmeister mit der Zahl der Siege gegenüber den Niederlagen. Alle sind der Meinung, dass es hier eine große Gefahr gibt, dass es tatsächlich verfassungswidrig ist. Es gab auch ein Unverständnis über den Prozess. Wir sind als Datenschutzbehörden früh eingebunden worden durch das Innenministerium, aber ab einem Zeitpunkt merkte man, dass die Alternativen nicht mehr gleichwertig geprüft werden, sondern dass das Ziel nach vorne gesetzt worden ist: Wir wollen jetzt die Registermodernisierung, egal wie. Das war etwas, was auch zur Verärgerung bei meinen Kollegen, insbesondere aus den Ländern, geführt hat. Bei den Kosten, die Sie angesprochen haben. Natürlich konnten wir aufgrund dieser schlechteren, nicht gleichwertigen Prüfung die Kosten nicht exakt ermitteln. Aber Sie können davon ausgehen, dass es keine Vermehrfachung der Kosten wäre, ein datenschutzfreundlicheres Modell wie ein Österreich Plus zum Beispiel zu verwenden, sondern dass es eine leichte Anhebung der Kosten wäre. Deswegen eher klein. Überhaupt, ein ganz kleiner Bestandteil in den Gesamtkosten der Digitalisierung der Register und des Online-Zugangs und natürlich vor allem eine Investition, die die viel größeren Schäden verhindern würde, die bei einem nachträglichen Scheitern oder Entziehen der Grundlage der Registermodernisierung auftreten würden, also bei einem Urteil des Bundesverfassungsgerichts.

Wir haben uns natürlich auch mit dem Thema der Komplexität befasst bei den vorgeschlagenen Alternativen. Sie müssen sich das technisch so vorstellen, dass es für die Anwenderinnen und Anwender, also die Behörden, die ein Register führen, völlig transparent ist, ob sie über einen direkten Datenabgleich, über einen Intermediär, der prüft, ob Sie abgleichen dürfen, also 4-Corner-Modell, oder ein Intermediär, der Ihre bereichsspezifischen Daten, die Sie in Ihrer Datenbank ganz normal pflegen sozusagen abbildet, auf dem, was in der anderen Datenbank ist. Es ist völlig transparent. Es ist der gleiche Vorgang einmal etabliert. Es ist nicht komplexer in der Bedienung. Von daher, es werden dadurch keine neuen Datenbanken entstehen und keine Bedienungsprobleme. Und auch die Komplexität der Berechnung, also die Frage, ist es eigentlich ein Mehraufwand, weil noch diese Abbildung stattfinden muss? Sie ist ein minimaler Mehraufwand übrigens gegenüber dem 4-Corner-Modell und gegenüber anders verzichtet. Das soll jetzt zum Beispiel im Steuerbereich so sein und lange Zeit bei den Kommunen auch nur ein relativ geringer Zusatzaufwand. Sie dürfen aber nicht vergessen, dass in den zehn Jahren seit der Etablierung des österreichischen Modells die Leistungsfähigkeit von IT irgendwo zwischen dem Fünfzigfachen und Hundertfachen zugenommen hat. Von daher können Sie solche Mehraufwendungen geringer Art, kleiner zweistelliger Prozentbereich, durch diese Vermehrfachung der Leistungsfähigkeit locker ausgleichen, wenn Sie den kleinen Exkurs einem Informatiker erlauben.

Vors. **Andrea Lindholz** (CDU/CSU): Herr Professor von Lewinski, bitte.

SV **Prof. Dr. Kai von Lewinski** (Universität Passau): Ja, danke. Ich soll Stellung nehmen zu der datenschutz- und verfassungsrechtlichen Einschätzung der einzelnen Aspekte und Maßnahmen im vorliegenden Gesetzentwurf. Dabei ist erst mal zu sagen, dass wahrscheinlich fast der größte Vorteil ist, dass der Gesetzentwurf nicht so auf das „Personenkennzeichen“ oder, wie es im Gesetzentwurf heißt, die „Identifikationsnummer“ fokussiert ist, sondern dass die dezentrale Registerlandschaft – das ist von Frau Berger und von anderen ja auch schon betont worden – der eigentliche datenschutzsichernde Asset ist, den wir hier in Deutschland haben durch den föderalen Aufbau – und ja nicht nur den föderalen Aufbau, sondern dann auch durch die auf die dritte Ebene, die Kommunen, runtergestufte Registerlandschaft. Das ist der entscheidende Punkt, der uns im Vergleich zu den Esten dieser Welt den Datenschutz auch in der Struktur absichert. Als einen weiteren Vorteil des Entwurfs kann man werten, dass, wie hier auch noch mal vorgeschlagen und wie anfangs auch in Österreich, die Zuständigkeit für die Registermodernisierungsbehörde nicht beim Bundesdatenschutzbeauftragten liegt. Es würde diese Behörde für den kleinen Gewinn das Vertrauen, das der Datenschutzbeauftragte natürlich genießt, für dieses Projekt zu gewinnen, es würde dadurch diese Behörde, die operativ eingebunden wird, dauerhaft kompromittieren. Es ist auf jeden Fall von Vorteil, das Bundesverwaltungsamt als eine Behörde, die in der Verwaltungszuständigkeit und damit auch in der Verantwortungslinie liegt, dass man diese hier als die zuständige Behörde gewählt

hat. Wir haben eine direkte politische Verantwortung. Wenn da was schiefgeht, dann kann man sofort den Bundesinnenminister entlassen, wenn es so schlimm denn kommt. Also, dass es hier in der Verwaltung bleibt, ist auf jeden Fall zu begrüßen.

Dass die Komplexität nicht weiter oder nur in Maßen erhöht wird, ist ebenfalls ein Vorteil, denn jede Komplexität – das ist auch verschiedentlich schon angesprochen worden – erhöht die Angriffsfläche. Das heißt, ein German Over-Engineering, das von Saarbrücken – und akademisch kann man nur den Hut davor ziehen – aus gemacht worden ist, erhöht natürlich immer und außerhalb der Theorie die Angriffsfläche.

Das Datencockpit ist verschiedentlich hier schon gelobt worden. Da würde ich in zweierlei Hinsicht etwas Wasser in den Wein gießen wollen: Zum einen ist das Datencockpit bei aller Dezentralität die Stelle, an der Daten zusammenfließen und deshalb ein interessanter Angriffspunkt. Also, da muss besonders Sorge getragen werden, dass das abgesichert ist. Und ein zweiter Punkt: Zweckbindungssicherung gegenüber nichtstaatlichen Stellen, sodass die zusammengeflossenen Daten in der Privatwirtschaft nicht genutzt werden dürfen. Ich erinnere hier an die Diskussion um das SCHUFA-Portal, das eben auch zu unechten SCHUFA-Auskünften geführt hat, etwa indem man da dann irgendwie Screenshots gemacht hat.

Zwei weitere Punkte, die wahrscheinlich von dem Entwurf gar nicht als Asset so nach vorn gestellt worden sind, will ich auch noch erwähnen: Und das ist die Trennung in Bereiche. Also gerade eigentlich, dass das 4-Corner-Modell nicht für jede Amtsstube durchgeführt wird, hätte natürlich auch Vorteile. Aber auch hier wieder: Wenn man aus der Mikroperspektive raus und ein bisschen in die Meso- und Makroebene geht, dann ist die Unterteilung in Bereiche, die wir jedenfalls realiter durch diesen Entwurf haben – nämlich: nur 50 Register sind betroffen, die Sicherheitsverwaltung gar nicht und die Steuerverwaltung (so unvollkommen das jetzt hier geregelt ist) ist auch ausgenommen. Also es kommt weniger datenschutzrechtlich darauf an, benachbarte Verwaltungsbereiche voneinander abzutrennen, sondern es kommt darauf an, gerade zur Verhinderung des Persönlichkeitsprofils die wirklichen Lebensbereiche voneinander zu trennen. Das ist das, was man mal datenschutzpsychologisch Rollenverschiebung und Rollenverschneidung genannt hat. Also, wenn das fortgeschrieben werden kann, dass das Steuersystem eine eigene Rolle spielt, dass der Sicherheitsbereich ausgenommen bleibt und dass man auch sonst noch vielleicht den Sozialbereich von dem Ausbildungsbereich usw. trennen kann und diese Trennungen verstärkt, also die Idee der Bereiche, dann ist das sicherlich etwas, was auch zukunftsgerichtet ist. Und der jetzige Entwurf – das geht ein bisschen auf das ein, was Herr von Notz vorgebracht hat, von dem ich nicht unmittelbar adressiert war – ist durchaus auch risikobegrenzend, also begrenzt auch das Risiko des Scheiterns. Zwar wird hier erst mal relativ viel Geld in die Hand genommen, um die Sache zum Laufen zu bringen. Solange man aber die Stammdaten, wie es ja bisher auch noch geschieht, in den Einzelregistern lässt, kann man auch ein nie auszuschließendes Scheitern vor dem Bundesverfassungsgericht auf sich zukommen lassen und könnte dann erst mal weitermachen. Und dann hätte man tatsächlich noch präzisere Vorgaben hinsichtlich der Bereiche, auf die eben die Einführung eines Personenkennzeichens zu begrenzen ist. Also, ich würde denken, die Mittel, die hier eingesetzt werden, sind jedenfalls – gerade, weil es so nah bei der bisherigen Struktur bleibt – bei einem nicht auszuschließenden Scheitern in Karlsruhe nicht verloren.

Vors. **Andrea Lindholz** (CDU/CSU): Dann haben wir als nächstes Herrn Professor Parycek.

SV **Prof. Dr. Peter Parycek** (Kompetenzzentrum Öffentliche IT am Fraunhofer FOKUS Institut und Donau-Universität Krems): Vielen Dank, Frau Vorsitzende. Ja, zu Österreich ist schon viel gesagt worden. Ich wollte nur ergänzen, dass es nicht zehn Jahre sind. Je nachdem, wann man es beginnt zu messen, 15 bis 20 Jahre, die ins Land gezogen sind, um es zu entwickeln. Und, ja, Österreich ist auch ein föderaler Staat. Also die Verwaltungsverfahren vor allem, die finden auf der Länder- und auf der kommunalen Ebene statt. Und hier muss man auch ganz klar sagen, dieses System hat bis heute für den Bürger und die Bürgerin keine Tragweite, weil die Verwaltungsverfahren auf der Landesebene nicht mit diesem System zusammenarbeiten. Das ist auf einige wenige Verfahren, also in der Stadt Wien, die ja führend ist, also als eine der führenden Städte gilt, gibt es aktuell zwei Verfahren, die einen direkten Zugriff auf die

Register nutzen, weil das System so komplex ist. Und ich glaube, das ist schon – jetzt können Sie natürlich an meinen Worten zweifeln – ein ziemlich starkes Faktum, dass die Stadt Wien, die ja auch große Vorteile durch eine direkte Anbindung an die jeweiligen Register hätte, bis heute erst sich an nur zwei ihrer insgesamt angebotenen Verfahren angebunden hat an die Bundesregister. Die Bundesregister: Ja, es gibt weiterhin auch lokale Melderegister, das ist schon vollkommen richtig. Aber in Österreich ist man den Weg beschritten, alle lokalen, also die Daten, die auch auf lokalen Registern teilweise verspeichert sind, in ein zentrales Register zusammenzuziehen. Deswegen heißt es auch Zentrales Melderegister ZMR. Ja, die Daten liegen auch weiterhin lokal, aber sind in einem zentralen Register abrufbar bearbeitbar. Und das ist ein völlig anderer Weg im Vergleich zu Deutschland. Wenn man sich da das Meldewesen anschaut, wo die lokalen Daten weiterhin lokal bleiben und nur bei Veränderungen die Veränderungsdaten ausgetauscht werden. Also, das muss man an der Stelle auch wirklich auch vorbringen. Das ist einzigartig. Also, mir ist kein Staat bekannt, der das geschafft hat, da kein zentrales Register aufzubauen. Das ist bei allen anderen genannten Ländern immer wieder der Fall, dass es dort zentrale Register gibt, wo die Daten auf alle Fälle zusammengesaugt werden, wenn man sich das so vorstellen kann, für die jeweilige Fachmaterie, das muss man auch dazu sagen. Also, das sind daher glaube ich schon Punkte, die in der Debatte ein bisschen immer wieder vielleicht nicht so stark herausgearbeitet werden. Weil von der Bundesseite ist es ein Erfolg, das muss man schon auch ganz klar sagen, weil diese Bundesregister so ausgestattet worden sind mit drei spezifischen Kennziffern, dass ein vollautomatisierter Zensus möglich ist. Das wurde 2012 das erste Mal erfolgreich durchgeführt. Daher aus Bundessicht ist es durchaus ein Erfolg. Aber dort finden ja auch nicht die Verwaltungsverfahren statt, das muss man an der Stelle wiederum unterstreichen, weil die Komplexität eben wie gesagt sehr hoch ist, was auf der Bundesebene, wo ich mich ja nur mit wenigen CIOs abstimmen muss, möglich ist zu etablieren. Das auf die Länderebene herunterzubrechen, wie man da an den Fakten sieht, ist eine große Schwierigkeit. Es gibt aktuell Länder, die überlegen jetzt, eigene quasi Identifier einzuführen.

Und vielleicht auch noch zwei Sätze zu den bereichsspezifischen Kennzeichen. Aktuell fordern die Länder eigentlich die letzten 10 bis 15 Jahre ein einheitliches Personenkennzeichen für ihren Landesbereich ein. Und heute im Tagesspiegel war zu lesen, dass nach offizieller Auskunft des Bundesinnenministeriums diskutiert wird, ob man reduziert auf vier bis fünf Bereiche. Also ich glaube, an diesen Elementen sieht man, das viel gelobte Modell ist vielleicht, wenn man ein bisschen dahinter schaut, doch nicht ganz so erfolgreich, wie es auf dem ersten Blick scheint. Ich würde daher auch wirklich abraten, von Österreich Plus und Österreich Minus zu sprechen. Es sind völlig andere Voraussetzungen. Wenn ich Daten zentral verspeichere, verarbeite, dann muss ich besondere Schutzmaßnahmen treffen. Das hat man in Österreich mit den pBKs (bereichsspezifische Personenkennzeichen) gemacht. Wenn ich diese Chance habe, als eines der wenigen Länder die Daten auf der lokalen Ebene zu lassen, dann habe ich eine ganz andere Ausgangssituation, eigentlich fast eine unglaublich gute Ausgangssituation. Und mit jedem Element, das man jetzt noch hinzufügt, steigt die Komplexität des Gesamtsystems und somit auch die Wahrscheinlichkeit des Scheiterns. Und IT-Großprojekte – das ist auch mehrfach angesprochen worden – haben den Hang, im öffentlichen Sektor zu scheitern. Die Liste ist lang. Der von mir zitierte Professor Mertens, der hat übrigens 2011 mit seiner Forschung aufgehört und hatte damals schon eine zweistellige Zahl von gescheiterten Projekten, die er untersucht hat. Das heißt, jedes Element, das man hinzugibt, birgt eine große Wahrscheinlichkeit des Scheiterns, währenddessen die Elemente, die sich jetzt im Gesetz finden, die sind ausgetestet, die sind europäisch standardisiert. Und wenn man die jetzt in einem föderalen System föderiert einsetzt, dann ist die Wahrscheinlichkeit, dass das auch ein erfolgreiches Projekt ist, durchaus vorhanden mit allen weiteren Elementen. Die kann man nicht gleich ins Gesetz hineinschreiben. Und die kann man auch auf Schaubildern schön darstellen. Aber sie in der Praxis umzusetzen, erfolgreich umzusetzen, das sind Rahmenbedingungen, da halte ich die Wahrscheinlichkeit für nicht sehr hoch. Es ist daher – und das ist glaube ich ganz wichtig – keine Kostenfrage. Also, dieses Argument wird immer wieder angeführt. Ich glaube, das ist eine Machbarkeitsfrage. Und wenn die Machbarkeit nicht gegeben ist, dann haben wir

weiterhin die datenschutzrechtlichen Spannungsverhältnisse, um es freundlich zu sagen, was den Artikel 5 betrifft, dann haben wir vielfach keinen Zugang zu den Verwaltungsleistungen, wie ich mit den Beispielen aus den Sozialbereich gebracht habe. Also, da stecken glaube ich schon auch große weitere Verantwortungen dahinter, die man da mit berücksichtigen muss. Und ja, man kann das System vielleicht früher evaluieren und dann festhalten: Braucht man mehr Bereiche? Kann man das 4-Corner-Modell auch noch in den jeweiligen Bereichen stärker einsetzen? Aber das muss man ausprobieren, testen, evaluieren und nach vier Jahren vielleicht dann noch mal Entscheidungen und neue Sicherungsmaßnahmen dazu geben, aber nicht versuchen, jetzt irgendwie alles miteinander zu kombinieren, um dann etwas entstehen zu lassen, was, ja, mit einer hohen Wahrscheinlichkeit leider nicht machbar sein wird.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Dann kommen wir zu Herrn Professor Richter.

SV **Prof. Eike Richter** (Hochschule der Akademie der Polizei Hamburg): Frau Abgeordnete Kaiser, vielen Dank für die Frage. Ich kann da gleich dran ansetzen. Wenn man dann wie gesagt davon ausgeht, dass man bei diesem Modell, das jetzt im Gesetzentwurf vorgeschlagen ist, also eine bereichsübergreifende Kennzeichnung, bleibt, also sich nicht die Frage der Erforderlichkeit stellt, dann finde ich es absolut geboten, dann eben das Modell mit Schutzmechanismen, die möglich sind oder weitere Maßnahmen, die das Risiko, das sich damit verbindet, für die Information der Selbstbestimmung und auch die Eingriffsintensität Rechnung zu tragen. Und ich glaube, mittlerweile sind wirklich ganz, ganz viele Dinge schon genannt, wo ja eben nicht mal ganz klar ist, warum das dann nicht auch gemacht wird. Ich lasse mal die technische Möglichkeit weg, die ich nicht einschätzen kann als Jurist, genauso wenig wie die finanzielle Möglichkeit, dazu kann ich natürlich nichts sagen, aber wenn man halt die Frage stellt, warum weitet man das 4-Corner-Modell eigentlich nicht auf die Datenübermittlung intern in den Bereichen aus? Da finde ich halt die Begründung etwas schwach. Da finde ich es wichtig, dass man da die Verschlüsselung ausdehnt und auch die Kommunikation innerhalb der Bereiche ansetzt. Das kann man ganz einfach machen, indem man den Gesetzestext an der Stelle anpasst, natürlich § 7. Dann wäre auch natürlich, was auch schon mehrfach gesagt worden ist, der Grundsatz der Zweckbestimmung und der Zweckbindung. Auch da finde ich, das ist bei jedem Gesetz, wo man datenschutzrechtlich draufguckt, guckt jeder sofort nach der Zweckbestimmtheit. An der Stelle könnte die auch klar nachgeschärft werden. Auch dafür liegen schon längst Vorschläge auf dem Tisch, dass man sagen kann, die Verarbeitung der Identifikationsnummer muss halt direkt beschränkt sein auf den Zweck, den sie nun mal hat und nicht auf weitere. Und andere Zwecke sind ausgeschlossen. Also auch eine negative Formulierung, um das klar zu formulieren, zum Beispiel die Nutzung durch nichtöffentliche Stellen.

Was ich mich gefragt habe, ist die Einbindung und die Auswahl der einzubeziehenden Register. Also, es werden 56 Register einbezogen. Wenn man sich die Liste anguckt, fragt man sich, wie ist das zustande gekommen? Und wenn man dann auch noch liest, dass die Bundesrechtsanwaltskammer lapidar mitteilt, dass sie ja eigentlich an keinem Verwaltungsverfahren beteiligt ist, dann frage ich mich, was dann dieses Register eigentlich genau, zumindest beim ersten Schritt da drin, soll. Das kann man sich ja sparen, finde ich. Also in der Hinsicht würde da auch noch mal die Anregung sein an der Stelle, die Auswahl quasi zu rationalisieren, zum Beispiel danach zu schauen, für welche Verwaltungsverfahren, zumindest beim ersten Schritt, braucht man denn überhaupt die Register? Ist man auf die Register denn angewiesen? Und das ist ja auch der Sinn der Sache gewesen, dass es eben die Unterstützung sein soll für das OZG. Und das OSZ setzt an den Verwaltungsleistungen an. Man hat früher immer Verwaltungsverfahren gesagt, aber da haben wir uns ja weit von entfernt. Jedenfalls müsste man im Grunde sagen, welche Register braucht man eigentlich für die Verwaltungsleistungen des OZG? Und das kann man im Zweifel auch genauso formulieren, dass eben nur solche Register einbezogen werden, die dort einen tatsächlichen Hilfsdienst liefern und nicht irgendwelche Register. Und das ist zumindest für mich nicht erkennbar gewesen. Da könnte man nachschärfen. Auch was für mich nicht erklärbar war: Der erste Schub an Registern wird im Gesetz formuliert und dann gibt es eine Verordnungsermächtigung für die Erweiterung. Also, das verstehe ich überhaupt gar nicht. Das

erscheint mir absolut widersprüchlich. Entweder man sagt, das hat Gesetzeshöhe, also erreicht den Parlamentsvorbehalt, in ein Register aufzunehmen oder nicht. Dann kann man alles per Verordnung regeln. So haben wir es ja im OZG gemacht, da sind ganz viele Verordnungsermächtigungen drin. Hier hat man eine Registeranlage gemacht per Gesetzbeschluss dann, so soll es werden. Und die Erweiterung läuft durch Verordnung. Ist für mich nicht nachvollziehbar, gerade wenn es darum vielleicht geht, gewichtigere Register zu erweitern.

Dann wäre für mich noch ein weiterer Punkt, den man auch ergänzen könnte, eben die Festlegung der Bereiche. Dazu ist schon viel gesagt und auch geschrieben worden, dass das im Grunde sehr lapidar erfolgt. Auch da wieder eine Verordnungsermächtigung, wo ich mir die Frage stelle: Wenn die Einteilung der Bereiche denn so wichtig ist, warum wird das dann nicht dann vom Parlament auch tatsächlich entschieden? Das erscheint mir ja auch nicht unmachbar. In der Hinsicht kann man das glaube ich vielleicht nachbessern, das müssen Sie selbst beurteilen. Was ein Punkt ist, den ich auch schwer einschätzen kann, das wäre aber auch noch mal zu überlegen, ist nämlich der Ausbau technischer Schutzmechanismen. Herr Professor von Lewinski hat das schon angesprochen. Man muss natürlich überlegen, dass dieses System, das dort gebaut wird, alle Ebenen des Staates übergreift, das heißt, es gilt wie bei jedem Gesamtsystem natürlich immer das Prinzip: Wo das schwächste Glied ist, ist der Angriffspunkt. Und dann ist gleich das gesamte System unter Umständen betroffen. Das haben wir hier ja jetzt schon mehrfach ausgeführt. Da frage ich mich an der Stelle tatsächlich: Wie sind die sicherheitsrechtlichen Vorkehrungen? Muss es nicht spezielle vielleicht noch mal geben, die man dort aufnehmen könnte? Da wird sich allgemein auf die allgemeine sicherheitsrechtliche Betrachtung berufen.

Und dann zuletzt, was auch Frau Bock schon angesprochen hatte, war der Ausbau des Datencockpits. Auch da sind so Kleinigkeiten, wo ich sagen muss, da kann man auf jeden Fall nachschärfen, nämlich der erste Punkt ist, dass wenn eine Ergänzung im OZG erfolgen soll, das ist wieder mal finde ich für unsere Gesetzgebung im Bereich E-Government, wenn man die über die Jahre verfolgt hat. Im Verwaltungsverfahrensgesetz ist es so geregelt – das ist ja kein Digitalgesetz, sollte es eigentlich mal werden ursprünglich, aber da sind wir ja irgendwie weit entfernt – da steht der Antragsteller, der Bürger und die Behörde im Mittelpunkt. Durch das E-Government-Gesetz und dann das OZG wurde immer mehr die Technik in den Mittelpunkt gerückt. Es steht nur noch drin, man macht eine Technikregulierung. Das ist wieder so typisch beim Datencockpit. Das Entscheidende ist doch für den Bürger, wenn man dadurch über das Datencockpit Transparenz erfahren will, dann muss das für den Bürger nutzbar und einfach sein. Warum steht da nicht einfach mal drin, dass das Datencockpit so gebaut sein muss, zum Beispiel, dass es einfach und zweckmäßig zu bedienen ist? § 10 Verwaltungsverfahrensgesetz besagt, dass der Grundsatz des deutschen Verfahrensrechts ist, das Verwaltungsverfahren einfach, zügig und zweckmäßig durchzuführen. Das wäre zum Beispiel ein wichtiger Punkt, wenn man denn sagen kann, da kann man die Transparenz auch leicht dann verwirklichen. Dann war auch noch zum Datencockpit schon längst die Anregung gekommen, Frau Bock hatte das auch schon mal gesagt, aber auch Herr Professor Kelber, die Protolldaten ist eins, wie sieht es mit den Bestandsdaten aus? Kann man die vielleicht auch dort einsehen? Das wäre ja auch nur mal ein Gedanke. Das alles finde ich, gerade auch die Registererweiterung, wenn man das kombiniert mit einer Form des überprüften Vorgehens, des Nachkontrollierens, des Nachschauens, das passt auch zu der Entwicklung, die sich technisch entwickelt. Also, die entwickelt sich nicht heute für die nächsten zehn Jahre und wir legen es einmal fest, sondern sie entwickelt sich immer weiter. Und das kombinierte Register hinzunimmt mit der Zeit, weil man das Gesetz aber auch gleichzeitig in der Struktur nachschaut, nachhält. Deswegen finde ich es eben wichtig, dass man dann solche Vorschriften wie Evaluation und Befristung nicht einfach nur so als, das kommt gleich bei Inkrafttreten noch dazu, sondern tatsächlich ernst nimmt an der Stelle und einen Regulierungslernprozess erzeugt, eine lernende Gesetzgebung erzeugt und produziert in diesem Bereich, wo die Innovationsdynamik doch so stark ist. Vielen Dank.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen Dank. Und den Schluss in der Runde macht noch Herr Professor Sorge, bitte.

SV **Prof. Dr.-Ing. Christoph Sorge** (Universität des Saarlandes, Saarbrücken): Jawohl, vielen Dank. Ich erlaube mir, mit der Antwort auf die Frage von Herrn Dr. Wirth anzufangen. Es ging noch mal um das österreichische Modell. Und es ist zwar schon viel darüber gesprochen worden, aber ich versuche doch noch mal, etwas zu ergänzen und vielleicht in eigenen Worten zusammenzufassen. Das österreichische Modell funktioniert mit einer Stammzahl, die jedem Bürger zugeordnet wird, die aber geheim gehalten ist, die also nur in einer zentralen Behörde, der Stammzahlenregisterbehörde und gegebenenfalls in der Bürgerkarte des Bürgers gespeichert ist, aber nicht an andere Behörden geht. Daraus wird jetzt ein sogenannter kryptografischer Hashwert abgeleitet. Wenn jetzt also die Stammzahl 4711 ist, wird ein kryptografischer Hashwert aus 4711, Bauen und Wohnen berechnet, wenn es um den bereichsspezifischen Identifikator oder die bereichsspezifische Kennziffer für den Bereich Bauen und Wohnen geht. Das kann man nicht mehr zurückrechnen. Und das kann auch keiner zurückrechnen und keiner kann die bereichsspezifischen Kennzeichen von verschiedenen Bereichen miteinander in Verbindung bringen. Das ist insofern also eine sehr elegante Lösung, um zum Identitätsmanagement zu kommen, sie hat aber eine Problematik oder einen Nachteil: Auch die Stammzahlenregisterbehörde kann aus ihren eigenen Mitteln nicht ohne weiteres zurückrechnen. Sie könnte höchstens, wenn sie alle Stammzahlen kennt, einmal durch alle Bürger durchgehen und schauen, ob dann die bereichsspezifische Kennziffer rauskommt, die man ihr geschickt hat. Also damit könnte sie einen Abgleich machen. Das ist im Alltag aber etwas unpraktisch. Also im Einzelnen mit dem Angriff geht das, das ist jetzt auch nicht etwas, das Stunden dauern würde, aber jedenfalls nichts, was in Millisekunden geht. Und deshalb muss man, um die passende Stammzahl zu finden zu einem Bürger, immer irgendeinen Ansatzpunkt haben zu dessen Identifikation. Also entweder speichert man sich gleich alle bereichsspezifischen Kennzeichen, dann wäre man letztendlich bei dem Österreich-Plus-Modell, wie es hier schon genannt wurde. Oder man speichert sich irgendwelche anderen identifizierenden Daten, wie es in Österreich ja auch gemacht wird. Man hat eben ja die direkte Anwendung und kann beispielsweise Personen anhand von Vorname, Nachname, Geburtsdatum, Geburtsort oder dergleichen identifizieren. Der große Vorteil des Modells ist, ich kann das beispielsweise auf einer Chipkarte auch auf dem Stand der Technik von vor 20 Jahren oder 25 Jahren ganz problemlos umsetzen. Das heißt, der Chipkarte sage ich, gib mir jetzt mal bitte eine bereichsspezifische Kennziffer für den Bereich Bauen und Wohnen. Und die Chipkarte berechnet mir das. Also dafür ist das ein sehr praktisches Modell, in ähnlicher Form übrigens auch im deutschen Personalausweis, technisch im Detail etwas anders, aber im Ergebnis ähnlich umgesetzt. Aber wie gesagt, man hat den Nachteil, man braucht an dieser Stelle diese Stammzahl und wenn man bereichsspezifische Kennzeichenzuordnung macht, braucht man irgendeine Form von Speicherung identifizierender Daten, damit man die richtige Stammzahl bekommt. Deshalb haben wir gesagt, es wäre geschickter, eben das andere Modell zu nehmen, das Österreich Plus, wie es jetzt hier genannt wurde. Nichtsdestotrotz, wenn man draufschaut als Theoretiker, würde man sagen, die Österreicher haben das erst mal sehr elegant gelöst. Ich hoffe, das beantwortet die Frage. Also direkt so umsetzen kann man es nicht, ohne eine Datenspeicherung bei diesem Intermediär, aber man kann eben die Grundidee adaptieren, und das ist das, was wir mit dem Alternativmodell Österreich Plus gemacht haben.

Zu diesem Modell. Also, Herr Höferlin hatte ja zwei Fragen an mich gerichtet. Die erste war nach dem Mehraufwand, der da entsteht. Also ist das schwierig, das System mit diesen Intermediären umzusetzen? Dazu ist die Antwort: Klar ist es schwierig, alle Bürger irgendwie einmal zu erfassen. Das heißt, es klingt interessant, das zunächst mit der Steuer-ID zu machen, denn da habe ich alle schon einmal erfasst. Es ist aber technisch jetzt genauso ein großer Aufwand, wenn ich jedem, der eine Steuer-ID hat, eben noch eine zweite ID oder 5 oder 10 oder 50 andere IDs zuordne. Also diese Zahlen zu erzeugen, wenn man die Einmaligkeit eben anhand der Steuer-ID aufhängen kann, das ist unproblematisch. Wie man damit umgehen will? Naja, mit Speichermengen und dergleichen – Herr Professor Kelber hat es schon angedeutet – haben wir keine Probleme. Der Aufwand entsteht letztendlich bei den Schutzmaßnahmen, die ja im Gesetz relativ knapp spezifiziert sind, beispielsweise das von uns vorgeschlagene Hardware-Sicherheitsmodul. Sowas wird routinemäßig schon

eingesetzt. Die Bundesrechtsanwaltskammer hat sich dafür entschieden bei einem besonderen elektronischen Anwaltspostfach beispielsweise, Banken, Versicherungen, Banken vor allem, setzen das seit vielen Jahren ein. Das ist jetzt also technisch keine Neuentwicklung. Das föderierte Identitätsmanagement tatsächlich wäre ein Mehraufwand. Man müsste sich eben einigen, welche Daten werden wo gehalten, wo sind die Intermediäre? Das ist ein teilweise politischer Prozess. Technisch müssten Dinge spezifiziert werden. Das ist sicherlich machbar, aber das ist jetzt nichts, was man in ein paar Wochen mal nebenbei macht. Ich rechne da schon mit einem höheren Umsetzungsaufwand. Das gleiche ist, wenn man den Intermediär, wie von uns vorgeschlagen, im Ausweis realisieren will. Der Ausweis ist technisch leistungsfähig genug, um das zu machen, aber er ist darauf ausgelegt, eben Ausweise einmalig nur bei einem Bereich zu identifizieren und nicht Personen, das heißt, man müsste die konkrete Umsetzung tatsächlich etwas ändern. Der große Aufwand allerdings, und damit gehe ich auf die letzte Frage von Herrn Höferlin ein, ist die Registermodernisierung an sich. Das heißt, das 4-Corner-Modell ist ja ohnehin vorgesehen. Die nötigen Datenübermittlungen sind ohnehin schon zu definieren. Die Frage ist jetzt: Was ist der Mehraufwand, den wir vorschlagen? Das ist einerseits die durchgehende Umsetzung des 4-Corner-Modells, also auch innerhalb von Bereichen beispielsweise. Man muss die Bereiche definieren. Auch das ist so oder so zu machen. Ich denke, man könnte es ins Gesetz schreiben, wie die Bereiche aussehen, aber man muss jedenfalls, egal ob man unser Modell ersetzt oder ein anderes, die Bereiche definieren. Also das ist Aufwand, das ist sogar relativ großer Aufwand, der aber auf jeden Fall anfällt. Was Zusatzaufwand sein könnte, wäre wenn man mehrere Intermediäre schafft, also mehr als die Regierung ohnehin vorgesehen hat, denn man könnte ja sagen, für bestimmte Bereiche hat man jeweils einen separaten Intermediär, der noch bestimmte Zuordnungen vornehmen kann. Diese zu definieren wäre bei uns ein Mehraufwand. Wenn man aber überhaupt nur einen kleinen Vorteil gegenüber dem Regierungsmodell erzielen will und überhaupt die bereichsspezifischen Kennzeichen nach dem sogenannten Österreich-Plus-Modell aufsetzen will, ist es keinesfalls ein Saarbrücker Over-Engineering, sondern das Modell ist bewusst an die Struktur angelehnt, die ohnehin im Regierungsentwurf vorgesehen ist. Das ist also nicht der Stand der Forschung des Identitätsmanagements, da sind wir mit dem Modell sehr, sehr weit hinterher, sondern es ist eine sehr grundlegende Anwendung. Der Speicheraufwand beispielsweise, wenn man diese Tabelle führen will, das ist die Größenordnung eines noch nicht mal ganz aktuellen Handys und es ist eine relationale Datenbank dahinter mit genau einer Tabelle. Das heißt, ich muss eine Tabelle speichern, die ein paar bis ein paar zig Gigabyte hat. Heutzutage im Grundsatz unproblematisch. Ich stimme zu, wenn man sowas nach dem Stand der Technik wirklich absichern will, braucht man Zusatzaufwand, auch wenn man etwas redundant umsetzen will, Sicherheit beim Zugriff, also dass es zuverlässig funktioniert. Dann ist das nicht so die Vorstellung, dass man sich einen Nachmittag hinsetzt und das programmiert. Im Grundmodell wäre das für einen Prototyp eine Umsetzung an einem Nachmittag, aber es ist jedenfalls nichts, was den deutschen Staat überfordern würde oder sollte. Ich hoffe, dass es das nicht tun würde. Sowas wie der Personalausweis ist technisch wesentlich komplexer, ist zwar nicht erfolgreich vermarktet, funktioniert aber technisch hervorragend. Die Corona-Warnapp ist eine technisch wesentliche komplexere Umsetzung, das heißt, ich sehe jetzt hier kein Risiko, dass man durch den Zusatzaufwand der Absicherung beziehungsweise der Einführung bereichsspezifischer Kennzeichen nach dem vorgeschlagenen Modell, das man es daran scheitern lassen könnte. Im Detail sind Dinge zu klären, aber das sind sie so oder so. Das heißt, ja, wir haben viel Aufwand, aber nicht viel Zusatzaufwand durch die bereichsspezifischen Kennzeichen. Soweit meine Sichtweise. Ich danke für die Aufmerksamkeit.

Vors. **Andrea Lindholz** (CDU/CSU): Vielen herzlichen Dank. Vielen herzlichen Dank Ihnen allen für Ihre ausführlichen Stellungnahmen und nochmal die vielen Hinweise. Ich bedanke mich auch nochmal bei den Kolleginnen und Kollegen. Die Anhörung können wir damit schließen und ich wünsche Ihnen allen eine gute Zeit, eine gute Weihnachtszeit und bleiben Sie gesund.

Schluss der Sitzung: 15:59 Uhr

Andrea Lindholz, MdB
Vorsitzende

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)667 A

Bundesvereinigung der kommunalen Spitzenverbände

Bundesvereinigung der kommunalen Spitzenverbände · Hausvogteiplatz 1 · 10117 Berlin

8.12.2020

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin

Nur per Mail an:
innenausschuss@bundestag.de

Bearbeitet von

PD Dr. Ariane Berger
Telefon 030 590097-313
E-Mail: Ariane.Berger@Landkreistag.de

Dr. Hanna Sommer
Telefon 030 37711-770
E-Mail: Hanna.Sommer@Staedtetag.de

Marc Elxnat
Telefon 030 77307-211
E-Mail: Marc.Elxnat@DstGB.de

Aktenzeichen
II/23

Stellungnahme zum

a) **Gesetzentwurf der Bundesregierung (BT-Drs. 19/24226)**
Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz -RegMoG)

b) **Antrag der Fraktion der FDP (BT-Drs. 19/24641)**
Verfassungskonforme Registermodernisierung – ohne steuerliche Identifikationsnummer

Die kommunalen Spitzenverbände bedanken sich für die Einladung zur Anhörung über den Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz - RegMoG) sowie den im Bezug genannten Antrag. Aus Sicht der kommunalen Spitzenverbände ist die Einführung einer einheitlichen Identifikationsnummer zur eindeutigen Zuordnung der betroffenen Person ausdrücklich zu begrüßen. Eine eindeutige Identifizierung der betroffenen Person ist Grundlage jedes behördenübergreifenden Datenaustauschs und zentrale Voraussetzung für die Umsetzung des Once Only-Grundsatzes. Die zügige Umsetzung des geplanten Gesetzesvorhabens ist Voraussetzung für eine gelingende Digitalisierung der Verwaltung und eine erfolgreiche Einführung von Online-Services im Sinne des Onlinezugangsgesetzes. Ergänzend verweisen wir insoweit zur Vermeidung von Wiederholungen auf unsere dem Bundesministerium des Innern, für Bau und Heimat (BMI) bereits vorliegende Stellungnahme vom 4.09.2020, die hier nochmals als **Anlage** beigefügt ist.

Zusammenfassend:

- Die kommunalen Spitzenverbände tragen die Einführung einer einheitlichen Identifikationsnummer zur eindeutigen Zuordnung der betroffenen Person dem Grunde nach mit.

- Der Verzicht auf die Einführung bereichsspezifischer Identitäten erfordert entsprechende freiheitssichernde Maßnahmen. Die vom Bund vorgeschlagenen verfahrensmäßigen, organisatorischen und technischen Sicherungen genügen aus unserer Sicht grundsätzlich den verfassungsrechtlichen Anforderungen.

- Der Gesetzentwurf enthält keine Entscheidung für eine zentrale oder dezentrale Datenhaltung. Aus Sicht der kommunalen Spitzenverbände kommt es entscheidend auf eine Beibehaltung der dezentralen Datenhaltung an.

Dies vorangestellt erlauben wir uns die nachfolgenden Anmerkungen, welche insbesondere Fragen der Datenhaltung, der Datenstandards, der Informationssicherheit, der Beteiligung der kommunalen Spitzenverbände und weitere Details betreffen.

- Der Gesetzentwurf regelt allein die Einführung und Verwendung einer Identifikationsnummer, enthält aber keine Entscheidung für eine zentrale oder dezentrale Datenhaltung. Aus Sicht der kommunalen Spitzenverbände kommt es für eine nicht zuletzt auch verfassungskonforme Ausgestaltung der Registermodernisierung entscheidend auf eine Beibehaltung der dezentralen Datenhaltung an. Dafür sprechen neben datenschutzrechtlichen Überlegungen insbesondere auch Gründe der Informationssicherheit. Die Speicherung von Daten an einem zentralen Ort begründet ein besonderes Gefahrenpotential. Hier kann eine Datenübermittlung bei dezentraler Speicherung die Verfügbarkeit der Daten wesentlich erhöhen.

- Die Entscheidung für eine dezentrale Datenhaltung beinhaltet zugleich, dass jede Form der Datenübertragung an eine zentrale Registermodernisierungsbehörde einen entsprechenden kostenfreien Rückkanal zu den dezentralen (kommunalen) Registern voraussetzt. Darüber hinaus muss gewährleistet sein, dass die jeweiligen für die dezentrale Datenhaltung verantwortlichen Behörden im Rahmen ihrer Aufgabenwahrnehmung umfangreiche Zugriffsrechte auf den jeweiligen zentralen Datenbestand erhalten.

- Für die Umsetzung im Bundesverwaltungsamt - Registermodernisierungsbehörde - ist eine Zeitschiene bis 2025 vorgesehen. Hierbei sollten die Auswirkungen auf z. B. öffentliche Stellen bzw. die benötigten Aufwände für die Anpassung der kommunalen Fachanwendungen und abweichenden Daten bzw. deren Konsolidierung berücksichtigt werden. Gleichwohl ist auch eine zentrale Finanzierung der Einmalaufwände für die Anpassung der kommunalen Fachverfahren durch den Bund notwendig (bspw. Einwohnermeldeverfahren, Personenstandswesen etc.).

- Die Anbindung von (kommunalen) Fachverfahren und die Ausarbeitung bzw. Weiterentwicklung allgemeiner Dateninhalts- und Datenaustauschstandards sind nicht Gegenstand des Gesetzes. Es handelt sich dabei um die zentralen Anforderungen an eine gelungene Registermodernisierung, die bereits jetzt in den Blick genommen werden müssen. Hier muss eine frühzeitige Einbindung der kommunalen Spitzenverbände erfolgen.

- Das Registermodernisierungsgesetz regelt darüber hinaus allein die rechtlichen Voraussetzungen der Personenidentifizierung im Rahmen der Registermodernisierung und überlässt die technische Ausgestaltung dem Verordnungsgeber (BMI). Angesichts der weitreichenden Verordnungsermächtigungen zu Gunsten des BMI bleibt den Ländern insoweit wenig Handlungsspielraum. Kritisch wird die nur beratende Rolle des IT-Planungsrates (reines „In Benehmen Setzen“) bei der Ausarbeitung der technischen Voraussetzungen betrachtet. Umso wichtiger erscheint es, die technischen Bedarfe der Kommunen in Bezug auf Schnittstellen zu den Fachverfahren und kommunalen Registern sowie Datenstandards und Anforderungen an Daten- und Informationssicherheit bereits jetzt unter Einbindung der kommunalen Spitzenverbände in den Blick zu nehmen.

- Die Datenübermittlung an eine zentrale Datenverwaltungsinstanz setzt eine entsprechende IT-Sicherheitsarchitektur voraus, welches beide Ebenen, sowohl die zentrale Datenverwaltung bei der Registermodernisierungsbehörde als auch die Datenhaltung bei den dezentralen Registern angemessen adressiert. Die Ausarbeitung eines IT-Sicherheitskonzepts sollte unter Einbindung der kommunalen Spitzenverbände und der entsprechenden kommunalen Expertise erfolgen und sich am IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik orientieren.

- Weiterhin ist darauf hinzuweisen, dass die Anlage „Register“ zu Art. 1 § 1 RegMoG die Bedarfe der kommunalen Ebene noch nicht hinreichend berücksichtigt. So fehlt u.a. eine Einbeziehung der Datenhaltung im Bereich des Unterhaltsvorschusses, der Gewerbeanzeigen, der Grundsteuer, Gewerbesteuer und der Zweitwohnungssteuer.

- Auch erscheint angesichts des nicht unerheblichen technischen Anpassungsaufwandes zur Einbindung der Identifikationsnummer (Speicherung) und im Rahmen der allgemeinen Datenbereinigung teilweise noch analog geführter Register die Frist nach Art. 1 § 2 Nr. 1 RegMoG als zu kurz bemessen.

- Offen bleibt im Gesetzentwurf auch der Umgang mit Unternehmen bzw. juristischen Personen, da die einheitliche Identifikationsnummer ausschließlich für natürliche Personen gilt. Die Kommunen erbringen gleichwohl Dienstleistungen für Unternehmen.

- Es muss weiterhin eine Regelung zu den nicht elektronischen Registern getroffen werden. Fraglich ist, wie mit Altregistern in Bezug auf das Registermodernisierungsgesetz umzugehen ist. Eine Nacherfassung zieht einen erhöhen Aufwand nach sich. Zur Wirksamkeit der Registermodernisierung scheint dies aber unerlässlich. Dies sollte im Gesetz klargestellt werden.

Mit freundlichen Grüßen

[redacted]

Dr. Uda Bastians
Beigeordnete
des Deutschen Städtetages

[redacted]

Dr. Kay Ruge
Stellvertreter des Hauptgeschäftsführers
des Deutschen Landkreistages

[redacted]

Alexander Handschuh
Grundsatzfragen, Digitalisierung
des Deutschen Städte- und Gemeindebundes

Bundesvereinigung der kommunalen Spitzenverbände

Bundesvereinigung der kommunalen Spitzenverbände · Hausvogteiplatz 1 · 10117 Berlin

Bundesministerium des Innern, für Bau und Heimat
Herrn
Dr. Udo Moewes
Referat V II 2 - Melderecht
Alt-Moabit 140
10557 Berlin

Nachrichtlich:

Herrn Ministerialdirigent
Ernst Bürger
Abteilung Digitale Verwaltung, Steuerung OZG
Alt-Moabit 140
10557 Berlin
Ernst.Buerger@bmi.bund.de

Per E-Mail: VII2@bmi.bund.de

Datum
04.09.2020

Bearbeitet von

Dr. Ariane Berger
Telefon (0 30) 59 00 97 - 313
E-Mail: Ariane.Berger@Landkreistag.de

Dr. Hanna Sommer
Telefon (0 30) 37711 - 770
E-Mail: Hanna.Sommer@Staedtetag.de

Marc Elxnat
Telefon (030) 773 07- 211
E-Mail: Marc.Elxnat@DStGB.de

Aktenzeichen
II, 10.02.21 D

Stellungnahme zum Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz)

Sehr geehrter Herr Dr. Moewes,
sehr geehrte Damen und Herren,

wir bedanken uns für die Gelegenheit, zum Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz - RegMoG) Stellung nehmen zu können. Aus Sicht der kommunalen Spitzenverbände ist die Einführung einer einheitlichen Identifikationsnummer zur eindeutigen Zuordnung der betroffenen Person grundsätzlich zu begrüßen. Eine eindeutige Identifizierung der betroffenen Person ist Grundlage jedes behördenübergreifenden Datenaustauschs und zentrale Voraussetzung für die Umsetzung des Once Only-Grundsatzes. Dies vorangestellt erlauben wir uns die nachfolgenden Anmerkungen, welche insbesondere Fragen

der Datenhaltung, der Datenstandards, der Informationssicherheit, der Beteiligung der kommunalen Spitzenverbände und weitere Details betreffen.

- Der Gesetzentwurf enthält (bislang) keine Entscheidung für eine zentrale oder dezentrale Datenhaltung. Aus Sicht der Kommunen kommt es ganz entscheidend auf eine Beibehaltung der dezentralen Datenhaltung an. Dafür sprechen bereits Gründe der Informationssicherheit. Die Speicherung von Daten an einem zentralen Ort begründet ein besonderes Gefahrenpotential. Hier kann eine Datenübermittlung bei dezentraler Speicherung die Verfügbarkeit der Daten wesentlich erhöhen.

- Die Entscheidung für eine dezentrale Datenhaltung beinhaltet zugleich, dass jede Form der Datenübertragung an eine zentrale Registermodernisierungsbehörde einen entsprechenden kostenfreien Rückkanal zu den dezentralen (kommunalen) Registern voraussetzt. Darüber hinaus muss gewährleistet sein, dass die jeweiligen für die dezentrale Datenhaltung verantwortlichen Behörden im Rahmen ihrer Aufgabenwahrnehmung umfangreiche Zugriffsrechte auf den jeweiligen zentralen Datenbestand erhalten.

- Für die Umsetzung im Bundesverwaltungsamt - Registermodernisierungsbehörde - ist eine Zeitschiene bis 2025 vorgesehen. Hierbei sollten die Auswirkungen auf z. B. öffentliche Stellen bzw. die benötigten Aufwände für die Anpassung der kommunalen Fachanwendungen und abweichenden Daten bzw. deren Konsolidierung berücksichtigt werden. Gerade zu Beginn der Registermodernisierung könnte die Datenabweichung, insbesondere der Validitätswerte (z. B. bei Ummeldungen, soweit die Daten des Zuzugswohnsitzes und dem jetzigen Wohnsitz abweichen) erheblichen Aufwand erzeugen. Gleichwohl ist auch eine zentrale Finanzierung der Einmalaufwände für die Anpassung der kommunalen Fachverfahren durch den Bund notwendig (bspw. Einwohnermeldeverfahren, Personenstandswesen etc.). Auch muss sichergestellt werden, dass in den Kommunen künftig wegfallende Gebühreneinnahmen durch entsprechende Landes- oder Bundesmittel kompensiert werden.

- Um die Umsetzung des Registermodernisierungsgesetzes in den Städten, Kreisen und Gemeinden zu gewährleisten, ist eine Kostenübernahme des kommunalen Aufwandes aus unserer Sicht unabdingbar. Der Referentenentwurf geht in der Begründung für die Verwaltung von einem zusätzlichen jährliche Erfüllungsaufwand von rund +112,5 Millionen Euro. Davon entfallen 54,3 Millionen Euro an jährlichem Erfüllungsaufwand auf den Bund und rund 58,2 Millionen Euro auf die Länder (inkl. Kommunen). Der einmalige Erfüllungsaufwand beträgt danach rund 915,7 Millionen Euro. Davon trägt der Bund rund 276,1 Millionen Euro und rund 639,6 Millionen Euro die Länder. Aus aktueller Sicht kann nicht abschließend beurteilt werden, ob diese Kosten realistisch sind oder aber tatsächlich höher liegen. Aus unserer Sicht fehlt eine angemessene Berücksichtigung der kommunalen Aufwände, da zum einen an verschiedenen Stellen, wie bspw. § 7, § 9 und § 10 den Städten und Gemeinden Verpflichtungen auferlegt werden und zum anderen notwendige Kosten für Support und die Schulung der Mitarbeiter nicht berücksichtigt werden. Hier brauchen wir eine klare Regelung im Gesetz, dass die Länder die kommunalen Kosten übernehmen müssen. Aufgrund der aktuellen Haushaltslage in den Kommunen wären solche Maßnahmen flächendeckend nicht möglich.

- Die Anbindung von (kommunalen) Fachverfahren und die Ausarbeitung bzw. Weiterentwicklung allgemeiner Dateninhalts- und Datenaustauschstandards sind nicht Gegenstand des Gesetzes. Es handelt sich dabei um die zentralen Anforderungen an eine gelungene Registermodernisierung, die bereits jetzt in den Blick genommen werden müssen. So kam es z. B. bei der Einführung des elektronischen Ausländerzentralregisters nachträglich zu langwierigen analogen Zertifizierungs- und Bestätigungsverfahren beim Bundesverwaltungsamt. Für eine Nachnutzung in Fachverfahren steht z. B. die Abwicklung der Leistungen nach dem Onlinezugangsgesetz und die Übergabe der daraus folgenden Buchungssätze an das Buchungssystem. Auch der Abruf von personengebundenen Daten anhand der Identifikationsnummer würde es ermöglichen, dass natürliche Personen wie bspw. Schuldner eindeutig identifiziert und künftig nicht mehr verwechselt werden können. Für das Abrufverfahren der Daten wäre es somit vorteilhaft, wenn ein automatisierter Massenstammdatenabgleich mit den Stammdaten möglich wäre (analog dem Abgleich im Einwohnerfachverfahren entweder direkt bei der Registermodernisierungsbehörde oder über die Meldebehörde). Dafür müssen in den Fachverfahren die Voraussetzungen geschaffen werden (u. a. Datenfeld für Steuer-ID). Es ist zu prüfen, ob eine Öffnung des Gesetzes über eine Experimentierklausel möglich ist, um analog zum Pilotvorhaben „Datencockpit“ weitere Datenabfragen zu erproben. Hier muss eine frühzeitige Einbindung der kommunalen Spitzenverbände erfolgen.

- Das Registermodernisierungsgesetz regelt darüber hinaus allein die rechtlichen Voraussetzungen der Personenidentifizierung im Rahmen der Registermodernisierung und überlässt die technische Ausgestaltung dem Verordnungsgeber (BMI). Angesichts der weitreichenden Verordnungsermächtigungen zu Gunsten des BMI bleibt den Ländern insoweit wenig Handlungsspielraum. Kritisch wird die nur beratende Rolle des IT-Planungsrates (reines „In Benehmen Setzen“) bei der Ausarbeitung der technischen Voraussetzungen betrachtet. Umso wichtiger erscheint es, die technischen Bedarfe der Kommunen in Bezug auf Schnittstellen zu den Fachverfahren und kommunalen Registern sowie Datenstandards und Anforderungen an Daten- und Informationssicherheit bereits jetzt unter Einbindung der kommunalen Spitzenverbände in den Blick zu nehmen.

- Die Datenübermittlung an eine zentrale Datenverwaltungsinstanz setzt eine entsprechende IT-Sicherheitsarchitektur voraus, welches beide Ebenen, sowohl die zentrale Datenverwaltung bei der Registermodernisierungsbehörde als auch die Datenhaltung bei den dezentralen Registern angemessen adressiert. Die Ausarbeitung eines IT-Sicherheitskonzepts sollte unter Einbindung der kommunalen Spitzenverbände und der entsprechenden kommunalen Expertise erfolgen und sich am IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik orientieren.

- Weiterhin ist darauf hinzuweisen, dass die Anlage „Register“ zu Art. 1 § 1 RegMoG die Bedarfe der kommunalen Ebene noch nicht hinreichend berücksichtigt. So fehlt u. a. eine Einbeziehung der Datenhaltung im Bereich des Unterhaltsvorschusses, der Gewerbeanzeigen, der Grundsteuer, Gewerbesteuer und der Zweitwohnungssteuer.

- Auch erscheint angesichts des nicht unerheblichen technischen Anpassungsaufwandes zur Einbindung der Identifikationsnummer (Speicherung) und im Rahmen der allgemeinen Datenbereinigung teilweise noch analog geführter Register die Frist nach Art. 1 § 1 Nr. 1 RegMoG als zu kurz bemessen.

- Im Gesetzentwurf wird ausgeführt, dass mit Zustimmung der Antragsstellenden die jeweilige Behörde die Basisdaten bei der neu geschaffenen Registermodernisierungsbehörde direkt abrufen kann. Hier sollte geklärt werden, ob die Zustimmung für jedes Verwaltungsverfahren erforderlich ist oder ob eine einmalige Zustimmung ausreichend ist und was im Falle einer Ablehnung erfolgt. Insofern sich der Nutzer mit dem Vertrauensniveau „hoch“ erstmals registrieren muss, wird durch die bislang geringe Nutzung des elektronischen Personalausweises auch die Nutzung des Datencockpits gering ausfallen. Zudem sollten im Gesetz die gesetzlichen Vertretungsmöglichkeiten klar geregelt werden.

- Offen bleibt im Gesetzentwurf auch der Umgang mit Unternehmen bzw. juristischen Personen, da die einheitliche Identifikationsnummer ausschließlich für natürliche Personen gilt. Die Kommunen erbringen gleichwohl Dienstleistungen für Unternehmen.

- Es muss weiterhin eine Regelung zu den nicht elektronischen Registern getroffen werden. Fraglich ist, wie mit Altregistern in Bezug auf das Registermodernisierungsgesetz umzugehen ist. Eine Nacherfassung zieht einen erhöhen Aufwand nach sich. Zur Wirksamkeit der Registermodernisierung scheint dies aber unerlässlich. Dies sollte im Gesetz klargestellt werden.

- Der Bereich Kommunalstatistik sollte mit besonderen Rechten (Zugriffsrechte bzw. Erhalt von Datenlieferungen) und Pflichten (statistische Geheimhaltung) im Gesetz und der neu entstehenden Registerlandschaft verankert werden. Abzüge aus dem Melderegister und weitere intrakommunale Datenlieferungen bzw. Zugriffe zwischen Fachämtern und Statistik sollten weiterhin - ohne Einschaltung einer Bundesbehörde - möglich sein. Der Gesetzesbegründung ist zu entnehmen, dass zu den zum Datenabruf befugten Stellen lediglich solche zählen sollen, die Verwaltungsleistungen nach dem Onlinezugangsgesetz erbringen. Der Bereich Statistik wird in der Begründung nur exemplarisch als "Lebensbereich" aufgeführt und eine zusätzliche Sicherung verlangt, indem Daten nur unter Einschaltung von Vermittlungsstellen in Verbindung mit der vorschlagsweisen Bereichsbildung ausgetauscht werden dürfen. Für die Statistik bedeutet dies, dass eine Zusammenführung von Daten unterschiedlicher Register und Bereiche explizit nicht mehr möglich ist. Für die Arbeit der kommunalen Statistikstellen ist dies jedoch eine elementare Arbeitsgrundlage.

- Aus kommunaler Sicht sollte zudem dringend eine Vollzugs- und Aufgabenkritik erfolgen mit dem Ziel, angesichts der neuen technologischen Möglichkeiten die Aufgabenübertragung vom Bund auf die Länder bzw. Kommunen kritisch zu hinterfragen und eine Neujustierung von Pflichtaufgaben vorzunehmen. Dies sollte zumindest parallel zur Einführung der einheitlichen Identifikationsnummer erfolgen. Diese Neuaufteilung von bestehende Aufgaben erleichtert im Ergebnis auch die technologische Umsetzung der Aufgaben aus dem OZG und der Registerführung und weist eindeutige Verantwortlichkeiten zu.

- Schließlich bitten wir um eine vertiefte verfassungsrechtliche Prüfung hinsichtlich der Einführung der Identifikationsnummer im Lichte des Urteils des Bundesverfassungsgerichts zur Volkszählung (BVerfG, Urteil vom 15-12-1983 - 1 BvR 209/83 u. a., Rn. 169). In der Literatur wird basierend auf dem Urteil davon ausgegangen, dass ein bereichsübergreifendes Personenkennzeichen gegen die allgemeine Handlungsfreiheit und die Menschenwürde verstoßen kann, wenn darüber

unter anderem eine Profilbildung ermöglicht wird (siehe z. B. Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, DSGVO Art. 87 Rn. 3). Zudem könnte das vorgesehene Modell dem Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. c) DSGVO widersprechen. Es muss sichergestellt werden, dass keinesfalls überschießende Daten im Zuge unserer Prozesse übermittelt werden.

Erlauben Sie uns darüber hinaus weitere Anmerkungen im Detail:

Zu Art. 1 RegModG

- Die Angaben zum Umfang der gespeicherten Daten gem. § 4 sind verglichen mit § 3 Bundesmeldegesetz nur ein Bruchteil der Daten, welche Kommunen als Meldebehörden speichern. Ebenso sind die Daten des § 4 Abs. 2 fast ausnahmslos im Personaldokument hinterlegt. Das Beibringen von sämtlichen Unterlagen und Nachweisen durch den Bürger zieht durch die Einführung aus kommunaler Sicht eine Veränderung nach sich, sodass wir nennenswerte Erleichterung für Bürger nicht erkennen. Eine Verbesserung in Fällen, in denen im dezentralen Register die Vermutung einer Doppelerfassung von Personen besteht, ist hinsichtlich der Datenqualität wiederum zu erwarten, da mittels eines Abgleiches mit einem zentralen Register die Gefahr von Doppelerfassungen minimiert wird. Die nach § 4 zu einer Person gespeicherten Daten sind in den Personenstandsregistern - soweit vorhanden - im Beurkundungsteil enthalten. Es erscheint daher sinnvoll, dass auch die Identifikationsnummer Teil der Beurkundung wird. Dies hat zur Folge, dass die Identifikationsnummer auch Bestandteil der Personenstandsurkunden wird.

- Meldebehörden tragen nach § 4 Abs. 3 Nr. 3 i. V. m. § 4 Abs. 5 Hinweise zur Richtigkeit der Daten ein und übermitteln das entsprechende Datum an das Bundeszentralamt für Steuern. Wir weisen darauf hin, dass es bzgl. die Richtigkeit der Daten permanent zu Abweichungen kommen kann. Beispielhaft hierfür sind Personenstandsangelegenheiten im Ausland oder weitere Staatsangehörigkeiten. In diesen Fällen hängt die Richtigkeit der Daten von der Vorlage entsprechender Nachweise durch die betroffene Person ab.

- Gemäß § 4 Abs. 3 werden einer Person weitere Daten zugeordnet, unter anderem auch die Auskunftssperre nach dem Bundesmeldegesetz. In diesem Zusammenhang ist zu beachten, dass sich auch aus dem Personenstandsrecht Sperrvermerke ergeben können, die in ihren Wirkungen über die Auskunftssperre im Melderegister hinausgehen (§ 64 PStG). Hierfür ist ebenfalls eine Regelung zu finden.

- Auch für das Standesamt müssen - dem Gesetzesentwurf folgend - künftig die neuen Identifikationsnummern der Ehegatten für die Beurkundung der Eheschließung, der Eltern für die Beurkundung einer Geburt und für den Verstorbenen und dessen Ehegatten oder Lebenspartner vorgelegt werden, da diese bei Neubeurkundungen zwingend einzutragen sind. Auch hier muss die Abfrage der Identifikationsnummern ohne großen Aufwand und kurzfristig erfolgen können. Da die Identifikationsnummer von neugeborenen Kindern nach heutigem Stand erst nach der Geburtsbeurkundung erteilt wird, muss für jede Geburt später die Identifikationsnummer ergänzt werden. Dies erhöht den Aufwand im Standesamt spürbar.

Die Basisdaten nach § 4, die den neuen Identifikationsnummern zugeordnet werden, ergeben sich aus den für die Steueridentifikationsnummern gespeicherten Daten. Die Daten werden ausschließlich mit dem Melderegister abgeglichen. Ein Abgleich mit den Personenstandsregistern des Standesamtes ist derzeit scheinbar noch nicht geplant. Da es eines der verfolgten Ziele ist, dass zukünftig Bürgerinnen und Bürger nicht mehr ihre Geburtsurkunden und vermutlich auch weitere Personenstandsurkunden vorlegen müssen, um ihren Personenstand nachweisen zu können, wäre ein Abgleich mit den Personenstandsregistern jedoch sinnvoll. Falls ein solcher Abgleich vorgenommen werden würde, müssten alle Standesämter aus ihren größtenteils noch in Papierregistern geführten Personenstandsregistern Urkunden erteilen.

Wenngleich wir den damit begründeten Aufwand sehen, ist dieser Abgleich wichtig, da die Erfahrung zeigt, dass die Daten in den Melderegistern oft von den Daten in den Personenstandsregistern abweichen. Teilweise werden die Standesämter auch nicht informiert, dass sich Personenstandsdaten wie z. B. Namen im Ausland geändert haben. Diese Änderungen werden oft nur den Melderegistern angezeigt.

Eine Fortschreibung der Personenstandsregister könnte in dem Zusammenhang erfolgen und würde zu einer Harmonisierung der betroffenen Register führen.

- Unter § 6 Abs. 2, welcher die Verwaltungsleistungen nach dem OZG betrifft, wird den öffentlichen Stellen ein intendiertes Ermessen auferlegt. Eine weitere Ermächtigungsgrundlage für die weitere Verarbeitung der Identifikationsnummer bei den öffentlichen Stellen enthält das Gesetz nicht, die entsprechenden Rechtsgrundlagen sollen in den für die jeweiligen öffentlichen Stellen geltenden Fachgesetzen entweder bereits vorhanden sein oder müssen später geschaffen werden. Die Kommunen bieten auch freiwillige Leistungen an, welche nicht zwangsläufig dem OZG unterliegen. Es ist zu prüfen, ob hierfür eine entsprechende Öffnungsklausel gefunden werden kann (bspw. über die bereits erwähnte Experimentierklausel).

  Ein Beispiel hierfür sind die Eintragungen bzw. Daten nach § 53 Bundesmeldegesetz (Zeugenschutz), wo es einer Konkretisierung zur Umsetzung der Arten von Auskunftssperren bedarf. Für die Durchführung von § 6 ist es nicht sinnvoll, die Postleitzahl anstatt des Vornamens zu verwenden, da dies möglicherweise zu Schwierigkeiten insbesondere bei Eingemeindungen führen kann.

- In § 7 Abs. 3 wird eine zehnjährige Frist den Gemeinden und Gemeindeverbänden zur Umsetzung der Verpflichtungen nach Abs. 2 bei Datenübermittlungen innerhalb einer Gemeinde oder eines Gemeindeverbands eingeräumt. Die Verpflichtung nach Abs. 2 schreibt für die Datenübermittlungen unter Nutzung einer Identifikationsnummer nach diesem Gesetz zwischen öffentlichen Stellen verschiedener Bereiche vor, dass diese über Vermittlungsstellen verschlüsselt in gesicherten Verfahren, die dem aktuellen Stand von Sicherheit und Technik entsprechen müssen, erfolgen. Auch hier müssen Verfahren entwickelt werden, welchen dem vorgenannten Standard entsprechen.

Zu Art. 2 RegModG

Aufgrund von Erfahrungen bei Auskünften nach der Datenschutzgrundverordnung stellt sich die Frage, an wen sich Bürgerinnen und Bürger künftig wenden können, wenn sie Rückfragen zu den Ergebnissen haben, die ihnen bei der Nutzung des

Datencockpits geliefert werden. Aufgrund der großen Anzahl beteiligter Rechtsgebiete (Anlage 1 zu Art. 1 RegModG) sollte proaktiv verhindert werden, dass sämtliche Anfragen oder Rückfragen in den Meldebehörden/Bürgerbüros der Kommunen landen.

Zu Art. 5 RegModG

- Die Ausweitung der gerichtsfreien Berichtigungsmöglichkeiten nach § 47 PStG sehen wir kritisch. Es sind nicht nur die Tatsache der fehlerhaften Beurkundung, sondern auch die richtigen Tatsachen zweifelsfrei nachzuweisen.

  Vermutlich wird es sich in den meisten Fällen um Reisepässe handeln. Diese Dokumente können jedoch allenfalls als Nachweis der Identität dienen. Zusätzliche beweiskräftige Unterlagen, insbesondere Personenstandsurkunden, sind vorzulegen. Aktuell werden diese Fälle gerichtlich nach § 48 PStG entschieden und ohne die erforderlichen Personenstandsurkunden abgelehnt. Hinzu kommt, dass sehr häufig in den Personenstandsregistern eine andere Identität eingetragen ist als in den neuen Ausweisdokumenten, so dass zunächst zu klären ist, ob Personenidentität besteht und welche der beiden Identitäten die richtige Identität ist. Dies lässt sich nicht allein durch die Vorlage eines neuen Passes klären. Falls hier jedoch die Fälle geregelt werden sollen, in denen lediglich der einschränkende Vermerk über die Identität einer beurkundeten Person gelöscht werden soll, müsste dies im zugrundeliegenden Gesetzestext klarer definiert werden.

  Welche Fälle mit dem neuen § 47 Abs. 1 Satz 3 geregelt werden sollen ist unklar: Personenstandsregister ohne weitere Prüfung mit den Daten des Identifikationsgesetzes zu berichtigen widerspricht dem deutschen Registerrecht, insbesondere wenn man berücksichtigt, dass die Daten aus dem Bundeszentralamt für Steuern und dem Melderegister entnommen wurden. Das Standesamt müsste wissen, welche Dokumente bei diesen Stellen vorgelegt wurden, um zu klären, ob das deutsche Personenstandsregister tatsächlich zu berichtigen ist. Dies wäre nur in den Fällen gegeben, in denen die Beurkundung von Anfang an falsch war. In anderen Fällen wäre keine Berichtigung, sondern eine Änderung der Personenstandsregister mit einem bestimmten Wirksamkeitsdatum zu beurkunden. Möglich ist auch, dass die hinterlegten Basisdaten falsch sind, weil nicht alle Daten des Personenstandsregisters in das Melderegister übernommen wurden. In diesen Fälle sollten die Basisdaten der Identifikationsnummer berichtigt werden.

  Nach § 47 Abs. 3 Satz 2 sollen Anhörungen von Beteiligten in den neu geregelten Fällen unterbleiben. Die Anhörung ist ein Bestandteil der verfassungsrechtlich garantierten Rechte auf rechtliches Gehör. Beteiligte nicht dahingehend anzuhören, ob sie mit einer Änderung einverstanden sind, wird als bedenklich eingestuft. Außerdem ist es zwingend erforderlich, dass Betroffene darüber informiert werden, dass sie die erhaltenen Urkunden nicht mehr verwenden dürfen, da diese durch die Berichtigung inhaltlich falsch geworden sind.

  Zusätzlich zu den bisherigen Daten soll anhand dieser Regelung auch die Identifikationsnummer registriert werden: Dies würde bedeuten, dass bei jeder Beurkundung auch die Identifikationsnummer aller Beteiligten zu überprüfen und einzugeben wäre (in einer Kommune mit rund 120.000 Einwohnern etwa 14.000 beteiligte Personen im Jahr). Weiterhin soll die Identifikationsnummer in den

Registern ergänzt werden, wenn diese bekannt wird. Auch ein Datenabgleich ist vorgesehen bei Differenzen und eine Erweiterung des Mitteilungsverkehrs. All dies bedeutet insgesamt einen enormen zeitlichen Mehraufwand in den Kommunen, welcher derzeit noch nicht abgeschätzt werden kann und nicht mit dem derzeit vorhandenen Personal zu bewältigen ist.

Unter § 21 Abs. 1 Nr. 5 PStG wird festgelegt, dass die Identifikationsnummer des Kindes zur Beurkundung vorliegt. Das Standesamt kann die Nummer jedoch noch nicht eintragen. Es würde sich daher um eine Folgebeurkundung (§ 27 PStG) handeln. Dies würde dazu führen, dass jeder Geburtseintrag zweimal durch den Standesbeamten bearbeitet werden müsste. Dies wiederum führt zu mehr Verwaltungsaufwand. Fraglich ist, ob die Änderung (§ 21 Abs. 1 Nr. 5) so zu lesen ist, als dass das Standesamt direkt die Registermodernisierungsbehörde anfragen kann, da die Person bisher noch keine Identifikationsnummer hat. Eine entsprechende Klarstellung ist vorzunehmen. Organisatorisch macht hier nur eine Echtzeitabfrage Sinn, damit die Aufwände bei der Beurkundung nicht verdoppelt werden.

- Aus dem Wortlaut der geplanten Änderung in § 47 PStG kann entnommen werden, dass die Berichtigung nur die Zusätze (§ 35 PStV) umfasst, da explizit nur auf diese eingegangen wird. Änderung der Personenidentität mit solchen Dokumenten (Dokumente des Heimatstaates, die zum Grenzübertritt berechtigen) ist daher nicht möglich und es verbleibt in solchen Fällen bei einer gerichtlichen Berichtigung.

- Ebenfalls sind gem. § 47 Abs. 1 S. 3 Nr. 3 PStG keine Daten bekannt, welche eine höhere Validität als die geprüften Daten des Standesbeamten haben. Sollten Berichtigungssachverhalte mit einer höheren Validität dem Standesbeamten angetragen werden, sollte auf die Vorlage der Dokumente bestanden werden.

- Laut § 55 Abs. 4 PStG soll in Personenstandsurkunden nach Abs. 1 die Identifikationsnummer nach § 139b der Abgabenordnung nicht aufgenommen werden. Dabei kann der Verzicht auf die Aufnahme der Identifikationsnummer in die Personenstandsurkunden technisch nur für die elektronischen Personenstandseinträge erfolgen. Hinsichtlich elektronischer Registerausdrucke wird der Verzicht auf die Angabe der Identifikationsnummer auch nicht möglich sein, da es sich um Beurkundungsinhalte handeln soll. Der Registerausdruck ist immer ein vollständiger Ausdruck aller dortigen Angaben. Inwieweit dies technisch umsetzbar ist, sollte im Vorfeld diskutiert werden. Bei Papierregistern müsste ein eigenhändiges Abdecken der Nummern bei einer Beglaubigung erfolgen.

Zu Art. 7, 8 und 9 RegModG

Sowohl in Art. 7 Ziff. 2, als auch in Art. 8 Ziff. 2 und Art. 9 Ziff. 2 wird das Pass-, Personalausweis- und eID-Karte-Register „in die Pflicht genommen“, im Falle nicht vorhandener Identifikationsnummern einen Datenabruf bei der Registermodernisierungsbehörde durchzuführen, um die Vergabe einer Identifikationsnummer zu erwirken. Hier ist mit einer spürbaren Verlängerung der mittleren Bearbeitungsdauer zu rechnen: Wenn die Ausstellung von Ausweisdokumenten, Pässen und eID-Karten von dem Vorhandensein einer Identifikationsnummer abhängig gemacht wird - was so verstanden werden könnte - muss die Antwort der Registermodernisierungsregisterbehörde synchron sein. Eine erneute Vorsprache der Bürgerinnen und Bürger sollte

vermieden werden. Die Bürgerämter im Bundesgebiet arbeiten - spätestens seit Beginn der Covid-19-Pandemie - komplett über Terminsysteme, bei denen es insbesondere darauf ankommt, dass die gebuchten Termine, für die Slots reserviert wurden, auch in einen Antrag/eine Dienstleistung umgewandelt werden. Ausfallzeiten im Bereich der Abwicklung von Terminen führen schnell zu einer Ressourcenverschwendung, die sich Bürgerämter nicht leisten können. Im Begründungsteil zu dem Gesetzentwurf (hier S. 78) wird von „seltenen Fällen" gesprochen, in denen die Identifikationsnummer fehlt. Hier sei angemerkt, dass hier potentiell mindestens all diejenigen Personen in Frage kommen, die von Amts wegen abgemeldet wurden. Darüber hinaus ist hier die Personengruppe der Menschen ohne festen Wohnsitz kritisch zu betrachten.

Schließlich muss diese Änderung im Rahmen der Erteilung von Passermächtigungen mit aufgegriffen werden, da insbesondere Flughafenstädte nicht selten Spontankunden aus anderen Städten schnellstmöglich - als unzuständige Behörden - mit Dokumenten versorgen müssen.

Zu Art. 19 RegModG

- Zu der Änderung des § 47 Abs. 1 PStV ist anzumerken, dass eine Berichtigung im Personenstandswesen nur bei Nachweisführung der korrekten Daten möglich ist. Es ist daher immer die höchste Validität anzunehmen, bzw. bei Gerichtsentscheiden sind die Festlegungen des Gerichtes ebenfalls so zu bewerten. Betreffend des § 56 PStV ergeben sich die gleichen Fragen wie bei § 21 PStG.

Wir bedanken uns nochmals für die Möglichkeit zur Stellungnahme und bitten um Berücksichtigung der vorstehenden Anregungen. In den laufenden Diskussionsprozess bringen wir uns gerne ein und stehen für Rückfragen zur Verfügung.

Mit freundlichen Grüßen
In Vertretung

[redacted]

Dr. Uda Bastians
Beigeordnete
Deutscher Städtetag

[redacted]

Dr. Kay Ruge
Beigeordneter
Deutscher Landkreistag

[redacted]

Alexander Handschuh
Sprecher
Deutscher Städte- und Gemeindebund

Professor Dr. Kai von Lewinski

Lehrstuhl für Öffentliches Recht, Medien- und Informationsrecht

UNIVERSITÄT PASSAU
Juristische Fakultät

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)667 B

An den
Deutschen Bundestag
– Innenausschuss –

Telefon 0851 509-2221
Telefax 0851 509-2222
E-Mail kai.lewinski@uni-passau.de
Datum 08.12.2020

Europa-, verfassungs- und datenschutzrechtliche Grundfragen des Registermodernisierungsgesetzes (RegMoG)*

* Der *Verf.* dankt herzlich seinem Assistenten *Marvin Gülker* für die umfangreiche Mitarbeit und fruchtreiche Diskussion.

I. Europarechtliche Grenzen für registerübergreifend einheitlichen Identifikator

Das europäische Recht macht in Art. 87 DSGVO spezifische, wenngleich recht unscharfe Vorgaben für „Kennzeichen von allgemeiner Bedeutung“.

1. „Kennzeichen von allgemeiner Bedeutung“

Was eine „nationale Kennziffer oder [ein] anderes Kennzeichen von allgemeiner Bedeutung“ (Art. 87 S. 1 DSGVO) ist, kann explizit der DSGVO nicht entnommen werden. Doch gilt Art. 87 DSGVO auch unterhalb der Schwelle einer *umfassenden* Geltung und Verwendung des Personenkennzeichens, solange ein solches **nicht nur in einem speziellen Bereich zum Einsatz** kommt, sondern darüber hinaus – eben – *allgemein*.

> Bei einer Verwendung bei über 50 Registern von etwa 200 (nach Bundesrecht) bestehenden ist die Identifikationsnummer nach dem IDNrG ein „Kennzeichen von allgemeiner Bedeutung“ mit Potential für eine „nationale Kennziffer“; jedenfalls unterfällt sie Art. 87 DSGVO.

2. Grundsätzliche Erlaubtheit

Aus der gestattenden Erwähnung von allgemeinen Personenkennzeichen in der DSGVO ist abzuleiten, dass solche **grundsätzlich mit europäischem Datenschutzrecht vereinbar** sind[1].

> Die **JI-RL (EU) 2016/680** für den Datenschutz im Sicherheitsbereich kennt keine dem Art. 87 DSGVO vergleichbare Regelung[2]. Ob und wie weit für den von der JI-RL geregelten Bereich eine Personenkennziffer möglich ist, mag bezweifelt werden. Die Anerkennung einer allgemeinen mitgliedstaatlichen Kennziffer durch Art. 87 DSGVO als *Grund*verordnung spricht allerdings dafür, dass eine solche gemeineuropäisch erlaubt ist. – Für das RegMoG kann dies allerdings dahinstehen, wenn und soweit die Register nach Anlage zu § 1 IDNrG-E nicht unter die JI-RL und damit nach Art. 1 Abs. 2 lit. d DSGVO nicht aus dem Anwendungsbereich der DSGVO fallen.
> Daneben ist darauf hinzuweisen, dass die europarechtliche Einführung automatischen Registerkommunikation (insb. Art. 14 der **Single Digital Gateway-VO (EU) 2018/1724**) und das darin enthaltene „Once-Only“-Prinzip sinnvoll nur über Personenkennzeichen implementierbar ist (wenngleich dieser Rechtsakt „Kennzeichen von allgemeiner Bedeutung“ o.ä. nicht ausdrücklich anspricht). – Weitere auf europäischer Ebene bereits eingeführte bereichsspezifische Kennzeichen[3] stützen diesen Befund.

3. Mitgliedstaatliche Ausgestaltung bei geeigneten Garantien

Es kann bei der mitgliedstaatlichen Ausgestaltung[4] also **von spezifischen Vorgaben der DSGVO abgewichen** werden, wenn und solange dies unter „Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Personen“ geschieht.

> Diese Regelung ist in mehrerlei Hinsicht sprachlich und inhaltlich verunglückt: „Wahrung der Garantien“ ist kein gutes Deutsch, und es fehlt bei der Neueinführung eines Personenkennzeichens der Bezugspunkt für die „Wahrung“. Auch sind diese Voraussetzungen ganz individualistisch auf die „betroffene Person“ fokussiert, was die systemische und gesellschaftliche Bedeutung einer Personenkennzeichens ausblendet, obwohl das europäische Datenschutzgrundrecht (Art. 8 GRCh; vgl. Art. 16 Abs. 1 AEUV) ansonsten die ausschließlich individualistische Perspektive des deutschen „Rechts auf Informationelle Selbstbestimmung“ gerade nicht in dem Maße teilt.

Was unter „geeigneten Garantien“ zu verstehen ist, wird von der DSGVO nicht explizit vorgegeben und ist in Rechtsprechung und Schrifttum bislang nur umrissweise und noch unscharf herausgearbeitet.

---

1 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 87 DSGVO, Rn. 9.
2 *Herbst*, in: Auernhammer, DSGVO/BDSG, 7. Aufl. 2020, Art. 87 DSGVO, Rn. 3.
3 Übersicht bei *v. Lewinski*, in: Wolff/Brink, BeckOK Datenschutzrecht, 34. Ed. 2020, Art. 87 DSGVO, Rn. 14.
4 Für die personenbezogene Datenverarbeitung müssen gleichwohl datenschutzrechtliche Erlaubnistatbestände vorliegen (etwa Art. 6 Abs. 1 UAbs. 1 lit. 4 i.V.m. Abs. 3 S. 1 lit. b DSGVO); Art. 87 DSGVO ist (nur) eine Öffnungsklausel, nicht aber (auch) ein Erlaubnistatbestand.

Die Garantien können **gesetzlicher, technischer oder organisatorischer Art** sein[5]. Ob sie in allen diesen drei Feldern zugleich bestehen müssen und wie ggf. ihr Zusammenspiel aussehen muss, ist noch nicht geklärt[6]. Dass allerdings eine „verbindliche rechtliche Grundlage" bestehen muss[7], scheint allein schon rechtstaatlich geboten. – Auf was die „Garantien" nun genau gerichtet sein müssen, ist freilich unklar. Es finden sich in der (deutschen) Kommentarliteratur vornehmlich unscharfe Formulierungen wie „allgemeine Maximen der DSGVO"[8]. Andere fordern ein vom „Wesenskern" des Art. 5 DSGVO geprägtes „Mindestschutzniveau"[9].

So lässt sich also nicht genau benennen, was im einzelnen durch Art. 87 DSGVO gefordert wird. Wenn manche meinen, aus den europarechtlichen Vorgaben ein dezidiertes Verbot von Persönlichkeitsprofilen herauslesen zu können[10], bleibt dies jedenfalls eine Begründung schuldig. Die Datenminimierung, insbesondere bei der Konzeption eines Personenkennzeichens, wird jedenfalls nicht als zwingende Vorgabe des Art. 87 DSGVO verstanden[11]. – Weil es für den europäische Datenschutz prägend ist, wird man für ein zweckoffenes Personenkennzeichen jedenfalls Regelungen zur **Zweckbegrenzung und Zweckbindung der solchermaßen verknüpften Daten** fordern müssen[12].

4. Zwischenergebnis: Unklare bzw. nur minimale europarechtliche Vorgaben

Der genaue Gehalt und die Reichweite der europarechtlichen Vorgaben des Art. 87 DSGVO ist unklar. Rechtsprechung fehlt, das Schrifttum changiert zwischen tastender Beschreibung und rechtspolitischem Wunschzettel. Als **allgemein konsentierten Kern** wird man einstweilen festhalten können, dass die DSGVO allgemeine Personenkennzeichen im Grundsatz zulässt, dass kompensierende „geeignete Garantien" jedenfalls auch rechtliche sein müssen und wohl auch, dass die PKZ einer Zweckbindung unterliegen muss.

> Erhellend, im Rahmen dieser Stellungnahme aber nicht leistbar, wäre ein **innereuropäischer Rechtsvergleich**. Die Regelung des Art. 87 DSGVO setzt erkennbar auf den Unterschiedlichkeiten in den Mitgliedstaaten[13] auf, einen politischen Willen zur Änderung bestehender Systeme hatte es erkennbar nicht gegeben. Insoweit muss man davon ausgehen, dass die zum Zeitpunkt des Beschlusses der DSGVO[14] bestanden habenden Systeme in anderen EU-Mitgliedstaaten eine Blaupause der DSGVO-Konformität abgeben.

II. Absolute Grenzen für registerübergreifend einheitlichen Identifikator

Da europarechtlich Einführung und Ausgestaltung von Personenkennzeichen weitgehend den Mitgliedstaaten überwiesen ist, besteht insoweit Umsetzungs- und Ausgestaltungsspielraum. Innerhalb dieses Spielraums machen die **mitgliedstaatlichen Verfassungsordnungen maßgeblich**e Vorgaben. Das Grundgesetz verbietet ein (allgemeines) Personenkennzeichen nicht als solches (→ 1.),

---

5 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 87 DSGVO, Rn. 23.

6 Vgl. *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 87 DSGVO, Rn. 26 („müssen in ihrer Gesamtheit gewährleisten"); pauschaler *Sorge/v. Lucke/Spiecker*, Registermodernisierung – Datenschutzkonforme und umsetzbare Alternativen, Dez. 2020, S. 23.

7 *Wedde*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 87 DSGVO, Rn. 15.

8 *Weichert*, in: Kühling/Buchner, DSGVO, 2. Aufl. 2018, Art. 87, Rn. 15–19, dort freilich mit der Spezifizierung, dass dies dann etwa die Zweckbindung, die Datenminimierung und die Transparenz einschlösse.

9 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 87 DSGVO, Rn. 24.

10 Ausdrücklich im Sinne einer Garantie i.S.d. Art. 87 S. 2 DSGVO *Herbst*, in: Auernhammer, DSGVO/BDSG, 7. Aufl. 2020, Art. 87 DSGVO, Rn. 9.

11 *Wedde*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 87 DSGVO, Rn. 17 („legt es nahe").

12 Gestaltungsoptionen bei *Wedde*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 87 DSGVO, Rn. 16; differenzierend *v. Lewinski*, in: Wolff/Brink, BeckOK Datenschutzrecht, 34. Ed. 2020, Art. 87 DSGVO, Rn. 45; zu einfach *Sorge/v. Lucke/Spiecker*, Registermodernisierung – Datenschutzkonforme und umsetzbare Alternativen, Dez. 2020, S. 22.

13 Kurzer Überblick bei *Wedde*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 87 DSGVO, Rn. 5, *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 87 DSGVO, Rn. 31, und *v. Lewinski*, in: Wolff/Brink, BeckOK Datenschutzrecht, 34. Ed. 2020, Art. 87 DSGVO, Rn. 13.

14 Womöglich wird man auf den Zeitpunkt des Beschlusses der EG-Datenschutzrichtlinie 95/46/EG zurückgehen können, die in ihrem Art. 8 Abs. 7 die Vorgängerregelung enthielt. Dort war freilich von „geeigneten Garantien" o.ä. (noch) keine Rede.

sondern lediglich die Bildung eines umfassenden Persönlichkeitsprofils (→ 2.). Das verfassungsrechtliche Verbot anlassloser Vorratsdatenspeicherung betrifft Personenkennzeichen nicht (→ 3.).

1. Nicht: Personenkennzeichen als solches

In der Bundesrepublik Deutschland hatte es **bislang kein allgemeines Personenkennzeichen** gegeben. In der rechts- und gesellschaftspolitischen Diskussion war es gleichwohl präsent, da es in der DDR ein einheitliches Personenkennzeichen gegeben hatte[15] und aus der nationalsozialistischen Zeit jedenfalls entsprechende Pläne bekannt sind[16]. Nicht zuletzt vor diesem Hintergrund war ein bundesdeutsches Personenkennzeichen 1976 im und vom Rechtsausschuss des Deutschen Bundestages politisch einstweilen beerdigt worden[17]. Das Schrifttum ist bei der Beurteilung der Frage der Erlaubtheit von Personenkennzeichen seit jeher bemerkenswert unscharf; Juristisches und Rechtspolitisches mischt sich in hohem Maße.

> Die Rede ist davon, dass „große Bedenken […] bestünden", „viele Menschen" eine PKZ als unzulässig ansähen und „verfassungsrechtliche Vorbehalte" bestünden[18] sowie allgemein von der „Angst vor dem Computer"[19].

Personenkennzeichen als solche ist aber in recht **triviales Datum**. Selbst wenn sie das Geburtsdatum, das Geschlecht oder Anfangsbuchstaben des Namens enthielte („sprechende PKZ"), wäre dies nicht sensitiv oder überhaupt oberhalb einer Alltäglichkeit[20]. Eine Kennziffer ohne wesentlichen semantischen Gehalt ist **als solche insoweit datenschutzrechtlich unkritisch**[21]. Auch sektorielle und bloße Ordnungsziffern (z.B. Passnummern) gelten allgemein als unbedenklich[22].

2. Umfassendes Persönlichkeitsprofil

Kritisch an einer PKZ ist, dass sie ein mächtiges Mittel für die Verknüpfung von Daten aus verschiedenen Lebensbereichen, Verwaltungssektoren und sozialen Rollen darstellt[23]. Dies würde dann das Erstellen von Persönlichkeitsprofilen ermöglichen – dem **Gottseibeiuns des Datenschutzrechts**.

Bemerkenswerterweise hat das deutsche Recht bislang aber noch keine Definition von „Persönlichkeitsprofil" oder deren Qualifikation als umfassendes Persönlichkeitsprofil entwickelt[24]. Dieses Defizit mag dadurch erklärlich sein, dass solche Persönlichkeitsprofile bislang in Deutschland nicht im Raum und zur Debatte standen. Wenn dies mit der ID-Nr. und dem RegMoG nun aber anders werden sollte, ist diese Grenze, die **aus der Rechtsprechung des BVerfG** stammt, zu vermessen.

In der **Mikrozensus-Entscheidung** von 1969 hat das Gericht es mit der Menschenwürde für unvereinbar erklärt, Menschen in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren[25]. Während in dieser Entscheidung noch offenblieb, ob die Daten aus staatlichen Registern überhaupt ausreichten, um ein solches Persönlichkeitsprofil zu erstellen, hat das BVerfG dann in der **Volkszählung-Entscheidung** von 1983 ausdrücklich davon gesprochen, dass „die Einführung eines einheitlichen, für alle Register und Dateien geltenden Personenkennzeichens" ein entscheidender Schritt hin zu einem solchen Persönlichkeitsprofil darstellen würde[26], was impliziert, dass aus den in der

---

15 *v. Lewinski*, in: Rüpke/v. Lewinski/Eckhardt, Datenschutzrecht, 2018, § 2 Rn. 40 m.w.N. in Fn. 89.
16 *Aly/Roth*, Restlose Erfassung, 2000, S. 54 ff., 132 ff.
17 *v. Lewinski*, in: Rüpke/v. Lewinski/Eckhardt, Datenschutzrecht, 2018, § 2 Rn. 50 m.w.N.
18 *Wedde*, in: Däubler/Wedde/Weichert/Sommer, EU-DSGVO und BDSG, 2. Aufl. 2020, Art. 87 DSGVO, Rn. 6, 19.
19 *v. Lewinski*, in: Wolff/Brink, BeckOK Datenschutzrecht, 34. Ed. 2020, Art. 87 DSGVO, Rn. 18.
20 Die Nutzung eines nicht-sprechenden Kennzeichens, das keine Rückschlüsse auf die Stammdaten zulässt, wird allgemein positiv bewertet. Es begünstigt einen gleichmäßigen und nicht-diskriminierenden Gesetzesvollzug (*Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 87 DSGVO, Rn. 16). Allerdings hat auch das sprechende Kennzeichen Vorteile, weil es leichter zu merken ist (Usability) und zudem die Subjektqualität des Betroffenen akzentuiert (vgl. *v. Lewinski*, in: Seckelmann, Digitalisierte Verwaltung. Vernetztes E-Government, 2. Aufl. 2019, S. 107, Rn. 43, dort aber auch zu den Gegenargumenten).
21 Vgl. *v. Lewinski*, in: Wolff/Brink, BeckOK Datenschutzrecht, 34. Ed. 2020, Art. 87 DSGVO, Rn. 20 f.
22 *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 87 DSGVO, Rn. 3.
23 Explizit *Herbst*, in: Auernhammer, DSGVO/BDSG, 7. Aufl. 2020, Art. 87 DSGVO, Rn. 5.
24 *v. Lewinski*, RDV 2003, S. 122, 123. – Die Diskussion ist in diesem Punkt seitdem nicht weitergekommen.
25 BVerfGE 27, S. 1, 6 – Mikrozensus.
26 BVerfGE 65, S. 1, 57 – Volkszählung

Verwaltung vorhandenen Informationen ein umfassendes und dann gegen die Menschenwürde verstoßendes umfassendes Persönlichkeitsprofil erstellt werden könnte.[27]

Nun kann man lange darüber diskutieren, ob diese Ausführungen tragend für die jeweiligen Entscheidungen waren oder nur obiter dicens, wie die Genese des Volkszählung-Urteils genau verlief[28] und ob das Gericht nach 50 bzw. 40 Jahren Technik- und Gesellschaftsentwicklung daran festhalten würde. Jedenfalls gibt es in der Rechtsprechung des BVerfG auch keine Anzeichen, dass es von dieser skizzierten Festlegung in der Zwischenzeit abgerückt wäre.

3. Nicht: anlasslose Vorratsdatenspeicherung

Die Verfassung verbietet die anlasslose Vorratsdatenspeicherung[29]. Doch handelt es sich bei einem Personenkennzeichen weder um anlasslose noch überhaupt um Datenspeicherung im Sinne dieser speziellen Verfassungsrechtsprechung. Zunächst einmal wird die ID-Nr. ja für eine konkrete Registeraustauschstruktur geschaffen und eingesetzt, ist also nicht anlasslos. Und dann ist die ID-Nr. zweifellos ein personenbezogenes Datum i.S.d. Datenschutzrechts, gleichwohl aber ein – in den Worten der Statistik gesprochen – „Hilfsmerkmal“ ohne einen semantischen Gehalt (→ 1. | S. 4).

4. Sonstige verfassungsrechtliche Gesichtspunkte

Nach der Entwurfsbegründung wird das IDNrG-E auf eine Bundeskompetenz kraft Natur der Sache gestützt[30]. Doch handelt es sich nicht um eine Sachmaterie, die schlechthin nur der Bund regeln könnte, da auch die Länder Register betreiben (können). Die alternativ angeführte **Annexgesetzgebungskompetenz**[31] passt insoweit besser. Denn soweit dem Bund die Kompetenz zur Regelung der jeweiligen Register zukommt, ist es sachgerecht, ihm auch die Kompetenz für eine registerübergreifende ID-Nr. zuzuerkennen (solange er nicht auch eine Nutzung dieser Nummer in ländereigenen Registern vorschreibt).

Ob und auf welcher Ebene der Staat womöglich eine Gewährleistungsverantwortung für die eindeutige Identifizierbarkeit von Menschen hat (vgl. Art. 24 Abs. 2 IPbpR und Art. 7 UN-Kinderrechtsübereinkommen) und ob dies auch Identifikatoren einschließen kann[32], soll hier nicht vertieft werden.

III. Verfassungsrechtliche Grenzen der Identifikationsnummer nach IDNrG-E

Ob die Einführung einer Identifikationsnummer wie die nach IDNrG-E möglich ist, bestimmt sich im Rahmen der dürren europarechtlichen Vorgaben (→ I.) und speziellen verfassungsrechtlichen Grenzen (→ II., → III.3.) nach dem **allgemeinen Gebot der Verhältnismäßigkeit** und bei kollidierenden Rechts- und Verfassungsgüter nach dem **Maßstab praktischer Konkordanz**.

1. Gesetzliche Grundlage

a) Gesetzes- und Parlamentsvorbehalt für Nummernraum

Für die Konzeption eines Nummernsystems („logischer Raum“) und die Errichtung und Einrichtung von Datenverarbeitungssystemen und -strukturen besteht kein ausdrücklicher und kein allgemeiner Gesetzesvorbehalt[33]. Doch ist der Zuschnitt eines „logischen Raumes“ keine bloß technische Designentscheidung, sondern eine Machtressource und deshalb rechtlich nicht irrelevant[34]. Entsprechend den verfassungsgerichtlichen **Maßstäben der Wesentlichkeit** und ggf. auch wegen

---

27 Ab wann „Teilabbilder der Persönlichkeit“ verfassungsrechtlich unzulässig werden, hat das BVerfG (BVerfGE 65, S. 1, 53 f. – Volkszählung) offengelassen (zu dezidiert deshalb Beschlussantrag Nr. I.3 der FDP (BT-Drucks. 19/24641).

28 Dazu *Pohle*, Datenschutz und Technikgestaltung, Diss. rer. nat. HU 2018, S. 144.

29 BVerfGE 65, S. 1, [46; BVerfGE 100, S. 313, 360; BVerfGE 115, S. 320, 350; BVerfGE 118, S. 168, 187.

30 Entwurfsbegründung, BR-Drucks. 563/20, S. 33 (= BT-Drucks. 19/24226).

31 Entwurfsbegründung, BR-Drucks. 563/20, S. 33 (= BT-Drucks. 19/24226).

32 *v. Lewinski*, in: Wolff/Brink, BeckOK Datenschutzrecht, 34. Ed. 2020, Art. 87 DSGVO, Rn. 6 ff., Rn. 17.

33 *v. Lewinski*, in: Seckelmann, Digitalisierte Verwaltung. Vernetztes E-Government, 2. Aufl. 2019, S. 107, Rn. 19.

34 *v. Lewinski*, in: Liber amicorum Ingolf Pernice, 2020, S. 65 ff.

Grundrechtseingriffen kann hier ein **Gesetzes- oder gar ein Parlamentsvorbehalt** bestehen[35]. Auch ist er europarechtlich geboten (→ I. 3. | S. 2) bei effizienterer Verdatung natürlicher Personen durch eine allgemeine Identifikationsnummer könnte man auch den (mitgliedstaatlichen) Gesetzgeber aufgrund des Gedankens des Art. 25 DSGVO für verpflichtet ansehen, „geeignete […] organisatorische Maßnahmen“ selbst zu treffen.

> Problematisch ist insoweit, dass nach § 7 Abs. 2 IDNrG-E „Bereiche“ gebildet werden sollen und innerhalb eines „Bereichs“, der auch aus zahlreichen Behörden bestehen kann, im IDNrG-E keine eigenen Sicherungs-, Protokollierungs- oder Überprüfungsvorschriften vorgesehen sind. Insoweit gelten die Sicherungs- und Zweckbestimmungsvorschriften des jeweils bestehenden Registerfachrechts unverändert fort, obwohl durch die Einfügung der Personenkennziffer in die Datenübermittlung eine neue Situation geschaffen wird. Ob die zusätzlichen Sicherungsmaßnahmen des IDNrG-E, wie namentlich das 4-Ecken-Modell, effektiv greifen, hängt vom Zuschnitt der Bereiche ab. Dieser Bereichszuschnitt ist aber unabhängig von den bestehenden Rechtsgrundlagen letztlich in das Belieben der Bundesregierung gestellt, die diesen gem. §§ 7 Abs. 2 S. 2, § 12 Abs. 1 Nr. 2 IDNrG-E durch Rechtsverordnung ohne Zustimmung des Bundesrates vornehmen kann. Je nach konkreter Ausgestaltung des betroffenen Registerfachrechts kann sich damit der **Bereichszuschnitt** als eine Maßnahme von besonderer Wesentlichkeit darstellen[36]. Die Wesentlichkeitslehre des BVerfG verlangt aber, dass Maßnahmen von hoher Grundrechtsrelevanz vom Parlament selbst entschieden werden[37]. Die konturlose Vorgabe in § 7 Abs. 2 S. 2 IDNrG-E, lediglich mindestens 6 Bereiche zu bilden, genügt dem Parlamentsvorbehalt bzw. der Wesentlichkeitslehre nicht, da sie nicht auf die Bedeutung(sbegrenzung) der Bereiche abstellt (Bsp.: Hundehalterregister, Katzenhalterregister, Hamsterhalterregister, Zierfischhalterregister, Gifttierhalterregister, alle anderen Bereiche der Verwaltung). Mangels normativer Wirkung ist das Beispiel in der Entwurfsbegründung[38] keine wesentliche Konturierung.
> Dass die Bundesregierung im Verordnungswege **weitere Register in die Registermodernisierung einbeziehen** kann (§ 12 Abs. 1 Nr. 1 IDNrG-E), ist vor dem Hintergrund der Wesentlichkeit ebenfalls problematisch[39].

b) Spezifisch datenschutzrechtliche Normenklarheit für Eingriffsnorm

Für die konkrete Nutzung (einschließlich bereits der Zuweisung) einer personenbezogenen Identifikationsnummer ergibt sich dann aus dem **grundrechtlichen Gesetzesvorbehalt** für Eingriffe in das Informationelle Selbstbestimmungsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG: „verfassungsmäßige Ordnung“; vgl. Art. 19 Abs. 1 GG), dass ein gestattendes Gesetz vorliegen muss[40].

Solche Schranken müssen dem Gebot der Normenklarheit genügen (**Bestimmtheitsgebot**). Verfassungsgerichtlich und v.a. auch in der Lehre ist für Eingriffe in das Informationelle Selbstbestimmungsrecht dieser einfache Gesetzesvorbehalt anhand des Rechtsstaatsprinzips dahingehend spezifiziert worden, dass die Rechtsgrundlage normklar sein müsse[41]. Das erfordert, dass der Verwendungszweck der Daten bereichsspezifisch und präzise bestimmt ist und Daten nicht zu noch nicht bestimmbaren Zwecken auf Vorrat gespeichert werden[42].

> Hinsichtlich der Regelungen zur Steuer-ID in den §§ 139a ff. AO sind insoweit keine durchgreifenden Bedenken geltend gemacht worden[43]. Man wird die Normtiefe und den Detailgrad der dortigen Regelungen als Anhalt für die Formulierung des § 139b AO-E und des IDNrG-E nehmen können.

---

35 Hierzu allgemein *v. Lewinski*, in: Seckelmann, Digitalisierte Verwaltung. Vernetztes E-Government, 2. Aufl. 2019, S. 107, Rn. 27 et pass.

36 Weitere Kriterien im Rahmen der Wesentlichkeitslehre, auf die hier aber nicht weiter eingegangen wird, sind u.a. die Größe des Adressatenkreises, die Langfristigkeit der Festlegung und die politische Umstrittenheit (*Grzeszick*, in: Maunz/Dürig, GG, 51. ErgLfg. 2007, Art. 20, Abschn. VI, Rn. 107).

37 *Schmidt-Aßmann*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Bd. II, 3. Aufl. 2004, § 26 Rn. 64; BVerfGE 49, S. 89, 126 f.

38 Entwurfsbegründung, BR-Drucks. 563/20, S. 75 (= BT-Drucks. 19/24226).

39 Beschlussantrag Nr. 2 der FDP (BT-Drucks. 19/24641).

40 *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke, GG, 14. Aufl. 2018, Art. 2, Rn. 18.

41 BVerfGE 65, S. 1, 44 – Volkszählung; *Di Fabio*, in: Maunz/Dürig, GG, 39. ErgLfg. 2001, Art. 2, Rn. 182; *Rudolf*, in: Merten/Papier, Handbuch der Grundrechte, 2011, § 90 Rn. 68.

42 BVerfGE 65, S. 1, 46 – Volkszählung; BVerfGE 115, S. 320, 365 – Rasterfahndung; *Lorenz*, in: Bonner Kommentar zum GG, 133. ErgLfg. 2008, Art. 2, Rn. 339 f.

43 BFH, DStR 2012, S. 283, Rn. 96; ausführlich *Zelyk*, Das einheitliche steuerliche Identifikationsmerkmal, 2012, S. 81 ff., S. 113 ff.

2. Verhältnismäßigkeit

Wie **jedes staatliche Handeln** müssen auch die Einführung und der Einsatz der Identifikationsnummer nach IDNrG-E dem aus dem Rechtstaatsprinzip abzuleitenden Verhältnismäßigkeitsgebot genügen. Danach dürfen nur **legitime Ziele** verfolgt werden, es müssen hierfür **geeignete Mittel** eingesetzt werden, die in dem Sinne **erforderlich** sein müssen, dass es nicht ein gleichermaßen effektives, aber weniger eingreifendes Mittel gäbe. Und schließlich muss das staatliche Handeln angemessen (**verhältnismäßig im eigentlichen Sinne**) sein, was insbesondere eine Abwägung mit anderen Rechts- und Verfassungsgütern beinhaltet.

a) Legitimes Ziel

Legitimes Ziel ist v.a. das Voranbringen der Digitalisierung und die Verbesserung der Verwaltungseffizienz[44]. Auch die Verbesserung der Leistungs- und Belastungsgerechtigkeit ist ein legitimes Ziel[45].

Zwar erwähnt das Grundgesetz nicht ausdrücklich die **Effizienz als Verfassungsgut**, doch gibt es in Art. 114 Abs. 2 S. 1 GG mit der „Wirtschaftlichkeit" und in Art. 108 Abs. 4 GG mit der Verbesserung des „Vollzug[s] der Steuergesetze" zu erkennen, dass es eine Verbesserung der Effizienz als legitim ansieht[46]. Zudem wird aus dem Rechtsstaats- (Art. 20 Abs. 3 GG) und insbesondere dann dem Sozialstaatsprinzip (Art. 20 Abs. 1 GG) gefolgert, dass der Staat diese Staatsziele auch effektiv verwirklichen können muss, was ohne eine effiziente Verwaltung nicht möglich ist[47].

Ähnliches gilt für die Digitalisierung (der Verwaltung). Sie ist zwar in der Verfassung nicht ausdrücklich angesprochen. Durch die Einfügung des Art. 91c GG hat sie jedoch grundgesetzlich Anerkennung gefunden, v.a. ist von der Verfassung der **„übergreifende Zugang zu Verwaltungsleistungen" ausdrücklich erwähnt**.

> Wenn man gegen die Ziellegitimität anführt, dass das RegMoG eine Struktur anlegt oder ansteuert, die zu einem verfassungswidrigen Persönlichkeitsprofil führen würde (**Slippery Slope-Argument**, „Salamitaktik", „Büchse der Pandora")[48], dann mag das rechts*politisch* beachtlich sein, verfassungsrechtlich ist es das nicht. Denn Demokratie basiert auf der potentiellen Reversibilität aller politischen Entscheidungen, so dass es insoweit keine rechtlichen Pfadabhängigkeiten gibt (Bsp.: Atomausstieg(e)). Es ist verfassungs*rechtlich* also gerade kein Argument gegen eine Maßnahme, dass eine mögliche zukünftige Maßnahme verfassungswidrig ist[49].

b) Geeignetheit

Geeignet ist ein Gesetz, wenn es dem (legitimen) Ziel förderlich ist; eine vollständige Verwirklichung muss nicht erreicht werden[50].

Die Einführung einer PKZ wie der ID-Nr. ist dazu geeignet, die erstrebte **Effizienzsteigerung und die Digitalisierung** zu befördern. Durch ein eindeutiges Personenkennzeichen wird es möglich, Verwaltungsprozesse zu digitalisieren und den zeitsparenden Once-Only-Grundsatz umzusetzen. Uneindeutigkeiten bei der Personenzuordnung führen zum Abbruch digitaler Verwaltungsprozesse[51] und damit zu Mehraufwand in der Verwaltung, da eine manuelle Zuordnung nötig wird. Leistungsmissbrauch durch Falschidentitäten kann verhindert werden[52] und die Schwelle für die Inanspruchnahme von Leistungen gesenkt.

> Zielbild einer modernen Registerlandschaft ist nach der Entwurfsbegründung der Abbau von Datenredundanzen in den verschiedenen Registern, sodass gleiche Daten nur bei jeweils einem originär zuständigen Register vorhanden sind[53]. Gegenüber einer redundanten Datenhaltung wird der

---

44 Entwurfsbegründung, BR-Drucks. 563/20, S. 31 (= BT-Drucks. 19/24226).
45 Vgl. Entwurfsbegründung, BR-Drucks. 563/20, S. 64 (= BT-Drucks. 19/24226).
46 Vgl. *Zelyk*, Das einheitliche steuerliche Identifikationsmerkmal, 2012, S. 99 ff.; *Gröpl*, in: Isensee/Kirchhof, Handbuch des Staatsrechts, Bd. V, 3. Aufl. 2007, § 121 Rn. 16.
47 *Zelyk*, Das einheitliche steuerliche Identifikationsmerkmal, 2012, S. 99 f.
48 Vgl. *Datenschutzkonferenz*, Entschließung v. 26.8.2020, DuD 2020, S. 712.
49 *Martini/Wagner/Wenzel*, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, 2017, S. 44.
50 *Kloepfer*, Verfassungsrecht, Bd. II, 2010, § 51 Rn. 98.
51 Entwurfsbegründung, BR-Drucks. 563/20, S. 31 (= BT-Drucks. 19/24226).
52 Zu den erklärten Zielen des Gesetzes gehören die Eliminierung von Karteileichen und Dubletten (Entwurfsbegründung, BR-Drucks. 563/20, S. 63 [= BT-Drucks. 19/24226]).
53 Entwurfsbegründung, BR-Drucks. 563/20, S. 31 (= BT-Drucks. 19/24226).

Pflegeaufwand dann reduziert[54]. Es ist insoweit überraschend, dass ausgerechnet die für alle Fachregister erheblichen sog. **„Basisdaten“** – Name, Geburtsdatum, Anschrift usw. (vgl. § 4 Abs. 2 IDNrG-E) – nicht etwa nur in der zentralen Datenbank beim BZSt, auf die gem. § 6 IDNrG-E über die Registermodernisierungsbehörde zugegriffen wird, vorgehalten werden sollen, sondern **weiterhin auch in allen Fachregistern vorhanden** sein werden. Auch die Fachdaten der einzelnen Register werden durch den Gesetzentwurf nicht diesem (Fern-)Ziel entsprechend zentralisiert, sondern bleiben unverändert. Die Beschränkung der Registermodernisierung auf Register i.S.d. OZG verhindert, dass die einzelnen Fachregister neben ihren eigenen Fachdaten nur noch die PKZ speichern und die Stammdaten bei Bedarf bei der Registermodernisierungsbehörde als zentraler Anlaufstelle abfragen. Mit der Einführung der Identifikationsnummer wird immerhin der Boden für eine mögliche Zentralisierung von Fach- und Basisdaten in der Zukunft gelegt, und die Identifikationsnummer steigert auch schon in der durch den Gesetzentwurf eingeführten Gestalt die Verwaltungseffizienz durch die Verbesserung der Automatisierbarkeit der Verwaltungsprozesse. Außerdem wird durch eine kontinuierliche Qualitätssicherung gem. § 10 IDNrG-E durch BZSt und Registermodernisierungsbehörde, die auch die Kommunikation von Änderungen an die Fachregister umfasst, die übergreifende Richtigkeit der Basisdaten gefördert.

c) Erforderlichkeit

Erforderlichkeit heißt, dass es keine den Zweck gleichermaßen fördernden, aber für Betroffene milderen Mittel geben darf[55].

aa) Alternative: Beibehaltung des Status quo

Ein „Weiter wie bisher“ (**Nulloption**) erreicht das Ziel der Verwaltungseffizienz nicht in gleichem Maße.[56] Die häufigen Uneindeutigkeiten bei der Personenfeststellung verhindern eine Automatisierung des Verfahrens, die ihrerseits für die Digitalisierung notwendig ist. Außerdem bliebe es bei der bisherigen Zahl von Personenverwechslungen[57].

Mit Blick auf eine Datenschutzfreundlichkeit der Nulloption ist anzumerken, dass Persönlichkeitsprofile auch ohne PKZ gebildet werden können. Schreibabweichungen und ähnliche Ungenauigkeiten können mittlerweile auch durch mustererkennende Programme (sog. „KI“) automatisiert behoben werden; tatsächlich existieren Algorithmen wie die Levenshtein-Distanz schon lange. Datenschutzorthodox würde der geltende Status quo des Verwaltungsalltags denselben Bedenken ausgesetzt sein wie die ID-Nr. nach dem RegMoG. Die verwaltungstechnische Verwendung von Name und Anschrift wird – soweit ersichtlich – aber nicht verfassungsrechtlich hinterfragt.

bb) Alternative: Registerharmonisierung ohne PKZ

Register können zwar auch ohne Nutzung einer Personenkennziffer harmonisiert werden, jedoch nur für den Moment. Nach der Harmonisierung würden sich die **Daten in den Registern wieder auseinanderentwickeln**[58], so dass das Ziel der Verwaltungseffizienz nicht erreicht wird.

cc) Alternative: Flächendeckende Einführung des 4-Corner-Modells

Nach dem vorliegenden Entwurf erfolgt eine Datenübermittlung gem. § 7 Abs. 2 IDNrG-E nur dann verschlüsselt und nach dem 4-Corner-Modell, wenn eine sog. „Bereichsgrenze“ überschritten wird. Bereiche nach § 7 Abs. 2 S. 2 IDNrG-E sollen, was aber aus dem Gesetz als solches nicht hervorgeht (→ 1. a) | S. 5), thematisch zusammenhängende Gruppen von Behörden wie z.B. „Inneres“, „Justiz“ oder „Gesundheit“ sein[59].

Datensicherheitserhöhend (und so mit Blick auf die Informationelle Selbstbestimmung milder) wäre es, wenn das 4-Ecken-Modell nicht nur bei bereichsübergreifenden, sondern auch bei bereichsinternen Datenübermittlungen verpflichtend wäre.[60] Insbesondere die automatisierte Prüfung auf die Rechtmäßigkeit der Datenübermittlung gem. § 7 Abs. 2 S. 5 u. 6 IDNrG-E, die dem Registerfachrecht oftmals fremd ist, würde den Grundrechtsschutz (durch Verfahren) verbessern.

---

54 Entwurfsbegründung, BR-Drucks. 563/20, S. 32 (= BT-Drucks. 19/24226).
55 *Kloepfer*, Verfassungsrecht, Bd. II, 2010, § 51 Rn. 100.
56 So aber *BfDI*, Stellungnahme v. 26.8.2020, S. 1 f. mit Verweis auf (ungenannt bleibende) Bundesministerien.
57 Entwurfsbegründung, BR-Drucks. 563/20, S. 32 (= BT-Drucks. 19/24226).
58 Entwurfsbegründung, BR-Drucks. 563/20, S. 32 (= BT-Drucks. 19/24226): „pflegeintensiv und fehleranfällig“.
59 Entwurfsbegründung, BR-Drucks. 563/20, S. 75 (= BT-Drucks. 19/24226).
60 So auch Beschlussantrag Nr. 5 von Bündnis 90/Grüne (BT-Drucks. 19/25029).

(Einzige) Rechtfertigung für die nicht flächendeckende Einführung flächendeckender Verschlüsselung ist der **Kostenaufwand**[61]. Hierdurch wird die Effizienz der Registermodernisierung beeinträchtigt. Zwar Wirtschaftlichkeit- bzw. (Verwaltungs-)Effizienz haben zwar – wie beschrieben (→ a) – S. 7) – Verfassungsrang, aber schon wegen seiner eher indirekten Begründung kann es für sich allein die Entscheidung für oder gegen eine Maßnahme nicht begründen[62]. Anders läge der Fall nur dann, wenn die Kosten so prohibitiv hoch wären, dass die Funktionsfähigkeit des Staates gefährdet wäre, denn in diesem Moment tritt neben die Kostenfrage noch ein weiterer Aspekt. Solch hohe Kosten würde aber auch die flächendeckende Einführung des 4-Ecken-Modells nicht generieren.

Eine flächendeckende Einführung des 4-Ecken-Modells, wie vom BfDI gefordert[63], würde jedoch die **potentielle Angriffsfläche erweitern**. Denn hierdurch würde es für nahe zusammenarbeitende Behörden sehr aufwendig, ihren Aufgaben nachzukommen; stets müsste die technisch komplexe Verbindung zu den Vermittlungsstellen auf- und wieder abgebaut werden. Außerdem würden so nahe zusammenarbeitende Behörden thematisch verwandte, aber ortsverschiedene Datenbanken führen, statt einer einzigen für den ganzen Bereich relevanten Datenbank, bei denen naturgemäß ein hohes Risiko einer Datenredundanz auftreten würde. Die Vermehrung der Datenbanken ginge auch mit eine Mehrung des Sicherungsaufwands einher, da jede Datenbank wiederum für sich abgesichert werden müsste. Sie stellt sich damit nicht mehr als milderes Mittel dar, ist womöglich aus datensicherheitsgründen nicht einmal gleichermaßen geeignet.

dd) Alternative: bPKZ-Modell (Österreichisches Modell)

Der Gesetzentwurf des RegMoG verfolgt ein Modell mit einer einheitlichen PKZ für alle Registern. Speziell in Österreich wird dagegen ein Modell eingesetzt, bei dem die Behörden verschiedener Bereiche unterschiedliche Kennziffern nutzen, die jeweils nur für ihren eigenen Bereich gültig sind (bereichsspezifische PKZ, bPKZ). Dieses Modell ist als mildere, gleich zweckförderliche Alternative vorgeschlagen worden[64].

> Gegenüber dem vom Gesetzentwurf verfolgten Modell ist das bPKZ-Modell deutlich aufwendiger und dadurch **kostspieliger**. Das bPKZ-Modell erreicht daher schon das Ziel der Verwaltungseffizienz nicht in demselben Maße.

Bei näherem Hinsehen erweist sich allerdings, dass sich die Eingriffsintensität zwischen dem RegMoG- und dem österreichischen Modell kaum unterscheidet: In beiden Modellen werden dieselben Daten erhoben und automatisiert verknüpfbar gemacht.

(1) Unterschiedliche Angriffsfläche

Ein **Unterschied** besteht allein bei einem **rechtswidrigen Zugriff von außen auf die Daten**[65]. Bei einem erfolgreichen Angriff auf irgendeine Behörde oder durch einen rechtswidrigen Abruf durch Behördenmitarbeiter würde bei dem Modell des Gesetzentwurfs die allgemeine ID-Nr. erlangt; demgegenüber bei einem Modell nach österreichischer Art nur die bereichsspezifische Kennziffer. In dieser Hinsicht hat das österreichische Modell auch noch einen anderen Vorteil: Weil die bereichsspezifischen Kennziffern nur eine auf ihren Bereich begrenzte Aussagekraft besitzen, sind sie für Angreifer weniger attraktiv. An einer allgemeinen, für alles geltenden Kennziffer kann dagegen ein Interesse verschiedener, insbesondere auch nichtstaatlicher Akteure wie der Werbewirtschaft, ausländischen Nachrichtendiensten oder kriminellen Hackern bestehen.

> Zwar ist **„Identitätsdiebstahl“** im Zusammenhang mit der Steuer-ID bislang noch nicht bekannt geworden, doch könnte sich die Attraktivität dieser Nummer mit ihrem flächendeckenden Einsatz ändern[66]. Deshalb wäre zu überlegen dass die Kennziffer von allen Beteiligten vertraulich behandelt

---

61 Entwurfsbegründung, BR-Drucks. 563/20, S. 76 (= BT-Drucks. 19/24226): Vermeidung unnötiger Umsetzungsaufwände.

62 *Zelyk*, Das einheitliche steuerliche Identifikationsmerkmal, 2012, S. 101; umfassend dazu *Reifegerste/Pentschew/Kempny*, Finanzbewusste Verhältnismäßigkeitsdogmatiken, 2020. – Die Gegenüberstellung von Grundrechtseingriff einerseits und Kosten bzw. Verwaltungseffizienz andererseits könnte auch erst auf der Stufe der Angemessenheitsprüfung (→ d) | S. 12) thematisiert werden.

63 *BfDI*, Stellungnahme v. 21.10.2020, S. 6 f.

64 *BfDI* (Fn. 63), S. 4 f.

65 Vgl. *BfDI* (Fn. 63), S. 5.

66 Hierzu auch Beschlussantrag Nr. I.8 der FDP (BT-Drucks. 19/24641).

werden muss. Sie ist zeitlebens unveränderlich, und so können auch noch Jahre oder Jahrzehnte später, wenn die Person umgezogen ist oder durch Heirat oder Geschlechtsumwandlung einen neuen Namen angenommen hat, zufällig oder absichtlich erlangte Daten dieser Person mit Sicherheit zugeordnet werden. Das kann etwa für Erpressungen nach der sogenannten „Doxing"-Technik relevant sein, bei der mit der Veröffentlichung kompromittierender Informationen gedroht wird. Solche Fälle sind erst jüngst auch im prominenten politischen Bereich vorgekommen[67], und es steht zu befürchten, dass bei Bekanntwerden der Kennziffer ein entsprechend größeres Risiko für potentielle Opfer besteht. Wird die Kennziffer, ggf. auch mit Einwilligung des späteren Opfers, von privatwirtschaftlichen Unternehmen gespeichert und werden diese gehackt, so kann der Angreifer die dort gespeicherten Daten über Jahre hinweg mit den Daten anderer erfolgreicher Angriffe zusammenführen und die Auswirkungen einer solchen Erpressung vervielfachen. Mag das durch einen einzelnen Angreifer unwahrscheinlich sein, darf man nicht vergessen, dass in den dunklen Ecken des Internets Daten aus unterschiedlichsten erfolgreichen Cyber-Angriffen rege gehandelt werden. Die Folgen einer zweifellosen und vom Betroffenen wegen der Unveränderlichkeit der Kennziffer nicht verhinderbaren Zusammenführung dieser Daten sind schwer überschaubar. Zwar wird auch die heutige Steuer-ID bereits von Stellen auch außerhalb der Finanzbehörden gespeichert. Doch wird die ID-Nr. durch die Anlage zu § 1 IDNrG-E in weitaus mehr Register eingeführt, als es heute der Fall ist. In je mehr Register die Identifikationsnummer eingeführt wird, desto größer wird ihr Aussagegehalt. Daher können die bisherigen Erfahrungen mit der Steuer-ID nur bedingt als Leitlinie herangezogen werden, zumal die einwilligungsbasierte Verarbeitung der Steuer-ID erst seit ca. 2 Jahren möglich ist (bis zum 28.5.2018 waren gem. § 139b Abs. 2 S. 3 AO a.F. entsprechende Einwilligungen unwirksam).

(2) Kompensatorische Sicherungen gegen Missbrauch

Schadensszenarien wirkt sich auch nur dann auf die rechtliche Bewertung aus, wenn hinreichende empirische Anhaltspunkte dafür bestehen, dass ein Angriff auf die gewählte Struktur erfolgreich sein kann. Solange das nicht der Fall ist, unterliegt das die IT-Sicherheits-Architektur und das sich daraus ergebende technische Sicherheitsniveau der **Einschätzungsprärogative des Gesetzgebers**.

Der Gesetzentwurf wirkt dem Missbrauch der ID-Nr. durch eine Reihe von Maßnahmen entgegen (4-Ecken-Modell, § 7 Abs. 2 IDNrG-E; Protokollierung aller Zugriffe, §§ 7 Abs. 2 , 9 IDNrG-E; Verschlüsselung, § 7 Abs. IDNrG-E; Löschpflicht. § 11 IDNrG-E; Datenschutzkontrolle, § 13 IDNrG-E; Strafnorm des § 17 IDNrG-E; ausführlich zu alldem → e) | S. 15).

Gleichwohl bleibt nicht-öffentlichen Stellen die Nutzung der Kennziffer weiterhin grundsätzlich erlaubt.[68] Da man das Sicherheitsniveau privater Unternehmen nicht in demselben Maße für gesichert ansehen kann wie dasjenige staatlicher Stellen, die Gefahr einer Profilbildung aber auch bei einem Bekanntwerden der Kennziffer nach Hacks eines Privatunternehmens besteht, sollte nichtöffentlichen Stellen die Erhebung und Verarbeitung der Kennziffer nur zu gesetzlichen Zwecken erlaubt werden[69], etwa im Rahmen der Geldwäscheverhinderungsvorschriften. Hierbei könnte man sich an den bereits bestehenden, restriktiven Regelungen für die Erhebung von Daten aus dem Personalausweis (§§ 14 ff. PAuswG) orientieren. Anders als der für die zur Identifikationsnummer ausgebaute Steuer-ID geltende § 139b AO enthält insbesondere § 20 Abs. 3 S. 1 PAuswG ein Verbot zur Nutzung der Seriennummer zur Bildung von Persönlichkeitsprofilen. Vor dem 25.5.2018 enthielt § 139b Abs. 2 S. 3 AO eine ähnlich strenge Fassung, die eine entsprechende Einwilligung des Betroffenen ausschloss. Das ist wegen einer vermuteten Europarechtswidrigkeit[70] gestrichen worden[71], doch können die Mitgliedstaaten aufgrund von Art. 87 S. 2 DSGVO „entsprechende Garantien" ja einführen, wozu eine Einwilligungsverbot durchaus gezählt werden kann.

Einen absoluten faktischen Schutz vor einer Datenzusammenführung können ohnehin weder das bPKZ- noch das RegMoG-Modell nicht gewähren. Eine echte Anonymität ist heute praktisch nicht mehr möglich, denn mithilfe von Big Data-Analysen ist es möglich, auch ohne einen zentralen Kennschlüssel herauszufinden, welche Datensätze zu ein und derselben Person gehören. Der zu betreibende Aufwand einer Re-Identifizierung ist im österreichischen Modell zwar höher. Denn dort wird die PKZ nicht bei den einzelnen Datenübermittlungsvorgängen eingesetzt, existiert aber als sog. „Stammzahl" gleichwohl und kann dazu genutzt werden, die einzelnen bereichsspezifischen Kennziffern zu einer Person zu berechnen. Auch in diesem Modell besteht deshalb **eine zentrale**

---

67 Vgl. *Brühl/v. Bullion*, Cyber-Attacke aus Mittelhessen, SZ v. 23.9.2020, S. 8.
68 Dagegen Beschlussantrag Nr. 6a) von Bündnis 90/Grüne (BT-Drucks. 19/25029).
69 *BfDI* (Fn. 63), S. 4 u. 6.
70 BT-Drucks. 18/12611, S. 95.
71 BGBl. I 2017, S. 2541, 2554.

Angriffsstelle. – Insoweit unterliegt es aber Einschätzungsprärogative des Gesetzgebers, wie weit er bei der Sicherung vor derartigen Analysemethoden gehen will.

> In diesem Punkt geht die Sicherheit des vom Gesetzentwurf verfolgten Modells sogar über diejenige des österreichischen Modells hinaus: Das in § 7 Abs. 2 IDNrG-E angeordnete 4-Ecken-Modell verhindert unbemerkte Zugriffe. Das ist mehr als die bloß faktische Sicherung durch unterschiedliche bereichsspezifische Kennnummern, da eine Verknüpfung durch Inverssuche immer noch versucht werden könnte. Die Protokollierung in den Vermittlungsstellen erleichtert die Suche nach den Urhebern eines rechtswidrigen Zugriffs und schafft so einen Abschreckungseffekt. Nicht im Übermittlungsverzeichnis vorgesehene Datenübermittlungen werden durch die Vermittlungsstellen sogar vollständig unterbunden, sodass es nicht möglich ist, durch Kompromittierung einer Behörde Zugriff auf alle Register zu erlangen.
> Freilich ist die dadurch erreichte Sicherheit abermals nicht perfekt. Ein Angreifer könnte verschleiert (z.B. mithilfe von „TOR“) über das Internet in eine Behörde eindringen und dann gleichsam „maskiert“ als diese Behörde Datenzugriffe in dem Umfang vornehmen, in dem das Übermittlungsverzeichnis es dieser Behörde gestattet. Die Protokollierung der Zugriffe bei den Vermittlungsstellen liefe dann ins Leere. Gegen einen derartigen Angriff schützt aber auch das Modell der bereichsspezifischen Kennzeichen nicht.

Zudem ist schon das 4-Ecken-Modell technisch anspruchsvoll. Ein Modell mit bereichsspezifischen Kennzeichen wie das österreichische Modell ist noch weitaus komplexer, was dann für die föderale Registerlandschaft Deutschlands noch mit 16+1 multipliziert werden müsste, und erfahrungsgemäß sind **komplexe IT-Landschaften anfälliger für Angriffe** als einfache. Das betrifft insbesondere auch den versehentlichen Einbau von Programmfehlern (Bugs). Da die genaue Angriffsfläche im Vorhinein nicht sicher bestimmt werden kann, greift insoweit die Einschätzungsprärogative des Gesetzgebers.

(3) Mehr Datenschutz durch dezentrale Registerlandschaft

Österreich hat, anders als Deutschland, seine Register auf Bundesebene zentralisiert[72]. Nach dem Gesetzentwurf (und entsprechend der verwaltungsföderalen Tradition in Deutschland) sollen die Register hierzulande auf den Ebenen von Bund, Ländern und Kommunen verbleiben. Das allein führt – freilich auf einer anderen Ebene als die ID-Nr. – durch eine Verteilung auf verschiedene Hoheitsträger zu **einem Mehr an Datenschutz im Sinne informationelle Gewaltenteilung**. Ein Angreifer müsste für eine umfassende Profilbildung viel mehr und ganz unterschiedliche Behörden angreifen.

> Getrennte und verteilte Datenbestände wirken der Bildung von Persönlichkeitsprofilen entgegen[73]. File-Trennung war ein ausdrückliches Gebot von Nr. 8 der Anlage zu § 9 BDSG a.F.[74].

ee) Alternative: NEU-ID

In einem Gutachten im Auftrag der Friedrich-Naumann-Stiftung von Anfang Dezember 2020 war als eine Alternative zum Modell des RegMoG eine „neuartiges bereichsspezifisches Personenkennzeichen (NEU-ID)“ vorgeschlagen worden[75], nach dem ein zentraler Intermediär eine Art Konkordanztabelle für alle Betroffenen führen soll. – Dieses Modell teilt mit dem „österreichischen“ bPKZ-Modell das Problem eines prominenten Angriffspunktes[76] (→ dd)(1) u. (2) | S. 9).

ff) Zwischenergebnis: Unterschiedlichkeiten und Einschätzungsprärogative

Zusammengefasst lässt sich sagen, dass das Modell des RegMoG und das „österreichische Modell“ sich mit Blick auf das Recht auf Informationelle Selbstbestimmung nicht kategorial und dann auch nur hinsichtlich Missbrauchsfällen, also in Bezug auf die Datensicherheit, unterscheiden. Was genau insoweit als sicher zu gelten hat, unterliegt letztlich im Rahmen des empirisch Nachgewiesenen der gesetzgeberischen Einschätzungsprärogative.

---

72 *Nationaler Normenkontrollrat*, Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren, 2017, S. 28.
73 *v. Lewinski*, in: Seckelmann, Digitalisierte Verwaltung. Vernetztes E-Government, 2. Aufl. 2019, S. 107, Rn. 42.
74 *v. Lewinski*, in: Seckelmann, Digitalisierte Verwaltung. Vernetztes E-Government, 2. Aufl. 2019, S. 107, Rn. 45.
75 *Sorge/v. Lucke/Spiecker*, Registermodernisierung – Datenschutzkonforme und umsetzbare Alternativen, Dez. 2020, insb. S. 34 ff. – Das Gutachten hat *Verf.* erst unmittelbar vor Fertigstellung seiner Stellungnahme erreicht, so dass auf dieses in diesem Rahmen nicht vertieft eingegangen werden kann.
76 *Sorge/v. Lucke/Spiecker*, Registermodernisierung – Datenschutzkonforme und umsetzbare Alternativen, Dez. 2020, S. 36.

Mit Blick auf das eigentliche Datenschutzrecht ist zu betonen, dass ein Personenkennzeichen nur der Mittel zu einem Zweck ist. Selbst wenn es einer strengen sektoralen Zweckbindung unterläge[77], die eigentlichen Daten aber gleichwohl frei fließen würden, würde das eigentliche Datenschutzziel, das ja auf die eigentliche Information zu einer Person schützen soll, nicht erreicht.

d) Angemessenheit

Schließlich muss die Einführung eines zentralen Personenkennzeichens auch angemessen sein, d.h. die Schwere des Grundrechtseingriffs darf nicht außer Verhältnis zu dem verfolgten Zweck stehen[78]. Hierfür sind alle Verfassungsgüter gegenüber und in Verhältnis zu setzen, nicht nur die individuellen Rechtsgüter der Grundrechtsträger, sondern auch verfassungsanerkannten öffentlichen Interessen des Gemeinwohls[79]. Die Schwere des Eingriffs in diese ist sodann mit der Dringlichkeit der ihn rechtfertigenden Gründe abzuwägen[80]. Dabei genügt nicht jedes Überwiegen der Individualinteressen, sondern diese müssen ersichtlich schwerer wiegen als das Gemeingut[81].

> Die im Rahmen der Angemessenheitsprüfung vorzunehmende Abwägung ist bei multipolaren Grundrechts- und Verfassungsrechtsverhältnissen nicht einfach (und nicht einfach zu beschreiben). Nachstehend werden deshalb die einschlägigen Verfassungsgüter kurz benannt (→ aa)), soweit möglich untereinander gewichtet (→ bb)) und dann Abwägungstopoi angeführt (→ cc)).

aa) Einschlägige Verfassungsgüter

(1) Der ID-Nr. entgegenstehende Verfassungsgüter

(i) Informationelles Selbstbestimmungsrecht

Im Vordergrund steht das Recht auf Informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG). Sein Kernbereich umfasst insbesondere das **Verbot der Erstellung von umfassenden Persönlichkeitsprofilen** (→ II. 2. | S. 4).

(ii) Nicht: Religionsfreiheit

> Nicht maßgeblich ist die Religionsfreiheit, selbst wenn ein Personenkennzeichen als religiös anstößig empfundene Ziffernfolgen wie die satanische „666“ enthält[82]. In der Zuweisung der Kennziffer ist auf der semantischen Ebene kein religiöser Bezug erkennbar.

(iii) Kommunale Selbstverwaltungsgarantie

Das IDNrG erfordert neue Software bei den Registerbehörden, die zu großen Teilen kommunal sind[83]. Gerade für kleinere und weniger leistungsstarke Kommunen können Ausgaben erforderlich sein, die dazu führen, dass andere kommunale Aufgaben vernachlässigt werden (müssen). Dies würde sie in der kommunalen **Organisations- und Finanzhoheit** (Art. 28 Abs. 2 GG) betreffen.

(2) Die ID-Nr. stützende Verfassungsgüter

(i) Verwaltungseffizienz und Wirtschaftlichkeitsgebot

Effizienz der Verwaltung ist ein Verfassungsgut, ebenso die Wirtschaftlichkeit (vgl. Art. 114 Abs. 1 S. 1 GG; → a) | S. 7).

---

77 Dies betonend *Hense*, in: Sydow, DSGVO, 2. Aufl. 2018, Art. 87, Rn. 3 m.Verw. auf § 291a SGB V.
78 *Kloepfer*, Verfassungsrecht, Bd. II, 2010, § 51 Rn. 102.
79 *Kloepfer*, Verfassungsrecht, Bd. II, 2010, § 51 Rn. 103.
80 Vgl. BVerfGE 81, S. 1, 19.
81 BVerfGE 44, S. 353, 373.
82 So BFH, DStR 2012, S. 283, 293 (zur Steuer-ID).
83 Es gibt ca. 5000 kommunale Melderegister (*BMI*, Registerübergreifendes Identitätsmanagement als Teil der Registermodernisierung, Abschlussbericht zur Sondierung eines registerübergreifenden Identitätsmanagements mit Einbezug der Erfahrungen mit der Steuer-Identifikationsnummer für die Innenministerkonferenz 17.-19. Juni 2020 v. 10.3.2020, S. 29).

(ii) Sozialstaatlichkeit

Auch wird in manchen Konstellationen die **Schwelle zum Zugang zu staatlichen (Sozial-)Leistungen abgesenkt** werden können, für deren Beantragung viele Nachweise erforderlich sind, so dass der „Papierkram" einen Teil der Leistungsberechtigten schon von der Antragstellung abschreckt.

(iii) Rechtstaatlichkeit, insb. beim Verwaltungsvollzug

Die Einführung der ID-Nr. dient auch der **Rechtmäßigkeit der Verwaltung**: Denn fehlerhafte Verwaltungsentscheidungen können folgen, wenn Daten z.B. verwechselt werden. Wird dies planvoll ausgenutzt, können Leistungserbringungen an Identitätsbetrüger die Folge sein[84].

(iv) Gleichheitsgrundsatz

Damit einhergehend ist auch der Gleichbehandlungsgrundsatz aus Art. 3 Abs. 1 GG betroffen.

bb) Gewichtigkeit der Verfassungsgüter

Grundsätzlich stehen alle Verfassungsgüter normhierarchisch auf derselben Stufe (abgesehen von der Menschenwürde als zentralem Wert des Grundgesetzes). Gleichwohl lässt die Verfassung Abstufungen zwischen ihnen erkennen.

(1) Recht auf Informationelle Selbstbestimmung

Das Recht auf Informationelle Selbstbestimmung wird neben Art. 2 Abs. 1 GG auch aus der Menschenwürde hergeleitet, die gem. Art. 1 Abs. 1 GG den höchsten Wert der Verfassung bildet. Diese wiederum gehört zum nach Art. 79 Abs. 3 GG änderungsfesten Kern der Verfassung. Als für die moderne Informations- und Datengesellschaft konstitutives Recht ist dem Recht auf Informationelle Selbstbestimmung daher ein hoher Stellenwert einzuräumen. Der **Menschenwürdekern** des Rechts auf informationelle Selbstbestimmung ist jedenfalls dann erreicht, wenn der Staat umfassende Persönlichkeitsprofile erstellt (→ II. 2. | S. 4).

> Auch bedeutet ein Personenkennzeichen nicht nur im Moment eine Gefährdung Informationeller Selbstbestimmung, sondern auch über die Zeit und in der Zukunft kumulierend[85].

(2) Kommunale Selbstverwaltung

Die kommunale Selbstverwaltung ist ein in Art. 28 Abs. 2 GG verankertes Gut von Verfassungsrang. Anders als das Recht auf Informationelle Selbstbestimmung weist sie allerdings keinen Bezug zur Menschenwürde auf. Jedoch darf sie jedenfalls **nicht faktisch entkernt** werden, wie es der Fall wäre, wenn die Registermodernisierung den Städten und Gemeinden untragbar hohe Kosten auferlegen würde.

Dies ist jedoch nicht der Fall. Denn die Kommunen werden von einer Verbesserung der Verwaltungseffizienz aufgrund des RegMoG profitieren. Auch wird das 4-Ecken-Modell bei den Kommunen verzögert eingeführt (§ 7 Abs. 3 IDNrG-E), was ihnen die Umstellung erleichtert. Eine gem. Art. 84 Abs. 1 S. 7 GG unzulässige Aufgabenzuweisung durch Bundesgesetz dürfte wohl nicht vorliegen[86].

(3) Verwaltungseffizienz und Wirtschaftlichkeitsgebot

Effizienz und Wirtschaftlichkeit der Verwaltung werden von der Verfassung zwar gebilligt[87]. Ihnen kommt als (nur) Verfassungsprinzip und nicht als harte Entweder/Oder-Regel eher eine **Hilfsfunktion** zu[88]. Für sich allein genommen können Effizienzaspekte deshalb Grundrechtseingriffe nicht rechtfertigen[89].

---

84 *BMI* (Fn. 83), S. 10.
85 Vgl. *Hansen*, in: Simitis/Hornung/Spiecker, Datenschutzrecht, 2019, Art. 87 DSGVO, Rn. 25.
86 Zur Vereinbarkeit des OZG mit Art. 28 Abs. 2 und Art. 84 Abs. 1 S. 7 GG *Hermann/Stöber*, NVwZ 2017, S. 1401, 1403, und *Siegel*, DÖV 2018, S. 185, 188.
87 *Gröpl*, in: Handbuch des Staatsrechts, Bd. V, 3. Aufl. 2008, § 121 Rn. 16.
88 *Gröpl*, in: Handbuch des Staatsrechts, Bd. V, 3. Aufl. 2008, § 121 Rn. 30.
89 *Zelyk*, Das einheitliche steuerliche Identifikationsmerkmal, 2012, S. 101.

(4) Rechtsbindung der Verwaltung

Anders als der eher mittelbare Ansatzpunkt der Effizienz und Wirtschaftlichkeit in Art. 114 Abs. 2 S. 1 GG wird die Gesetzbindung der Verwaltung in Art. 20 Abs. 3 GG ausdrücklich angesprochen. Sie gehört gem. Art. 79 Abs. 3 GG zum **änderungsfesten Kern der Verfassung** und ist damit ein Verfassungsgut von hohem Range.

(5) Gleichheitsgrundsatz

Der durch die Einführung eines Personenkennzeichens begünstigte Gleichbehandlungsgrundsatz aus Art. 3 Abs. 1 GG ist ein Grundrecht und ein **elementarer Bestandteil des Rechtsstaats** und überhaupt **gerechter Ordnung**.

(6) Zwischenergebnis: Datenschutz versus Rechtsanwendungsgleichheit

Wie in vielen anderen Datenschutzkonstellationen stehen das Rechts auf Informationelle Selbstbestimmung und der effektive Verwaltungsvollzug, durch den der Gleichheitssatz wie auch das Rechtstaatsgebot verwirklicht werden, einander gegenüber Dies ist früher oft in den bösen und überspitzten Satz vom „Datenschutz als Täterschutz“ gefasst worden, enthält aber hinsichtlich der **Spannungslage** ein wahres Körnchen.

cc) Abwägung der Verfassungsgüter (Praktische Konkordanz)

Wie verfassungsrechtliche Spannungslagen allgemein ist dies auch hier im Wege Praktischer Konkordanz aufzulösen. Dabei geht es darum, allen in Frage stehenden Verfassungsgütern zu bestmöglicher Geltung zu verhelfen[90].

(1) Transparenz

Beeinträchtigungen Informationeller Selbstbestimmung durch die Identifikationsnummer kompensiert das RegMoG durch Transparenz[91]. Verlangt ist, dass der Betroffene wissen muss, wer was wann bei welcher Gelegenheit über ihn weiß[92]. Im Datencockpit gem. § 10 OZG-E können die Betroffenen nachvollziehen, wer wann welche Daten ausgetauscht hat. So wird der Aspekt der Nachvollziehbarkeit als Teil des Rechts auf Informationelle Selbstbestimmung zur Geltung gebracht.

(2) Datensparsamkeit durch Ermöglichung von Pseudonymisierung

Die Registermodernisierung ermöglicht datensparsam in weiterem Umfang als bisher **pseudonyme Datenübermittlungen zwischen den Behörden** unter weitgehendem Verzicht auf die Stammdaten. Denn die ID-Nr. enthält selbst keine chiffrierten Informationen, und aus ihr allein können keine Rückschlüsse auf die Person gezogen werden, was ebenfalls im Sinne der Datenminimierung ist[93].

> Der Gesetzentwurf meint, die perspektivisch angestrebte Zentralisierung aller jeweiligen Fachdaten bei nur einem jeweils zuständigen Register und der PKZ-Datenbank beim BZSt diene durch die Vermeidung von Dubletten ebenfalls dem Gebot der Datenminimierung[94]. Dies ist insoweit nicht ganz richtig, als die Daten immer noch erhoben werden. Wo sie intern gespeichert werden, ist für den Betroffenen unerheblich. Datensparsamkeit heißt, Daten nach Möglichkeit gar nicht zu erheben. Bei der Registermodernisierung, bei der einzelne Daten lediglich „verschoben“ und zentralisiert werden, ist dieser Aspekt aber nicht wesentlich.

Die einzelnen Fachregister selbst arbeiten allerdings nicht pseudonym (vgl. dazu bereits oben → b) | S. 7). Da sie aber auch mit den Betroffenen kommunizieren müssen und eine „Reduktion auf die Nummer“ mit Blick auf die Menschenwürde (Art. 1 Abs. 1 GG) problematisch wäre, ist eine vollständig pseudonyme Behördenarbeit ohnehin nicht möglich.

Dass **nicht mehr benötigte Daten gelöscht** werden müssen[95], ist in § 11 IDNrG-E vorgesehen.

---

90 *Kingreen/Poscher*, Grundreche Staatsrecht II, 35. Aufl. 2019, § 6 Rn. 376.
91 Vgl. zur Notwendigkeit von Transparenz BVerfGE 125, S. 260, 335 – Vorratsdatenspeicherung.
92 BVerfGE 65, S. 1, 43 – Volkszählung.
93 Ausarbeitung des Wissenschaftlichen Dienstes des Bundestags WD3-3000-196/20, 16.9.2020, S. 20.
94 Entwurfsbegründung, BR-Drucks. 563/20, S. 67, s.a. auch S. 69 (= BT-Drucks. 19/24226).
95 BVerfGE 125, S. 260, 332 f. – Vorratsdatenspeicherung.

(3) Zweckbindung

Ferner müssen die **Zwecke der Datennutzung eindeutig bestimmt** sein[96]. Die Nutzungskataloge im IDNrG-E und in den Fachgesetzen sind eine Umsetzung des Gebots der Zweckbindung. In den Vorgaben der Zweckbindung finden sich Datenschutz und Rechtstaatlichkeit in praktischer Konkordanz. Insoweit besteht zwischen diesen Vorgaben keine Spannung.

(4) Datenqualität und Gleichbehandlungsgrundsatz

Die Verwaltungseffizienz und der Gleichbehandlungsgrundsatz wird durch die Einführung von Digitalisierung und Automatisierung verbessert, etwa durch Unterbindung von Identitätsbetrug bei der Gewährung staatlicher Leistungen. Soweit es um die **Verbesserung der Datenqualität** geht, besteht kein Spannungsverhältnis zum Recht auf Informationelle Selbstbestimmung, das insoweit den vergleichbaren Grundsatz der Datenrichtigkeit kennt.

Soweit angeführt wird, die automatisierte Datenverarbeitung und v.a. auch automatisierte Einzelentscheidung wäre datenschutzerheblich[97], ist dies durchaus richtig, **von Art. 22 DSGVO und etwa § 37 BDSG**[98] **bereits adressiert**, also insoweit zu praktischer Konkordanz gebracht.

dd) Zwischenergebnis

Verwaltungseffizienz, insb. digitaler Verwaltung, steht stets in einem gewissen Spannungsfeld zum Datenschutzgrundrecht. Im Rahmen dieses Ziels aber setzt der Gesetzentwurf die betroffenen Verfassungsgüter in eine Verhältnis, in dem sie im Zusammenspiel jeweils zur Geltung kommen. Es gibt keine Aspekte, bei denen das jeweils andere Rechtsgut außer Betracht gelassen worden wäre.

e) Gesetzlich-technisch-organisatorische Sicherungen auf objektivrechtlicher Ebene

Bei umfassenden staatlichen Datenerhebungen kann die Verhältnismäßigkeit im engeren Sinne auch jenseits individueller Grundrechtsbetroffenheit nur dann bejaht werden, wenn auch gewisse organisatorisch-technische Sicherungen eingezogen werden, die unabhängig von einem konkreten Eingriff gelten und eher im Vorfeld verortet sind[99]. Die Rechtsprechung verlangt im Rahmen der Angemessenheit technisch-organisatorische Maßnahmen in einem von Art, Umfang, denkbaren Verwendungen, Anlass, Umständen und Missbrauchsgefahr abhängigen Maße[100]. Auf diese Weise wird systemischen Gefahren vorgebeugt.

> Zwar gibt die Verfassung konkrete technische Sicherheitsmaßnahmen für die Verarbeitung sensibler Daten nicht vor[101]. Doch hat das BVerfG sich in seinem **Urteil zur Vorratsdatenspeicherung** umfassend zu technisch-organisatorischen Schutzmaßnahmen bei der staatlichen Sammlung einer großen Menge sensibler Daten geäußert[102]. Es erscheint daher naheliegend, die strikten Kriterien der Entscheidung zur Vorratsdatenspeicherung auch für die PKZ heranzuziehen[103].

aa) Datensicherheit nach dem Stand der Technik

Zwar gibt es keine absolute Sicherheit im IT-Bereich. Gleichwohl muss aber dynamisch der Stand der Technik berücksichtigt werden[104]. Im Entwurf fehlen zwar Vorgaben zur Absicherung der PKZ-Datenbank und der Register selbst. Da aber das **allgemeine Datenschutzrecht**, das **IT-Sicherheitsrecht** und die **bisherigen Regeln zur Absicherung der Steuer-ID-Datenbank** weiter anwendbar sind, folgen Vorgaben zur technischen Datensicherheit aus dem BSI-G, ggf. entsprechenden Regelungen der Länder, § 139d AO i.V.m. der StIdV und. der 2. BMeldDÜV sowie aus Art. 5

---

96 BVerfGE 125, S. 260, 327 f. – Vorratsdatenspeicherung.
97 *Martini/Wagner/Wenzel* (Fn. 49), S. 22 Fn. 124: Grund: Menschen sind erst spät eingeschaltet, Fehler werden dann womöglich nicht mehr entdeckt.
98 Zu weiteren Fachregelungen *Herbst*, in: Auernhammer, DSGVO/BDSG, 7. Aufl. 2020, Art. 22 DSGVO, Rn. 29.
99 BVerfGE 125, S. 260, 325 – Vorratsdatenspeicherung.
100 BVerfGE 150, S. 1, Rn. 221 – Zensus 2011; auch schon BVerfGE 65, S. 1, 45 f. – Volkszählung.
101 BVerfGE 125, S. 260, 326 – Vorratsdatenspeicherung.
102 BVerfGE 125, S. 260, 325 ff. – Vorratsdatenspeicherung.
103 *Martini/Wagner/Wenzel* (Fn. 49), S. 46.
104 BVerfGE 125, S. 260, 326 – Vorratsdatenspeicherung.

Abs. 1 lit. f DSGVO. Die Anforderungen an die Datensicherheit richten sich nach der Sensitivität der Daten[105], welche bei einer unveränderbaren PKZ als hoch einzustufen ist.

> Den Stand der Technik referenziert der Gesetzentwurf bei der Transportsicherheit ausdrücklich (§ 7 Abs. 2 S. 1 IDNrG-E). Wie man § 7 Abs. 2 S. 4 Hs. 2 IDNrG-E entnehmen kann („ohne Kenntnis der Nachrichteninhalte"), ist eine **Ende-zu-Ende-Verschlüsselung** gemeint; dies wird in der Begründung auch ausdrücklich klargestellt[106]. Außerdem soll die Behördenkommunikation nur über ein **besonders gesichertes Netz des Bundes und der Länder** nach dem IT-NetzG erfolgen. Die Gefahr eines erfolgreichen Angriffs auf die Datenübertragung ist dadurch deutlich verringert.
> Es fehlt eine IT-Sicherheitsanalyse. Im Abschlussbericht für die Innenministerkonferenz[107] finden sich lediglich ein paar unsystematische Überlegungen zu Möglichkeiten von Außen- und Innentätern.
> Hinzuweisen ist darauf, dass vom Datencockpit gem. § 10 OZG-E aber auch eine eigenständige Gefahr ausgeht. Es ist der einzige Ort, an dem trotz des 4-Ecken-Modells alle Daten zusammenfließen. Es ist daher geboten, es stark zu sichern (nicht bloß Benutzername/Passwort); außerdem sollten die Daten nur der Kategorie nach, aber nicht die Daten selbst benannt werden. Damit kann ein Hacker, der die Zugangsdaten des Betroffenen erlangt, nicht viel anfangen. Dem wird das Gesetz gerecht[108].

bb) Effektive Kontrolle

Auch ist die Einhaltung der technischen Standards und IT-Sicherheit zu kontrollieren, und es muss eine **unabhängige Datenschutzinstitution** eingeschaltet werden[109]. Die in § 13 IDNrG-E vorgesehene regelmäßige Überprüfung der Registermodernisierungsbehörde durch den BfDI entspricht diesem Erfordernis.

Daneben muss die Einhaltung der IT-Sicherheit und der Vorschriften des technisch-organisatorischen Datenschutzes auch durch die registerführenden Stellen (**Eigenkontrolle**) überprüft werden. Auf Missbrauch wird sowohl ex ante als auch ex post geprüft. Die Vorabprüfung erfolgt gem. § 8 Abs. 3 IDNrG-E durch automatisierten Abgleich mit dem Verzeichnis erlaubter Datenübertragungen (DVDV). Die Protokollierung nach § 9 IDNrG-E erlaubt eine nachträgliche Prüfung, ebenso das Stichprobenverfahren nach § 8 Abs. 4 IDNrG-E.

Ferner gibt es die reguläre Fachaufsicht durch die vorgesetzte Behörde und die Aufsicht nach den jeweiligen Landesdatenschutzgesetzen durch die Datenschutzaufsichtsbehörden.

> Eine demgegenüber bloß schwache Maßnahme ist die in § 16 IDNrG-E vorgeschriebene Evaluierung des Gesetzes, da von ihr keine Verbindlichkeit ausgeht. Sie ist auch weniger auf den konkreten Verwaltungsvollzug, sondern eher auf den (Änderungs-)Gesetzgeber gerichtet.

cc) Effektiver Rechtsschutz

Die Datenübermittlung ist in einer Weise durchzuführen, die dem Betroffenen die Möglichkeit effektiven Rechtsschutzes gewährt[110]. Durch die **Protokollierung das Datencockpit** hat der Einzelne die Möglichkeit, die Datenübertragungen zu erkennen und sie ggf. gerichtlich zu beanstanden.

dd) Effektive Sanktionierung

Dies muss durch (generalpräventive) **Sanktionen für Verstöße gegen die IT- und Datensicherheit** flankiert werden[111]. Die unbefugte Verarbeitung der ID-Nummer ist gem. § 17 IDNrG-E eine Straftat. Das schreckt vom rechtswidrigen Gebrauch ab und sorgt dafür, dass das hohe Gewicht des Rechts auf Informationelle Selbstbestimmung in der Wahl des Mittels berücksichtigt wird, ohne dass die angestrebte Verwaltungseffizienz dabei zurückstehen müsste.

---

105 EuGH, NJW 2014, S. 2169, Rn. 54 f. – Digital Rights Ireland.
106 Entwurfsbegründung, BR-Drucks. 563/20, S. 65 f. (= BT-Drucks. 19/24226).
107 *BMI* (Fn. 83), S. 31.
108 Vgl. Entwurfsbegründung, BR-Drucks. 563/20, 84 (= BT-Drucks. 19/24226).
109 BVerfGE 125, S. 260, 327 – Vorratsdatenspeicherung.
110 BVerfGE 125, S. 260, 335 – Vorratsdatenspeicherung.
111 BVerfGE 125, S. 260, 327 – Vorratsdatenspeicherung.

3. Absolute Grenze: umfassendes Persönlichkeitsprofil

Dem verfassungsrechtlichen Verbot von umfassenden Persönlichkeitsprofilen wird durch die gezielte **Vermeidung eines „Superregisters“**[112] entsprochen. Jedenfalls derzeit soll die ID-Nr. nicht für alle Register eingeführt werden, sondern nur für einen Teil. Eine umfängliche Datenverknüpfung ist damit derzeit noch nicht gegeben[113]. Auch bleibt die zentrale Datenbank beim Bundeszentralamt für Steuern (§ 4 Abs. 1 IDNrG-E), also einer Fach- und keiner zentralen Behörde.

IV. Koda: Holistik der Verfassungsmäßigkeit von Personenkennzeichen

Der vorliegende Entwurf zur Einführung einer Identifikationsnummer führt nicht zu umfassenden Persönlichkeitsprofilen. Weil diese absolute Schranken-Schranke für die Verdatung der Gesellschaft nicht überschritten wird, ist eine die Schranken insb. des Rechts auf Informationelle Selbstbestimmung wahrende und verhältnismäßige Regelung, jedenfalls in Praktischer Konkordanz mit konfligierenden Verfassungsgütern, möglich.

Es ist allerdings nicht zu verkennen, dass mit der Einführung eines übergreifenden Personenkennzeichens in Deutschland konzeptionell das Fundament für eine umfassende Verdatung der Gesellschaft gelegt wird. Wie weit man sich hier auf eine abschüssige Bahn begibt und nur noch wenige Scheiben von der Salami abschneiden muss, ist eine rechtspolitische Frage, die vorliegend nicht erörtert worden ist (→ III. 2. a) | S. 7).

Hinzuweisen ist auch noch auf die Wechselwirkung zwischen Sozial- und Leistungsstaat einerseits und Personenkennzeichen andererseits. Je mehr Lebensbereiche der Staat erfasst, reglementiert und verwaltet, desto eher wird er in der Lage sein, umfassende Persönlichkeitsprofile zu erstellen. Insoweit stehen der Ausbau des Sozial- und Leistungsstaats und Personenkennzeichen in einer Wechselbeziehung, in der sie sich ab einer bestimmten jeweiligen Ausbaustufe gegenseitig hemmen.[114]

gez. Lewinski

– Prof. Dr. Kai v. Lewinski –

Zentrale Rechtsprechung, ausgewähltes Schrifttum und Dokumente

BVerfG, Beschl. v. 16.7.1969 – 1 BvL 19/63, BVerfGE 27, S. 1 ff. – Mikrozensus.
BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, S. 1 ff. – Volkszählung.
BFH, Urt. v. 18.1.2012 – II R 49/10, DStR 2012, S. 283 ff. – Steuer-ID.

Kirchberg, Personenkennzeichen – Ende der Privatsphäre, ZRP 1977, S. 137 ff.
v. Lewinski, Persönlichkeitsprofile und Datenschutz bei CRM, RDV 2003, S. 122 ff.
v. Lewinski, Datenbanken sowie Ordnungs- und Personenziffern, in: Seckelmann, Digitalisierte Verwaltung. Vernetztes E-Government, 2. Aufl. 2019, S. 107 ff.
v. Lewinski, “Data Spaces”: Data Structures as a Question of Law, in: HIIG (Hrsg.) Don’t Give Up, Stay Idealistic and Try to Make the World a Better Place (Liber Amicorum Ingolf Pernice), Berlin 2020, S. 65 ff.
v. Lewinski, Einheitsnummer für jeden Bürger, NJW-aktuell 46/2020, S. 12 f.
Martini/Wagner/Wenzel, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, Gutachten, Speyer 2017.
Sorge/v. Lucke/Spiecker gen. Döhmann, Registermodernisierung – Datenschutzkonforme und umsetzbare Alternativen, Dez. 2020.
Weichert, Die Wiederbelebung des Personenkennzeichens – insbesondere am Beispiel der Einführung einer einheitlichen Wirtschaftsnummer, RDV 2002, S. 170 ff.
Zelyk, Das einheitliche steuerliche Identifikationsmerkmal, 2012.

[112] Begriff von *Martini/Wagner/Wenzel* (Fn. 49), S. 2 f.
[113] Ausarbeitung des Wissenschaftlichen Dienstes des Bundestags WD3-3000-196/20, 16.9.2020, S. 15.
[114] Vergleichbare Bedenken hinsichtlich der Ausweitung des Einsatzes der Steuer-ID bei *Bundesrat*, Stellungnahme zum RegMoG (BR-Drucks. 563/20 (Beschluss)), S. 1 f.

BMI, Personenkennzeichen (betrifft: 7), Juni 1971.
Nationaler Normenkontrollrat, Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren, Oktober 2017 (Ab S. 28 wird das österreichische Modell knapp erklärt.).
BMI, Abschlussbericht zur Sondierung eines registerübergreifenden Identitätsmanagements mit Einbezug der Erfahrungen mit der Steuer-Identifikationsnummer für die Innenministerkonferenz 17.–19. Juni 2020 v. 10.3.2020.
IT-Planungsrat, Eckpunktepapier zur Registermodernisierung vom April 2020 (Erklärt auf S. 28 das 4-Corner-Modell kurz).
BfDI, Stellungnahme zum RegMoG v. 4.5.2020.
BfDI, Stellungnahme zum RegMoG v. 26.8.2020.
BfDI, Hintergrundpapier zur Registermodernisierung und Schaffung eines einheitlichen Personenkennzeichens v. 28.8.2020.
Wissenschaftlicher Dienst des Bundestags, Ausarbeitung WD3-3000-196/20 v. 16.9.2020.
BfDI, Stellungnahme zum RegMoG v. 21.10.2020.

Gesetzentwurf der Bundesregierung für das RegMoG, BR-Drucks. 563/20 (= BT-Drucks. 19/24226 [noch unredigiert]).
Beschlussantrag FDP-Bundestagsfraktion (BT-Drucks. 19/24641 [noch unredigiert]).
Beschlussantrag der Bundestagsfraktion von Bündnis 90/Grüne (BT-Drucks. 19/25029 [noch unredigiert]).

Deutscher Bundestag

Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)667 C

RECHTSWISSENSCHAFTLICHE FAKULTÄT
UNIVERSITÄT DES SAARLANDES

Lehrstuhl
für Rechtsinformatik

Prof. Dr. Christoph Sorge

Postfach 15 11 50
66041 Saarbrücken

Besucheranschrift:
Campus C3 1, Raum 1.25
66123 Saarbrücken

Tel. 0 681 / 302-51 22
Sekr. 0 681 / 302-51 20
E-Mail christoph.sorge@uni-saarland.de
Web www.legalinf.de

Saarbrücken, 10. Dezember 2020

Stellungnahme zum Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze

Kernthesen

- Die Schaffung einer Verknüpfungsmöglichkeit zwischen Registern stellt einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung dar.
- Ein solcher Eingriff kann gerechtfertigt sein, aber jedenfalls nur, wenn ausreichende Schutzmaßnahmen vorgesehen sind.
- Der vorliegende Entwurf führt dazu, dass die Steuer-ID zu einem allgemeinen Personenkennzeichen wird. In der vorgesehenen Ausgestaltung ist ein solches allgemeines Personenkennzeichen verfassungswidrig.
- Die vorgesehenen Schutzmaßnahmen sind lückenhaft; die vorgesehenen Intermediäre können durch das Vorliegen eines allgemeinen Personenkennzeichens leichter umgangen werden, als dies nötig wäre.
- Die Einführung eines allgemeinen Personenkennzeichens ist schon deshalb nicht erforderlich, weil alternative Modelle mit bereichsspezifischen Personenkennzeichen existieren. In Österreich ist ein entsprechendes Modell etabliert. Angepasste Varianten sind auch in Deutschland, sogar auf Grundlage der durch den Entwurf des Registermodernisierungsgesetzes ohnehin vorgesehenen Struktur und mit überschaubarem Aufwand möglich.
- Auch ein System mit bereichsspezifischen Kennzeichen braucht zusätzliche rechtliche, technische und institutionelle Sicherungen, um datenschutzkonform umgesetzt werden zu können.
- Der vorliegende Entwurf läuft aufgrund dieser Bedenken Gefahr, durch das Bundesverfassungsgericht für nichtig erklärt zu werden. In diesem Fall würden sich Kosten- und Zeitaufwand bis zum Erreichen einer verfassungskonformen Lösung erheblich erhöhen.

A. Vorbemerkung

Die vorliegende Stellungnahme beruht – neben meiner eigenen Forschungserfahrung im Bereich des technischen Datenschutzes und angrenzender Rechtsfragen – wesentlich auf Erkenntnissen, die ich bei der Erstellung eines Gutachtens zu der Thematik gemeinsam mit Prof. Dr. rer. publ. Jörn von Lucke (Lehrstuhl für Verwaltungs- und Wirtschaftsinformatik, Zeppelin-Universität Friedrichshafen) und Prof. Dr. iur. Indra Spiecker gen. Döhmann (Lehrstuhl für Öffentliches Recht, Informationsrecht, Umweltrecht, Verwaltungswissenschaft, Goethe-Universität Frankfurt) gewonnen habe. Ich erlaube mir, an dieser Stelle lediglich einige der Kernaussagen wiederzugeben und für ausführliche Begründungen auf das Gutachten zu verweisen.

B. Einleitung

Der Wunsch nach einer verbesserten Datenqualität in staatlichen Registern ist nachvollziehbar. Falsche bzw. veraltete Daten können als Grundlage staatlicher Entscheidungen problematisch sein; schon ein Umzug, nach dem die Betroffenen nur noch mit erhöhtem Aufwand zu erreichen sind, erzeugt zusätzliche Kosten. Die Notwendigkeit, Daten zur Person bei den unterschiedlichsten Behörden immer wieder angeben zu müssen, kann zu Frustration bei den Betroffenen führen – wenngleich die meisten Bürger/innen nicht im ständigen Austausch mit Behörden stehen.

Eine Möglichkeit, Inkonsistenzen zu erkennen und Interaktionen mit der Verwaltung einfacher zu gestalten, liegt darin, Datenabrufe aus anderen Registern grundsätzlich möglich zu machen.

Diesen Erwägungen gegenüber steht die Feststellung, dass das Zusammenführen und der Abgleich von Daten aus verschiedenen Registern auch Grundlage für eine umfassende Profilbildung und Überwachung aller registrierten Personen sein kann: Sind Abrufe zur Erreichung legitimer Zwecke möglich, so gilt dies grundsätzlich auch für Abrufe zu illegitimen Zwecken. Schon die Schaffung einer Verknüpfungsmöglichkeit zwischen Registern stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung dar.

Technische und organisatorische Schutzmaßnahmen können dazu eingesetzt werden, diesen Risiken zu begegnen. Eine verfassungsgemäße Registermodernisierung, auch unter Schaffung (streng begrenzter) Datenübermittlungen zwischen Registern aus verschiedenen Verwaltungsbereichen, ist somit grundsätzlich möglich. Dem Entwurf des Registermodernisierungsgesetzes (RegMoG-E) ist dies jedoch nicht gelungen.

Diese Feststellung muss trotz einiger begrüßenswerter Ansätze und Sicherungsmechanismen getroffen werden, die im RegMoGE vorgesehen sind. Positiv hervorzuheben ist die Einführung eines Datencockpits, das Datenübermittlungen zwischen verschiedenen Registern und Behörden für die Betroffenen transparent machen soll.

Zum anderen ist ist auch die Einschaltung von Intermediären (Registermodernisierungsbehörde bzw. Vermittlungsstellen) eine sinnvolle Maßnahme, wenn auch nicht konsequent umgesetzt. Sofern Vermittlungsstellen eingesetzt werden, ist das 4-Corner-Modell vorgesehen. Im Kern wird dabei auf den Schutz durch einen „doppelten Umschlag“ gesetzt: Inhaltsdaten werden so verschlüsselt, dass die Intermediäre diese nicht lesen können. Lediglich Metadaten sind ihnen zugänglich. Auch diese Schutzmaßnahme ändert aber nichts an einem Grundproblem des Entwurfs.

C. Steuer-ID als allgemeines Personenkennzeichen

Dieses Problem besteht in der Weiterentwicklung der Steuer-ID zu einem allgemeinen Personenkennzeichen – wovon bei der zunächst vorgesehenen Verwendung in über 50 Registern unterschiedlichster Bereiche jedenfalls auszugehen ist. Verschärft wird dieses Problem bei einer späteren Ausdehnung auf zahlreiche weitere Register.

I. Risiken

Sieht man davon ab, dass das 4-Corner-Prinzip nicht für alle Datenübermittlungen vorgesehen ist, verbleibt ein offensichtliches Risiko: Die Steuer-ID als allgemeines Personenkennzeichen ermöglicht die Zuordnung von Daten auch unter Umgehung der Intermediäre. Zwar sind rechtliche Hürden eingerichtet; die Möglichkeit rechtswidrigen Handelns erscheint aber jedenfalls nicht fernliegend. Auch rechtmäßiges Zusammenführen von Daten konstituiert im Übrigen einen (wenn auch ggf. gerechtfertigten) Grundrechtseingriff.

Risiken entstehen nicht nur durch Verarbeitungsvorgänge öffentlicher Stellen. Steuer-IDs sind schon jetzt auch privaten Akteuren wie Arbeitgebern und Banken bekannt. Sollte das RegMoG-E in Kraft treten, ist ein adäquater Schutz der Steuer-ID kaum noch denkbar. Mit jeder Datenbank, in der Steuer-IDs gespeichert sind, steigt das Risiko erfolgreicher Cyberangriffe.

II. Verfassungswidrigkeit des vorgesehenen allgemeinen Personenkennzeichens

Für eine ausführliche Darstellung der verfassungsrechtlichen Problematik des vorgesehenen allgemeinen Personenkennzeichens wird auf das angehängte Gutachten verwiesen. Zusammenfassend lässt sich Folgendes feststellen:

- Der mit dem RegMoG-E zunächst angestrebte Zweck der Registermodernisierung ist legitim, wenn auch verfassungsrechtlich nicht von besonderem Gewicht. Für weitreichendere Ziele wie das „No-Stop-Government“ ist aber fraglich, ob diese überhaupt verfassungskonform umsetzbar sind.
- Die Einführung eines allgemeinen Personenkennzeichens ist für die Erreichung des angestrebten Ziels nicht erforderlich. Das gleiche Ziel lässt sich, mit geringerem Risiko, durch bereichsspezifische Kennzeichen erreichen. In Österreich ist ein entsprechendes System bereits etabliert. Das RegMoG-E geht in der Begründung zwar darauf ein, lehnt es jedoch aufgrund „größerer rechtlicher, technischer und organisatorischer Komplexität“ und dem außerordentlichen Kosten- und Zeitaufwand ohne weitere Nachweise ab. Während eine exakt identische Umsetzung tatsächlich problematisch sein könnte, lässt sich das Grundprinzip ohne weiteres übertragen. Wie bereichsspezifische Personenkennzeichen mit der Struktur des RegMoG-E in Einklang gebracht werden können, wird in Abschnitt D. skizziert.

- Das RegMoG-E betrifft einen außerordentlich großen Personenkreis. Gleichzeitig ist die Quantität der mit dem allgemeinen Personenkennzeichen verknüpften Daten schon nach dem jetzigen Stand sehr groß, mit der perspektivischen Ergänzung um weitere Register nahezu uferlos. Zugriffe auf diese Daten können zunächst ohne Kenntnis der Betroffenen erfolgen, auch wenn durch die Protokollierung und das Datencockpit eine nachträgliche Kontrolle möglich ist. Eine hinreichende Zweckbindung – die unter anderem auch ein Verbot der Verwendung des allgemeinen Personenkennzeichens durch Private beinhalten müsste – ist nicht vorgesehen. Der vorgesehene Missbrauchsschutz ist unzureichend, da unbestimmt. Bei der Bewertung der vorgesehenen Verknüpfungsmöglichkeiten ist auch die Gesamtbelastung der Bürger mit Informationseingriffen des Staates in den Blick zu nehmen. Es gilt zu verhindern, dass die gesamtheitliche Datenerfassung die Bürger dem Eindruck einer Totalüberwachung aussetzt. All dies führt dazu, dass die im RegMoG-E vorgesehenen Eingriffe selbst dann die Verhältnismäßigkeitsprüfung nicht bestehen, wenn man entgegen dem obigen Ergebnis davon ausgeht, die Einführung eines allgemeinen Personenkennzeichens sei für das angestrebte Ziel erforderlich.

Aufgrund der unzureichenden Konkretisierung gehen meine Co-Autoren und ich im Übrigen davon aus, dass auch die Verordnungsermächtigung des § 7 Abs. 2 S. 2 im Entwurf des Identifikationsnummerngesetzes (IDNrG-E) verfassungswidrig ist. Weder hat der Gesetzgeber vorgeben, welche Kriterien zur Bestimmung von Bereichen herangezogen werden sollen, noch hat er die Zahl bestimmt (lediglich die Untergrenze von sechs Bereichen ist benannt), noch hat er vorgegeben, welche Zielsetzung mit der Bereichsaufteilung einhergehen soll.

D. Alternativmodelle

Wie bereits ausgeführt, sind bereichsspezifische Personenkennzeichen im Vergleich zu allgemeinen Personenkennzeichen vorzugswürdig und ermöglichen eine verfassungskonforme Umsetzung der Registermodernisierung. Vergleichbar sind solche Kennzeichen etwa mit der heutigen Verwendung der Steuer-ID. Indem das RegMoG-E die Einführung verschiedener Verwaltungsbereiche vorsieht, liegt – trotz der unzureichenden Konkretisierung – bereits nahe, dass für diese Bereiche auch jeweils eigene Kennzeichen sinnvoll sind.

Auch die im RegMoG-E ebenfalls vorgesehenen Intermediäre erleichtern die Entwicklung alternativer Modelle für die Registermodernisierung. Zwei dieser Alternativen (Stammzahl-Modell nach österreichischem Vorbild und NEU-ID-Modell) sind im angehängten Gutachten dargestellt. Bei beiden werden bereichsspezifische Personenkennzeichen verwendet. Bereichsübergreifende Anfragen werden über die – im RegMoG-E ohnehin vorgesehenen – Intermediäre vermittelt, die aber die Zusatzfunktion erhalten, bereichsspezifische Kennzeichen zu „übersetzen“. Ein Intermediär bekommt also etwa eine Anfrage mit dem bereichsspezifischen Kennzeichen aus dem Bereich Meldewesen und leitet sie mit dem bereichsspezifischen Kennzeichen aus dem Bereich Steuern weiter. Bei der Weitervermittlung der Antwort wird der Vorgang in umgekehrter Richtung vorgenommen. Die Inhaltsdaten können, wie im RegMoG-E vorgesehen, weiterhin so verschlüsselt werden, dass der Intermediär auf diese nicht zugreifen kann.

Der im Vergleich zum RegMoG-E entstehende Mehraufwand betrifft im Wesentlichen nur die Intermediäre; auch dort ist er gering. Dass Intermediäre bereichsspezifische Kennzeichen einander

zuordnen können (und im Fall eines erfolgreichen Angriffs ggf. Dritte die gleiche Fähigkeit erhalten), ist keine Verschlechterung gegenüber dem durch das RegMoG-E vorgesehenen Modell. Wird ausschließlich die Steuer-ID verwendet, bestehen diese Zuordnungsmöglichkeiten ohnehin.

Dennoch ist auch in diesen Modellen mit bereichsspezifischen Kennzeichen ein zusätzlicher Missbrauchsschutz vorzusehen. Im o.g. Gutachten schlagen wir insbesondere die *institutionelle Unabhängigkeit der Intermediäre* vor. Diese könnten z.B. in Verantwortung der Datenschutzaufsichtsbehörden betrieben werden. Die Verteilung der Intermediärsrolle in einem *föderierten Ansatz*, etwa mit einem Intermediär pro Bundesland, ist mit etablierten technischen Verfahren möglich und kann Risiken weiter mindern. Auch plädieren wir für eine *Beschränkung der „Übersetzungsmöglichkeit"* der Intermediäre auf diejenigen bereichsspezifischen Kennzeichen, für die eine entsprechende *Notwendigkeit und Rechtsgrundlage* besteht; dies ist auch technisch abzusichern, beispielsweise durch *Hardware-Sicherheitsmodule*.

Mittelfristig sollte für geeignete Anwendungsfälle die Wahrnehmung der Intermediärs- und damit der „Übersetzungsfunktion" zwischen verschiedenen Bereichen auch beim jeweils Betroffenen, z.B. in einer App oder dem Personalausweis, angedacht werden.

E. Fazit

Gegen den vorliegenden Entwurf bestehen insgesamt also schwerwiegende Bedenken. Neben der grundsätzlichen Problematik, die durch die Schaffung einer Möglichkeit zum Zusammenführen von Daten aus zahlreichen Registern ergeben, ist auch die vorgesehene Umsetzung problematisch. Die Verfügbarkeit technischer Alternativen bei gleichzeitig hohem Missbrauchsrisiko wirkt sich auf die verfassungsrechtliche Bewertung aus. Ich halte es daher für riskant, das Gesetzgebungsverfahren fortzuführen und die Idee eines allgemeinen Personenkennzeichens weiter zu verfolgen. Die Gefahr, dass die vorgesehene Verwendung der Steuer-ID sich als verfassungswidrig herausstellt, ist groß. In diesem Fall dürften auch die sich ergebenden Kosten höher sein, als wenn bereits jetzt Alternativen entwickelt werden.

Gleichzeitig fügen sich die vorgeschlagenen Alternativmodelle so gut in die vorgesehene Struktur des RegMoG-E ein, dass einer zügigen Erarbeitung eines neuen Entwurfs nichts im Wege steht.

Saarbrücken, 10. Dezember 2020

Christoph Sorge

FRIEDRICH NAUMANN
STIFTUNG Für die Freiheit.

REGISTER-MODERNISIERUNG

Datenschutzkonforme und umsetzbare Alternativen

Kurzanalyse zum Entwurf des Registermodernisierungsgesetzes

Christoph Sorge, Jörn von Lucke und Indra Spiecker gen. Döhmann

ANALYSE

Impressum

Herausgeber
Friedrich-Naumann-Stiftung für die Freiheit
Truman-Haus
Karl-Marx-Straße 2
14482 Potsdam-Babelsberg

/freiheit.org
/FriedrichNaumannStiftungFreiheit
/FNFreiheit

Autoren
Prof. Dr.-Ing. Christoph Sorge,
Lehrstuhl für Rechtsinformatik, Universität des Saarlandes

Prof. Dr. rer. publ. Jörn von Lucke,
Lehrstuhl für Verwaltungs- und Wirtschaftsinformatik,
Zeppelin Universität Friedrichshafen

Prof. Dr. iur. Indra Spiecker gen. Döhmann, LL.M. (Georgetown),
Lehrstuhl für Öffentliches Recht, Informationsrecht, Umweltrecht,
Verwaltungswissenschaften, Goethe-Universität Frankfurt

Redaktion
Dr. Maximilian Spohr
Liberales Institut
Friedrich-Naumann-Stiftung für die Freiheit

Produktion
COMDOK GmbH

Kontakt
Telefon +49 30 220126-34
Telefax +49 30 690881-02
E-Mail service@freiheit.org

Stand
Dezember 2020

Zentrale Aussagen und Empfehlungen

1. Der vorliegende Gesetzesentwurf zur Registermodernisierung (RegMoG-E) ist aus technischen und rechtlichen Gründen abzulehnen

2. Mit dem Entwurf ordnet die Regierung allen Bürger:innen in Gestalt der Steuer-ID ein **allgemeines Personenkennzeichen** zu, auch wenn zunächst nicht alle Register eingebunden werden.

3. Mittels eines solchen Systems können künftige Regierungen oder die Europäische Union erleichtert ein **Profil- und Überwachungssystem** über alle Bürger ausbauen.

4. Ein solches Gesetz wird mit hoher Wahrscheinlichkeit vor dem BVerfG scheitern

5. So droht in einigen Monaten ein Neustart des Vorhabens mit erheblichen Ver¬zögerungen und unnötigen Kosten.

6. Bundesregierung und der IT-Planungsrat müssen das laufende Gesetzgebungsverfahren stoppen!

7. Es gibt technisch und rechtliche besser Alternativen:

→ Alternative **„Stammzahl-Modell“**: orientiert sich am österreichischen Ansatz. Hier werden aus einer pro Person eindeutigen, geheim gehaltenen Stammzahl bereichsspezifische Kennzeichen mittels einer kryptographischen Hashfunktion abgeleitet. Intermediäre, die im RegMoG-E ohnehin vorgesehen sind, können diese Ableitung im Fall bereichsübergreifender Anfragen vornehmen. Die bereichsspezifischen Kennzeichen müssen allerdings sehr lang sein.

→ Alternative **„NEU-ID-Modell“**: es werden stattdessen bestehende oder zufällig generierte neue bereichsspezifische Kennzeichen verwendet. Auch hier erfolgt die Zuordnung dieser Kennzeichen durch ohnehin vorgesehene Intermediäre, die dafür entsprechende Zuordnungstabellen speichern müssen. Weitere personenbezogene Daten wie Namen oder Anschriften liegen ihnen nicht vor. Der Ansatz kommt mit kurzen, somit für Menschen gut handhabbaren bereichsspezifischen Kennzeichen aus.

→ Beide Ansätze müssen mit zusätzlichen Maßnahmen komplementiert werden: Dazu gehören die institutionelle Unabhängigkeit der Intermediäre und die Verteilung der Intermediärsrolle in einem föderierten Ansatz. Auch sollten Intermediäre möglichst nur diejenigen bereichsspezifischen Kennzeichen übersetzen können, für die eine entsprechende Notwendigkeit und Rechtsgrundlage besteht; dies ist auch technisch abzusichern, beispielsweise durch Hardware-Sicherheitsmodule. Mittelfristig sollte für geeignete Anwendungsfälle die Wahrnehmung der Intermediärs- und damit der Übersetzungsfunktion zwischen verschiedenen Bereichen auch beim Bürger, z.B. in einer App oder dem Personalausweis, angedacht werden.

→ Völlig risikofrei sind auch diese verbesserten Ansätze nicht – sie reduzieren aber die Risiken für den Datenschutz und die IT-Sicherheit, indem sie eine Umgehung der schon im Regierungsentwurf vorgesehenen Intermediäre erschweren.

8. Diese Alternativen könnten binnen weniger Monate und ohne nennenswerte Eingriffe in die bestehende Registerstruktur realisiert werden

Inhalt

A. Einführung

Mit dem Gesetzentwurf der Bundesregierung zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze, Registrierungsmodernisierungsgesetz (RegMoG-E)[1], plant das Bundesministerium des Innern, für Bau und Heimat (BMI) die Modernisierung der deutschen Verwaltungslandschaft durch die Einführung einer registerübergreifenden Identifikationsnummer. Zu diesem Zweck soll die bisher ausschließlich für Steuerverfahren genutzte Identifikationsnummer nach § 139b AO auf andere Bereiche erweitert werden. Alle anderen relevanten 56 registerführenden Stellen sollen innerhalb von fünf Jahren diese Identifikationsnummer als zusätzliches Ordnungsmerkmal zu Personendaten in ihren jeweiligen Registern speichern.

Bereits seit Bekanntwerden des Referentenentwurfs im Juli 2020 diskutiert die Öffentlichkeit über Sinn und Zweck einer solchen Kennziffer. Besondere Aufmerksamkeit erlangten die kritischen Stellungnahmen des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI)[2] und der Datenschutzkonferenz (DSK)[3]. Die erweiterte Verwendung der Identifikationsnummer ist vor dem Hintergrund, dass bereits bei Einführung vor deren schleichender Ausweitung gewarnt wurde,[4] als äußerst umstritten anzusehen.

I. Gesetzesentwurf der Bundesregierung

Bei dem RegMoG-E handelt es sich um ein Artikelgesetz, das mehrere Gesetze ändert beziehungsweise einführt. Von besonderer Bedeutung ist hierbei die Einführung des Identifikationsnummerngesetzes (IDNrG-E)[5]. Zu diesem Zweck wird die Verwendung der Steueridentifikationsnummer nach §§ 139a, b AO ausgeweitet.[6] Eine Identifikationsnummer wird nach dem Entwurf neben Steuerpflichtigen jeder natürlichen Person zugeordnet, die bei einer öffentlichen Stelle ein Verwaltungsverfahren führt (Art. 3 Nr. 1 RegMoG-E). Nach § 1 IDNrG-E wird diese Identifikationsnummer als zusätzliches Ordnungsmerkmal in 56 Register eingeführt, die in der Anlage zum IDNrG-E aufgelistet sind. Beispielhaft lassen sich hier Melderegister, Personenstandsregister und Ausländerzentralregister, aber auch Zentrales Fahrerlaubnisregister, Schuldnerverzeichnis und Beitragskontendatenbank nennen.

Für jede natürliche Person, die eine Identifikationsnummer erhalten hat, speichert das Bundeszentralamt für Steuern sogenannte Basis- und weitere Daten (§ 4 Abs. 1 IDNrG-E). Unter Basisdaten (§ 4 Abs. 2 IDNrG-E) versteht der Entwurf etwa Familienname, Vorname, Geburtsort und -datum, Geschlecht, Staatsangehörigkeit und andere. Weitere Daten (§ 4 Abs. 3 IDNrG-E) sind Auskunftssperren nach dem Bundesmeldegesetz, Datum des letzten Verwaltungskontakts (Monat und Jahr) und Validitätswerte (Hinweise zur Richtigkeit bestimmter Basisdaten, vgl. § 4 Abs. 5 IDNrG-E).

Zur Übermittlung dieser Daten sieht der Entwurf die Einrichtung einer Registermodernisierungsbehörde vor, die beim Bundesverwaltungsamt angesiedelt ist (§ 3 Abs. 1 S. 2 IDNrG-E). Sie dient als zwischengeschaltete Instanz zwischen den Behörden, die mittels der Identifikationsnummer auf Daten der Person zugreifen wollen. So können bei Übermittlung von mindestens Identifikationsnummer und Geburtsdatum alle Basis- und weitere Daten nach § 4 Abs. 2 und 3 IDNrG-E der Person an die abrufende Behörde übermittelt werden, soweit die Daten zur Aufgabenerfüllung erforderlich sind (§ 6 Abs. 3 Nr. 2 IDNrG-E). Umgekehrt kann bei Angabe von mindestens Familiennamen, Wohnort, Postleitzahl und Geburtsdatum die Identifikationsnummer ermittelt werden (§ 6 Abs. 3 Nr. 1 IDNrG-E). Nach Übermittlung der angeforderten Daten muss die Registermodernisierungsbehörde diese löschen (§ 11 IDNrG-E).

Ferner sieht Art. 2 RegMoG-E die Einführung eines sogenannten Datencockpits im Rahmen einer Modifizierung des Onlinezugangsgesetzes (OZG) vor. In diesem Datencockpit kann eine natürliche Person Auskunft zu Datenübermittlungen unter Rückgriff auf die Identifikationsnummer erhalten (§ 10 Abs. 1 OZG). Das Datencockpit zeigt lediglich Protokolldaten an (§ 10 Abs. 2 OZG), auf die nur die betroffene Person Zugriff hat (§ 4 Abs. 4 OZG). Diese Protokolldaten erheben die jeweiligen Stellen bei allen Datenübermittlungen unter Nutzung einer Identifikationsnummer (§ 9 Abs. 1 S. 1 IDNrG-E). Die Registermodernisierungsbehörde protokolliert darüber hinaus alle Datenübermittlungen von und zur Registermodernisierungsbehörde selbst (§ 9 Abs. 1 S. 2 IDNrG-E). Neben der Übermittlung an das Datencockpit dürfen diese Protokolldaten nur zur datenschutzrechtlichen Prüfung und zur Wahrnehmung von Betroffenenrechten verwendet werden (§ 9 Abs. 2 IDNrG-E). Nach zwei Jahren sind die Protokolldaten – vorbehaltlich zu begründender Ausnahmen – zu löschen (§ 9 Abs. 3 IDNrG-E).

Die verbleibenden Artikel des RegMoG-E beziehen sich auf Änderungen von Gesetzen zu Fachregistern, in denen zukünftig auch die übergreifende Identifikationsnummer gespeichert werden soll.[7]

[1] RegMoG-E: Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung, Bundestagsdrucksache 19-24226, Deutscher Bundestag, Berlin 2020. Online: https://dip21.bundestag.de/dip21/btd/19/242/1924226.pdf.
[2] *BfDI 2020*, Hintergrundpapier zur Registermodernisierung und Schaffung eines einheitlichen Personenkennzeichens [BfDI 2020].
[3] DSK 2020, Entschließung vom 26.08.2020, Registermodernisierung verfassungskonform umsetzen.
[4] Vgl. *BfDI 2010*, 23. Tätigkeitsbericht (2009/2010), S. 106.
[5] Art. 1 RegMoG-E: Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung.
[6] Vgl. zur Vergabe der Identifikationsnummer auch den Verweis des § 5 Abs. 2 IDNrG-E auf § 139b AO iVm. der Steueridentifikationsnummernverordnung.
[7] *Wissenschaftlicher Dienst des Deutschen Bundestages 2020,* Gutachten Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes, S. 5 [Wiss. Dienst BTag, Gutachten].

II. Anforderungen an eine zeitgemäße Registermodernisierung

Zum eigentlichen Zweck der Registermodernisierung bei Bund, Ländern und Kommunen hat sich das Koordinierungsprojekt Registermodernisierung des IT-Planungsrats im April 2020 in einem Eckpunktepapier[8] geäußert. Diese abgestimmten Ergebnisse wurden in der 32. Sitzung des IT-Planungsrats vom 24. Juni 2020 von diesem zur Kenntnis genommen und bilden damit die Grundlage für die bis Ende 2020 anzufertigende Gesamtkonzeption für eine modernisierte Registerlandschaft. Im Kern geht es um den Aufbau eines registerübergreifenden Identitäts- und Qualitätsmanagements, um einen einfachen Datenaustausch zwischen allen beteiligten Stellen, um eine verbesserte Datenhaltung in Registern und elektronisch geführten Datenbeständen, um einen verbesserten Datenschutz, verbesserte Datensicherheit und Transparenz der Zugriffe sowie perspektivisch um eine Erweiterung der Registerlandschaft, um alle benötigten Daten vorzuhalten.

Das RegMoG-E der Bundesregierung, welches das Konzept des IT-Planungsrats aufgreift, ist ein zentrales Element für diese verwaltungsebenenübergreifende Modernisierung, die auch der Nationale Normenkontrollrat seit 2017 fordert.[9] Erstens soll nach Vorstellungen des IT-Planungsrats das registerübergreifende Identitäts- und Qualitätsmanagement künftig die Qualitätssicherung bestehender Datenbestände übernehmen und so zu einer inhaltlich optimalen Aufstellung beitragen. Dabei gilt es vor allem, Inkonsistenzen zu erkennen, Dubletten und Schreibfehler zu beseitigen sowie Namen und Adressen auf den aktuellen Stand zu bringen. Dies hat Korrekturen in allen beteiligten Registern zur Folge und kann über gemeinsame Basisdaten einfach realisiert werden. Zugleich soll eine Anbindung an föderale Integrationsbemühungen seitens der Europäischen Union vorbereitet werden.[10] Zweitens soll mit einem Architekturmodell, dem Ausbau von Standards und Schnittstellen, einer Anpassung der Transportwege und einer Erweiterung des Zugriffs- und Rechtemanagements auf neuer rechtlicher Grundlage der Datenaustausch zwischen allen zu beteiligenden Stellen verbessert werden.[11] Drittens gilt es alle datenhaltenden Behörden digital zu ertüchtigen, um mit gezielten Vollständigkeits-, Qualitäts- und Datensparsamkeitsmaßnahmen eine Verbesserung der Datenhaltung in der Bundesrepublik insgesamt zu erreichen. So werden die Etablierung eines Unternehmensregisters, eines Gebäude- und Wohnungsregisters und eines statistischen Bildungsregisters angedacht.[12] Ab 2030 wird ein künftig jährlicher registerbasierter Zensus (Volkszählung) in Erwägung gezogen.[13] Da dies alles zu einem „gläsernen Bürger" führen kann, sollen viertens weitere Datenschutz- und Sicherheitsmaßnahmen vor einer staatlichen Profilbildung sowie ein Datencockpit für mehr Transparenz des Bürgers über behördliche Zugriffe auf seine Daten etabliert werden.[14] Welche konkreten Vorstellungen allerdings diesem letzten Punkt Rechnung tragen sollen und wie eine (Selbst-)Kontrolle des Staates unter diesen Bedingungen gelingen soll, bleibt weitgehend offen.

Begründet durch den hohen gesellschaftlichen Stellenwert, der dem Datenschutz in Deutschland beigemessen wird sowie einer Tradition papierbasierter Aktenführung ist in der Bundesrepublik Deutschland auf staatlicher Ebene kaum ersichtlich, welche Daten die einzelnen Behörden von Bund, Land und Kommunen insgesamt über ihre Bürger vorhalten. Deutsche Behörden sind verpflichtet, die von ihnen erhobenen Daten nur für die gesetzlich definierten Zwecke zu verwenden. Die Erstellung von Persönlichkeitsprofilen der Bürger durch eine Zusammenführung der vorhandenen Lebens-, Verhaltens- und Personaldaten ist staatlichen Stellen untersagt. Dies leitet sich aus dem deutschen Grundgesetz ab und gilt auch auf europäischer Ebene. Darüber hinaus sind diese Grundsätze auch der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs zu entnehmen.[15]

Im Vergleich zu vielen anderen europäischen Staaten ist Deutschland beim E-Government weder Vorreiter noch Treiber der technischen Entwicklung. Auf Grund des föderalen Mehrebenensystems dauert jede Umsetzung verwaltungsebenenübergreifender Modernisierungsansätze typischerweise länger. Durch Kompromisse ist sie wegen der unterschiedlichen Vorstellungen im Wettbewerb der politischen Ideen aber auch ausgewogener. Elektronische Register und die elektronische Akten- und Vorgangsbearbeitung lösen in den kommenden Jahren die letzten Bücher und Papierakten ab. Mit dem OZG und dem RegMoG wollen sich Bund, Länder und Kommunen für die digitale Zukunft leistungsfähig und bürgernah aufstellen.

Vor diesem Hintergrund erzeugt der von der Bundesregierung eingebrachte RegMoG-E erhebliche Irritationen. Mit einem allgemeinen Personenkennzeichen, das zunächst auf 57 Register – perspektivisch sogar auf alle derzeit bestehenden 220 und alle zukünftig zu entwickelnden Register (zum Beispiel das Register des Forschungsdatenzentrums mit den Versicherungsdaten aller gesetzlich Krankenversicherten nach § 303d DVG) ausgeweitet werden soll und kann –, wird (bewusst oder unbewusst) eine wesentliche Grundlage für die mögliche Generierung von Persönlichkeitsprofilen aller Bürger quer über die gesamte Verwaltung gelegt. Mit einer weiteren Gesetzesänderung und neuartigen Profilbildungsprogrammen könnten künftige Machthaber plötzlich und rasch wissen, was der Staat wirklich weiß und dies für oder gegen die Bürger einsetzen. Danach wäre aber technisch durchaus

[8] *IT-Planungsrat* 2020, Eckpunkte für die Registermodernisierung – Bestehende Anforderungen, vorläufige Architekturskizze sowie sich daraus ergebende Maßnahmen im Rahmen des IT-Planungsratsprojekts Registermodernisierung.
[9] Vgl. *Nationaler Normenkontrollrat 2017,* Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren.
[10] Vgl. *IT-Planungsrat* 2020, S. 3, S. 17 und S. 34.
[11] Vgl. *IT-Planungsrat* 2020, S. 4 und S. 18.
[12] Vgl. *IT-Planungsrat* 2020, S. 4 und S. 19.
[13] Vgl. *Nationaler Normenkontrollrat/McKinsey & Company* 2017, S. 21-23 und Körner/Krau¬se/Ram-sauer 2019.
[14] Vgl. *IT-Planungsrat* 2020, S. 2-3, S. 17-20 und S. 33-35.
[15] BVerfG 1 BvR 16/13 Rn. 90 ff. und EuGH ECLI:EU:C:2020:790 Rn.71 ff.

realisierbar, was nach geltendem Recht unzulässig ist und im Gesetzesentwurf zu Recht unter Strafe gestellt wird. Gerade deswegen stellt sich mit dem Gesetzesentwurf auch die Frage an den Gesetzgeber, ob der Staat in die Lage versetzt werden soll, auf Knopfdruck alles über seine Bevölkerung wissen zu können.

Der Datenschutz verfolgt ganz andere, höhere Ziele. Datenschutz besitzt für die Bundesrepublik Deutschland und ihre Bürger eine hohe Bedeutung. Dieser Stellenwert speist sich aus den Erfahrungen des Dritten Reiches, der Diktatur des Nationalsozialismus und der Deutschen Demokratischen Republik. Bürger wurden damals erfasst, überwacht, selektiert, verhaftet und ermordet. Dies darf sich niemals wieder wiederholen. Die Ermöglichung freiheitlichen Handelns durch den Datenschutz und IT-Sicherheit und damit ihre Funktion als Rückgrat von Demokratie, Grundrechtsverwirklichung und gleichen Verwirklichungschancen der Bürger ist vor diesem Hintergrund nicht zu unterschätzen.

Die Bundesrepublik ist von einem föderalen Mehrebenensystem geprägt, in dem es bis zu sieben Ebenen, mehr als 11.000 Gebietskörperschaften und mehr als 30.000 zuständige Ämter und Behörden gibt, die öffentliche Aufgaben wahrnehmen und gemeinsam über 5.900 Verwaltungsleistungen erbringen. Diese Komplexität der Aufbau- und Ablauforganisation ist für Bürger wie Verwaltung herausfordernd, aber politisch auch so gewollt. Mit dem Onlinezugangsgesetz soll Bürgern und Unternehmen nun der Zugang zu Verwaltungs-leistungen bis 2022 flächendeckend digital ermöglicht werden. Der Normenkontrollrat und die Bundesregierung erachten dazu auch eine Registermodernisierung als dringend erforderlich. Die wahrnehmbare Trennung der verschiedenen Ebenen wird damit reduziert.

In einer offenen Gesellschaft sollen zugleich alle Bürger die Freiheit haben, zu sein und zu agieren, wie sie sind und sein möchten. Der Staat darf deswegen nicht in die Lage versetzt werden, über umfassende Aktivitätsprofile aller seiner Einwohner zu verfügen, um diese zu einem (politisch) konformen Verhalten zu bewegen. Die zunehmende smarte, KI-basierte und plattformbasierte Überwachung im öffentlichen wie im privaten Raum eröffnet hier allen evidenzbasierten, verhaltenswissenschaftlichen Ansätzen in Echtzeit neuartige Möglichkeiten, die von Vertretern der Zivilgesellschaft und vieler Parteien zunehmend mit Sorge betrachtet werden. Vertreter vieler Sicherheitsbehörden haben dazu eine berufsbedingte, nachvollziehbar andere Einschätzung. Diese Behörden profitieren von umfassenden Profilen der gesamten Bevölkerung, etwa um mit Hilfe leistungsstarker IT-basierter Polizeianalysedienste präventiv potenzielle Gefährder frühzeitig zu identifizieren oder um nach Anschlägen rasch verfassungsfeindliche Netzwerke zu enttarnen und zu verhaften. Eine Zusammenarbeit mit zahlreichen Plattformen wäre für die Sicherheitsbehörden eine weitere, bereichernde Option.

Je nach Gefährdungslage kommen Entscheider im politischen Raum also zu unterschiedlichen Einschätzungen, wie staatliche Behörden mit den personenbezogenen Daten jetzt und in Zukunft umgehen sollen. Mit der Einführung einer Identifikationsnummer als allgemeines Personenkennzeichen würde in der Bundesrepublik Deutschland die Grundlage gelegt, dass die vorhandenen bereichsspezifischen Profile zu einem Bürger rasch zu einem umfassenden Gesamtprofil zusammen¬gefügt werden könnten. Die Bundesregierung sieht diese Gefahr durchaus. Sie schlägt mit dem Gesetzesentwurf einige organisatorische und strafrechtliche Maßnahmen vor, die dies dauerhaft unterbinden sollen. Darüber würde sich aber eine künftig gewählte, überwachungs- und selektionsfreudige Bundesregierung mit einer simplen wie gezielten Gesetzesänderung hinwegsetzen können. Die neu geschaffene Möglichkeit der Zusammenführung von Registerdaten durch ein allgemeines Personenkennzeichen ermöglicht zudem schon sofort eine – wenn auch rechtswidrige – Zusammenführung von Daten aus verschiedenen Registern unter Umgehung vorgesehener Schutzmechanismen. Die Bevölkerung müsste mit diesen Risiken und Nebenwirkungen dauerhaft leben. Dies ist aus verschiedenen Gründen inakzeptabel.

Das Ziel eines freiheitsermöglichenden Staates und einer gelebten offenen Gesellschaft muss dauerhaft der transparente Staat, nicht aber der „gläserne Bürger" sein. Die Bürger sollen verstehen können, wie der Staat funktioniert, welche Behörde welche Aufgaben erledigt und gegen wen bzw. gegen was sich effektiver Rechtsschutz zur Kontrolle richten kann. Diesem Auftrag widmet sich unter anderem das OZG. Die Behörden müssen die öffentlichen Aufgaben, die ihnen die Gesetzgeber übertragen, auch erfüllen können. Dazu benötigen sie Haushaltsmittel, Stellen, qualifiziertes Personal und organisatorische Prozesse, aber auch gewisse personenbezogene Daten der Bürger, die sie datenschutzkonform und zweckgerichtet zu verwenden und zur Erfüllung ihrer Zwecke sicher zu bewahren haben. Soweit dies zur öffentlichen Aufgabenerfüllung erforderlich ist, sollte jede Behörde in der Lage sein, bei Bedarf einen Ausschnitt eines Bildes aus dem Leben des Bürgers auf Basis der vorliegenden Daten in dem jeweiligen Amt oder Bereich zu generieren.

Trotz zunehmender Gesamtüberwachung und weitreichender Ausforschungsmöglichkeiten darf ein „gläserner Bürger" aber nicht Realität werden, denn dieser würde weder seine Kontrollfunktion noch seine Freiheitsdimension ausleben können. Daher dürfen der Staat und die Verwaltung nicht durch Informationstechnologien in die Lage versetzt werden, auf Knopfdruck zu einem Bürger ein umfassendes, detailliertes Profil auf Basis aller oder vieler vorliegender Datenbestände in den vorhandenen Registern von Bund, Ländern und Kommunen zu erstellen. Ebenso sollten sie kein neuartiges umfassendes Register mit allen Daten selbst erzeugen können.

Diese Gefahr würde nun mit dem Gesetzesentwurf zur Registermodernisierung und der Einführung einer Identifikationsnummer als einer allgemeinen, registerübergreifenden und zentralen Personenkennziffer, wie dort vorgesehen, ohne weitere Sicherungen deutlich gesteigert. Verfassungs- und europarechtlich ist dies nicht zulässig, wie in Teil B gezeigt wird.

III. Optionen für Personenkennzeichen

Die Bundesrepublik Deutschland und ihre Gesetzgeber haben sich bisher, auch basierend auf den erlebten Erfahrungen der Jahre 1933–1945 (nationalsozialistische Diktatur des Dritten Reiches), insbesondere mit Blick auf die Reduzierung von Häftlingen auf eine Nummer, sowie der Erfahrungen der Jahre 1949–1989 (kommunistische Diktatur der DDR), klar gegen allgemeine Personenkennzeichen ausgesprochen. Bisherige Versuche einzelner Fraktionen, ein allgemeines Personenkennzeichen einzuführen, scheiterten.

In vielen anderen europäischen und außereuropäischen Staaten wurden die Stärken und Schwächen sowie Chancen und Risiken dieses Ansatzes jedoch anders bewertet. Diese Staaten haben eine allgemeine Personenkennziffer oder ein Personenkennzeichen eingeführt, die Bürger ihr Leben lang im Kontakt mit Behörden und staatlichen Stellen verwenden. Auch Unternehmen nutzen seit vielen Jahrzehnten Kundennummern, damit sie im Bedarfsfall alle Daten zu einer Person (Kunde) rasch zuordnen können. In den Mitgliedstaaten der Europäischen Union werden verschiedene Konzepte verfolgt.[16]

Auch die Bundesrepublik Deutschland hat sich, in Anerkennung ihrer Geschichte, zur Vereinfachung von Verwaltungsvorgängen Personenkennzeichen bedient. Diese sind allerdings bereichsspezifisch ausgerichtet. Die Steuer-ID, die Renten¬versicherungsnummer, die Krankenversicherungsnummer und die Personenkennziffer der Bundeswehr sind Beispiele für bekannte bereichsspezifische Kennzeichen. Sie dürfen allerdings nur in einem bestimmten Verwaltungs- und Lebensbereich für bestimmte Aufgaben eingesetzt werden und erlauben keine weitere, gar flächendeckende Verwendung in anderen Lebens- und Verwaltungsbereichen.

Personenkennzeichen sind alphanumerische Zeichenfolgen, die zur eindeutigen Identifizierung von Personen innerhalb einer größeren Personengruppe dienen sollen. Aus dem Blickwinkel der Verwaltungsinformatik und der Verwaltungswissenschaft bestehen zahlreiche Optionen zur Gestaltung von Personenkennzeichen. Diese Optionen und Alternativen lassen sich in einem morphologischen Kasten (**Abbildung 1**) darstellen.

Abb. 1 | Morphologischer Kasten zu Personenkennzeichen

PK / ID-NR	AUSPRÄGUNGSFORMEN				
Einzigartigkeit	einzigartig			mehrfach vergeben	
Sichtbarkeit	nicht-sprechend			sprechend	
Ziffern oder Zeichen und Umfang des Zeichensatzes	numerische Ziffernreihenfolge (0-9)			alphanumerische Zeichenreihenfolge (0-9, A-Z, a-z)	
Prüfziffer	mit Prüfziffer			ohne Prüfziffer	
Typus von Personenkennzeichen	allgemeine Verwendung (aPK: wesentliche Bereiche)		bereichsübergreifende Verwendung (2wPK: 2 oder wenige Bereiche)		bereichsspezifische Verwendung (bPK: 1 Bereich)
Vorgehen bei der Vergabe	zentrale Vergabe			dezentrale Vergabe	
Zu erfassende Personengruppe	Deutsche Bürger	Ausländer	Steuerzahler	Natürliche Personen	Juristische Personen
Basisdatensatz	mit Basisdatensatz			ohne Basisdatensatz	

In der Regel sollten Personenkennzeichen einzigartig sein, damit sie Personen eindeutig identifizieren. Eine mehrfache Vergabe eines Personenkennzeichens mag sich als sinnvoll erweisen, etwa wenn der vorherige Träger des Kennzeichens verstorben und das Reservoir verfügbarer Ziffern oder Zeichenkombinationen erschöpft ist. Ein solches Vorgehen würde jedoch dem eigentlichen Zweck des Kennzeichens für Personen widersprechen und muss wegen des Risikos von Fehlzuordnungen schon prinzipiell verworfen werden.

Personenkennzeichen könnten sprechend angelegt sein. Dann lassen sich bestimmte Daten direkt aus dem Kennzeichen ablesen, etwa bei der Personenkennziffer der Bundeswehr das Geburtsdatum, der erste Buchstabe des Nachnamens und der Meldebezirk (früher das zuständige Kreiswehrersatzamt). Nicht-sprechende Personenkennzeichen verhindern diese Sichtbarkeit prinzipiell und machen die Person hinter dem Kennzeichen für Dritte nicht gläsern.

[16] Vgl. *Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann* 2019, Art. 87 Rn. 31f.

Kennzeichen können aus einer rein numerischen Ziffernreihenfolge oder aus einer alphanumerischen Zeichenreihenfolge bestehen. Bei einer Nummer wird deswegen von einer Personenkennziffer, bei einem Zeichencode von einem Personenkennzeichen gesprochen. Je länger die Personenkennziffer oder das Personenkennzeichen ist, desto größer ist das Reservoir an verfügbaren Zeichenkombinationen. Bei einer numerischen Ziffernreihenfolge gibt es bis zu 10 Möglichkeiten (0-9), bei einer alphanumerischen Zeichenreihenfolge bestehen bis zu 62 Optionen (0-9 & A-Z & a-z) pro Zeichenposition. Eine Mischung von Groß- und Kleinschreibung wäre in der praktischen Umsetzung allerdings fehleranfällig. 36 Optionen (0-9 & A-Z) sind auch gut handhabbar. Sollen mindestens 84 Millionen Bundesbürger erfasst werden, bedarf eine numerische Personenkennziffer in der Bundesrepublik zumindest 9 numerischer Zeichen, ein alphanumerisches Personenkennzeichen zumindest 5 alphanumerischer Zeichen.

Prüfziffern in Personenkennzeichen dienen dazu, Fehler bei der manuellen Eingabe oder Datenübermittlung zu erkennen. Nach einem vereinbarten Algorithmus werden dazu die Ziffern oder Zeichen verrechnet. Das Ergebnis entspricht der Prüfziffer, die dem restlichen Kennzeichen angehängt oder vorangestellt wird und in der Praxis als Teil des Kennzeichens betrachtet wird. Zahlendreher und andere Fehleingaben generieren dagegen eine andere Prüfziffer, so dass Nutzer bei Fehleingaben zeitnah auf ihre Fehler hingewiesen werden können.

Ein allgemeines Personenkennzeichen (aPK) wird innerhalb eines Staates von allen Behörden, von vielen Behörden oder den wesentlichen Behörden verwendet, um Personen eindeutig zu identifizieren. Entscheidend ist dabei nicht die allein Anzahl der Behörden (im Vergleich zur Gesamtzahl aller Behörden), sondern die Breite der abgedeckten Lebensbereiche, in denen die Kennziffer verwendet wird. aPK werden in der Regel zentral vergeben, um sicherzustellen, dass jede Person auch nur ein einziges Mal erfasst und jede Personenkennziffer nur ein einziges Mal vergeben wird. Auf Grund der eigenen historischen Vergangenheit hat sich der Gesetzgeber in der Bundesrepublik Deutschland bisher klar gegen die Einführung eines aPK positioniert. Stattdessen werden mehrere bereichsspezifische Personenkennzeichen in paralleler Anwendung genutzt. Rund um deren Einführung wurde aus Sorge vor dem „gläsernen Bürger“, wie etwa bei der Steuer-ID, auch intensiv debattiert, inwieweit solche Kennzeichen genutzt werden dürfen.

Ein bereichsübergreifendes Personenkennzeichen (2wPK) im eigentlichen Sinne wird innerhalb eines Staates von Behörden nur zweier oder weniger Bereiche verwendet, um Personen eindeutig zu identifizieren. Diese Nutzung einer Kennziffer in mehreren Bereichen mag sinnvoll sein, bedarf jedoch gleichfalls einer gesetzlichen Grundlage. Zum Beispiel kann die im Bereich der Pflegeversicherung existierende Pflegeversichertennummer gemäß § 101 SGB XI ganz oder teilweise mit der Krankenversichertennummer der Krankenkassen übereinstimmen.

Bereichsspezifische Personenkennzeichen (bPK) sind zur Erfüllung öffentlicher Aufgaben in einem bestimmten Bereich der Verwaltung notwendig, um dort die relevanten Personen eindeutig identifizieren zu können. Sie werden als Kennziffern nur innerhalb dieses klar bestimmten Aufgabenbereichs des Staates von einer oder wenigen Behörden vergeben und verwendet. Jeder Bereich pflegt eine andere Systematik zur Generierung der Personenkennziffern. Für den jeweiligen Bereich können diese zentral oder dezentral (landesweit, regional oder lokal) vergeben werden. Jeder personenbezogene Datenaustausch zwischen Behörden bedarf einer gesetzlichen Grundlage und einer detaillierten Regelung. Behörden haben in der Regel keinen Zugriff auf andere bereichspezifische Personenkennziffern und die dahinterliegenden personenbezogenen Daten.

Aus diesem Grunde werden Bürger bisher bei allen Anträgen aufgefordert, auch alle erfor-derlichen Nachweise und Unterlagen mit ihren personenbezogenen Daten miteinzureichen. Diese liegen der zuständigen Stelle in der Regel nicht vor. Die Vorgehensweise entwickelte sich historisch in einer Welt von räumlich getrennten Amtsstuben. Sie entsprach den Abläufen einer papierbasierten Verwaltung, in der sich Ämter über Akten organisieren und über Vorgänge bis zur Entscheidungsfindung steuern. Die zunehmende Digitalisierung ermöglicht seit mehr als 50 Jahren einen automatisierten Datenaustausch zwischen Behörden. Dieser ist aber nur zulässig, wenn er über entsprechende Gesetze vom Gesetzgeber zur Erfüllung bestimmter öffentlicher Aufgaben etabliert worden ist. In Zeiten einer umfassenden Digitalisierung und intelligenten Vernetzung sollen künftig mit „Once-Only“ und „No-Stop-Government“, vielleicht sogar mit „No-Government“, diese aus heutiger, digitaler Sicht suboptimalen Vorgehensweisen zeitnah dauerhaft überwunden werden.[17]

Im Bereich der Gefahrenabwehr haben sich mit dem Gemeinsamen Terrorismusabwehrzentrum (GTAZ), dem Gemeinsamen Extremismus- und Terrorismusabwehrzentrum (GETZ) und dem Gemeinsamen Internetzentrum (GIZ) mehrere Kooperations- und Kommunikationsplattformen etabliert. Dort treffen sich Verbindungsbeamte verschiedener Sicherheitsbehörden regelmäßig zu Lagebesprechungen, um im Rahmen der eigenen Zuständigkeiten einen besseren Überblick über die Gesamtsituation zu gewinnen und um ihre Informationen zu Gefährdern zu verdichten. Ein allgemeines Personenkennzeichen würde diesen Plattformen die Zusammenarbeit erleichtern. Zugleich wird das Interesse an einer solchen Zusammenarbeit auch bei anderen Stellen wachsen.

Die Größe des durch ein Personenkennzeichen zu erfassenden Personenkreises variiert mit Aufgabe und Verwaltungsbereich. Erfasst werden könnten Personengruppen jeder Art, etwa alle Bundesbürger mit deutscher Staatsangehörigkeit, alle Ausländer mit einer ausländischen Staatsangehörigkeit, alle Steuerzahler, alle natürlichen Personen oder alle juristischen Personen. Am Beispiel von Personen mit zwei Staatsangehörigkeiten lässt sich zeigen, dass sich diese Personenkreise durchaus auch überschneiden könnten. Die jeweils zu erfassende Personengruppe wird im dazugehörigen Gesetz vom Gesetzgeber genau definiert.

[17] Vgl. Stocksmeier/Hunnius 2018, S. 263-264.

Große Bestände personenbezogener Daten werden heute in der Regel in Registern und den dahinterliegenden Datenbanksystemen gespeichert. Der Gesetzgeber legt in Gesetzen den Umfang der in den Registern zu speichernden personenbezogenen Daten und die Zugangsbestimmungen fest. Solche Register können sehr klein gehalten werden, so dass nur die unbedingt nötigen Daten gespeichert und verarbeitet werden. Natürlich könnten diese Register auch sehr umfangreich gestaltet werden, wenn etwa eine öffentliche Aufgabe dies erfordert. Aus einer Datenschutzperspektive wird dies aber kritisch gesehen. Der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) gebietet, darauf hinzuwirken, dass keine oder möglichst wenig personenbezogene Daten verarbeitet und gespeichert werden.[18] Das datenschutzrechtliche Gebot der Zweckbindung (Art. 5 Abs. 1 lit. b DSGVO) soll zudem sicherstellen, dass Daten nur für den Zweck verarbeitet werden, für den sie erhoben werden.

Vorstellbar ist, in einem separaten, eigenständigen Register jede Personenkennziffer um einen Basisdatensatz zu ergänzen. Ein solches Vorgehen ist besonders bei einer allgemeinen Personenkennziffer sinnvoll, da sich mit einem gemeinsam genutzten Basisdatensatz die Datenqualität in den anderen Registern verbessern lässt. Im Rahmen der Registermodernisierung soll die Datenqualität der Register von Bund, Ländern und Kommunen substanziell erhöht und dazu auf die Basisdaten des Bundeszentralamts für Steuern als Stammdaten gesetzt werden. Ziel ist es, automatisiert unzutreffende oder fehlerhafte Einträge zu identifizieren, zu korrigieren und in allen betroffenen Registern zu aktualisieren. Gegebenenfalls wird dazu auch ein persönliches Erscheinen in der kommunalen Meldebehörde erforderlich sein. Alternativ könnte man auf die Anlage von separaten Basisdatensätzen zu dem Personenkennzeichen auch verzichten und wie gehabt auf die Datenpflege in den jeweiligen Registern verweisen.

IV. Optionen für Identitätsnummernsysteme

Mit der Entscheidung für einen bestimmten Ansatz eines Personenkennzeichens fällt zugleich auch die Entscheidung über das damit verbundene Identitätsnummernsystem. Bei dessen Gestaltung gibt es grundsätzlich mehrere Optionen und Alternativen, die es in gebotener Kürze zu reflektieren gilt.

Identitätsnummernsysteme dienen dazu, größere Personengruppe derart zu erfassen, dass Personen mit einem Personenkennzeichen (im RegMoG-E: Identitätsnummer) eindeutig identifiziert werden können. Aus dem Blickwinkel der Verwaltungsinformatik und der Verwaltungswissenschaft bestehen hier einige Optionen zur Gestaltung von Identitätsnummernsystemen, die sich über einen morphologischen Kasten (**Abbildung 2**) sehr verständlich darstellen lassen.

Abb. 2 | Morphologischer Kasten zu Identitätsnummernsystemen

ID-NR-SYSTEM	AUSPRÄGUNGSFORMEN				
Typus von Personenkennzeichen	allgemeines Personenkennzeichen (aPK)	bereichsübergreifendes Personenkennzeichen (2wPK)	bereichsspezifisches Personenkennzeichen (bPK)		
Vorgehen bei der Vergabe	Personenkennzeichen zentral vergeben		Personenkennzeichen dezentral vergeben		
Inhaltliche Gestaltung des Personenkennzeichens	Steuer-ID	Andere existierende Register-ID	NEU-ID/Stammzahl in Form von einer Zufallszahl	Keine zentrale ID	
Identifizierung in anderen Registern	Steuer-ID	Bisherige Register-ID	Hashwert auf Stammzahl und Bereichs-Bezeichner	Zufallszahl	
Zu erfassende Personengruppe	Deutsche Bürger	Ausländer	Steuerzahler	Natürliche Personen	Juristische Personen
Verortung der Speicherung der Basisdatensätze zu allen Personen	Basisdatensatz beim Bundeszentralamt für Steuern (BZSt)		ohne Basisdatensatz		
Einsatz einer Intermediär-internen Datenbank mit allen bPKs	Verzicht auf Intermediär-interne ID-Datenbank		Pseudonymisierte Intermediär-interne ID-Datenbank		
Registermodernisierung	Registermodernisierungsbehörde (BVA)		Verzicht auf Registermodernisierungsbehörde		
Verortung der Intermediäre zu den BZSt-Basisdatensätzen	Intermediär zum BZSt-Basisdatensatz bei BVA (Registermodernisierungsbehörde)		Intermediär zum BZSt-Basisdatensatz bei Datenschutzaufsichtsbehörde		

[18] Vgl. Abschnitt B.IV.2

ID-NR-SYSTEM	AUSPRÄGUNGSFORMEN			
Vermittlungsstellen für Anfragen auf BZSt-Basisdatensätze	Keine Vermittlungsstelle für Anfragen	Zentrale Vermittlungsstelle für Anfragen	Verbund von Vermittlungs-stellen für Anfragen	
Prüfung der Zugriffe auf BZSt-Basisdatensätze	Keinerlei Prüfung der Zugriffe	Software-basierte Prüfung der Zugriffe	Hardware-basierte Prüfung der Zugriffe	Ständige Prüfung durch Sachbearbeiter
Freigabe von Daten durch Bürger bei bereichs-übergreifenden Abfragen	Freigabe von Daten ohne Bürgereinbindung	Anlassbezogene Freigabe von Daten durch Bürger	Freigaben von Daten stets durch Bürger erforderlich	

Grundsätzlich können Identitätsnummernsysteme auf allgemeine Personenkennzeichen (aPK), auf bereichsübergreifenden Personenkennzeichen (2wPK) oder auf bereichsspezifischen Personenkennzeichen (bPK) aufgebaut werden. Das Kennzeichen dient zur eindeutigen Identifizierung aller erfassten Personen quer über die gesamte öffentliche Verwaltung (aPK), in wenigen klar angegrenzten Bereichen der Verwaltung (2wPK) oder in einem eindeutig umgrenzten Verwaltungsbereich (bPK). Da Identitätsnummernsysteme zum Umgang mit personenbezogenen Daten verwendet werden, bedürfen sie in der Bundesrepublik Deutschland stets einer gesetzlichen Grundlage.

Die Personenkennzeichen in einem Identitätsnummernsystem können zentral oder dezentral vergeben werden. Dies hängt davon ab, ob es eine einzige Vergabestelle oder mehrere Vergabestellen, etwa bei Ländern, Bezirken, Landkreisen, Städten oder Gemeinden, geben soll. Durch technische Maßnahmen ist sicherzustellen, dass jede Identitätsnummer nur ein einziges Mal an eine Person eindeutig vergeben werden darf.

Zur inhaltlichen Gestaltung des zentralen Personenkennzeichens eignen sich verschiedene Ansätze. Diese bedienen sich entweder einer Systematik oder einfach des Zufalls. Dazu kann auf bestehenden Systematiken, wie etwa der Steuer-ID oder anderen etablierten Personenkennzeichen, aufgesetzt werden, solange dies nicht gegen geltendes Recht verstößt. Es könnten auch vollkommen neue Identitätsnummern (NEU-ID) vergeben werden, systematisch oder durch Zufallszahlen generiert. Im letzten Fall muss unbedingt sichergestellt werden, dass bei allen Zufällen keine Zahl doppelt vergeben wird. Der gewählte Ansatz sollte zur Fehlervermeidung über eine integrierte Prüfziffer verfügen. Schließlich kann auf eine zentrale Identitätsnummer zur Identifizierung auch verzichtet werden.

Zur Identifizierung von Personen in den Registern kann auf die vorhandene Steuer-ID oder die bisherige Register-ID gesetzt werden. Zudem lassen sich mit einer Hashfunktion auf Basis einer Stammzahl neuartige bereichsspezifische Personenkennzahlen generieren (vgl. dazu Abschnitt D.III). Die Alternative eine Zufallszahl besteht auch hier.

Je nach Aufgabe und Aufgabenbereich wird die zu erfassende Personengruppe unterschiedlich sein: Staatsbürger, Ausländer, Steuerzahler, natürliche Personen oder juristische Personen kommen in erster Linie in Betracht. Dies muss im Gesetz genau geregelt sein.

Zu jedem Eintrag im Identifizierungsnummernsystem können Basisdaten vorgehalten werden, etwa im Bundeszentralamt für Steuern. Dies ist denkbar, wenn mit ihrer Hilfe die Daten-qualität in den angeschlossenen Registern verbessert, eine Registerbereinigung anvisiert oder eine Registerzentralisierung verfolgt werden soll. Ein solches Basisdatenregister könnte auch nur zeitlich begrenzt für die Dauer der Datenqualitätssicherung eingerichtet werden. Aus Gründen des Datenschutzes und der Datenminimierung könnte andererseits auch auf ein Basisdatenregister verzichtet werden.

Wird auf ein aPK verzichtet, so kann mit einer pseudonymisierten und ausschließlich von einem Intermediär nutzbaren ID-Datenbank eine vergleichbare Lösung auf Basis bereichsspezifischer Personenkennzeichen realisiert werden. Sie müsste aber besonders vor Angriffen geschützt werden.

Soll eine Registermodernisierung vorgenommen werden, bedarf es einer Registermodernisierungsbehörde. Andernfalls kann auf diese verzichtet werden.

Für Zugriffe von Behörden auf Register und Basisdaten kann für die Rolle eines vertrauenswürdigen Intermediärs sowohl auf die Registermodernisierungsbehörde (beim Bundesverwaltungsamt, BVA) als auch auf die Datenschutzaufsichtsbehörde gesetzt werden.

Berechtigte Anfragen könnten ohne Vermittlungsstelle direkt an die jeweiligen Behörden, über eine zentrale Vermittlungsstelle, einen Verbund an 1+16 Vermittlungsstellen oder einen Verbund bestehender Vermittlungsstellen kommen.

Berechtigte Anfragen auf die Basisdaten beim Bundeszentralamt für Steuern müssen stets mit einem Personenkennzeichen und einem Identifier für die anfragende Stelle verbunden sein. Vor einer Rückantwort sollte die Berechtigung zur Abfrage überprüft werden. In einem geschlossenen, vertrauenswürdigen System könnte ggf. darauf verzichtet werden. In einem offenen System kann auf bewährte softwarebasierte (Passwörter, Zertifikate) und hardware-basierte Schutzmechanismen (PKI-basierte Smartcard) gesetzt werden, was aus Gründen der Beschleunigung und des Bürokratieabbaus sinnvoll erscheint. Im Hintergrund könnten zudem Überwachungssysteme laufen, die automatisch alle Anfragen der Behörden dahingehend überprüfen, ob sie zulässig sind. Allerdings darf nicht vergessen werden, dass es sich um Abfragen personenbezogener Daten handelt. Daher könnten theoretisch auch qualifizierte Sachbearbeiter die

Prüfaufgabe übernehmen. Jedoch würde dies zu einer „Engstelle“ in den Abläufen führen und den gesamten Vorgang stark verlangsamen.

Vorstellbar wäre auch eine Einbindung der Bürger in all diese Freigabeprozesse. Vielleicht würde dies viele Bürger überfordern, bei einer Vielzahl von Abfragen im Rahmen der Qualitätssicherung und Registerkonsolidierung sogar verunsichern und den Freigabeprozess auch richtig lähmen. Andererseits kann es aber Fälle geben, in denen ein Zugriff ohne den Bürger nicht gewährt werden darf, weil der Grundrechtseingriff zu groß wäre, der Bürger dann aber doch und nur ausnahmsweise einer Behörde den Zugriff etwa auf seine Krankenversicherungsdaten erlaubt. Insofern kann eine anlassbezogene Freigabe von Daten durch den Bürger in einigen Fällen eine zweite Option sein. Aus Gründen des Büro-kratieabbaus wird die Verwaltung darauf setzen, Daten ohne Freigabe durch den betroffenen Bürger zu erhalten. Aus Gründen des Datenschutzes sollte der Zugriff stets protokolliert werden und für den Bürger über das Datencockpit nachverfolgbar sein.

B. Kurzanalyse zum Entwurf des Registermodernisierungsgesetzes

I. Morphologischer Kasten der Identitätsnummer des RegMoG-Eeme

Abb. 3 | Morphologischer Kasten zum Personenkennzeichen Steuer-ID

PK / ID-NR	AUSPRÄGUNGSFORMEN				
Einzigartigkeit	einzigartig			mehrfach vergeben	
Sichtbarkeit	nicht-sprechend			sprechend	
Ziffern oder Zeichen und Umfang des Zeichensatzes	numerische Ziffernreihenfolge (0-9)			alphanumerische Zeichenreihenfolge (0-9, A-Z, a-z)	
Prüfziffer	mit Prüfziffer			ohne Prüfziffer	
Typus von Personenkennzeichen	allgemeine Verwendung (aPK: wesentliche Bereiche)		bereichsübergreifende Verwendung (2wPK: 2 oder wenige Bereiche)		bereichsspezifische Verwendung (bPK: 1 Bereich)
Vorgehen bei der Vergabe	zentrale Vergabe			dezentrale Vergabe	
Zu erfassende Personengruppe	Deutsche Bürger	Ausländer	Steuerzahler	Natürliche Personen	Juristische Personen
Basisdatensatz	mit Basisdatensatz			ohne Basisdatensatz	

Der RegMoG-E setzt auf die Steueridentifikationsnummer (Steuer-ID) nach §§ 139a, b AO als Identitätsnummer. Diese Steuer-ID (Abbildung 3) ist ein einzigartiges, nicht-sprechendes Personenkennzeichen. Sie setzt sich aus 10 Ziffern plus einer Prüfziffer zusammen. Bisher wird sie als bereichsspezifisches Personenkennzeichen der Steuerverwaltung eingesetzt. Mit dem RegMoG-E würde sie zu einem allgemeinen Personenkennzeichen (mit allen Folgen) werden.

Die Steuer-ID wird zentral vom Bundeszentralamt für Steuern an alle potentiellen Steuerzahler vergeben, was alle deutschen Staatsangehörigen, alle Unionsbürger und alle weiteren Ausländer in Deutschland umschließt. Erfasst werden so alle natürlichen Personen. Die Basisdaten werden als Stammdaten zentral beim Bundeszentralamt für Steuern gespeichert.

II. Anwendung der DSGVO und rechtlicher Prüfungsmaßstab

Die Regelungen des RegMoG-E führen zur Verarbeitung personenbezogener Daten im Sinne von Art. 4 Abs. 1 Nr. 1, 2 DSGVO, sodass der sachliche Anwendungsbereich der DSGVO nach Art. 2 Abs. 1 DSGVO grundsätzlich eröffnet ist. Informationen wie Name und Geburtsort werden der Identifikationsnummer zugeordnet, sodass diese ein personen-bezogenes Datum darstellt.[19]

Der rechtliche Entscheidungsspielraum des deutschen Bundesgesetzgebers bemisst sich daher an den Regelungen des Grundgesetzes und des Rechts der Europäischen Union. Das BVerfG sieht sich, soweit die Grundrechte des Grundgesetzes durch den Anwendungsvorrang des Unionsrechts verdrängt werden, dazu berufen, dessen Anwendung durch deutsche Stellen am Maßstab der Unionsgrundrechte neben dem deutschen Verfassungsrecht zu prüfen.[20] Prüfungsmaßstab ist daher einerseits das deutsche Verfassungsrecht, andererseits aber auch das europäische Recht. Denn das RegMoG-E nutzt die Öffnungsklausel des Art. 6 Abs. 2 und Abs. 3 DSGVO sowie des Art. 87 DSGVO (vgl. dazu auch Abschnitt B.IV). Obwohl die DSGVO als Verordnung grundsätzlich direkt anwendbar ist und kein nationales Recht vorsieht, ermöglichen ausnahmsweise die Öffnungsklauseln mitgliedstaatliche Rechtsetzung im Anwendungsbereich der DSGVO. Somit sind deutsches und europäisches Recht in diesem nicht vollständig unionsrechtlich determinierten Bereich nebeneinander anzuwenden[21]. Dies gilt auch für das Verfassungsrecht.

III. Verfassungsrecht, insbesondere Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Bereits im Mikrozensus-Urteil von 1969 stellte das BVerfG fest, dass die zwangsweise Registrierung und Katalogisierung eines Menschen durch den Staat und die hieraus folgende Objektifizierung nicht mit der Würde des Menschen vereinbar ist.[22] Hierauf aufbauend entwickelte das BVerfG 1983 im Volkszählungsurteil[23] das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. In demselben Urteil spricht das Gericht an, dass ein „einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal", das die unbeschränkte Verknüpfung von erhobenen Daten mit Datenbeständen bei Behörden ermöglicht und zur Erstellung von Persönlichkeitsprofilen führt, verfassungswidrig wäre.[24] Grundsätzlich schützt das Recht auf informationelle Selbstbestimmung vor jeder staatlichen Erhebung und Verarbeitung personenbezogener Daten,[25] ermöglicht aber zur Wahrung überwiegender verfassungsrechtlicher Werte eine Rechtfertigung von Eingriffen.

1. Einstufung und Zulässigkeit eines allgemeinen oder bereichsspezifischen Personenkennzeichens

Den soeben geschilderten Ausführungen des BVerfGs[26] zu Personenkennzeichen wird ein generelles Verbot von Personenkennzeichen nicht entnommen.[27] Vor diesem Hintergrund unterscheidet die Literatur zwischen *allgemeinen* und *bereichsspezifischen* Personenkennzeichen.[28] Danach sind allgemeine Personenkennzeichen als grundsätzlich verfassungswidrig einzustufen. Denn sie würden die vom BVerfG ausdrücklich erwähnte, abzulehnende Zusammenführung der bei den Verwaltungsbehörden vorhandenen Datenbeständen ermöglichen. So sieht etwa der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) die Einführung eines zentralen Personenkennzeichens an sich als verfassungswidrig an[29], hält dagegen den Einsatz von bereichsspezifischen Kennzeichen mit entsprechenden technischen Sicherheitsvorkehrungen aber für grundsätzlich möglich.[30]

Die Identifikationsnummer in ihrer gegenwärtigen Form ist ein bereichsspezifisches Personenkennzeichen.[31] Auch der Bundesfinanzhof urteilte 2012, dass die Identifikationsnummer nach § 139a AO zumindest zu jenem Zeitpunkt verfassungsrechtlichen Ansprüchen genüge.[32] Hierbei unterstreicht die Urteilsbegründung, dass die Identifikationsnummer nur zu steuerlichen Zwecken verwendet werden darf, sodass die genannten Bedenken gegenüber einem allgemeinen Personenkennzeichnen hier nicht zum Tragen kamen.[33] Der Hinweis in der Begründung des Gesetzentwurfs auf die höchstrichterlich bestätigte Verfassungskonformität der Steueridentifikationsnummer als Grundlage für die Reform[34] ist insofern nicht zutreffend.[35]

Nach dem IDNrG-E soll die Identifikationsnummer nunmehr bei über 50 Registern als zusätzliches Ordnungsmerkmal eingetragen werden. Zwar konnten 2017 bundesweit 214 verschiedene Register verzeichnet werden[36]; die vom Entwurf betroffenen Register entstammen jedoch unterschiedlichsten Lebensbereichen, z.B. den Versicherungskonten der Rentenversicherungsträger, der Grundsicherung für Arbeitssuchende, der gesetzlichen Unfallversicherung, der Fahreignung, der Handwerksrolle, den allgemeinbildenden und beruflichen Schulen/Ausbildungswesen, dem Waffenregister, der Gewährung von Elterngeld, Insolvenzen, Aufenthaltsberechtigungen oder auch dem Liegenschaftskataster. Selbst § 7 Abs. 2 IDNrG-E geht von einer Einteilung in zumindest sechs unterschiedliche Verwaltungsbereiche aus.[37]

[19] *Martini/Wagner/Wenzel* 2017, S. 5 m.w.N; Wiss. Dienst BTag 2020, Gutachten, S. 5 f.
[20] BVerfG NJW 2020, 314 (1. Leitsatz).
[21] Vgl. BVerfG NJW 2020, 300 Rn. 41 f.
[22] BVerfGE 27, 1, 6.
[23] BVerfGE 65, 1 ff.
[24] BVerfGE 65, 1, 53.
[25] *Di Fabio*, in: Maunz/Dürig 2020, Art. 2 f., Rn. 176.
[26] BVerfGE 65, 1, 53.
[27] *Martini/Wagner/Wenzel* 2017, S. 30.
[28] *Martini/Wagner/Wenzel* 2017, S. 30 f. m.w.N.; der gleichen Einteilung folgt *Wiss. Dienst* BTag, Gutachten, S. 14 ff.
[29] *BfDI* 2020, S. 4.
[30] Vgl. *BfDI* 2020, S. 8
[31] Vgl. *Martini/Wagner/Wenzel* 2017, S. 30 f.
[32] *BFH* 2012, Urt. v. 18.1.2012 – II R 49/10.
[33] *Humanistische Union* 2020, S. 8 mit Verweis auf BFH, Urteil vom 18.1.2012 – II R 49/10 Rn. 59 ff.
[34] RegMoG-E, S. 72.
[35] *BfDI* 2020, S. 7, Humanistische Union 2008, S. 8.
[36] *Statistisches Bundesamt* 2017, S. 4.
[37] Beispielhaft genannt werden Inneres, Justiz, Wirtschaft und Finanzen, Arbeit und Soziales, Gesundheit, Statistik, RegMoG-E, S. 81.

Jedenfalls kann ein allgemeines Kennzeichen nicht nur dann vorliegen, wenn alle oder ein Großteil der nationalen Register das Kennzeichen als zusätzliches Ordnungsmerkmal aufnehmen müssen. Ein rein quantitativer Maßstab führt zu großem Missbrauchspotential, da bestimmte Register gezielt ausgelassen werden könnten, um den höheren verfassungsrechtlichen Maßstab zu umgehen. Umgekehrt ist ein allgemeines Personenkennzeichen nicht bereits dann gegeben, wenn mehr als ein Bereich erfasst ist. Sobald allerdings – wie vorliegend – eine Vielzahl von wesentlichen Lebensbereichen über eine gemeinsame Personenkennziffer verknüpft wird, ist von einem allgemeinen Kennzeichen auszugehen.[38] Demnach wäre deren Erweiterung, wie im RegModG-E vorgesehen, grundsätzlich als sehr problematisch anzusehen.

Als alternative Lesart wird teilweise vertreten, dass das BVerfG – insbesondere vor dem Hintergrund der Strahlkraft des Urteils – nur die Profilbildung als solche ausschließen wollte.[39] Verfassungswidrig seien vielmehr die Verknüpfungsmöglichkeiten personenbezogener Daten, die sich aus der Einführung eines Personenkennzeichens ergeben.[40] Ferner seien heutzutage durch den technischen Fortschritt viele weitere Möglichkeiten zur Profilbildung ohne weiteres verfügbar, sodass sich die Frage stellt, ob ein Verbot eines Personenkennzeichens überhaupt diesen Zweck erreichen kann. Sinnvoller sei hingegen die Erörterung technischer und organisatorischer Mittel, welche die Gefahren aus der Profilbildung reduzieren können.[41] Aber auch nach dieser Auffassung sind die Grenzen, die das BVerfG aufgezeigt hat, überschritten. Denn die Breite der verknüpften Register und damit die Abrufmöglichkeiten der darüber erschließungsfähigen Daten dringen in den Bereich der Profilbildung vor. Diese wird von der DSGVO an verschiedenen Stellen als eine besonders problematische Datenverarbeitung mit hohen Risiken eingestuft.[42]

Die weiter unten (Teil D) vorgeschlagenen Alternativen schränken zwar die Abrufmöglichkeiten per se nicht ein; dies wäre der wirkungsvollste Schutz. Sie erschweren aber die Umgehung des vorgesehenen Prozesses und damit eine zu Lasten des Bürgers wirkende Verknüpfung der Daten ohne Zweckbindung und Kontrollmöglichkeit. Damit wird auch der Missbrauch durch Dritte und auch ein Identitätsdiebstahl erschwert, wie er beispielsweise in Staaten mit allgemeinen Personenkennzeichen wie den USA mit der Social Security Number vorkommt und dort eine große Gefahr darstellt.

2. Verfassungswidrigkeit der Ermächtigung zum Erlass einer Rechtsverordnung in § 7 Abs. 2 S. 2 IDNrG-E

Für Datenübermittlungen zwischen öffentlichen Stellen verschiedener Bereiche sieht § 7 Abs. 2 S. 2 IDNrG-E i.V.m. § 12 Abs. 1 Nr. 2 eine Rechtsverordnungsermächtigung zugunsten der Bundesregierung vor. Rechtsverordnungen unterliegen gemäß Art. 80 Abs. 1 S. 2 GG erheblichen Anforderungen, um der damit verbundenen Delegation von gesetzgeberischen Aufgaben an die Exekutive und damit einer verfassungsrechtlich unerwünschten Durchbrechung des Gewaltenteilungsprinzips nach Art. 20 Abs. 3 GG entgegenzuwirken; das Wesentlichkeitsprinzip dient also der negativen Kompetenzabgrenzung.[43] Die Beantwortung der (politischen) Kernfrage, ob die Verwaltung handeln darf, liegt beim Gesetzgeber. Grundsätzlich gilt, dass der Gesetzgeber *„alle Fragen, die für die Ausübung der Grundrechte wesentlich sind, unabhängig davon, ob im konkreten Fall Freiheitsrechte oder Gleichheitsrechte betroffen sind“*, selbst zu regeln hat.[44]

Die Einführung einer Personenkennziffer für alle Bürger und Steuerzahler, wie vom RegMoG-E vorgesehen, berührt in erheblicher Weise das Recht auf informationelle Selbst-bestimmung und ist vom BVerfG kritisch beurteilt worden[45].

Die Einordnung von Datenbeständen in Bereiche i.S.d. RegMoG-E hat erhebliche Auswirkungen auf das Verfahren der Datenübermittlung und die Möglichkeit des Rechtsschutzes für betroffene Bürger, zumal nach § 7 Abs. 2 S. 7 IDNrG-E die Datenübermittlung innerhalb von Bereichen privilegiert verlaufen soll. Erfolgt also eine – grundsätzlich zulässige – Delegation der näheren Ausgestaltung nach Art. 80 Abs. 1 S. 2 GG, muss der Gesetzgeber in besonderem Maße Inhalt, Zweck und Ausmaß vorgeben. Dies ist aber nicht der Fall. Weder hat der Gesetzgeber vorgeben, welche Kriterien zur Bestimmung von Bereichen herangezogen werden sollen, noch hat er die Zahl bestimmt (lediglich die Untergrenze von sechs Bereichen ist benannt), noch hat er vorgegeben, welche Zielsetzung mit der Bereichs-aufteilung einhergehen soll. Die Rechtsverordnungsermächtigung nach § 12 Abs. 1 Nr. 2 IDNrG-E erwähnt allerdings allein Anzahl und Abgrenzung.

Ebenfalls verstößt die Verordnungsermächtigung in § 12 Abs. 3 IDNrG-E gegen Art. 80 Abs. 1 S. 2 GG. Danach kann „das jeweils zuständige Bundesministerium“ das Verfahren nach § 7 Abs. 2 IDNrG-E auch für Datenübermittlungen innerhalb eines Verwaltungsbereichs bestimmen. Dem lässt sich entnehmen, dass der Gesetzgeber davon ausgeht, dass Verwaltungsbereiche sich einem Bundesministerium zuordnen lassen. Allerdings – wie etwa der Zuschnitt des Bundes-

[38] Im Ergebnis ebenso BfDI, 2020, S. 8; wohl auch Humanistische Union 2020, S. 7 f.; Wiss. Dienst BTag, 2020, Gutachten, S. 16 f. nimmt zwar ein allgemeines Personenkennzeichen an, trifft jedoch keine verbindliche Aussage zu dessen Zulässigkeit.
[39] *Martini/Wagner/Wenzel* 2017, S. 31 ff.
[40] *Martini/Wagner/Wenzel* 2017, S. 31
[41] *Hornung* 2005, S. 161 f.; ebenso Martini/Wagner/Wenzel 2017, S. 33.
[42] *Scholz*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art.4 Nr. 4, Rn. 1.
[43] Vgl. *Voßkuhle*, JuS 2001, 118 f.
[44] Vgl. BVerfGE 47, Rn. 99.
[45] Siehe oben Einstufung und Zulässigkeit eines allgemeinen oder bereichsspezifischen Personenkennzeichens.

ministeriums des Innern, für Bau und Heimat illustriert – ändern sich zum einen Zuständigkeiten von Bundesministerien, zum anderen sind sie oft so breit aufgestellt, dass man nicht von lediglich einem Bereich ausgehen kann. Das Baurecht und das Sicherheitsrecht sind nach grundständigem Verständnis unterschiedliche Verwaltungsmaterien; nach welchen Kriterien hier ein Verwaltungsbereich angenommen werden soll, bleibt offen und verstößt damit – auch unter Bestimmtheitsanforderungen nach Art. 20 Abs. 3 GG – gegen das Grundgesetz.

3. Verhältnismäßigkeit eines Eingriffs in Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG

Folgt man der Ansicht nicht, dass die Einführung eines allgemeinen Personenkennzeichens bereits grundsätzlich als verfassungswidrig einzustufen ist, wäre der Eingriff in das allgemeine Persönlichkeitsrecht in der Ausprägung des Rechts auf informationelle Selbstbestimmung gem. Art. 2 Abs. 1, Art. 1 Abs. 1 GG jedenfalls unverhältnismäßig.

a) Legitimes Ziel und seine Bedeutung

Das RegMoG-E soll die Funktions- und Leistungsfähigkeit sowie die Effektivität der Verwaltung verbessern und in Vorbereitung des sogenannten Once-Only-Prinzips auch zu einer Entlastung und Vereinfachung der Bürger in der Kommunikation mit der Verwaltung führen.[47] Ferner soll ein registerbasierter Zensus ermöglicht werden.[48]

Wie eingangs geschildert, gehen die Ziele allerdings noch deutlich darüber hinaus. Mittel- und langfristig ist mit dem RegMoG-E der erste Schritt zu gänzlich neuartigen Governance-Modellen eröffnet, die allerdings ganz erheblichen verfassungsrechtlichen Bedenken begegnen, auch wenn sie sich im Gewand der Kosteneinsparung, des bürgernahen schlanken Staats und der Effizienzgewinne präsentieren.[49] Deutlich wird dies unmittelbar über § 16 IDNrG-E, in dem weitere Ziele bekannt gemacht werden: Damit wird ersichtlich auch eine Verbreiterung des Datenaustauschs nicht nur innerhalb der Verwaltung und mit dem Bürger angestrebt, sondern eine breite Verwendung der Identifikationsnummer – letztlich auch für den privaten Bereich.

Hierbei handelt es sich im geschilderten ersten Schritt von Kosteneinsparung, Vereinfachung von Verwaltungsvorgängen und Zensusermöglichung um legitime Ziele der Effektivität der Verwaltung, der Akzeptanzsteigerung der Kommunikation zwischen Bürger und Staat und der Vereinfachung und Anpassung von Verwaltungsvorgängen. Diese Ziele können allerdings kein sonderlich großes Gewicht beanspruchen; sie sind verfassungsrechtlich nicht geboten und werden von Schutzpflichten, die von Grundrechten ausgehen, nicht erfasst. Europarechtlich mag in einzelnen Fällen die Nutzung von bereichsspezifischen Personenkennziffern vorgegeben sein; eine allgemeine, dem Anwendungsvorrang unterfallende Verpflichtung zur Einführung einheitlicher Personenkennzeichen lässt sich aber daraus nicht ableiten.

Es ist durchaus sehr zweifelhaft, ob die dahinterstehenden weitreichenden Ziele des Once-Only- und des No-Stop-Governments mit einem demokratischen freiheitlichen Rechtsstaat überhaupt in Einklang gebracht werden können angesichts der damit einhergehenden Machtverschiebungen, Verletzung der Kernelemente von Persönlichkeits- und Datenschutzrechten sowie Standardisierung mit Aufgabe von Minderheitenschutz.[50]

b) Geeignetheit und Erforderlichkeit

Eine Personenkennziffer, wie vom RegMoG-E vorgesehen, steigert auch die Wahrscheinlichkeit der Verwirklichung dieser eben skizzierten begrenzten Ziele des ersten Schritts und ist daher geeignet.

Hinsichtlich eines gleich effektiven, milderen Mittels stellen sich allerdings erhebliche Zweifel, gibt es doch weitere Alternativen, die weniger eingriffsintensiv eine Verwaltungsmodernisierung im Registerwesen voranbringen.

Das RegModG-E verfolgt ein Konzept des 4-Corner-Modells mit „doppeltem Umschlag". Die weiterleitende Stelle nach § 7 IDNrG-E kann also die Inhalte nicht zur Kenntnis, sondern lediglich die Metadaten, die zur Erfüllung der Vermittlung erforderlich sind. Dadurch, dass solche Zwischenstellen vorgesehen sind, ist für die registerführenden Behörden eine gemeinsame Identifikationsnummer – wie sie das RegModG-E einführen soll – nicht erforderlich. Dies gilt umso mehr, als technische Ausgestaltungsmöglichkeiten weitere Beschränkungen erlauben, ohne die Funktionalität einzuschränken.[51]

So lässt sich auf das österreichische Modell des zentralen Identitätsmanagements bei Behörden verweisen, ohne hier in Details zu gehen:[52] In Österreich wird jeder natürlichen Person eine sog. „Stammzahl" zugeordnet, die allerdings nur einer einzigen zentralen Instanz, der Stammzahlenregisterbehörde[53], vorliegt. Diese Stammzahl wird jedoch mit keinen weiteren personenbezogenen Daten verknüpft. Anhand dieser Stammzahl werden mittels eines Algorithmus bereichsspezifische Kennzahlen erstellt, die von den jeweiligen Fachregistern aufbewahrt werden. Möchte eine Behörde Daten von einer anderen Behörde abrufen, schickt sie ihre bereichsspezifische Kennzahl in verschlüsselter Form an die Stammzahlenregisterbehörde. Diese wiederum stellt die bereichsspezifische Kennzahl der anderen Behörde in verschlüsselter Form zur Verfügung. Mit beiden Kennzahlen kann die abfragende Behörde nun die Daten bei der anderen Behörde beantragen.

[46] Dazu gleich noch unten unter B.3.c)(5).
[47] Vgl. RegMoG-E, S. 37 und S. 70.
[48] RegMoG-E, S. 70 f.
[49] Siehe dazu auch noch unten unter B.3.c)(5).
[50] Siehe dazu noch unten unter B.3.c)(5).
[51] Siehe dazu unten Teil D.
[52] Siehe dazu unten Teil D.
[53] Bis 28.12.2018 war dies die Datenschutzbehörde der Bundesrepublik Österreich. Nun ist das Bundesministerium für Digitalisierung und Wirtschaftsstandort die neue Stammzahlenregister-behörde, vgl. https://www.dsb.gv.at/aufgaben-taetigkeiten/stammzahlenregisterbehoerde.html.

Bei der Übertragung der Daten schickt die andere Behörde die verschlüsselte Kennzahl der ersten Behörde mit, damit diese die Daten zuordnen kann. Zu keinem Zeitpunkt erlangt eine der beiden Behörden Kenntnis über die (unverschlüsselte) bereichsspezifische Kennzahl der anderen Behörde.[54] Ein solches Vorgehen kann die zuvor benannten Risiken der staatlich veranlassten Profilbildung und eines ungehinderten Zugriffs auf Bürgerdaten deutlich reduzieren; es ist gleich geeignet und somit ein milderes Mittel.

Das RegMoG-E geht in der Begründung zwar auf das österreichische Modell ein, lehnt dieses jedoch aufgrund „größerer rechtlicher, technischer und organisatorischer Komplexität" und den außerordentlichen Kosten- und Zeitaufwand ohne weitere Nachweise ab.[55] Die Überzeugungskraft dieses Arguments ist fraglich: Es besteht (mit dem österreichischen Modell) bereits im deutschsprachigen Raum ein funktionierendes, weniger eingriffsintensives Instrument, das angesichts digitalisierter Abläufe schnell und effektiv eingesetzt werden kann. Die Datenschutzkonferenz (DSK) hat daher zu Recht dazu aufgefordert, ein solches Modell für Deutschland ernsthaft zu prüfen.[56]

Zudem zeigt das vorliegende Gutachten im Folgenden eine Reihe von Alternativen auf und entwickelt einzelne davon in Tiefe und Breite.[57] Diesen lässt sich entnehmen, dass die vom Gesetz vorgesehene Einführung einer Identifikationsnummer nicht alternativlos ist, sondern vielmehr die Ziele des Gesetzgebers auch auf anderen, weniger eingriffsintensiven Wegen erreicht werden können.

c) Angemessenheit

Sollten die vorgestellten Alternativen trotzdem als weniger effektiv erachtet und damit die Erforderlichkeit des im Gesetzesentwurf vorgesehenen deutschen Wegs des RegMoG-E bejaht werden, wäre auch die Angemessenheit kritisch zu betrachten.[58] Tatsächlich sprechen gute Gründe dafür, davon auszugehen, dass eine zentrale Identifikationsnummer den verfassungsrechtlichen Test der Angemessenheit nicht besteht.

Im Rahmen der Angemessenheit erfolgt eine Abwägung zwischen der Schwere des Eingriffs in die Grundrechte, allen voran in das Recht auf informationelle Selbstbestimmung, und der Intensität des verfolgten Ziels. Dabei kann der Gesetzgeber Ausgleichsmaßnahmen vorsehen, mittels derer die eigentliche Schwere des Eingriffs abgemildert und somit die Interessenabwägung zugunsten der Verwirklichung des Ziels verschoben wird.

(1) Eingriffsintensität in das Recht auf informationelle Selbstbestimmung

In seiner Rechtsprechung hat das BVerfG verschiedene Parameter festgelegt, die zur Bestimmung der Eingriffsintensität in das Recht auf informationelle Selbstbestimmung herangezogen werden können. Allen voran bemisst sich die Schwere eines Eingriffs an Art bzw. Qualität, Umfang bzw. Quantität, Verwendung bzw. Kontext und Missbrauchspotenzial bzw. negativen Konsequenzen der Daten und ihrer Verarbeitung.[59]

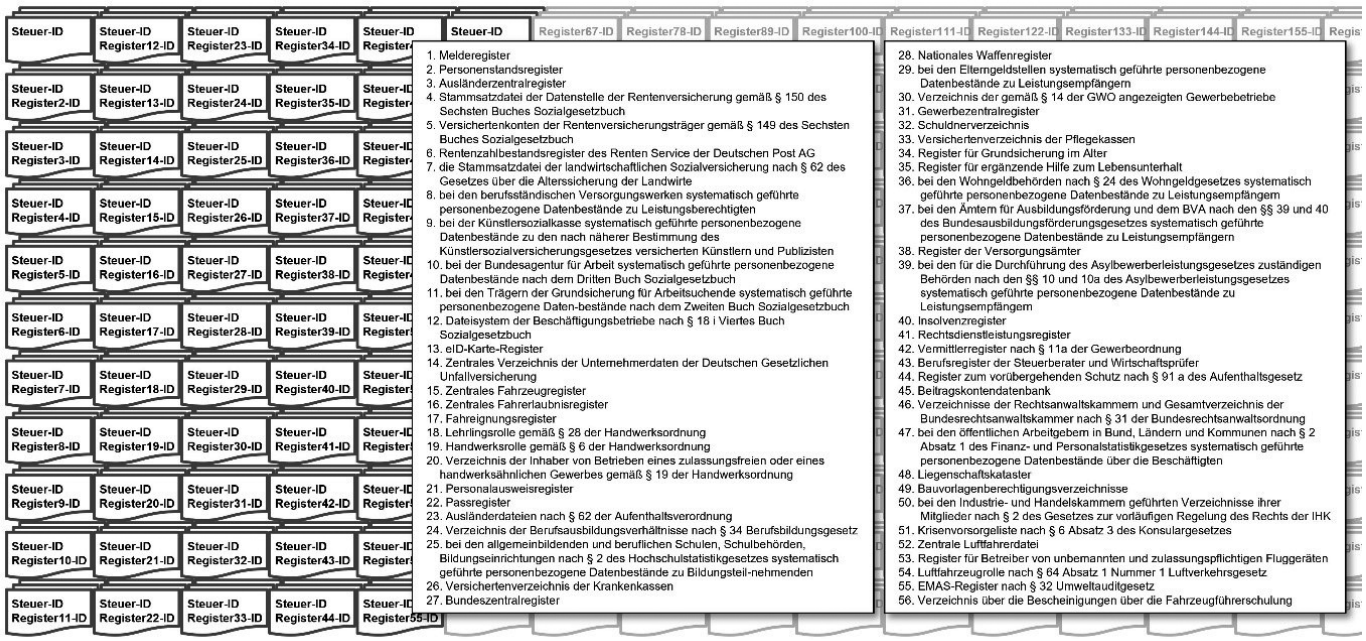
Der Umfang des Eingriffs durch die Anwendung auf die schon jetzt über 50 im Anhang des IDNrG-E gelisteten Register aus verschiedensten Lebensbereichen ist beträchtlich. Die Verwendungsbereiche könnten mit einfachem Gesetz auch erweitert werden. Neuartige Register ließen sich mühelos aufbauen und integrieren. So könnte zukünftig auch der Datenbestand und die Pseudonyme des Forschungsdatenzentrum erschlossen werden, das über § 303d Digitales Versorgungsgesetz (DVG) für wesentliche Daten aller gesetzlich Versicherten eingerichtet werden soll.[60] Die Quantität der damit verarbeitbaren und zugänglichen Daten ist uferlos groß.

Auch der betroffene Personenkreis ist als außerordentlich groß einzustufen: Gemäß § 139a Abs. 1 S. 1 AO in Art. 3 RegMoG-E betrifft dies künftig alle Steuerpflichtigen und jede sonstige natürliche Person, die bei einer öffentlichen Stelle ein Verwaltungsverfahren führt. Durch diese Regelung ist von einer Zuteilung der Identifikationsnummer an nahezu alle natürlichen Personen auf Bundesgebiet auszugehen. Ein quantitativ größerer Eingriff ist kaum vorstellbar; er entspricht dem Personenkreis, den das BVerfG in den Volkszählungs- und Mikrozensusurteilen betrachtet und als zu weitreichend beurteilt hat.

Alleine die Möglichkeiten, die dadurch entstehen, innerhalb von Minuten mit einem handelsüblichen Laptop die Daten von mehr als 83 Millionen Bürgern und Steuerpflichtigen schon jetzt aus 57 Registern verknüpfen und dann mit gezielten Anfragen auswerten zu können, sind nicht mehr überschaubar, geschweige denn vorhersehbar, und können kaum gerechtfertigt werden.

[54] Vgl. zu diesem Absatz Ausführungen und Schaubild von Nationaler Normenkontrollrat 2017, S. 42 f.; für weitere Details, insbesondere in rechtlicher Hinsicht s. *Martini/Wagner/Wenzel* 2017, S. 36 ff.
[55] Vgl. RegMoG-E, S. 38
[56] *DSK* 2020, S. 2.
[57] Siehe unten Teil D.
[58] Vgl auch *Wiss. Dienst BTag* 2020, Gutachten, S. 22: „offen".
[59] Vgl. BVerfG NJW 2020, 2699, 2707.
[60] Siehe oben Abschnitt A.II

Abb. 4 | Gesamtüberblick der künftig über die Steuer-ID erschließbaren Register



Zusätzliche Sorge bereitet der Drang vieler Software- und Plattformanbieter, ihre Software cloud-basiert als Service über eine Plattform anzubieten und gleichzeitig ihre Kunden zu einer Öffnung ihrer Datenbestände zu drängen. Sollte eine Behörde in Zukunft, etwa für eine komplexe KI-basierte Analyse von personenbezogenen Datenbeständen, die weltweit nur ein einziger Anbieter beherrscht, Dritten einen Zugang zu ihren bisher geschützten Registern eröffnen müssen, lassen sich auch diese Folgen nicht mehr überschauen. Ein solcher Dienst könnte selbst zu wesentlichen neuen Erkenntnissen auf Grundlage der allgemeinen Personenkennzeichen gelangen und künftig immer wieder gezielt nach dem Personenkennzeichen suchen. Vielleicht sähe ein solcher Algorithmus es sogar als erforderlich an, sich Kopien aller relevanten Datensätze mit den Personenkennzeichen anzufertigen, um noch bessere Ergebnisse zu erzielen. Zumindest hätten ausländische Nachrichtendienste, in deren Staaten solche Anbieter ansässig sind, ebenfalls ein großes Interesse an diesen Beständen. Gerade für den Bereich der Inneren Sicherheit lässt sich nicht dauerhaft ausschließen, dass einige verantwortliche Stellen entsprechende Analysedienste nutzen werden.[61]

Die Intensität eines Eingriffs nimmt insbesondere mit der Möglichkeit von Folgeeingriffen und anderen Maßnahmen, die aus der Verknüpfung von Datensätzen resultieren, zu.[62] Zwar sind die zu übermittelnden Daten in § 4 Abs. 2 und 3 IDNrG-E grundsätzlich begrenzt; die potentielle Verbindung mit den Daten aus den verschiedenen Registern führt jedoch zu einem höheren Risiko. Insbesondere das Datum des letzten Verwaltungskontakts gemäß § 4 Abs. 3 Nr. 2 kann zur Gefahr eines übergreifenden Trackings und einer Profilbildung durch die Behörden führen.[63] Daher ist, sollte man der oben genannten Ansicht folgen, dass das BVerfG im Volkszählungsurteil nicht generell gegen allgemeine Personenkennzeichen entschieden hat, sondern lediglich einer Profilbildung entgegenwirken wollte, jedenfalls darüber die Schwelle der Zulässigkeit nach dieser Rechtsprechung überschritten.

Dies gilt erst recht, weil die Registermodernisierungsbehörde im Rahmen ihrer Aufgaben auch Qualitätssicherung der Datenbestände vorsehen soll. Dazu erfolgt gem. § 7 Abs. 1 S. 2 IDNrG-E eine Prüfung auf Vollständigkeit und Schlüssigkeit, ohne dass hierfür eine vergleichbare Regelung wie bei Datenübermittlungen unter Nutzung der Identifikationsnummer nach § 7 Abs. 2 IDNrG-E durch Vermittlungsstellen vorgesehen ist – nämlich dass dies ohne Kenntnis der Nachrichteninhalte erfolgen soll, also nach dem 4-Corner-Modell mit doppeltem Umschlag. Selbst wenn man davon ausgehen sollte, dass dies auch für Abs. 1 vorgesehen ist, ist die Bedeutung dieser Schutzmaßnahme so gewichtig, dass der Gesetzgeber sie hätte vorsehen müssen, um deren Anwendung auch in der Registermodernisierungsbehörde sicherzustellen.[64] Denn mit der Möglichkeit der Kenntnisnahme von allen Abfragen entsteht auf Meta- und Inhaltsebene eine erhebliche Gefahr für eine Profilbildung über Bürger.

Weitere Kriterien der Rechtsprechung zur Beurteilung der Eingriffsintensität sind die Veranlassung eines Eingriffs bzw. ein Vorkontakt.[65] Im Gegensatz zur Auffassung des *Wissenschaft-*

[61] Vgl. oben Abschnitt A.II
[62] BVerfG NJW 2008, 1505, 1508.
[63] Vgl. GI 2020, S. 6.
[64] Auf die Sicherheitsmaßnahmen gehen wir in Teil D erneut ein.
[65] Vgl. BVerfG NJW 2020, 2699, 2707.

lichen Dienstes des Bundestages[66] kann es aber vorliegend keinen Unterschied hinsichtlich Eingriffsintensität zwischen einem durch eine Bürgerin angestoßenen Verwaltungsverfahren und der Prüfung der Register ohne Anlass durch diesen selbst geben. In vielen Lebensbereichen (bspw. beim Führen eines KFZ oder dem Erwerb einer Immobilie) ist wegen des gesetzlichen Erlaubnisvorbehalts ein Verwaltungskontakt notwendig, um individuelle Freiheiten auszuüben. In solchen Fällen gibt es keine Möglichkeit, den Eingriff zu verhindern; insbesondere ist keine Opt-out-Möglichkeit vorgesehen. Insofern ist die Annahme eines weniger intensiven Eingriffs hier verfehlt. Zudem fehlt es gerade an der zurechenbaren Veranlassung: Die Steuer-ID wird bereits für Kinder mit der Geburt vergeben, ohne dass eine Steuerpflicht vorliegt.

Hinsichtlich der intensitätserhöhenden Heimlichkeit[67] des Eingriffs ist zwar positiv hervorzuheben, dass mit dem Datencockpit nach § 10 OZG-E eine Möglichkeit des Bürgers geschaffen wird, sämtliche Eingriffe nachzuvollziehen. Dennoch ist der eigentliche Eingriff zunächst ohne Kenntnis des Betroffenen möglich und vorgesehen. Sollte es zu einer missbräuchlichen Verwendung der Identifikationsnummer kommen, ist eine Feststellung und das Ersuchen von Rechtsschutz nur im Nachgang möglich. Dies ist bei Informationen zusätzlich problematisch, da hier ein zwangsweises Vergessen kaum möglich ist und daher Eingriffe grundsätzlich irreversibel sind. Bei einer rein nachträglichen Kontrolle ist auch zu beachten, dass die Hemmschwelle zur Nachprüfung seitens betroffener Bürger steigen könnte.

Der RegMoG-E berücksichtigt zudem nicht, dass für einzelne Personen besondere Anforderungen an den Schutz aus persönlichkeitsrechtlichen, betriebsspezifische oder auch, lebens- und gesundheitsrechtlichen Gründen bestehen können. In diversen Registern besteht daher die Möglichkeit von Sperrvermerken, für deren Übernahme in die neu geschaffenen Verfahren keine Vorkehrungen getroffen sind.[68]

Schließlich werden schon über die Basisdaten auch besondere Kategorien personenbezogener Daten i.S.v. Art. 9 DSGVO (Sterbetag, § 4 Abs. 2 Nr. 10 IDNrG-E) oder Art. 3 I GG (Geschlecht, § 4 Abs. 2 Nr. 7 IDNrG-E) zugeordnet und gespeichert, denen ein besonderes Diskriminierungspotential innewohnt. Über die Verknüpfung mit den diversen Registern erfolgen zudem Zugriffe auf weitere besondere Daten, mindestens über die Register nach Nr. 2., 4.-12. sowie 29. und 33.-35. Schließlich sind eine Reihe der in den Registern vorgehaltenen und über die Identifikationsnummer erreichbaren Daten in besonderer Weise als persönlichkeitsrelevant einzustufen, weil sie essentielle, üblicherweise von besonderen Geheimhaltungsverpflichtungen wie dem Sozialgeheimnis erfasste Informationen über das Leben der Bürger offenbaren können.

(2) Zweckbindung

Verpflichtet der Gesetzgeber Behörden dazu, Datenbestände anzulegen, muss er das verfassungsrechtlich bedingte Gebot der Zweckbindung beachten.[69] Der Gesetzgeber ist zudem verpflichtet, durch ergänzende Folgeregelungen festzustellen, dass eine Erweiterung der Verwendungsmöglichkeiten unter Umgehung des Zweckbindungsgebots nicht stattfindet.[70] Wie der Entwurf eine solche schleichende Erweiterung der Anwendungsbereiche der Identifikationsnummer verhindern will, ist unklar. Ohne weiteres können weitere Register verknüpft werden. Als schlechtes Vorbild dient ausgerechnet die Steueridentifikationsnummer selbst, bei deren Einführung ausdrücklich versichert wurde, dass eine Ausweitung auf andere Lebensbereiche nicht stattfinden würde.[71] Angesichts einer strengen Zweckbindung ist auch nicht ausreichend, dass das IDNrG-E als solches in § 5 Abs. 1 Nr. 1 und 2 lediglich Zuteilung und Abruf der Daten vorsieht. Genauso ist der Verweis in § 6 Abs. 2 IDNrG-E auf andere Rechtsgrundlagen für Verarbeitungen anhand der Identifikationsnummern dem Maßstab des BVerfG nicht angemessen. Die mangelnde Zweckbindung führt dazu, dass auch Private die Identifikationsnummer verwenden können.[72] Daher sollte der Entwurf die privatwirtschaftliche Nutzung der Identifikationsnummer ausdrücklich verbieten, um einer Profilbildung durch Unternehmen vorzubeugen.[73]

Verstärkend kommen noch die besonderen Bindungen der Steuerverwaltung hinzu. Sie darf für ihre Besteuerungsverfahren keine allgemeinen Personenkennzeichen verwenden. Ein angenommener Gesetzesentwurf würde damit auch die Grundlagen der Steuererhebung zerstören und unerwünschte Folgewirkungen für die Finanzierung des Staates auslösen.[74]

Dass ein gesetzliches Verbot der Verknüpfung eines Kennzeichens mit anderen Datenbeständen oder Kennziffern durchaus auch ausdrücklich gesetzlich festgeschrieben werden kann, zeigt die Regelung zur Krankenversichertennummer.[75] Bereits bei deren Einführung bestand die Befürchtung, dass eine Verknüpfung mit der Rentenversicherungsnummer zum Entstehen eines unzulässigen Personenkennzeichens führen könnte.[76] Aus diesem Grund erließ der Gesetzgeber die Regelung in § 290 Abs. 1 S. 4 SGB V, die eine Verbindung der beiden Nummern explizit verbietet.

(3) Unbestimmter Missbrauchsschutz

Einer missbräuchlichen Verwendung der Daten trägt das IDNrG-E durch Strafvorschriften in § 17 IDNrG-E und technischen Schutzvorkehrungen in § 7 Abs. 2 IDNrG-E in gewissem Umfang Rechnung.[77] Allerdings spezifiziert § 8 Abs. 2 S. 1 IDNrG-E nicht, welche technischen und organisatorischen Maßnahmen die Registermodernisierungsbehörde zu ergreifen hat, und auch die abrufende Stelle wird nach

[66] Wiss. Dienst BTag, Gutachten, S. 21.
[67] BVerfG NJW 2020, 2699, 2707.
[68] BRat 2020, S. 10 ff.
[69] BVerfG NJW 2020, 2699, 2708.
[70] BVerfG NJW 2020, 2699, 2708.
[71] Vgl. *Schaar*, ZD 2011, 49.
[72] *Wiss. Dienst BTag* 2020, Gutachten S. 21.
[73] Vgl. auch *DAV* 2020, S. 5.
[74] Siehe auch *BRat* 2020, S. 2
[75] Vgl. *Hornung* 2005, S. 162.
[76] *BfDI* 2004, S. 165.
[77] *Wiss. Dienst BTag* 2020, Gutachten, S. 21.

§ 8 Abs. 2 S. 2 IDNrG-E nur unbestimmt verpflichtet sicherzustellen, dass nur befugte Personen die Daten abrufen können. Angesichts der hohen Eingriffsintensität steigen aber auch die Anforderungen an die Bestimmtheit der gesetzgeberischen Regelungen. Eine generelle Aussage, welche die Verantwortung vollständig auf die Behörden auslagert und nur die Verpflichtung aus der DSGVO wiederholt, genügt diesen Anforderungen nicht. Zudem fehlt es an einer konkretisierten Verpflichtung zur beständigen Anpassung und Überprüfung.[78] Die Überprüfung durch den BfDI nach § 13 IDNrG-E kann interne Vorgänge nicht ersetzen.

Zudem wird zwar keine sprechende Personenkennziffer vorgesehen, wohl aber eine offene, also eine jedermann grundsätzlich zugängliche.[79] Damit ist eine missbräuchliche Nutzung kaum wirksam verhindert.

(4) Übermaß an Grundrechtseingriffen/Totalüberwachung

Schließlich ist das RegMoG-E in der Gesamtschau der Maßnahmen der staatlichen Zugriffsrechte auf die Daten der Bürger zu betrachten. Das BVerfG hat in seiner Rechtsprechung immer wieder betont, dass die staatliche Datenverarbeitung nicht *auf eine Totalerfassung der Kommunikation oder Aktivitäten der Bürger insgesamt angelegt sein darf*;[80] *sie muss eine Ausnahme bleiben.*[81] Sie darf nicht einmal als Schritt hin zu einer Gesetzgebung verstanden werden, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielte. Eine solche Gesetzgebung wäre, unabhängig von der Gestaltung der Verwendungsregelungen, von vornherein mit der Verfassung unvereinbar.[82] Es ist also die Gesamtbelastung der Bürger mit Informationseingriffen des Staates in den Blick zu nehmen, um zu verhindern, dass die gesamtheitliche Datenerfassung die Bürger nicht dem Eindruck einer Totalüberwachung aussetzt. Dies entspricht der ersten (!) Empfehlung der Datenethikkommission, nämlich Totalüberwachung zu verhindern[83] und den Rechtsrahmen risikoadäquat zu bestimmen[84]. Diesbezüglich erleichtert und in der Folge erweitert eine Identifikationsnummer, wie sie im RegMoG-E nach dem Gesetzeszweck vorgesehen ist, die Zugriffsmöglichkeiten der Verwaltung auf die beim Staat gespeicherten Datensätze der Bürger erheblich. Angesichts der ohnehin weitreichenden und in den letzten Jahren zunehmenden Möglichkeiten diverser Behörden, auf Daten von Bürgern zuzugreifen, ist eine solche weitreichende Verknüpfung nicht hinnehmbar.

(5) Once-Only und No-Stop-Government

Problematisch erscheint insoweit auch das Ziel des Gesetzgebers, mit Hilfe einer Identifikationsnummer Vorstellungen wie Once-Only und andere neuartige Verwaltungstätigkeiten ohne Einbindung der Bürger[85] umzusetzen, dafür aber Grundprinzipien des Datenschutzes in Frage zu stellen.

Once-Only steht für ein Leitbild aus der Europäischen Union, demnach Bürger ihre Daten der gesamten Verwaltung nur noch ein einziges Mal mitteilen sollen. Die Verwaltung muss von sich aus in der Lage sein, diese Daten, etwa aus einem übergreifenden Stammdatenregister oder aus dem jeweiligen bereichsspezifischen Register, abzurufen. Damit wird die Idee der Datensparsamkeit aufgegriffen und die Zweckbindung der erfassten Daten gelöst. In der Folge wird der Komfort einer einmaligen Dateneingabe im Kontakt mit der Verwaltung zum Abwägungsinteresse gegenüber den Interessen des Bürgers, nicht ausgeforscht und dem Staat aus¬geliefert zu sein. Dies kann angesichts der erheblichen Grundrechtseingriffe kein überwiegender Belang sein, zumal der Bürger nur in einzelnen Bereichen in häufigem oder regelmäßigem Kontakt mit Behörden steht, der Komfortgewinn also gering ist und vor allem auch durch andere Mittel erzielt werden kann.[86] Once-Only-by-default verstößt ohnehin gegen die bisherigen Datenschutzbestimmungen.[87]

No-Stop-Government steht für ein Leitbild von Verwaltung, bei dem die Bürger die Verwaltung nicht mehr spüren oder wahrnehmen und Behörden von sich aus für den Bürger aktiv werden. Bürger könnten, aber müssten Anträge nicht mehr selbst stellen. Technisch würde damit auf Kundenbeziehungsmanagementsysteme quer über den gesamten öffent-lichen Sektor gesetzt, die Zugriff auf alle relevanten Datenbestände erhalten, den künftigen Bedarf eines Bürgers von sich aus erkennen und proaktiv tätig werden. Die Grundüberlegung des Rechtsstaats und der Demokratie, dem Bürger eine umfängliche Kontrolle über „seinen" Staat zu ermöglichen, wäre damit ad absurdum geführt, bis hin dazu, dass die Technikkonzerne, die solche Konzepte bereitstellten, mit ihren normativen Vorstellungen Staatlichkeit bestimmten und nicht ein gewaltenteilender Staat mit einer Letztverantwortung gegenüber dem Bürger und Gerichten.

Die Einführung der Identifikationsnummer ist ein wesentlicher Schritt auf diesem Wege der Zusammenführung der Daten. Welche Mächtigkeit für den Staat und die zugrundeliegende, möglicherweise von privater Seite betriebene Infrastruktur dadurch entsteht, wird daran sichtbar, dass heutige IT-Systeme innerhalb kürzester Zeit (in Sekundenschnelle bei Nutzung der Datenverarbeitungskapazitäten eines durchschnittlichen Laptops) die Daten von mehr als 83 Millionen Bürgern und Steuerpflichtigen aus mindestens 56 Registern verknüpfen und auswerten können. Sind die Daten einmal zusammengeführt, lassen die Folgen sich nicht mehr beherrschen. Hier stellt sich die Frage, ob solche weitreichenden Vorstellungen zur Registermodernisierung überhaupt mit der Verfassung

[78] Vgl. BVerfGE 125, 260 (326 f.).
[81] *Wiss. Dienst BTag* 2020, Gutachten, S. 20.
[80] Vgl. BVerfGE 125, 260 (322 f.) und die – im Zuge der Umorganisation der BfDI – erfolgte Stellungnahme der BfDI, https://www.bundestag.de/blob/344116/3259a3ff-471bfda524b8ae4138e63f77/vosshoff-data.pdf.
[81] Vgl. BVerfGE 125, 260 (324).
[82] Vgl. BVerfGE 125, 260 (323).
[83] *Datenethikkommission* 2019, S. 18 und S. 89.
[84] *Datenethikkommission* 2019, S. 18 und S. 96 ff.
[85] Vgl. *Stocksmeier/Hunnius* 2018, S. 262 f.
[86] Siehe gleich unten Teil D.V.
[87] Unterkomplex *Martini/Wenzel*, DVBl. 2017, 749, der vor allem die Kosteneinsparungen und Effizienzgewinne und nicht die Bürgerrechte in den Vordergrund rückt (Fn. 6).

und den europäischen Datenschutzanforderungen in Übereinklang bringen lassen, wenn die eigentlichen Ziele der Politik Machine-2-Machine (Government), Once Only, No Stop Government oder No Government sein sollten.[88]

4. Verstoß gegen Gleichheitsgrundsätze und Art. 12 und 14 GG

Die Anknüpfung der Identifikationsnummer an die Steuer-ID nach § 139b AO behandelt natürliche Personen unabhängig von ihrer Funktion im Steuerverfahren gleich. Es wird nicht zwischen ihrer Rolle als „Privatperson" oder ihrer Rolle als „verantwortlich Handelnde im Wirtschaftsverkehr" beziehungsweise als „Einzelunternehmer oder freiberuflich Tätiger" unterschieden, obwohl unterschiedliche Anlässe für die Erfassung gegeben sind. Personen, die also gleichzeitig auch in anderer Funktion von § 139b AO erfasst sind, werden daher zusätzlich und ohne Differenzierung identisch mit natürlichen Personen behandelt. Eine eineindeutige Identifikation von Personengesellschaften als eigenständiges Rechtssubjekt, von juristischen Personen und von sonstigen Organisationen fehlt.[89]

IV. Europarecht

Auch unter europarechtlichen Gesichtspunkten stößt das RegMoG-E auf erhebliche Bedenken, sowohl aus primär- (Art. 7 und Art. 8 EU-GRCh) als auch sekundärrechtlichen Erwägungen (DSGVO).

1. Primärrecht

Das Datenschutzrecht wird von Art. 7 und Art. 8 GR-Ch geschützt; beide Grundrechte stehen in einem „engen Zusammenhang"[90] mit sich überschneidenden Schutzbereichen.[91] Bezüglich der Eingriffsintensität und der Verhältnismäßigkeit zeigen sich bisher zum Verständnis des BVerfGs erhebliche Überschneidungen, bis hin dazu, dass in den jüngeren Entscheidungen zur Vorratsdatenspeicherung eine Verschärfung offenbar wurde[92]. Daher kann insgesamt davon ausgegangen werden, dass die obigen Bedenken aus dem nationalen Verfassungsrecht in ähnlicher Weise auch der Wertung des EU-Primärrechts entsprechen. Dies gilt insbesondere für die weitreichende Verknüpfung und die mangelnde Bestimmtheit und Zweckbeschränkung.

2. Sekundärrecht (DSGVO)

Spezielle Ausprägung hat der Datenschutz in der EU mit der DSGVO gefunden. Diese ist anwendbar,[93] wenngleich die Öffnungsklauseln des Art. 6 Abs. 2 und Abs. 3 dem nationalen Gesetzgeber weite Gestaltungsspielräume einräumen.[94]

a) Art. 87 DSGVO

Die DSGVO sieht grundsätzlich die Einführung einer sog. Nationalen Kennziffer oder anderer Kennzeichen von allgemeiner Bedeutung in Art. 87 S. 1 DSGVO vor und trifft Regelungen dazu. Die Mitgliedstaaten können die spezifischen Bedingungen einer Verarbeitung dieser Kennziffer selbst bestimmen. Es handelt sich bei der Regelung um eine optionale Öffnungsklausel.[95]

(1) Nationale Kennziffer oder Kennzeichen von allgemeiner Bedeutung

Eine Legaldefinition für die Begriffe der nationalen Kennziffer und der anderen Kennzeichen von allgemeiner Bedeutung sieht die DSGVO nicht vor. Die Literatur versteht unter dem Begriff der nationalen Kennziffer eine in der Regel staatlich zugeteilte Zeichenkette, die jeweils eindeutig einen bestimmten Bürger oder Einwohner identifiziert und die umfassend oder zumindest für mehrere definierte Sektoren oder Lebensbereiche verwendet wird.[96] Wann ein anderes Kennzeichen allgemeine Bedeutung erlangt, ist nicht abschließend geklärt. Es handelt sich bei der nationalen Kennziffer jedenfalls um einen Unterfall eines Kennzeichens allgemeiner Bedeutung.[97]

Ob die Steuer-ID nach § 139a AO bereits in gegenwärtiger Form unter die Regelung des Art. 87 DSGVO fällt, ist umstritten; eine wohl knappe Mehrheit in der Literatur bejaht dies.[98] Die Gegenauffassung vertritt hingegen zumeist das Argument, dass eine „allgemeine Bedeutung" bei bereichsspezifischen Kennzeichen nicht vorliegen kann.[99] Durch die Ausweitung der Identifikationsnummer auf 56 weitere Register im Rahmen des RegMoG-E, die alleine durch die Zuordnung auch dem Anwendungsbereich der DSGVO unterliegen, wird jedoch auch nach der Gegenauffassung jedenfalls von einem Kennzeichen von allgemeiner Bedeutung auszugehen sein.[100] Davon geht auch die Begründung des RegMoG-E aus, wonach der Gesetzentwurf von der Öffnungsklausel des Art. 87 S. 1 DSGVO ausdrücklich Gebrauch macht.[101]

[88] Siehe dazu z.B. die Entscheidung und Empfehlung des IT-Planungsrats, https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/26_Sitzung/TOP2_Anlage_OZGUmsetzungskatalog.pdf?__blob=publicationFile&v=4 (Stand 4/2018), S. 263 ff.
[89] *BRat* 2020, S.4
[90] EuGH Rs. C-92/09 und C-93/09, EuZW 2010, 939 Rn. 47.
[91] EuGH Rs. C-92/09 und C-93/09, EuZW 2010, 939 Rn. 52.
[92] Vgl. *Schiedermair*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Einleitung, Rn.173.
[93] Siehe oben unter Anwendung der DSGVO und rechtlicher Prüfungsmaßstab.
[94] Siehe oben unter Anwendung der DSGVO und rechtlicher Prüfungsmaßstab.
[95] *Hansen* 2019, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 8.
[96] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 12.
[97] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 12.
[98] *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87, Rn. 7; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 14; *Pauly*, in: Paal/Pauly 2019, Art. 87 DSGVO Rn. 2; *Gola*, in: Gola 2018, Art. 87.
[99] *von Lewinski*, in: BeckOK 2020, Art. 87 Rn. 53; wohl auch Weichert, in: Kühling/Buchner 2020, Art. 87 Rn. 22; *Martini/Wagner/Wenzel* 2017, S. 5.
[100] *Wiss. Dienst BTag* 2020, Gutachten, S. 6 f. mit Hinweis auf die Existenz von insgesamt 214 Registern in Deutschland.
[101] RegMoG-E, S. 40.

(2) Grenzen der Öffnungsklausel: Geeignete Garantien

Art. 87 S. 2 DSGVO schreibt vor, dass die Mitgliedstaaten im Falle einer Einführung eines entsprechenden Kennzeichens geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen festlegen müssen. Hiervon umfasst sind gesetzliche, technische und organisatorische Maßnahmen.[102] Aus dieser Formulierung ergeben sich Mindestanforderungen, die erfüllt sein müssen; die Vorgaben der DSGVO sind im Prinzip einzuhalten und die Prüfung des notwendigen Schutzniveaus geboten. Dies ist für den gesamten Lebenszyklus der Kennungen und der Verarbeitung zu gewährleisten.[103] Zu solchen geeigneten Garantien gehören enge Zweckbindung, Verwendungs- und Weitergabebeschränkungen, Begrenzung der Form der Verarbeitung, die Ausgestaltung des Kennzeichens, frühestmögliche Pseudonymisierung und Umkodierungen, Schutz vor Täuschung und Manipulation sowie ausreichender Rechtsschutz einschließlich Sanktionstatbeständen.[104] Es müssen die wesentlichen Elemente des Schutzniveaus der DSGVO, und damit die wesentlichen Prinzi-pien aus Art. 5 DSGVO[105] und seiner Konkretisierungen wie z.B. die besonderen Anforderungen des Art. 32 DSGVO, gewahrt bleiben, nämlich enge Zweckbindung, Vorhersehbarkeit, Datenminimierung, Speicherbegrenzung, Rechtmäßigkeit einschließlich Bestimmbarkeit, Richtigkeit, Transparenz und Rechenschaftspflicht. Der gänzliche Verzicht auf einzelne Prinzipien ist damit ebenso wenig vereinbar wie eine deutliche Reduktion der meisten dieser Garantien.

Schon deshalb mit der DSGVO nicht vereinbar ist die Einzelansicht, der Grundsatz der Zweckbindung sei nicht von den Garantien iSd. Art. 87 S. 2 DSGVO erfasst, weil das Ver-knüpfungspotential eines solchen Kennzeichens die allgemeine Wiederverwendbarkeit voraussetze.[106] Dieser Zirkelschluss von der möglichst breit gewünschten Verwendungsmöglichkeit auf die Verwendungszulässigkeit wird auch in anderen Bereichen der DSGVO nicht mitgegangen, zum Beispiel beim Profiling: Aus dem unbegrenzten technischen Können folgt gerade kein unbegrenztes normatives Dürfen. Es ist auch nicht erkennbar, dass die Begrifflichkeit der Garantien in Art. 87 S. 2 DSGVO anders zu verstehen wäre als in anderen Vorschriften in der DSGVO, etwa in Art. 6 Abs. 4 lit. e) DSGVO.[107] Die Vorschrift baut auf einer Vorgängervorschrift in der DS-RL auf und soll den Mitgliedstaaten ermöglichen, bestehende Kennzeichen fortzuführen.[108]

Auch wenn die vorgesehene Identifikationsnummer eine Reihe von gebotenen Sicherungen und Garantien enthält, sind diese dennoch nicht ausreichend. Denn die Zweckbindung wird faktisch unterlaufen, indem eine Vielzahl von Registern verknüpft wird; die technischorganisatorischen Sicherungen werden nicht konkretisiert und vorgegeben; der Überwachungsdruck wächst dadurch in unangemessener Weise. Auf die angesprochenen Grundrechtsverkürzungen kann verwiesen werden.[109]

b) Art. 6 Abs. 1 lit. e) i.V.m. Art. 6 Abs. 2 und Abs. 3 DSGVO

Fraglich ist, ob parallel zu Art. 87 DSGVO auch die Vorschrift des Art. 6 Abs. 1 lit. e) DSGVO i.V.m. Art. 6 Abs. 2 und Abs. 3 DSGVO zu beachten ist. Sie ermöglicht den Mitgliedstaaten, eigene Regelungen für die Legitimation von Datenverarbeitungen – also auch Zuweisungen von Identifikationsnummern – im öffentlichen Interesse – also für Verwaltungszwecke – vorzunehmen.

(1) Verhältnis zwischen Art. 87 und Art. 6 DSGVO

Art. 6 Abs. 1 lit. e) DSGVO deckt bereits nach seinem Wortlaut einen deutlich weiteren Raum ab als Art. 87 DSGVO. Zweck des Art. 87 DSGVO ist insofern die Klarstellung, dass der Gesetzgeber Personenkennzeichen grundsätzlich einführen kann.[110] Aufgrund der für solche Kennzeichen typischen Risiken bestünde anderenfalls die Möglichkeit, dass Zweifel an deren Rechtmäßigkeit aufträten.[111] Das dogmatische Verhältnis zwischen Art. 87 DSGVO und Art. 6 DSGVO ist jedoch nicht eindeutig.

Nach dem Wortlaut sieht Art. 87 S. 1 DSGVO nur spezifische Regelungen für die Verarbeitung des Kennzeichens als solches vor. Hiervon umfasst sind alle Verarbeitungsvorgänge im Sinne von Art. 4 Nr. 2 DSGVO, also auch die Erschaffung und Übertragung des Kennzeichens. Ob dies jedoch auch auf jene Daten zutrifft, die im Rahmen des IDNrG-E zusammen mit der Identifikationsnummer abgefragt und übermittelt werden, ist fraglich. So vertritt eine Ansicht, dass Art. 87 S. 1 DSGVO die Schaffung einer Rechtsgrundlage für die Zuteilung des Kennzeichens und die hierfür erforderlichen Stammdaten ermöglicht.[112] Die Übermittlung von Daten, die mit dem Kennzeichen verbunden sind, können hiernach jedoch nicht auf die Regelung in Art. 87 S. 1 DSGVO gestützt werden.[113]

Art. 87 S. 1 DSGVO enthält keinen eigenen Erlaubnistatbestand für Verarbeitungen unter Verwendung eines solchen Kennzeichens.[114] Die Vorschrift stellt vielmehr eine Angemessenheitsregelung auf.[115] Eine entsprechende Verarbeitung muss demnach bereits nach den Art. 6 und 9 DSGVO zulässig sein.[116] Die Erlaubnistatbestände in Art. 6 DSGVO sind nach der Systematik der DSGVO grundsätzlich als abschließend einzustufen.[117] Diese Auslegung wird darüber hinaus dem Zweck von Art. 87 DSGVO gerecht, die grundsätzliche Zulässigkeit von Kennzeichen zu betonen.

[102] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 23.
[103] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 24 f.
[104] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 26 ff.
[105] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 25.
[106] *Von Lewinski*, in: BeckOK 2020, Art. 87 Rn. 45.
[107] Auch hier sind alle Grundsätze des Art. 5 DSGVO zu wahren: *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 4 Rn. 65.
[108] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 2.
[109] Siehe oben unter Angemessenheit.
[110] *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87 Rn. 1; *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87 Rn. 1.
[111] *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87 Rn. 1; Hansen, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87 Rn. 9.
[112] *Martini/Wagner/Wenzel* 2017, S. 8 mit dem Hinweis, dass bei anderweitiger Ansicht Art. 6 Abs. 3 S. 1 DSGVO als einschlägig zu betrachten sei.
[113] *Martini/Wagner/Wenzel* 2017, S. 11,
[114] *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87 Rn. 11; *Weichert*, in: Kühling/Buchner 2020, Art. 87 Rn. 4
[115] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 8.
[116] *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87 Rn. 11; Weichert, in: Kühling/Buchner 2020, Art. 87 Rn. 4.
[117] *Schulz*, in: Gola 2018, Art. 6 Rn. 9.

Welche Ansicht die Bundesregierung in dieser Frage vertritt, lässt sich der Begründung des Entwurfs nicht unmittelbar entnehmen; ausdrücklich wird das RegMoG-E auf Art. 87 DSGVO gestützt[118]. Die vorhandenen Ausführungen zu Art. 6 DSGVO beschränken sich jedoch auf pauschale Hinweise zur Rechtmäßigkeit der Datenverarbeitung bei Übertragung von Daten nach § 6 III IDNrG-E.[119] Der Gesetzentwurf muss allerdings auch die Voraussetzungen des Art. 6 DSGVO neben Art. 87 DSGVO einhalten.

(2) Voraussetzungen von Art. 6 Abs. 3 DSGVO

Art. 6 Abs. 1 lit. e) DSGVO ist – im Gegensatz zu den meisten anderen in Art. 6 Abs. 1 DSGVO aufgeführten Alternativen – kein eigenständiger Erlaubnistatbestand.[120] Vielmehr dient die Norm im Zusammenspiel mit Art. 6 Abs. 3 DSGVO als „Scharnier"; der eigentliche Erlaubnistatbestand ist in dem vom Mitgliedstaat erlassenen Recht zu sehen.[121] Abs. 2 ist als weiter denn Abs. 3 zu verstehen; Abs. 3 betrifft nur die Zulässigkeit der Datenverarbeitung i.V.m. Art. 6 Abs. 1 lit. c) und lit. e) DSGVO sowie benennt in Abs. 3 S. 2 weiterreichende Angaben im Zusammenhang mit der Rechtsgrundlage.[122] Die Vorschriften des RegMoG-E schaffen eine Rechtsgrundlage für die Verarbeitung von Daten auf der Basis des Art. 6 Abs. 1 lit. e) DSGVO, so dass zunächst Abs. 3 vorrangig den Prüfungsmaßstab vorgibt.

Demnach sind „spezifische Bestimmungen" im mitgliedstaatlichen Recht zulässig, welche die Umsetzung der Grundsätze der Datenverarbeitung in Art. 5 DSGVO konkretisieren[123] und zu kohärenten Gesamtregelungen beitragen, welche die Risikosituation einer bestimmten Form der Datenverarbeitung umfassend regeln[124].

Dem Gesetzgeber ist also nicht verwehrt, z.B. einheitliche Regelungen für die Verwendungen bereichsspezifischer Personenkennziffern zu schaffen. Gleichwohl stellen weder Abs. 2 noch Abs. 3 Regelungen dar, die ein grundsätzliches Abweichen von den Prinzipien der DSGVO erlaubten. Daher gilt auch hier, dass die nicht vereinbaren Regelungen des RegMoG-E nicht über Art. 6 Abs. 2 bzw. Abs. 3 DSGVO legitimiert werden können.

c) Zu berücksichtigende Prinzipien, insb. Art. 5 DSGVO

Ohnehin ist zu berücksichtigen, dass die Nutzung einer Öffnungsklausel, also auch von Art. 87 DSGVO, nicht von den Bindungen der DSGVO gänzlich freistellt, sondern weiterhin grundsätzlich alle Vorgaben der DSGVO umzusetzen sind.[125] Insbesondere eine Berücksichtigung der Grundsätze des Art. 5 DSGVO ist notwendig.[126]

(1) Datenminimierung

Der Grundsatz der Datenminimierung nach Art. 5 Abs. 1 c) DSGVO gebietet es, personenbezogene Daten auf das für die Zwecke der Verarbeitung notwendige Maß zu begrenzen. Die Erhebung des letzten Verwaltungskontakts nach § 4 Abs. 3 Nr. 2 IDNrG-E als „Lebenszeichen"[127] einer natürlichen Person ist insofern für die Zwecke des Gesetzes, ein registerübergreifendes Identitätsmanagement zu schaffen und damit Redundanzen zu verringern, verfehlt.[128] Hier besteht die Gefahr eines übergreifenden Tracings von Bürgern; um die Datenqualität durch die Validitätswerte festzustellen, genügt laut der *Gesellschaft für Informatik* insoweit auch das Datum der letzten Aktualisierung der Validitätswerte.[129]

Ähnliches gilt für die Form der Übertragung der Daten bei der Abfrage durch Behörden. Soll etwa festgestellt werden, dass es sich vorliegend um einen deutschen bzw. EU-Staatsbürger handelt (vgl. das Basisdatum „Staatsangehörigkeiten" in § 4 Abs. 2 Nr. 8 IDNrG-E), reicht regelmäßig bereits die bejahende oder verneinende Beantwortung dieser Frage.[130]

Daneben besteht die Gefahr, dass Register Daten erhalten bzw. die Identifikationsnummer hinzufügen sollen, die keine Verwendung dafür haben. So kritisiert die Bundesrechtsanwaltskammer (BRAK), dass im Gesamtverzeichnis bei der BRAK (IDNrG-E Anlage Nr. 46) lediglich Namen und Doktorgrad eingetragen seien und keinerlei Verwaltungsleistungen erbracht würden.[131] Die in der Anlage des IDNrG-E genannten Register bedürfen somit zumindest einer weiteren Überprüfung.

(2) Zweckbindung

Personenbezogene Daten müssen gemäß Art. 5 Abs. 1 b) DSGVO für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden. Ein eindeutiger Zweck ist von anderen möglichen Zwecken klar zu unterscheiden; er muss ausdrücklich benannt, inhaltlich präzise und konkret bestimmt sein.[132] Die Art. 29 Working Party erachtet vor diesem Hintergrund pauschale Zweckbestimmungen wie „Verbesserungen der Nutzererfahrung", „Marketing", „IT-Sicherheit" und

[118] RegMoG-E, S. 72.
[119] Vgl. RegMoG-E, S. 80
[120] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 1, Rn. 71.
[121] *Roßnagel* in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 1, Rn. 71.
[122] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 2, Rn. 7.
[123] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 3, Rn. 38.
[124] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 6 Abs. 3, Rn. 38; ders., DuD 2018, 477.
[125] *Hansen*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 87, Rn. 24; punktuelle Abweichungen erlaubend: *Ehmann*, in: Ehmann/Selmayr 2018, Art. 87 Rn. 9; einen zumindest, der DSGVO gleichwertigen Mindestschutz fordert *Pauly*, in: Paal/Pauly 2019, Art. 87, Rn. 3; a.A. *von Lewinski*, in: BeckOK 2020, Art. 87, Rn. 44, der nur einzelne Grundsätze der DSGVO für anwendbar hält.
[126] *Martini/Wagner/Wenzel* 2017, S. 7; vgl. Forderungen hinsichtlich Transparenz und Zweckbindung bei *Pauly*, in: Paal/Pauly 2019, Art. 87 Rn. 3 und *Weichert*, in: Kühling/Buchner 2020, Art. 87 Rn. 15.
[127] So RegMoG-E, S. 77.
[128] Mit Verweis auf das Prinzip der Datensparsamkeit vgl. auch GI 2020, S. 6.
[129] *GI* 2020, S. 6.
[130] Vgl. *Martini/Wagner/Wenzel* 2017, S. 10.
[131] BRAK, S. 2 f. Der RegMoG-E nennt nach Kritik an der Verwendung des Begriffs „Anwaltsverzeichnis" im Referentenentwurf nun ausdrücklich die Verzeichnisse der Rechtsanwaltskammern und das Gesamtverzeichnis der BRAK.
[132] *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 5 Rn. 76.

„zukünftige Forschung" für nicht ausreichend.[133] Grundsätzlich gilt, dass der Zweck desto bestimmter festgelegt sein muss, je eingriffsintensiver eine Maßnahme ist.[134]

Dem Gesetzentwurf gelingt keine klare Zweckbestimmung. § 1 IDNrG-E schreibt zunächst verschiedene Ziele des Gesetzes fest; in § 5 IDNrG-E wird sodann ausdrücklich der Zweck der Identifikationsnummer bestimmt. Während die Zweckbestimmung in § 5 Abs. 1 Nr. 1 und 2 IDNrG-E („Zuordnung der Datensätze zu einer Person" und „Abgleich von Datensätzen einer natürlichen Person […]") noch als ausreichend bestimmt angesehen werden kann, gilt dies nicht für § 1 IDNrG-E. Die Verbesserung der Datenqualität wird in der Gesetzes-begründung zwar als einer der Zwecke der Datenverarbeitungen genannt (bspw. für die Erhebung des Datums des letzten Verwaltungskontakts); ist jedoch nur eines der Ziele in § 1 IDNrG-E. Es ist auch unklar, inwieweit dies in Bezug auf alle 56 Register erreicht wird und nicht vielmehr eine pauschale Zusammenfassung darstellt. Die Eingrenzungsfunktion, die über die Zweckbestimmtheit erreicht werden soll, ist kaum gewahrt; für Bürger ist kaum erkennbar, wer Zugriff auf die Identifikationsnummer und die damit verbundenen Informationen haben kann, soll und darf. Insoweit § 1 IDNrG-E auch als Zweckbestimmung dienen soll, ist dies inhaltlich nicht ausreichend präzise dargestellt, erst recht nicht, wenn man die Gefahr der Profilbildung und der Verstärkung der Machtasymmetrie zu Lasten der Bürger als eingriffsintensiv ansieht. Gerade diese Wertung ist der DSGVO jedoch zu entnehmen.[135]

Letztlich besteht mit dem Entwurf die Gefahr, dass neben der ohnehin schon breiten Zweckbestimmung umfangreiche Zweckänderungen unter den allgemeinen Regelungen der Art. 5 Abs. 1 lit. b) und Art. 6 Abs. 4 DSGVO möglich werden.[136] Vor diesem Hintergrund schlägt der BfDI vor, der Identifikationsnummer mit der Identifikation von natürlichen Personen gegenüber der Verwaltung einen einzigen Zweck zuzuordnen.[137] Ferner wäre ein ausdrücklicher Hinweis, dass die Identifikationsnummer auch nur zu diesem Zweck verarbeitet werden darf, zu begrüßen.[138]

(3) Transparenz

Art. 5 Abs. 1 lit. a) Alt. 3 DSGVO sieht vor, dass personenbezogene Daten in einer für die betroffenen Person nachvollziehbaren Weise verarbeitet werden müssen. Das RegMoG-E schafft mit der Einführung des Datencockpits nach § 10 OZG-E einen Mechanismus, der dem Bürger veranschaulicht, welche Datenverarbeitungen die Verwaltung im Zusammenhang mit der Identifikationsnummer durchführt. Als Reaktion auf Kritik des BfDI[139] wurde in § 10 Abs. 2 S. 2 2. HS und S. 3 OZG-E eine Regelung geschaffen, die die Aufbewahrung der Daten auf die Dauer der jeweiligen Nutzersession begrenzt.

Sollte sich das Datencockpit als Mittel zur Vermittlung von Transparenz bei der Datenverarbeitung durch Behörden bewähren, könnte der Gesetzgeber eine Erweiterung des Datencockpits auch auf andere Verwaltungsbereiche in Betracht ziehen.[140]

(4) Datenqualität und -richtigkeit

Personenbezogene Daten müssen schließlich gemäß Art. 5 Abs. 1 lit. d) DSGVO sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Die Datenqualität ist zwar eines der Ziele des Gesetzentwurfs. Die Erreichung dieses Ziels durch das RegMoG ist fraglich. Vielmehr wird von den einzelnen Fachbehörden verlangt, ihrerseits geprüfte Daten mit Daten unbekannter Qualität zu ersetzen, sodass es auch zu einer Verschlechterung der Datenqualität kommen kann.[141] Ebenso wenig ist eindeutig geregelt, welche Behörde für die Richtigkeit der Daten zuständig ist und wie mit potentiellen Dubletten umgegangen werden soll.[142] Diesbezüglich fehlt es also auch an der Bestimmtheit der Vorgaben.

V. Zwischenfazit

Dem RegMoG-E und insbesondere dem IDNrG-E stehen in ihrer aktuellen Form erhebliche verfassungsrechtliche und europarechtliche Bedenken entgegen. Zwar ist die Einführung eines Datenschutzcockpits im OZG-E grundsätzlich als Transparenzmaßnahme gegenüber den Bürgern zu begrüßen. Transparenz alleine vermag jedoch nicht die Intensität des Eingriffs durch die bereichsübergreifende Identifikationsnummer auszugleichen, zumal diese Transparenz nur zu einem nachgelagerten Rechtsschutz befähigt. Hier sind weitere Schutzmaßnahmen gefragt, um der Rechtsprechung des BVerfGs in der Folge des Volkszählungsurteils und den Vorstellungen des europäischen Gesetzgebers zur DSGVO ausreichend Rechnung zu tragen.

Besonders bedenklich ist die Tatsache, dass das BMI laut eigener Gesetzesbegründung weitere Datenschutzmaßnahmen pauschal aus Kosten- und Zeitgründen ablehnt.[143] Die deutsche Verwaltung bedarf zweifellos einer Modernisierung, um Redundanzen zu verringern und die Effizienz zu steigern; in Zeiten von verstärkter digitaler Kommunikation durch Covid-19 gilt dies erst recht. Mit dem österreichischen Modell gibt es auf europäischer Ebene jedoch bereits eine funktionsfähige Variante eines digitalen Identitätsmanagements, die – auch bei einiger berechtigter Kritik an diesem Modell[144] – deutlich datenschutzfreundlicher gestaltet ist als der aktuelle nationale Gesetzesentwurf. Insofern wird vom Gesetzgeber nicht erwartet, das Rad sprichwörtlich „neu zu erfinden" oder eine ähnliche Kraftanstrengung wie zur Etablierung der Corona-App zu stemmen. Darüber hinaus sendet der Staat

[133] Art. 29 Working Party, S. 16.
[134] Vgl. *Roßnagel*, in: Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 5 Rn. 69 ff.
[135] So etwa in Art. 35 Abs. 3 lit. a), siehe hierzu auch *Karg*, in Simitis/Hornung/Spiecker gen. Döhmann 2019, Art. 35, Rn. 37 ff.
[136] *BfDI* 2020, S. 9.
[137] *BfDI* 2020, S. 9.
[138] So auch die *DRV* 2020, S. 10.
[139] *BfDI* 2020, S. 10.
[140] So auch gefordert von dem *BfDI*, S. 10 und BDA, S. 2.
[141] *Databund*2020, S. 2.
[142] *Databund* 2020, S. 2.
[143] RegMoG-E, S. 3.
[144] Siehe noch unten Teil D.

ein falsches Signal, die ursprünglich nur für die Steuerverwaltung angedachte Identifikationsnummer nunmehr nachträglich auf alle Lebensbereiche auszuweiten. Eine solche Funktionsexplosion („function creep“) hat das Potential, das Vertrauen in den Gesetzgeber zu erschüttern und sollte daher möglichst verhindert werden.

Abb. 5 | Morphologischer Kasten zum Identitätsnummernsystem RegMoG

ID-NR-SYSTEM	AUSPRÄGUNGSFORMEN				
Typus von Personenkennzeichen	**allgemeines Personenkennzeichen (aPK)**	bereichsübergreifendes Personenkennzeichen (2wPK)	bereichsspezifisches Personenkennzeichen (bPK)		
Vorgehen bei der Vergabe	**Personenkennzeichen zentral vergeben**		Personenkennzeichen dezentral vergeben		
Inhaltliche Gestaltung des Personenkennzeichens	**Steuer-ID**	Andere existierende Register-ID	NEU-ID/Stammzahl in Form von einer Zufallszahl	Keine zentrale ID	
Identifizierung in anderen Registern	**Steuer-ID**	Bisherige Register-ID	Hashwert auf Stammzahl und Bereichs-Bezeichner	Zufallszahl	
Zu erfassende Personengruppe	**Deutsche Bürger**	**Ausländer**	**Steuerzahler**	**Natürliche Personen**	Juristische Personen
Verortung der Speicherung der Basisdatensätze zu allen Personen	**Basisdatensatz beim Bundeszentralamt für Steuern (BZSt)**		ohne Basisdatensatz		
Einsatz einer Intermediär-internen Datenbank mit allen bPKs	**Verzicht auf Intermediär-interne ID-Datenbank**		Pseudonymisierte Intermediär-interne ID-Datenbank		
Registermodernisierung	**Registermodernisierungsbehörde (BVA)**		Verzicht auf Registermodernisierungsbehörde		
Verortung der Intermediäre zu den BZSt-Basisdatensätzen	**Intermediär zum BZSt-Basisdatensatz bei BVA (Registermodernisierungsbehörde)**		Intermediär zum BZSt-Basisdatensatz bei Datenschutzaufsichtsbehörde		
Vermittlungsstellen für Anfragen auf BZSt-Basisdatensätze	Keine Vermittlungsstelle für Anfragen	**Zentrale Vermittlungsstelle für Anfragen**	Verbund von Vermittlungsstellen für Anfragen		
Prüfung der Zugriffe auf BZSt-Basisdatensätze	Keinerlei Prüfung der Zugriffe	**Software-basierte Prüfung der Zugriffe**	Hardware-basierte Prüfung der Zugriffe	Ständige Prüfung durch Sachbearbeiter	
Freigabe von Daten durch Bürger bei bereichsübergreifenden Abfragen	**Freigabe von Daten ohne Bürgereinbindung**	Anlassbezogene Freigabe von Daten durch Bürger	Freigaben von Daten stets durch Bürger erforderlich		

Das RegMoG-E führt also zu einem Identitätsnummernsystem (**Abbildung 5**), das mit der Steuer-ID auf einem allgemeinen Personenkennzeichen aufsetzt, das vom Bundeszentralamt für Steuern zentral vergeben und in allen relevanten Registern gespeichert wird. Zur eindeutigen Identifizierung von Personen in allen relevanten Registern reicht die Steuer-ID aus. Erfasst werden alle potentiellen Steuerzahler. Damit wird die gesamte Bevölkerung einbezogen. Beim Bundeszentralamt für Steuern werden Basisdaten gespeichert. Zugriffe auf diese Basisdaten und alle Anfragen erfolgen nur über die Registermodernisierungsbehörde. Eine separate ID-Datenbank bei Intermediären ist auf Grund dieser Konstellation nicht erforderlich. Alle Zugriffe werden automatisiert geprüft. Die Bürger selbst sind in diese Abfragen nicht eingebunden. Sie werden über das Datenkonto auf Zugriffe informiert.

Insgesamt hat damit das RegMoG-E die folgenden Konsequenzen,
die abschließend in einer SWOT-Analyse (**Abbildung 6**) zusammengefasst wurden:

Abb. 6 | SWOT-Analyse zum Identitätsnummernsystem RegMoG-E

STÄRKEN

- → Schneller und einfacher Zugriff der Verwaltung auf die bereichsspezifischen Datensätze
- → Verringerung der Zugangsbeschränkungen für nahtloses E-Government (Once-Only)
- → Existierende ID wird genutzt, Neuvergabeprozess entfällt
- → Steuer-ID als Anknüpfungspunkt betont die Bedeutung der Finanzverwaltung

SCHWÄCHEN

- → Gefahr des „gläsernen Bürgers“
- → Keine Beachtung der Vorgaben der Datenethikkommission
- → Alternativen werden unterkomplex betrachtet
- → Überbewertung der Bedeutung von Once-Only für die Bürger

CHANCEN

- → Erleichterter und künftig registerbasierter Zensus
- → Genauere Datenbestände
- → Missbrauch durch mehrere Identitäten parallel eingeschränkt
- → Einfachere Steuerung des Bürgers möglich

RISIKEN

- → Vorschnelles Agieren des Gesetzgebers und dadurch Nicht-Beachtung wesentlicher Problemlagen
- → Verstoß gegen nationale und europäische Grundrechte, insbesondere das Recht auf informationelle Selbstbestimmung
- → Überlagerung der inhaltlichen Fragen durch Konflikt des BVerfGs mit dem EuGH
- → Selbstbestimmung/Datenschutzgrundrecht
- → Verstoß gegen Bestimmtheits-anforderungen der Verfassung
- → Verstoß gegen das Demokratie- und Rechtsstaatsprinzip
- → Erschwernis für die Steuerverwaltung mangels Weiterverwendbarkeit der Steuer-ID.
- → Verstoß gegen den Gleichbehandlungsgrundsatz
- → Unpräzise, Art. 80 Abs. 1 S. 2 GG widersprechende Auslagerung von Entscheidungsspielräumen an die Verwaltung
- → Ermöglicht Profilbildung
- → Keine Beschränkung des Once-Only auf Bereiche, in denen regelmäßig und häufig Bürgerkontakte bestehen
- → Verlagerung der negativen Effekte von Bürokratie und fehlender Organisation in der Verwaltung auf den Bürger und dessen Freiheitsrechte
- → Missbrauchsgefahr einer Einzelidentität durch leichteren Identitätsdiebstahl (vgl. Social Security Number in den USA)

C. Drei Optionen: Kein neues Personenkennzeichen, ein neues allgemeines Personenkennzeichen oder ein neues bereichsspezifisches Personenkennzeichen

Mit Blick auf die erfolgte Bewertung des vorliegenden Gesetzesentwurfs stellt sich die Frage, welche Optionen es derzeit für die vom Normenkontrollrat eingeforderte und von der Bundesregierung und dem IT-Planungsrat forcierte Registermodernisierung noch gibt. Nüchtern betrachtet gibt es drei Optionen (**Abbildung 7**). Erstens kommt der Verzicht auf eine Einführung eines neuen Personenkennzeichens in Betracht. Ebenso wäre die Einführung eines neuen bereichsspezifischen Personenkennzeichens vorstellbar. Die dritte Option wäre die Einführung eines neuen allgemeinen Personenkennzeichens.

Abb. 7 | Optionen für Personenkennzeichen zur Registermodernisierung in Deutschland

Der Verzicht auf eine Einführung eines neuen Personenkennzeichens entspräche dem Status Quo. Dies verhindert zwar eine substantielle Registermodernisierung, setzt die Bevölkerung aber auch nicht den Gefahren, Risiken und Nebenwirkungen eines neuen Personenkennzeichens aus. Aus einer Datenschutzperspektive mag dieser Weg der Besitzstandswahrung große Unterstützung finden. Eine Registerkonsolidierung und modernisierung wäre aber nur mit hohem manuellem Aufwand möglich und würde auch die Umsetzung des OZG erschweren. Diese Option wird in diesem Gutachten nicht weiter verfolgt.

Mit dem RegMoG-E wird ein Vorschlag zur Einführung eines neuen allgemeinen Personenkennzeichens auf Basis der bisher bereichsspezifisch eingesetzten Steuer-ID eingebracht. Auf diesen Vorschlag, der zentral und registerübergreifend angelegt ist, wurde in der Analyse und Bewertung in Teil B bereits detailliert eingegangen. Die in diesem Zusammenhang ebenfalls denkbaren Alternativen einer neuartigen allgemeinen Identifikationsnummer ohne Rückgriff auf die Steuer-ID sowie auf Grundlage biometrischer Merkmale (wie dem Gesichtsprofil oder der Fingerabdrücke) werden nicht weiter verfolgt, weil sie ebenso nicht verfassungskonform wären und sich daher für einen Einsatz in der Bundesrepublik Deutschland generell nicht eignen.

Die Idee einer neuartigen bereichsspezifischen Identifikationsnummer, die ausschließlich zu Zwecken der Identifizierung von Personen im Rahmen von Registerzugriffen eingesetzt werden darf, ist eine überlegenswerte und ebenso rasch umsetzbare Alternative. Sichtbare Schwächen des vorliegenden Gesetzesentwurfs sind dabei beseitigt. Ausgangsbasis ist eine neuartige Identifikationsnummer (NEU-ID), die bisher noch keinerlei Verwendung findet. Andere Ansätze auf bestehenden bPKs wurden nicht weiter betrachtet, da diese dann zu aPKs würden und damit verworfen werden müssten. Dies hindert jedoch nicht daran, etwa die Gruppe aller Inhaber einer Steuer-ID als Ausgangsbasis für die Erzeugung neuer bPK zu verwenden.

In der folgenden Analyse in Kapitel D werden zwei machbare Varianten näher betrachtet, an denen die bestehenden Optionen verständlich aufgezeigt werden können.

→ **VARIANTE 1** (Stammzahl-Modell) greift mit einer geheim gehaltenen Stammzahl und daraus generierten Hash-werten als weiteren neuen bPK einige Ideen aus Österreich auf. Nur die Registermodernisierungsbehörde (BVA) kennt und verwendet die Stammzahlen. Auf Basis der Stammzahl und eines Bezeichners pro Register generiert sie nach österreichischem Vorbild alle hash-basierten bPKs. Anschließend übermittelt sie diese zur ausschließlich lokalen Speicherung an die jeweiligen Register. Auf eine Speicherung aller Personenkennzeichen in einer eigenständigen ID-Datenbank wird vollkommen verzichtet. Die Basisdaten verbleiben beim Bundeszentralamt für Steuern. Die Registermodernisierungsbehörde kann eine Registerkonsolidierung initiieren, indem sie zu jeder Person die jeweiligen Basisdaten bei allen Registern abfragt, diese dann qualitätssichert und an die bereichsspezifischen Register zurückspielt. Alle anderen Anfragen laufen über Vermittlungsstellen und die Registermodernisierungsbehörde. Behörden untereinander sind nicht in der Lage, aus ihren jeweiligen bereichsspezifischen Identifikationsnummern heraus alle Daten zu einer Person zusammenzuführen.

→ **VARIANTE 2** (NEU-ID-Modell) setzt auf eine neuartige bereichsspezifische NEU-ID und eine neue, zentrale und besonders geschützte ID-Datenbank bei einer Datenaufsichtsbehörde, etwa dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit. In diesem neuen pseudonymisierten Register werden zu jeder Person alle bestehenden bPKs oder weitere neu zu generierende bPKs gespeichert, aber keinerlei Basisdaten. Die Basisdaten verbleiben weiterhin beim Bundeszentralamt für Steuern. Die Registermodernisierungsbehörde (BVA) übernimmt die Aufgaben der Registermodernisierung. Alle Anfragen laufen über Intermediäre (wie die Vermittlungsstellen). Die bereichsspezifische Identifikationsnummer NEU-ID muss für den gesamten Personenkreis neu vergeben werden. Sie wird aber nur innerhalb dieser ID-Datenbank verwendet. Der Aufbau und der dauerhafte Schutz einer solchen ID-Datenbank wird sich datenschutzrechtlich als Herausforderung erweisen, erlaubt aber Bund, Ländern und Kommunen die gewünschte Registerkonsolidierung.

D. Vorstellung und Bewertung der Ansätze auf Basis einer neuartigen bereichsspezifischen Personenkennziffer

I. Ausgangspunkt: Kern des Regierungsentwurfs-Modells aus technischer Sicht

Abb. 8 | Modell Regierungsentwurf (vereinfacht)

Ausgangspunkt der folgenden Überlegungen hin zu einer datenschutzfreundlicheren Vernetzung staatlicher Register ist das in Teil B bereits erläuterte Modell des RegMoG-E (vgl. **Abbildung 8**). Bereichsübergreifende Datenabfragen laufen grundsätzlich über einen Intermediär – entweder die beim Bundesverwaltungsamt eingerichtete Registermodernisierungsbehörde als Intermediär zum Bundeszentralamt für Steuern (vgl. **Abbildung 9**) oder eine Vermittlungsstelle.

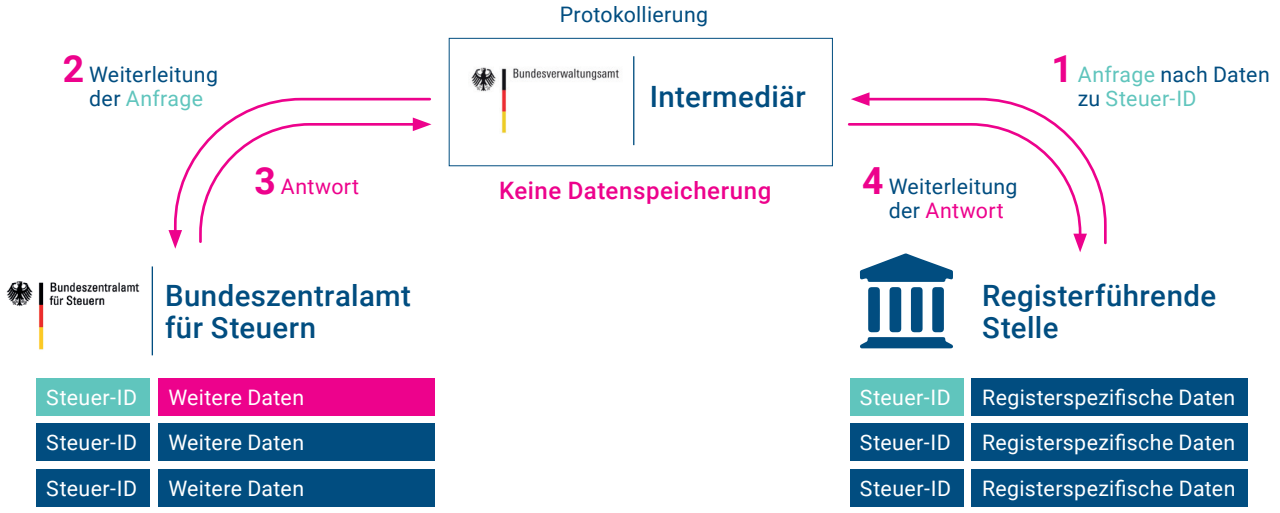
Für den Fall der Übermittlung über eine Vermittlungsstelle ist im Regierungsentwurf das sogenannte 4-Corner-Modell mit „doppeltem Umschlag" vorgesehen. Das bedeutet, dass die eigentlichen Inhalte einer Anfrage so verschlüsselt sind, dass der weiterleitende Intermediär sie nicht zur Kenntnis nehmen kann, sondern lediglich die zur Erfüllung seiner Aufgabe benötigten Metadaten erhält. Dies ist zunächst positiv zu bewerten. Grundsätzlich ist es damit möglich, einen Intermediär so zu betreiben, dass er den Betroffenen nicht identifizieren kann und insbesondere dessen Steuer-ID nicht erhält.

Für die Registermodernisierungsbehörde als Intermediär wird das 4-Corner-Modell im Regierungsentwurf aber gerade nicht gesetzlich normiert.[145] Es ist auch nicht mit der dort verankerten Umsetzung der Prüf- und Protokollierungspflichten vereinbar: Nach § 9 Abs. 1 S. 2 IDNrG-E werden „Datenübermittlungen zwischen der Registermodernisierungsbehörde und dem Bundeszentralamt für Steuern sowie Datenabrufe bei der Registermodernisierungsbehörde […] bei der Registermodernisierungsbehörde protokolliert". Die nach § 10 OZG-E vorgesehene Anzeige im Datencockpit erfordert eine Zuordnung der Protokolldaten zur jeweils betroffenen Person, so dass der potentielle Vorteil, bei der Registermodernisierungsbehörde nicht direkt mit der Steuer-ID umgehen zu müssen, nicht realisiert werden kann. Bezüglich der Vermittlungsstellen wäre dieser Vorteil hingegen noch realisierbar, da § 9 Abs. 1 IDNrG-E hier lediglich die Protokollierung „durch die jeweiligen Stellen" vorschreibt. Eine explizite Klarstellung, dass die Steuer-ID den Vermittlungsstellen nicht zugänglich sein darf, gibt es allerdings nicht. § 7 Abs. 2 S. 4 IDNrG-E fordert lediglich, dass diese ihre „Aufgabe ohne Kenntnis der Nachrichteninhalte erbringen können" müssen. Da die Vermittlungsstellen aber die Übermittlungsberechtigung abstrakt „kontrollieren und protokollieren" (§ 7 Abs. 2 S. 5 IDNrG-E), bleibt unklar, ob die Steuer-ID als Teil des Nachrichteninhalts angesehen wird oder aber Teil der zu protokollierenden Metadaten ist.

[145] Vgl. BfDI 2020, S. 7f. Auch für bereichsinterne Übermittlungen ist das 4-Corner-Modell nicht vorgesehen.

Fest steht allerdings, dass für eine Registermodernisierung nach diesem Konzept eine Verwendung der Steuer-ID als aPK nicht notwendig ist. Indem sie die Zusammenführung von Datensätzen eines Betroffenen unter Umgehung der Intermediäre vereinfacht, führt sie vielmehr zu einem zusätzlichen Risiko[146] und stellt die Rolle der Intermediäre sowie mit ihr die Sicherheitsfunktion des 4-Corner-Modells (s.u.) in Frage. Zur Erreichung der benötigten Funktionalität genügt es, wenn im Zusammenspiel mit dem Intermediär die angefragte Behörde (etwa das Bundeszentralamt für Steuern) die Anfrage zuverlässig einem gespeicherten Datensatz zuordnen und die angeforderten Daten übermitteln kann. Hierfür wird aus technischer Sicht keine gemeinsame ID (aPK) benötigt.[147]

Abb. 9 | Ablauf eines Datenabrufs nach Regierungsentwurf



Für die Weiterentwicklung des Modells ist eine Erkenntnis wichtig: Intermediäre, deren Einführung ohnehin vorgesehen ist, können außer der reinen Weiterleitung von Nachrichten auch zusätzliche Aufgaben erhalten. Statt der Verwendung der Steuer-ID oder eines sonstigen allgemeinen Personenkennzeichens (aPK) ist die Verwendung bereichsspezifischer Personenkennzeichen (bPK) so bereits mit einer kleinen technischen Modifikation des Modells aus dem Regierungsentwurf möglich. Indem die anfallende Aufgabe der Verwaltung von bPK den Intermediären zugeteilt wird, kann ein Zusatzaufwand bei den zahlreichen registerführenden Stellen ganz oder größtenteils vermieden werden.

Als Argument gegen die Einführung von bPK mag angeführt werden, es sei für den Einzelnen nicht leistbar, sich zahlreiche bPK zu merken. Dieses Argument trägt aber aus folgenden Gründen nicht:

→ Auch die Steuer-ID merken sich vermutlich die wenigsten Bürger. Insofern sind mehrere bPK, die die Betroffenen sich ebenfalls nicht merken, keine deutliche Verschlechterung. Die Situation ist vergleichbar mit dem Umgang eines Bürgers mit mehreren Kontonummern, Versicherungsnummern etc.

→ Im Rahmen des E-Government kann Software — oder besser noch, zumindest in einer langfristigen Betrachtung, der Personalausweis — die Aufgabe der Verwaltung mehrerer bPK des Betroffenen, auch direkt im Zusammenhang mit der ohnehin benötigten Authentifizierung, übernehmen.

→ Das ohnehin einzurichtende Datencockpit kann dem Betroffenen nach erfolgter Authentifizierung Auskunft über seine bPK in verschiedenen Bereichen geben. Eine entsprechend gesicherte Abfragemöglichkeit sollte zumindest geprüft werden.

→ Als Authentifizierungsmerkmal, etwa am Telefon, ist die Steuer-ID ohnehin kaum geeignet — dafür ist sie schon jetzt und erst recht bei einer zukünftigen Verwendung als aPK zu vielen Dritten bekannt. Daher bringt es den Betroffenen auch wenig Mehrwert, sich die ID zu merken. bPK könnten in vielen Fällen, zumindest in Ermangelung besserer Alternativen, als ein Authentifizierungsmerkmal unter mehreren durchaus für die telefonische Verwendung geeignet sein.

→ Auch heute schon können Behörden Bürger ohne Vorlage einer Kennziffer identifizieren — im schlimmsten Fall bringen die bPK hier keine Verbesserung.

[146] Vgl. bereits *Sorge/Leicht*, ZRP 2020, S. 242 (243).
[147] Vgl. *Sorge/Leicht*, ZRP 2020, S. 243.

ERGÄNZENDE INFORMATIONEN

Dass die Einführung von bPK auch für Deutschland sinnvoll sein kann, ist durch die Einführung von bPK in Form der „Restricted Identification" des deutschen Personalausweises sowie des elektronischen Aufenthaltstitels in anderem Kontext bereits anerkannt. Dort werden ausweis- und anbieterspezifische Kennziffern erzeugt[148]. Ein direkter Einsatz der so erzeugten Kennziffern für die Registermodernisierung scheidet in der aktuellen Umsetzung zwar deshalb aus, weil die Kennziffern an den konkreten Ausweis und nicht an die Person gebunden sind, sich bei der Ausstellung eines neuen Ausweises also ändern. Das hindert aber weder an einer Einbindung des Ausweises in eine nationale Identitätsmanagement-Strategie noch daran, das Konzept von bPK fortzuentwickeln.

Wir stellen daher in den folgenden Abschnitten technische Modelle für die Umsetzung der Registermodernisierung mit bPK vor.

II. Vorschlag: Einführung neuer bereichspezifischer Personenkennzeichen

Die konkrete Umsetzung von bPK für die Registermodernisierung ist in verschiedenen Varianten möglich.
Abbildung 10 fasst die wesentlichen Optionen zusammen.

Abb. 10 | Morphologischer Kasten zu einem bereichspezifischen Personenkennzeichen

PK / ID-NR	AUSPRÄGUNGSFORMEN				
Einzigartigkeit	einzigartig			mehrfach vergeben	
Sichtbarkeit	nicht-sprechend			sprechend	
Ziffern oder Zeichen und Umfang des Zeichensatzes	numerische Ziffernreihenfolge (0-9)			alphanumerische Zeichenreihenfolge (0-9, A-Z, a-z)	
Prüfziffer	mit Prüfziffer			ohne Prüfziffer	
Typus von Personenkennzeichen	allgemeine Verwendung (aPK: wesentliche Bereiche)		bereichsübergreifende Verwendung (2wPK: 2 oder wenige Bereiche)		bereichsspezifische Verwendung (bPK: 1 Bereich)
Vorgehen bei der Vergabe	zentrale Vergabe			dezentrale Vergabe	
Zu erfassende Personengruppe	Deutsche Bürger	Ausländer	Steuerzahler	Natürliche Personen	Juristische Personen
Basisdatensatz	mit Basisdatensatz			ohne Basisdatensatz	

Wir setzen mit unserem Vorschlag auf ein einzigartiges, nicht-sprechendes Personenkennzeichen. Dieses setzt sich aus mindestens 9 alphanumerischen Zeichen einschließlich einer Prüfziffer zusammen. Die Personenkennzeichen werden zentral vergeben und sollten alle deutschen Staatsangehörigen, alle Unionsbürger und alle Ausländer in Deutschland abdecken. Erfasst werden so alle natürlichen Personen. Die dazugehörigen Stammdaten sollen als Basisdaten gespeichert werden, etwa beim Bundeszentralamt für Steuern.

Mögliche technische Umsetzungen betrachten wir in den folgenden Abschnitten.

Bereits hier sei darauf hingewiesen, dass in keiner Variante die Gefahr einer bereichsübergreifenden Profilbildung völlig ausgeschlossen werden kann: Sobald für irgendeinen (legitimen) Zweck, etwa die Registerkonsolidierung, bPK einander zugeordnet werden können, ist es grundsätzlich möglich, eine solche Zuordnung auch für andere Zwecke zu nutzen.

[148] Vgl. BSI TR 03110 Part 2, Version 2.21, S. 31 f.

III. Stammzahl-Modell

Abb. 11 | Bereichsspezifische Personenkennziffer nach dem Stammzahl-Modell

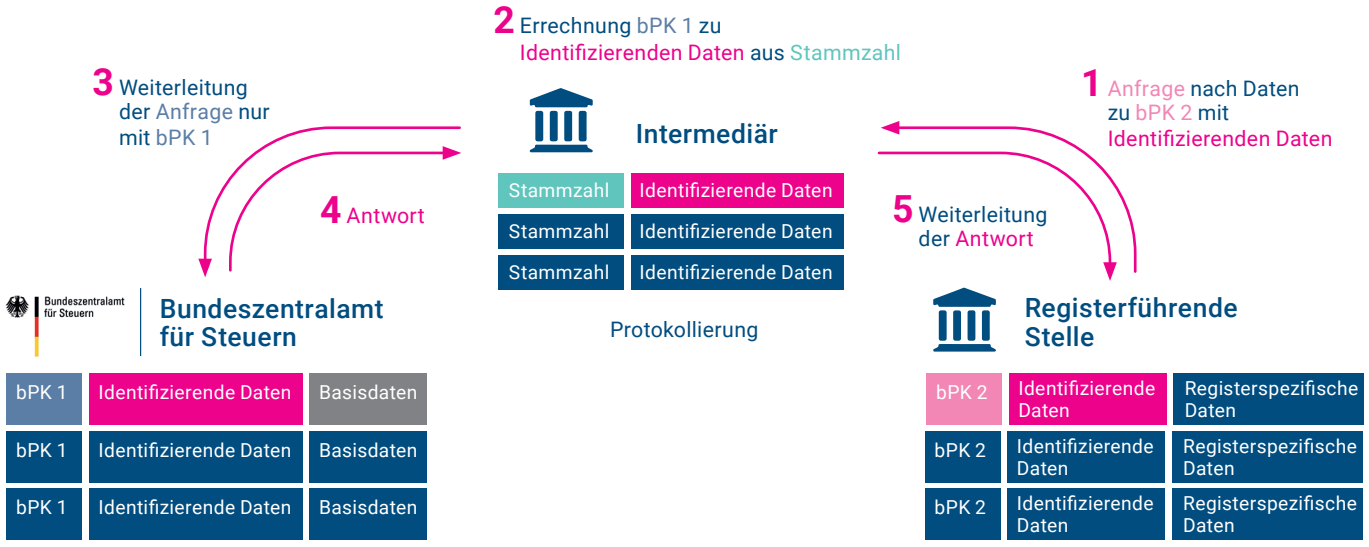
Abbildung 11 zeigt die Struktur einer Variante zur Umsetzung von bPK für die Registermodernisierung, die auf dem österreichischen Modell bereichsspezifischer Personenkennzeichen beruht.[149] Die österreichische Registerstruktur unterscheidet sich von der deutschen, so dass eine vollständige Übernahme des österreichischen Modells nicht möglich ist; der technische Kern ist aber übertragbar.

Hier wird jeder Person eine *Stammzahl* zugeordnet, die geheim gehalten wird und nicht vorhersehbar bzw. erratbar sein darf. Beispielsweise könnte jedem Inhaber einer Steuernummer eine ausreichend lange Zufallszahl als Stammzahl zugeordnet werden.

Die bPK wird aus der Stammzahl abgeleitet, indem eine kryptographische Hashfunktion auf die Stammzahl und die Bezeichnung des Bereichs (etwa „Steuer“) angewendet wird. Kryptographische Hashfunktionen garantieren – neben anderen Eigenschaften – dass aus der bPK nicht auf die Stammzahl zurückgeschlossen werden kann.[150] Auch lassen sich ohne Kenntnis der Stammzahl die bPK der gleichen Person für verschiedene Bereiche einander nicht zuordnen. Die Ausgabe einer kryptographischen Hashfunktion wird gelegentlich auch als „Fingerabdruck“ bezeichnet.[151] Kryptographische Hashfunktionen sind in der IT-Sicherheit schon lange etabliert; unter anderem werden sie im Rahmen der Erzeugung digitaler Signaturen eingesetzt und sind eine wesentliche technische Grundlage von Blockchains.

Auch, wenn die Stammzahl nicht aus einer bPK errechnet werden kann, wäre es denkbar, dass ein Angreifer systematisch Stammzahlen durchprobiert, zugehörige bPK mit Hilfe der Hashfunktion ableitet und mit tatsächlich vergebenen bPK vergleicht. Dem begegnet man mit einer ausreichenden Länge der Stammzahlen, die sich an der Länge der Schlüssel symmetrischer Verschlüsselungsverfahren orientieren kann (128 bis 256 bit).[152]

Abb. 12 | Ablauf eines Datenabrufs im Stammzahl-Modell



Will nun eine Behörde Daten aus einem anderen Bereich abfragen, schickt sie – in gleicher Weise wie im Regierungsentwurf vorgesehen – eine Anfrage an den Intermediär, dem die Stammzahl vorliegt (vgl. **Abbildung 12**).

Hier ergibt sich zunächst eine Schwierigkeit bei der Zuordnung der Anfrage zu einer Stammzahl durch den Intermediär. Aus der bPK kann auch der Intermediär die Stammzahl nicht berechnen. Ohne weitere Informationen hat er keinen Anhaltspunkt, welche der bei ihm gespeicherten Stammzahlen zu der bPK aus der Anfrage passt. Folglich benötigt er zumindest einen Minimaldatensatz zur Identifikation der Person, zu der eine Stammzahl gehört – etwa Nachname, Geburtstag und Geburtsort.[153] Dieser Datensatz ist folglich beim Intermediär zu speichern (oder muss zumindest für ihn abrufbar sein). Auch in der Anfrage muss dieser Datensatz so übermittelt werden, dass der Intermediär darauf zugreifen kann – bei Verwendung des Konzepts „doppelter Umschlag" muss der Datensatz also Teil der Metadaten einer Anfrage sein und nicht nur Teil der Inhaltsdaten im „inneren Umschlag", den der Intermediär nur verschlüsselt weiterleitet. Der Datensatz muss keine eindeutige Identifikation zulassen; kommen mehrere Personen in Frage, kann der Intermediär jeweils die bPK der entsprechenden Person ableiten, bis die bPK aus der Anfrage gefunden wird.

Der Intermediär berechnet nun (in Schritt 2) die bPK des anderen Bereichs und leitet die Anfrage gemeinsam mit der errechneten bPK (im Bild: bPK1) weiter. Auch bei der Weiterleitung der Antwort wird die dort enthaltene bPK wieder ersetzt.

Der Ansatz vermeidet damit die Verwendung einer einzelnen aPK, die zahlreichen Behörden und Unternehmen bekannt ist. Die sich ergebende Registerarchitektur ist sehr ähnlich zu der aus dem Regierungsentwurf. Es entsteht geringer Mehraufwand bei den Intermediären, wohingegen in den eingebundenen Registern lediglich eine bPK statt der Steuer-ID verwendet werden muss. Die Verschlüsselung der Kommunikationsinhalte kann in gleicher Weise wie im Regierungsentwurf, insbesondere auch nach dem Konzept des „doppelten Umschlags", umgesetzt werden. Voraussetzung ist lediglich die Übermittlung des jeweiligen bPK (sowie der o.g. identifizierenden Minimaldaten) in den Metadaten statt als Teil der verschlüsselten Inhaltsdaten, um deren Zuordnung durch den Intermediär zu ermöglichen.

Da der Intermediär die bPK aller Bereiche ableiten kann, ist neben einer zentralen Speicherung von Basisdaten bei einer Stelle (wie dem Bundeszentralamt für Steuern) auch eine verteilte Variante denkbar, bei der auf Daten unterschiedlicher Bereiche zurückgegriffen werden muss.

Eine Stärke des Ansatzes besteht darin, dass auch bei der Einführung neuer Behörden bzw. Bereiche die Ableitung von bPK nur anhand von Stammzahl und Bereichsbezeichner möglich ist. Dies ermöglicht perspektivisch eine einfache Integration in Systeme wie den elektronischen Personalausweis. Dieser bringt bereits die technische Basis für die sichere Speicherung der Stammzahl mit und könnte dezentral bPK erzeugen – selbst wenn die entsprechende Behörde bzw. der entsprechende Bereich zum Ausstellungszeitpunkt des Ausweises noch nicht existierte.

Unter Umständen könnte der Ansatz damit eine vertretbare Lösung darstellen, die im Vergleich mit dem gegenwärtigen Regierungsentwurf eine Verbesserung des Datenschutz- und Sicherheitsniveaus erreichen kann.

Er leidet aber unter mehreren Schwächen:

→ Bestehende IDs können nicht einfach integriert werden, sondern müssen durch neuartige bPK ersetzt oder ergänzt werden.

→ Um Kollisionsfreiheit (Ausschluss mehrfacher Verwendung der gleichen bPK) zu garantieren, müssen die bPK lang sein. Aktuelle Hashfunktionen haben oft eine Ausgabe mit einer Länge von 256 bit, was zwar für die Verwendung in IT-Systemen völlig unproblematisch ist. Sollen jedoch in der Praxis Menschen mit den bPK umgehen (z.B. Eintrag in Papierformulare oder Übermittlung per Telefon), ist eine Kürzung auf 80 bis 100 bit vermutlich möglich, ohne das Risiko zufälliger Kollisionen einzugehen. Dies entspricht aber immer noch einer mindestens 16stelligen alphanumerischen (also aus Buchstaben und Ziffern bestehende) Zeichenfolge.

→ Verwendet man als Intermediär lediglich eine zentrale Behörde, so hat dieser die Fähigkeit, alle bPK aller eingetragenen Personen einander zuzuordnen.[154] Das erhöht zwar die Flexibilität der Lösung. Jedoch bedeutet die grundsätzlich beliebige Zuordnungsmöglichkeit auch die Gefahr einer Profilbildung, wenn keine entgegenwirkenden technischen und organisatorischen Maßnahmen getroffen und dauerhaft aufrechterhalten werden. Gleichzeitig ist der Intermediär ein „Single Point of Attack". Im Fall eines erfolgreichen

[149] Vgl. Zum österreichischen Modell, insb. zur Erzeugung und zum Schutz von Stammzahl und bPK §§ 6 ff. des österreichischen E-GovG (Öst. Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen, E-Government-Gesetz – E-GovG).

[150] Vgl. *Stallings* 2017, Cryptography and Network Security (7th edition), S. 349.

[151] Vgl. *Katz/Lindell* 2014, Introduction to Modern Cryptography (2nd edition), S. 182.

[152] Bei 128 bit gibt es 2^{128} Möglichkeiten (340282366920938463463374607431768211456 oder ca. $3{,}4*10^{38}$ in Dezimalschreibweise), bei 256 bit sind es 2^{256} oder $1{,}16*10^{77}$ Möglichkeiten – also eine 78stellige Zahl. Schon bei 128 bit ist systematisches Durchprobieren nicht realistisch möglich.

[153] Alternativ kann bei einem Intermediär, der die Rolle der Vermittlungsstelle aus dem Regierungs-entwurf übernimmt, auch eine Tabelle mit Zuordnungen der bPK nur aus den vom Intermediär betreuten Bereiche gespeichert werden. In diese Umsetzung entstünde eine Mischform aus dem Stammzahl-Modell und dem unten vorgeschlagenen Neu-ID-Ansatz.

[154] Dies gilt, obwohl die bPK im Normalbetrieb nicht gespeichert werden. Gehen wir von je 100 bPK aus, die aus bereits vorliegenden Stammzahlen von ca. 100 Millionen Personen abgeleitet werden. Insgesamt wären dies 10 Milliarden bPK. Aktuelle Grafikkarten schaffen bis ca. 1 Milliarde Hashberechnungen pro Sekunde, könnten diese Berechnung also in 10 Sekunden durchführen; spezielle Hardware schafft die etwa für Bitcoin Mining notwendigen Hashberechnungen mit einer Rate von über 10 Billionen Berechnungen pro Sekunde, wäre also theoretisch in einer Millisekunde fertig. Durch Begrenzungen praktischer Rechnerarchitekturen mögen sich die Vorgänge etwas verlängern; sie stellen aber jedenfalls kein Hindernis für einen motivierten Angreifer dar. Anschließend lassen sich die bPK ohne nennenswerten Aufwand einander zuordnen. Zwar gibt es Techniken, die den Vorgang der Hashberechnung verlangsamen. Eine solche Verlangsamung wirkt sich aber im gleichen Maß auf die Ableitung der bPK im Normalbetrieb aus. Wenn die Ableitung von bPK schnell genug sein muss, um auch bei Lastspitzen im Normalbetrieb zu funktionieren, kann sie nicht gleichzeitig langsam genug sein, um Missbrauch durch Erzeugung von Tabellen mit allen bPK aller Personen zu verhindern. Es sind folglich ergänzende Maßnahmen erforderlich.

Angriffs oder Missbrauchs fällt die Lösung schlimmstenfalls auf den Stand des Regierungsentwurfs zurück.

→ Verteilt man die Rolle des Intermediärs auf mehrere Stellen – wie im Ansatz durch die Einführung von Vermittlungsstellen bereits in § 7 Abs. 2 IDNrG-E vorgesehen –, so gibt es zwei Möglichkeiten: Entweder werden bei jeder dieser Stellen die Stammzahlen aller Personen gespeichert, für die die Vermittlungsstelle zuständig ist. Diese Möglichkeit bedeutet somit aber auch mehr Angriffspunkte und Missbrauchsmöglichkeiten bzw. aus anderer Sicht einen höheren Aufwand für die Absicherung der Stammzahlen. Oder es wird eine Hierarchie von Stammzahlen und bPK erzeugt: Aus der zentralen Stammzahl werden bPK wie oben beschrieben erzeugt und an Vermittlungsstellen gegeben, die daraus wiederum nach dem gleichen Prozess Unter-bPK für die ihnen zugeordneten Bereiche erzeugen. Das ist technisch machbar, gerade bei sich überschneidenden Zuständigkeiten von Vermittlungsstellen erhöht sich die Komplexität des Systems damit aber erheblich.

→ Da alle bPK bei diesem Ansatz aus einer Stammzahl abgeleitet werden, ist die Neuvergabe einer bPK (etwa im Fall eines „Identitätsdiebstahls") mit der Neuvergabe der Stammzahl und damit aller anderen bPK verbunden.

Insgesamt kann festgehalten werden, dass dieses Modell gegenüber dem des Regierungsentwurfs bereits deutlich datenschutzfreundlicher und auch mit nur geringem Mehraufwand umsetzbar ist. Die Nachteile des Ansatzes fallen aber durchaus ins Gewicht, so dass keine uneingeschränkte Empfehlung dafür ausgesprochen werden kann. Eine Übersicht der wesentlichen Stärken und Schwächen in Form einer SWOT-Analyse ist in Abbildung 13 dargestellt. Im Folgenden entwickeln wir den Alternativansatz NEU-ID, der die benannten Schwächen weitgehend vermeidet.

Abb. 13 | SWOT-Analyse zum Identitätsnummernsystem Stammzahl-Modell

STÄRKEN

- → Bereits deutlich datenschutzfreundlicher im Vergleich zum Regierungsentwurf
- → Weitestgehendes Beibehalten der aktuellen Registerstruktur möglich
- → Verzicht auf Einführung einer aPK
- → Datenaustausch zwischen Behörden ohne Kenntnis der jeweils anderen bPK möglich
- → bPK für neu eingeführte Bereiche mit Kenntnis der Stammzahl jederzeit einfach errechenbar (auch z.B. bei Umsetzung im Personalausweis)

SCHWÄCHEN

- → Notwendigkeit, bei den Intermediären identifizierende Daten zu speichern
- → Intermediäre werden zu einem attraktiveren Ziel für Angreifer
- → Notwendigkeit, bPK neu zu generieren
- → Länge der bPK erschwert Handhabung etwa am Telefon
- → Erhöhter Aufwand bei verteilter Realisierung

CHANCEN

- → Reichweitenbegrenzung von Profilbildungen durch bPK
- → Einbindung des Personalausweises perspektivisch möglich
- → Reduktion der Datenspeicherung in einzelnen Registern durch einfache und datenschutzkonforme Abrufmöglichkeiten

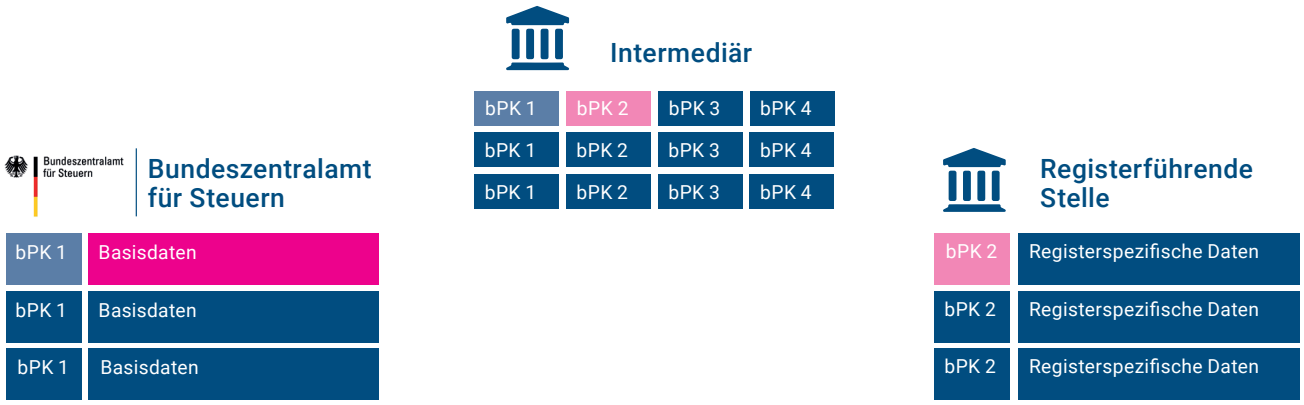
RISIKEN

- → Weiterhin bestehende, wenn auch gemilderte Gefahr bereichsübergreifender Datenzusammenführung zur Profilbildung
- → Möglichkeit der Erstellung von Transaktionsprofilen
- → Möglichkeit von Datenpannen bei den Intermediären

IV. Neuartige bereichsspezifische Personenkennzeichen (NEU-ID)

Statt des Minimaldatensatzes speichert der Intermediär die bPK verschiedener Bereiche bei diesem Ansatz selbst. Somit liegt beim Intermediär – nur – eine Tabelle vor, die für jede Person eine Liste von bPK enthält, aber keine weiteren Informationen zur Person (vgl. **Abbildung 14**). Die Festlegung einer Stammzahl ist bei dieser Variante nicht erforderlich. Bei den Intermediären, die die Rolle der Vermittlungsstellen aus dem Regierungsentwurf übernehmen, sind diejenigen Teile der Tabelle gespeichert, die für die konkrete Aufgabenerfüllung benötigt werden: Soll zwischen zwei Bereichen vermittelt werden, werden auch nur die bPK dieser beiden Bereiche gespeichert.

Abb. 14 | Grundkonzept NEU-ID

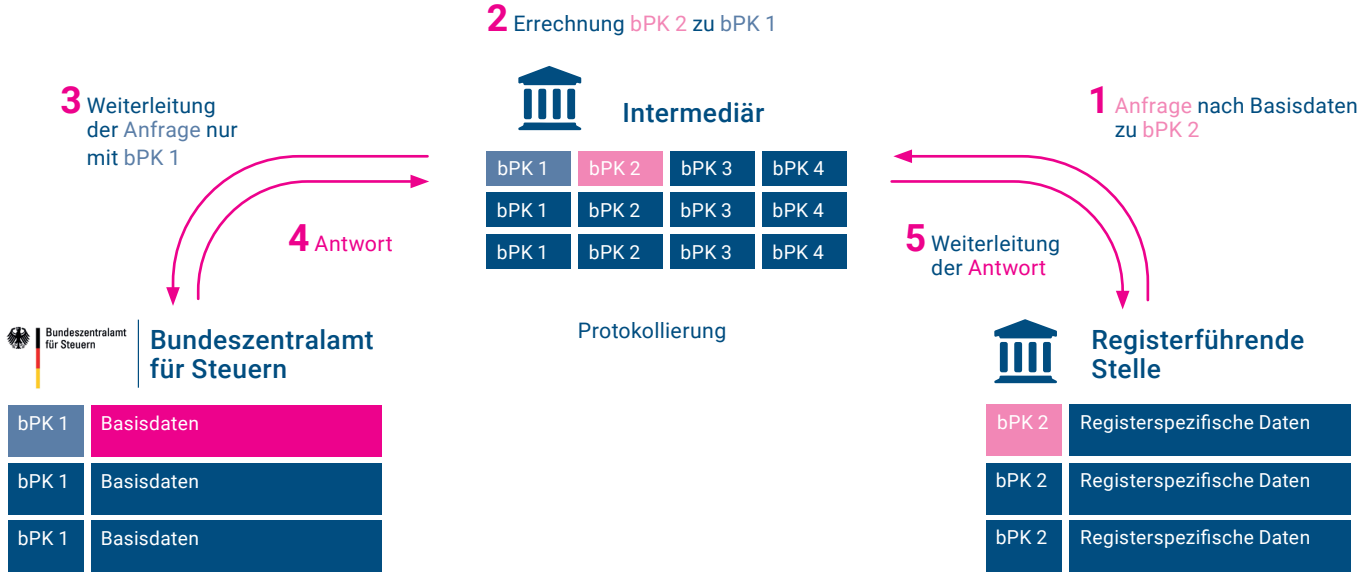


bPK müssen nicht mehr die Ergebnisse von Hash-Berechnungen sein. Die Speicherung der bPK in einer Tabelle erlaubt einerseits die Weiterverwendung bereits bestehender bPK wie der Steuer-ID. Andererseits können neue bPK erzeugt werden. Diese können deutlich kürzer sein als im oben dargestellten Stammzahl-Modell – wo die Länge der bPK zufällige „Kollisionen", also doppelt erzeugte bPK, vermeiden soll. Die Gefahr, dass zufällig zwei identische bPK erzeugt werden, besteht nämlich deshalb nicht, weil neu erzeugte bPK einfach in der bestehenden Tabelle mit den bereits bestehenden abgeglichen werden können. Da keine Anforderung besteht, dass eine bPK ein Hashwert einer Stammzahl sein muss, kann im Fall einer solchen Kollision die bPK schlicht so oft zufällig neu erzeugt werden, bis keine Kollision mehr auftritt.

Die Erzeugung kann in den einzelnen Bereichen oder – um einfacher die Kollisionsfreiheit zu garantieren – beim (zentralen) Intermediär vorgenommen werden. Um die Handhabung außerhalb von IT-Systemen fehlertolerant zu gestalten, sollte eine Prüfziffer[155] verwendet werden.

Abbildung 15 zeigt beispielhaft den Ablauf bei einem Datenabruf vom Bundeszentralamt für Steuern. Ganz wie im Stammzahl-Modell übernimmt der Intermediär die Zuordnung von bPKs und sorgt dafür, dass die bPK eines Bereichs nicht an einen anderen Bereich weitergeleitet wird. Hier wird auch nochmals deutlich, dass der Intermediär für die Zuordnung keinerlei andere Daten braucht als die bPK selbst. Ist der Intermediär, etwa als Vermittlungsstelle, nur für wenige Bereiche zuständig, benötigt er auch nur die bPK dieser Bereiche.

Abb. 15 | Ablauf eines Datenabrufs im NEU-ID-Modell



[155] Eine Prüfziffer (vgl. Abschnitt A.III) wird der eigentlichen ID angehängt oder vorangestellt. Sie wird nach einer öffentlich bekannten Rechenvorschrift berechnet. Wird die ID nebst Prüfziffer eingegeben, so kann die neu errechnete Prüfziffer mit der eingegebenen verglichen und ein Eingabefehler mit hoher Wahrscheinlichkeit erkannt werden.

Eine Risikoerhöhung im Vergleich zum oben beschriebenen Stammzahl-Modell scheint sich dadurch zu ergeben, dass die Zuordnung unterschiedlicher bPK den Intermediären jederzeit möglich ist. Tatsächlich ist dies beim Stammzahl-Modell aber auch so, denn dort liegen die zur Berechnung der bPK erforderlichen Informationen ebenfalls vor – wenn auch nicht in sofort verfügbarer und nutzbarer Form, sondern nur als Stammzahl.[156] Die wesentlichen, oben aufgeführten Vorteile blieben bei der neuen Variante erhalten. Da der Intermediär die benötigten bPK kennt, reicht es, wenn Anfragen seitens einer registerführenden Stelle deren bPK als Teil der Metadaten beinhalten. Weitere identifizierende Daten, wie beim Stammzahl-Modell vorgesehen, müssen weder an den Intermediär übermittelt noch dort gespeichert werden. Ist der anfragenden Stelle keine bPK bekannt, wird diese wie bereits im RegMoG-E nach dem 4-Corners-Modell vorgesehen verschlüsselt an die Stelle (im Beispiel: Bundeszentralamt für Steuern) weitergeleitet, die die Basisdaten speichert. Die Antwort enthält eine bPK, die dann wiederum in die bPK des anfragenden Bereichs übersetzt wird. Risiken, die sich bereits grundsätzlich aus dem Vorhandensein einer Zuordnung von bPK ergeben, bleiben bestehen.

Die technische Umsetzung des Ansatzes ist völlig unproblematisch. Rechnet man – auch zukünftige Generationen berücksichtigend – mit einer Milliarde Personen, die jeweils 100 bPK[157] benötigen, müssen 100 Milliarden unterschiedliche bPK möglich sein. Dies gilt jedenfalls, wenn die gleiche bPK nicht in mehreren Bereichen (auch für unterschiedliche Personen) verwendet werden soll. Ein solches bPK kann in weniger als 5 Byte[158] (ggf. zzgl. einer Prüfziffer, die aber beim Intermediär nicht gespeichert werden müsste) repräsentiert werden, so dass alle bPK der derzeit in Deutschland lebenden Personen in unter 50 Gigabyte Speicher unterzubringen wären.[159] Auf dem heutigen Stand der Technik sind solche Datenmengen problemlos handhabbar; schon gängige Smartphones haben eine höhere Speicherkapazität. Die angenommenen Werte sind dabei eher hoch gegriffen – vermutlich genügen deutlich weniger als 100 bPK pro Person. Zu den Stärken des Ansatzes gehört, dass eine solche kurze bPK praktisch für die menschliche Verwendung ist und beispielsweise auch telefonisch durchgegeben werden kann – etwa als 9-stellige alphanumerische Zeichenfolge (also Buchstaben und Ziffern)[160] oder in 4 Codewörtern (z.B. „Kellner Straße Maus Montag").

Auch bei dieser Variante besteht die Möglichkeit der Profilbildung unter Mitwirkung des Intermediärs. Dieser hat zwar wenige Informationen über einzelne Personen und kennt insbesondere nicht ihre Namen. Die jeweiligen bPK sind aber dennoch als personenbezogene Daten einzuordnen (vgl. zum Begriff Abschnitt B.II). Im dargestellten Grundmodell genügt es insbesondere beim zentralen Intermediär, wenn dieser Kenntnis über eine einzelne bPK erlangt, um einer Person all ihren anderen bPK zuordnen zu können. Missbrauch durch Innentäter oder erfolgreiche Angriffe auf den Intermediär lassen die Variante, ebenso wie das oben dargestellte Stammzahl-Modell, auf das Datenschutz- und Sicherheitsniveau des Regierungsentwurfs zurückfallen.

Die wesentlichen Stärken und Schwächen des NEU-ID-Ansatzes sind in **Abbildung 16** zusammengefasst.

Abb. 16 | SWOT-Analyse zum Identitätsnummernsystem NEU-ID

STÄRKEN

- •Wesentlich datenschutzfreundlichere und zugleich funktionale Implementierungsvariante
- Weitestgehendes Beibehalten der aktuellen Registerstruktur möglich
- Verzicht auf Einführung einer aPK
- Datenaustausch zwischen Behörden ohne Kenntnis der jeweils anderen bPK möglich
- Kurze bPK erleichtern Nutzung etwa am Telefon
- Speicherung ausschließlich von bPK bei den Intermediären

SCHWÄCHEN

- Weitgehend zentralisierte Verwaltung und Vergabe von bPK notwendig
- Intermediäre werden zu einem attraktiven Ziel für Angreifer (vgl. Stammzahl-Modell)

CHANCEN

- Reichweitenbegrenzung von Profilbildungen durch bPK
- Eignung des Ansatzes für die weitere Verteilung von Identitätsmanagement-Aufgaben mit föderalem Ansatz
- Einbindung des Personalausweises perspektivisch möglich
- Reduktion der Datenspeicherung in einzelnen Registern durch einfache und datenschutzkonforme Abrufmöglichkeiten

RISIKEN

- Weiterhin bestehende, wenn auch gemilderte Gefahr bereichsübergreifender Datenzusammenführung zur Profilbildung
- Möglichkeit der Erstellung von Transaktionsprofilen
- Möglichkeit von Datenpannen bei den Intermediären

V. Optionen für die Verbesserung beider Modelle

Zusätzlich kommen einige Lösungsansätze in Frage, die zusammengenommen weiter dazu beitragen können, die oben dargestellten Risiken zu reduzieren – ob beim NEU-ID-Modell oder beim Stammzahl-Modell. Wir beschreiben diese in den folgenden Abschnitten.

1. Institutionelle Unabhängigkeit des Intermediärs

Die Einrichtung des zentralen Intermediärs beim Bundesverwaltungsamt – einer Behörde im Geschäftsbereich des BMI – ist aus fachlicher Sicht nachvollziehbar. Das Vertrauen in die auch langfristig sichergestellte, ausschließlich zweckgebundene Verwendung der Zuordnungsmöglichkeiten ließe sich aber durch die Einrichtung bei einer unabhängigen, nicht weisungsgebundenen Stelle erheblich erhöhen, weshalb wir diese Variante als klar vorzugswürdig ansehen. Denkbar ist dies etwa unter der administrativen Verantwortung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit oder der Datenschutzbeauftragten der Bundesländer (vgl. nächster Punkt). Für zusätzliche Vermittlungsstellen, wie im Regierungsentwurf angelegt, gilt im Prinzip das Gleiche; allerdings ist hier eine Risikoreduktion je nach konkreter Funktion zumindest beim NEU-ID-Modell auch denkbar, indem dort lediglich die bPK sehr weniger Bereiche gespeichert werden (s.u.).

Weitere Aufgaben der Registermodernisierungsbehörde neben der Intermediärsrolle werden durch diesen Vorschlag nicht berührt.

2. Föderierter Ansatz

Ein sogenanntes föderiertes Identitätsmanagement, bei dem auf eine zentrale Datenbank mit Identitätsinformationen verzichtet wird, ist bereits gängig.[161] Es setzt lediglich Vertrauen zwischen den Institutionen voraus, die die Identitäten (und ggf. Authentifizierung) der anderen Teilnehmer des föderierten Identitätsmanagement-Systems anerkennen und nutzen. Dies lässt sich, wie schon die Bezeichnung nahelegt, leicht mit der föderalistischen Struktur der Bundesrepublik Deutschland in Einklang bringen. Angesichts der Bedeutung der Verwaltungshoheit der Länder wären zumindest Ansätze eines föderierten Identitätsmanagements auch im Rahmen der Registermodernisierung nach Auffassung der Autoren ohnehin wünschenswert. Verschiedene Umsetzungsvarianten sind denkbar. Die einfachste Lösung wäre wohl, die zentrale Intermediärsrolle[162] zwar beizubehalten, aber statt einer Bundesbehörde je einen zuständigen Intermediär pro Bundesland vorzusehen – was Verwaltungskooperationen mehrerer Länder natürlich nicht ausschließt. Die Identifikation des jeweils zuständigen Intermediärs anhand des Wohnsitzlandes dürfte sich unproblematisch gestalten. Im Einzelfall, wenn das aktuelle Wohnsitzland der anfragenden Stelle nicht bekannt ist, kann sich die Notwendigkeit ergeben, eine Anfrage an alle in Frage kommenden Intermediäre zu senden.

Für die Erzeugung der bPK müssen den Intermediären im NEU-ID-Modell jeweils Nummernbereiche zugeordnet werden. Beim Stammzahl-Modell kann dies entfallen, da die Stammzahlen ohnehin so lang sein müssen, dass zufällige Kollisionen nicht auftreten. In beiden Modellen sind Vorkehrungen für die Übermittlung von Datensätzen bei Umzug und Konsistenzprüfungen zu treffen. Eine Anbindung an das geplante Datencockpit lässt sich leicht ergänzen – in gleicher Weise, wie dies für die Intermediäre (Registermodernisierungsbehörde, Vermittlungsstellen) des Regierungsentwurfs möglich ist. Alle weiteren Abläufe blieben bei diesem Ansatz unverändert. Die höhere Anzahl an Intermediären bedeutet in der Summe vermutlich höhere Kosten, insbesondere angesichts des Aufwands zur Absicherung – allerdings wird gleichzeitig die Problematik des „Single Point of Attack" abgemildert. Die Funktion der Vermittlungsstellen lässt sich in vergleichbarer Weise verteilt realisieren; wenn diesen aber jeweils nur die bPK weniger Bereiche vorliegen, kann im NEU-ID-Modell ggf. auch eine zentralisierte Umsetzung unter Umständen vertretbar sein.

3. Bürger als lokale Intermediäre

Die Intermediärsfunktion muss nicht in allen Fällen überhaupt durch eine Behörde ausgeübt werden. So ließe sich für viele Verfahren als Regelfall die Übernahme der Funktion durch den Betroffenen selbst – technisch umgesetzt entweder in einer App, die digital signierte Informationen von den zuständigen Behörden speichert und verwaltet, ohne allerdings die Daten an den technischen Betreiber des Betriebssystems oder der App weiterzugeben, oder in einer Weiterentwicklung des elektronischen Personalausweises – etablieren. Der Rückgriff auf die Datenbank bei einer Behörde wäre dann nur noch in Fällen notwendig, bei denen der Betroffene nicht mitwirken kann oder will – also z.B. bei Verlust des Ausweises oder bei Vorgängen wie dem Zensus,

[156] Vgl. Fn. 153.

[157] Der Regierungsentwurf (§ 7 Abs. 2 S. 2) geht von mindestens sechs Bereichen aus, bei denen eine bereichsübergreifende Kommunikation unter Einschaltung von Vermittlungsstellen realisiert wird. Die tatsächlich sinnvolle Zahl einzurichtender Bereiche wird vermutlich über sechs, aber deutlich unter den 100 Bereichen der hier vorgenommenen, bewusst großzügigen Abschätzung liegen.

[158] 5 Byte entsprechen 40 bit. Das genügt, um 2^{40} Möglichkeiten zu repräsentieren; dies entspricht etwa 1,1 Billionen oder ca. dem Zehnfachen der nach obiger Rechnung benötigten 100 Milliarden. Für deren Repräsentation würden 37 bit genügen, doch sind ganze Byte in der Ver¬arbeitung ggf. einfacher und lassen eine Reserve für mögliche Erweiterungen. Lässt man zu, dass die gleiche bPK in mehreren Bereichen – dann für jeweils andere Personen – gültig ist, lässt sich die Länge auf 30 bit reduzieren.

[159] Bei der Weiterverwendung bereits bestehender bPK wird sich der Speicherbedarf etwas ändern, nicht aber dessen Größenordnung.

[160] Um 40 bit in 8 Stellen – also 5 bit pro Stelle – zu codieren, muss es pro Stelle 32 Möglichkeiten geben, also 10 Ziffern zzgl. 22 Buchstaben. Die 9. Stelle kann als Prüfziffer dienen. Das gleiche Prinzip lässt sich für Codewörter anwenden. Lässt man 4096 gültige Wörter zu, entspricht dies 12 bit pro Wort. In 4 Codewörtern lässt sich die bPK also einschließlich einer Prüfziffer darstellen.

[161] Etwa im elektronischen Rechtsverkehr nach dem SAFE-Standard („Secure Access to Federated E-Justice/E-Government"), vgl. https://www.it-planungsrat.de/DE/Projekte/Anwendungen/SAFE/sAFE.html

[162] Also die im Regierungsentwurf für die Registermodernisierungsbehörde beim Bundesverwaltungs¬amt vorgesehene Rolle beim Abruf und der Übermittlung von Daten.

die eine Mitwirkung des Einzelnen zu aufwendig erscheinen lassen. Diese Variante dürfte sich kurzfristig nur schwer umsetzen lassen, erscheint mittelfristig aber aus Gründen des Datenschutzes und der Transparenz durchaus erwägenswert. Eine besonders elegante Umsetzung der Variante ist im Stammzahl-Modell möglich, da mit Kenntnis der Stammzahl eine einfache Erzeugung von bPK auch für im Vorhinein nicht festgelegte Bereiche besteht.

4. Einschränkung möglicher Zuordnungen

In der bisherigen Darstellung haben wir die Einschränkung möglicher Zuordnungen zwischen den bPK verschiedener Bereiche nicht problematisiert – also die Frage, ob grundsätzlich bPK aus jedem Bereich in bPK jedes anderen Bereichs überführt werden können sollen. Der Regierungsentwurf geht aber bereits davon aus, dass keine beliebigen Kommunikations-beziehungen zwischen registerführenden Stellen unterschiedlicher Bereiche zugelassen sind. Neben dem Abruf der Basisdaten, die beim Bundeszentralamt für Steuern gespeichert werden, sind nach § 7 Abs. 2 IDNrG-E auch sonstige Datenübermittlungen zwischen öffentlichen Stellen möglich; hier wird aber die abstrakte Übermittlungsberechtigung durch eine Vermittlungsstelle geprüft, die also die Rolle eines Intermediärs einnimmt. Dieses Konzept sollte in dem von uns vorgeschlagenen Modell nicht nur beibehalten werden; vielmehr sollten auch die Zuordnungen von bPK, die für legitime Zwecke nicht benötigt werden, weitestgehend technisch verhindert werden. Will man Basisdaten weiterhin beim Bundeszentralamt für Steuern speichern, wären Anfragemöglichkeiten des dafür verwendeten Intermediärs also auf die Zuordnung eines beliebigen andere bPK auf die beim Bundeszentralamt für Steuern verwendete bPK (vermutlich die Steuer-ID) und umgekehrt beschränkt.

Auch die im Regierungsentwurf vorgesehenen Vermittlungsstellen dürfen keine beliebigen Zuordnungen vornehmen. bPK von Bereichen, aus denen andere Bereiche keine Daten abrufen müssen oder für die die Vermittlungsstelle nicht zuständig ist, dürfen dort nicht dauerhaft gespeichert werden. Im Stammzahl-Modell lässt sich dies nur eingeschränkt umsetzen, etwa wie oben beschrieben durch die Nutzung einer Hierarchie von Stammzahlen und bPK. Das NEU-ID-Modell erlaubt hier eine einfache, recht flexible Umsetzung. Auch dort kann es aber vorkommen, dass einer Vermittlungsstelle mehr Zuordnungen möglich sind, als tatsächlich vorgenommen werden dürfen. Entsprechende Einschränkungen sind zumindest durch Zugriffsregeln durchzusetzen. Wie im Regierungsentwurf vorgesehen,[163] dürfen Anfragen, bei denen abstrakt keine Übermittlungsberechtigung vorliegt, nicht beantwortet werden und sind zu protokollieren. Der Unterschied zum Regierungsentwurf liegt in unserem Ansatz darin, dass dem Anfragenden aus einem anderen Bereich die Ziel-bPK nicht vorliegt und eine Umgehung des Intermediärs somit erschwert wird.

5. Technische Sicherheit

Selbstverständlich ist der Intermediär nach dem Stand der Technik abzusichern. Dies ergibt sich – neben den Erwägungen aus dem nationalen Verfassungsrecht[164] – auch unionsrechtlich aus Art. 87 DSGVO i.V.m. Art. 5 Abs. 1 lit. f) und Art. 24 DSGVO.[165] Dieser sieht vor, dass die Verwendung von nationalen Kennziffern, sowie von anderen Kennziffern von allgemeiner Bedeutung, nur unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Personen zulässig ist. Der Gesetzgeber muss diese Garantien daher u.a. durch geeignete technische und organisatorische Maßnahmen sicherstellen.[166] Aufgrund der hohen Anzahl potentiell Betroffener im Fall einer Verletzung des Schutzes der gespeicherten personenbezogenen Daten ist ein strenger Maßstab an diese Vorkehrungen anzulegen.[167]

Ein geeignetes Mittel, das bei beiden Modellen in die entsprechende Sicherheitsarchitektur integriert werden kann, sind sogenannte Hardware-Sicherheitsmodule (HSM). Solche Geräte sind beispielsweise in der Finanzbranche üblich, werden aber auch beim besonderen elektronischen Anwaltspostfach eingesetzt. Im Normalbetrieb lassen HSM nur vorher definierte Anfragen zu; darüber hinaus gehende Daten werden nicht preisgegeben.[168] Es besteht somit auch ein Schutz gegen Innentäter; Angriffe auf die Hardware führen i.d.R. zur Zerstörung der Daten. So lassen sich Zugriffsbeschränkungen sicher umsetzen und die Rate von Anfragen limitieren. Soll, etwa wegen Hardware-Defekten, eine Übertragung des Inhalts eines HSM auf ein anderes erfolgen, ist ein über den Normalbetrieb hinausgehender Zugriff erforderlich. Dieser lässt sich an Bedingungen knüpfen – in der Regel die Verwendung mehrerer kryptographischer Schlüssel, die bei verschiedenen Personen hinterlegt sind. Hier könnten wiederum die Datenschutzaufsichtsbehörden in Spiel kommen.

Es sei an dieser Stelle betont, dass die Verwendung eines HSM alleine noch keine Sicherheit erzeugt; vielmehr muss auch ein HSM in eine Sicherheitsarchitektur eingebunden werden, die sowohl technische als auch organisatorische Maßnahmen umfasst.

6. Beschränkung des Verwendungszwecks

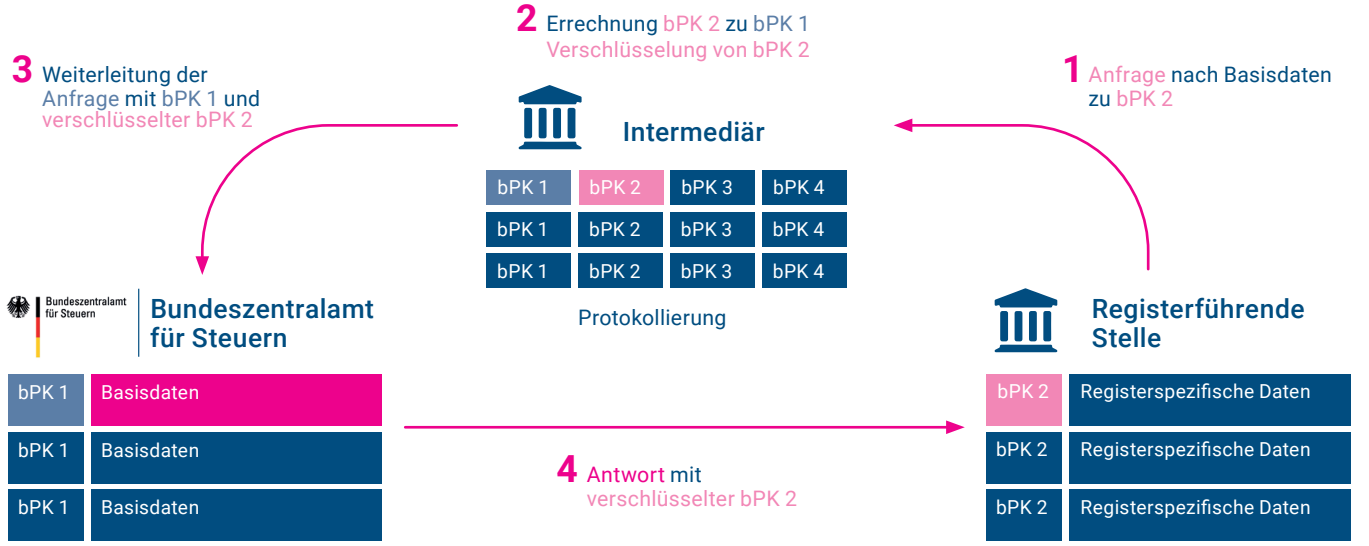
Es ist durchaus denkbar, die Zuordnung von bPK lediglich auf wenige, festgelegte Zwecke wie den Zensus zu beschränken. Die Abwägung zwischen den Vorteilen durch eine weitergehende Registerkonsolidierung und den Risiken für die Privatsphäre der Betroffenen soll an dieser Stelle nicht vertieft werden. Sie muss jedoch vom Gesetzgeber reflektiert werden.

[163] Vgl. § 7 Abs. 2, § 9 Abs. 1 IDNrG-E.
[164] Siehe oben unter B. III.
[165] Siehe oben unter B. IV. 2.
[166] Vgl. *Pauly in Paal/Pauly*, DSGVO, 2. Aufl. 2018, Art. 87 Rn. 3; *Ehmann* in *Ehmann/Selmayr*, DSGVO, Art. 87 Rn. 9.
[167] Siehe oben unter B. III. 3. c) (1).
[168] Ausführlich zur Funktionsweise von Hardware-Sicherheitsmodulen *Smith* in *Rosenberg* (Hrsg.) 2010, Handbook of Financial Cryptography and Security, 257ff.

ERGÄNZENDE INFORMATIONEN

Eine weitere Option besteht darin, einer Behörde aus einem Bereich die bPK eines anderen Bereichs verschlüsselt zugänglich zu machen – und zwar, wie mit asymmetrischer Kryptographie problemlos machbar, dass Behörden immer nur die für ihren eigenen Bereich gültige bPK entschlüsseln können. Somit ist neben den durch den Regierungsentwurf bereits vorgesehenen Abläufen auch eine direkte Kommunikation der Behörden untereinander machbar, wobei eine Behörde fremde bPK nie im Klartext zu sehen bekäme. Die vorgesehene Protokollierung von Datenabrufen, die der Transparenz gegenüber dem Bürger dient, müsste dann anhand der Abrufe der verschlüsselten bPK erfolgen oder dezentral durch die beteiligten Behörden angestoßen werden. Beispielhaft ist dieser Ablauf in **Abbildung 17** dargestellt.

Abb. 17 | Variante mit verschlüsselter Übermittlung von bPK



VI. Zwischenfazit

Wir möchten an dieser Stelle betonen, dass die hier entwickelten Modelle – einschließlich der dargestellten Ergänzungen des Grundmodells – nicht als Idealmodell einer IdentitätsmanagementInfrastruktur für die öffentliche Verwaltung in Deutschland angesehen werden sollten. Vielmehr sind diese Modelle bewusst so gestaltet, dass die bestehenden Register möglichst wenig angepasst werden müssen. Ausgangspunkt unserer Überlegungen ist der Regierungsentwurf, dessen grundsätzliche Architektur vorliegend übernommen und nur dort angepasst wird, wo wir Möglichkeiten sehen, Missbrauchspotentiale ohne Einschränkungen der Funktionalität zu reduzieren.

Abbildung 18 und **Abbildung 19** zeigen die wesentlichen Eigenschaften beider Modelle für bereichsspezifische Personenkennzeichen in einer zusammenfassenden Darstellung. Sie sehen die weitgehend zentrale Vergabe der bPK vor – im Stammzahl-Modell als Ableitung aus einer zufällig gewählten Stammzahl pro Betroffenem, bei NEU-ID direkt als Zufallszahl oder durch Übernahme bestehender bPK. Es ist grundsätzlich die Erfassung beliebiger Personengruppen möglich; wir gehen hier von natürlichen Personen (Deutschen und in Deutschland lebenden Ausländern) aus.

Beide Modelle ermöglichen den Zugriff auf einen Basisdatensatz, der wie im Regierungsentwurf vorgesehen beim Bundeszentralamt für Steuern gespeichert werden kann. Sie erzwingen ihn jedoch nicht. Das Stammzahl-Modell leitet bPK bei Bedarf aus Stammzahlen ab; im NEU-ID-Modell werden bPK beim Intermediär gespeichert. Während sonstige Aufgaben der Registermodernisierungsbehörde unberührt bleiben, favorisieren wir in beiden Modellen eine Wahrnehmung der Rolle zumindest des zentralen Intermediärs bei einer unabhängigen Stelle wie den Datenschutz-Aufsichtsbehörden. Dieses Vorgehen reduziert die Wahrscheinlichkeit eines Missbrauchs (wie die Herausgabe von bPK-Zuordnungen ohne Rechtsgrundlage) und reduziert schlimmstenfalls die Zahl der davon Betroffenen. Die Folgen möglicher Sicherheitsvorfälle können durch einen föderierten Ansatz (Verteilung von Intermediären bzw. Vermittlungsstellen) reduziert werden. Schränkt man die möglichen bPK-Zuordnungen so weit wie möglich ein und reduziert mit geeigneten technischorganisatorischen Maßnahmen – insbesondere auch durch sichere Hardware (HSM), die wir bei beiden Modellen favorisieren – die Erfolgswahrscheinlichkeit externer und interner Angreifer, so lässt sich bereits zeitnah ein akzeptables Datenschutzniveau erreichen. Die Umsetzung einer lokalen Intermediärsfunktion, die die Zuordnungen – und damit die Freigabe der dadurch zugreifbaren Daten – direkt beim Betroffenen vor-

nimmt, mag erst mittelfristig umgesetzt werden können. Sie kann die ansonsten vorgesehenen Intermediäre nicht ersetzen, aber in geeigneten Anwendungsfällen die Kontrolle des Bürgers über seine personenbezogenen Daten stärken.

Als Leitbild kann insgesamt gelten: Legitime Zuordnungen zwischen den bPK verschiedener Bereiche bleiben möglich, illegitime können zuverlässiger als nach dem Regierungsentwurf verhindert werden. Wir gehen davon aus, dass die meisten Aspekte des von uns vorgeschlagenen Modells sich bereits kurzfristig realisieren lassen. Unverzichtbar erscheint uns aber dessen Weiterentwicklung, insbesondere mit dem Ziel, den Betroffenen möglichst weitreichende Kontrolle über den Umgang mit ihren personenbezogenen Daten zu geben.

Es kann an dieser Stelle nicht deutlich genug betont werden, dass die Struktur der Register an sich durch die hier entwickelten Modelle nicht tangiert wird. Im Vergleich zum Regierungsentwurf ersetzt lediglich eine bPK die dort vorgesehene Steuer-ID. Wesentliche Änderungen betreffen nur den vorgesehenen Intermediär.

Abb. 18 | Morphologischer Kasten zum Identitätsnummernsystem Stammzahl-Modell

ID-NR-SYSTEM	AUSPRÄGUNGSFORMEN				
Typus von Personenkennzeichen	allgemeines Personenkennzeichen (aPK)	bereichsübergreifendes Personenkennzeichen (2wPK)	**bereichsspezifisches Personenkennzeichen (bPK)**		
Vorgehen bei der Vergabe	**Personenkennzeichen zentral vergeben**		Personenkennzeichen dezentral vergeben		
Inhaltliche Gestaltung des Personenkennzeichens	Steuer-ID	Andere existierende Register-ID	**Stammzahl als Zufallszahl generiert**	Keine zentrale ID	
Identifizierung in anderen Registern	Steuer-ID	Bisherige Register-ID	**Hashwert auf Stammzahl und Bereichs-Bezeichner**	Zufallszahl	
Zu erfassende Personengruppe	**Deutsche Bürger**	**Ausländer**	Steuerzahler	**Natürliche Personen**	Juristische Personen
Verortung der Speicherung der Basisdatensätze zu allen Personen	**Basisdatensatz beim Bundeszentralamt für Steuern (BZSt)**		ohne Basisdatensatz		
Einsatz einer Intermediär-internen Datenbank mit allen bPKs	**Verzicht auf Intermediär-interne ID-Datenbank**		Pseudonymisierte Intermediär-interne ID-Datenbank		
Registermodernisierung	**Registermodernisierungsbehörde (BVA)**		Verzicht auf Registermodernisierungsbehörde		
Verortung der Intermediäre zu den BZSt-Basisdatensätzen	Intermediär zum BZSt-Basisdatensatz bei BVA (Registermodernisierungsbehörde)		**Intermediär zum BZSt-Basisdatensatz bei Datenschutzaufsichtsbehörde**		
Vermittlungsstellen für Anfragen auf BZSt-Basisdatensätze	Keine Vermittlungsstelle für Anfragen	Zentrale Vermittlungsstelle für Anfragen	**Verbund von Vermittlungsstellen für Anfragen**		
Prüfung der Zugriffe auf BZSt-Basisdatensätze	Keinerlei Prüfung der Zugriffe	Software-basierte Prüfung der Zugriffe	**Hardware-basierte Prüfung der Zugriffe**	Ständige Prüfung durch Sachbearbeiter	
Freigabe von Daten durch Bürger bei bereichsübergreifenden Abfragen	Freigabe von Daten ohne Bürgereinbindung	**Anlassbezogene Freigabe von Daten durch Bürger**	Freigaben von Daten stets durch Bürger erforderlich		

Abb. 19 | Morphologischer Kasten zum Identitätsnummernsystem NEU-ID

ID-NR-SYSTEM	AUSPRÄGUNGSFORMEN				
Typus von Personenkennzeichen	allgemeines Personenkennzeichen (aPK)		bereichsübergreifendes Personenkennzeichen (2wPK)		**bereichsspezifisches Personenkennzeichen (bPK)**
Vorgehen bei der Vergabe	**Personenkennzeichen zentral vergeben**			Personenkennzeichen dezentral vergeben	
Inhaltliche Gestaltung des Personenkennzeichens	Steuer-ID	Andere existierende Register-ID		**NEU-ID in Form von einer Zufallszahl**	Keine zentrale ID
Identifizierung in anderen Registern	Steuer-ID	**Bisherige Register-ID**		Hashwert auf Stammzahl und Bereichs-Bezeichner	**Zufallszahl**
Zu erfassende Personengruppe	**Deutsche Bürger**	**Ausländer**	Steuerzahler	**Natürliche Personen**	Juristische Personen
Verortung der Speicherung der Basisdatensätze zu allen Personen	**Basisdatensatz beim Bundeszentralamt für Steuern (BZSt)**			ohne Basisdatensatz	
Einsatz einer Intermediär-internen Datenbank mit allen bPKs	Verzicht auf Intermediär-interne ID-Datenbank			**Pseudonymisierte Intermediär-interne ID-Datenbank**	
Registermodernisierung	**Registermodernisierungsbehörde (BVA)**			Verzicht auf Registermodernisierungsbehörde	
Verortung der Intermediäre zu den BZSt-Basisdatensätzen	Intermediär zum BZSt-Basisdatensatz bei BVA (Registermodernisierungsbehörde)			**Intermediär zum BZSt-Basisdatensatz bei Datenschutzaufsichtsbehörde**	
Vermittlungsstellen für Anfragen auf BZSt-Basisdatensätze	Keine Vermittlungsstelle für Anfragen		Zentrale Vermittlungsstelle für Anfragen		**Verbund von Vermittlungs-stellen für Anfragen**
Prüfung der Zugriffe auf BZSt-Basisdatensätze	Keinerlei Prüfung der Zugriffe	Software-basierte Prüfung der Zugriffe		**Hardware-basierte Prüfung der Zugriffe**	Ständige Prüfung durch Sachbearbeiter
Freigabe von Daten durch Bürger bei bereichs-übergreifenden Abfragen	Freigabe von Daten ohne Bürgereinbindung		**Anlassbezogene Freigabe von Daten durch Bürger**		Freigaben von Daten stets durch Bürger erforderlich

E. Abschließende Bewertung und Empfehlung

Zielsetzung aller Beteiligten sollte es sein, das RegMoG auf einen verfassungsgemäßen Weg zu bringen.

Der vorliegende Gesetzesentwurf, der einen erheblichen Modernisierungsschub für die Bundesrepublik Deutschland und E-Government bringen soll, kann diesen hohen Erwartungen aus technischen wie rechtlichen Gründen nicht gerecht werden. Idealerweise würde der Entwurf die Grundlagen für ein leistungsfähiges, datenschutzkonformes, sicheres und vertrauenswürdiges Identitätsnummernsystem legen, um die in der Einführung des Gesetzesentwurf aufgezählten Probleme dauerhaft zu lösen. Im Falle einer Umsetzung bekommen die Bürger allerdings eine allgemeine Personenkennziffer und ein digitales Identitätsnummernsystem auf Basis der Steuer-ID. Künftige Regierungen oder die Europäische Union könnten dies rasch zu einem Profil- und Überwachungssystem über alle Bürger ausbauen. Diese Gefahr besteht nicht nur theoretisch. Mit Blick auf die Machtübernahmen in einigen mittlerweile autokratisch regierten Staaten ist sie ganz reell. Wir halten es für wichtig, auch diesen Aspekt bei der Gesetzgebung im Blick zu halten.

Dass mit dem vorliegenden Gesetzesentwurf die Steuer-ID zu einem allgemeinen Personenkennzeichen wird, erscheint – auch, wenn zunächst nicht alle Register eingebunden werden – unzweifelhaft. Wir sehen deshalb eine große Wahrscheinlichkeit, dass dieses Gesetz im Fall seines Inkrafttretens durch das Bundesverfassungsgericht für nichtig erklärt werden wird.

Ursprünglich sollte das Gesetz mit Verweis auf Kosten- und Zeitargumente vor der Weihnachtspause durch den Bundestag und den Bundesrat gehen. Gelänge dies, würde in einigen Monaten ein vollkommener Neustart des Vorhabens drohen. Dies hätte erhebliche Verzögerungen und zusätzliche unnötige Kosten zur Folge. An diesen hat zu diesem Zeitpunkt keiner der Beteiligten ein Interesse, weder die Bundesregierung noch die Datenschutzbeauftragten und auch nicht die Bürger. Das reale Risiko von vielen Verfassungsbeschwerden, die im Vorfeld und bei der ersten Lesung im Deutschen Bundestag bereits angekündigt wurden, muss bei der weiteren Abwägung berücksichtigt werden.

Insofern wären die Bundesregierung und der IT-Planungsrat gut beraten, sich trotz des laufenden Gesetzgebungsverfahren bereits mit Alternativen auseinanderzusetzen und diese so vorzubereiten, dass im Falle eines Scheiterns ein überzeugender Alternativplan ausgearbeitet vorliegt und nicht noch weitere wertvolle Zeit verloren geht.

Mit Blick auf die Optionen und vorhandenen Alternativen zu Personenkennzeichen und Identitätsnummernsystemen gilt festzuhalten, dass der Vorschlag des RegMoG der Bundesregierung keineswegs alternativlos ist. Allerdings muss auch der Wille vorhanden sein, den eingeschlagenen Pfad zu verlassen, sollte sich dieser als für die Sache ungeeignet erweisen.

Das Gutachten zeigt auf, dass es jenseits der Steuer-ID als Identitätsnummer weitere Optionen für Personenkennzeichen und Identitätsnummernsysteme gibt. Diese können zeitnah untersucht, bewertet und bei Bedarf professionell umgesetzt werden. Dazu müsste die Analyse und Konzeption verschiedener Lösungsmodelle für ein Identitätsmanagement noch einmal geöffnet und eine nachhaltige Lösung gefunden werden.

Wir haben mit diesem Gutachten zwei Varianten vorgestellt, die aus unserer Sicht beide eine substantielle Verbesserung gegenüber dem Vorschlag der Bundesregierung bedeuten.[169] Ohne Risiko sind auch diese Ansätze nicht, denn wenn Daten für legitime Zwecke wie die Registerkonsolidierung zusammengeführt werden können, ist dies im Grundsatz auch immer für illegitime Zwecke möglich. Die Ansätze reduzieren die Risiken für den Datenschutz jedoch, indem sie eine Umgehung der schon im Regierungsentwurf vorgesehenen Intermediäre erschweren. Gleichzeitig können sie ohne nennenswerte Eingriffe in die bestehende Registerstruktur realisiert werden. Sollte sich eine dieser beiden Optionen oder ein anderer Ansatz als zielführender erweisen, wären die Bundesregierung und der IT-Planungsrat in der Lage, binnen weniger Monate einen überzeugenderen, professionelleren Ansatz in ein neues Gesetzgebungsverfahren einzubringen und diesen zeitnah umzusetzen.

Zugegeben würde dies zu einem Ende des laufenden Gesetzgebungsverfahrens führen. Die noch erforderlichen strukturellen Überarbeitungen am Entwurf wären aber zu einschneidend, als dass der Gesetzgeber diesen durch Anpassungen noch retten könne. Der bisherige Erkenntnisgewinn im Diskurs um die beste Lösung war jedoch hoch und lohnenswert. Insofern kann es auf dem bestehenden Erkenntnisniveau mit einer besseren Lösung rasch in einem weiteren Gesetzgebungsverfahren weitergehen.

Unabhängig vom Ausgang der Debatte im Ausschuss handelt es sich bei dem RegMoG um ein Gesetz mit erheblichen Folgen für alle Bürger und Einwohner der Bundesrepublik Deutschland. Hierbei gibt es unterschiedliche und politisch sehr umstrittene Positionen quer durch alle Parteien und öffentliche Institutionen. Politisch ist das legitim, aber für den Staat und das hohe Vertrauen seiner Bürger in Bund, Länder und Kommunen auch riskant.

[169] Vgl. für eine zusammenfassende Darstellung Abschnitt D.VI

Literatur

Article 29 Data Protection Working Party, Opinion on Purpose Limitation, 2013, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Brink, Stefan/Wolff, Heinrich Amadeus (Hrsg.), Beck'scher Onlinekommentar, 23. Edition 2020 (zitiert als *Bearbeiter*, in: BeckOK)

Bundesamt für Sicherheit in der Informationstechnik, Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Part 2, Version 2.21, 2016, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf?__blob=publicationFile&v=3, (zitiert als BSI TR 03110 Part 2)

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), BfDI, Hintergrundpapier zur Registermodernisierung und Schaffung eines einheitlichen Personenkennzeichens, 2020, https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Hintergrundpapier-Registermodernisierung.html

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), 23. Tätigkeitsbericht zum Datenschutz 2009 und 2010, 2010, https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/23TB_09_10.pdf?__blob=publicationFile&v=9

Bundesbeauftragter für den Datenschutz, Tätigkeitsbericht zum Datenschutz 2003 und 2004, 2004, https://www.bfdi.bund.de/SharedDocs/Publikationen/Taetigkeitsberichte/TB_BfDI/20TB_03_04.html

Bundesrat, Empfehlungen der Ausschüsse zum Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (RegMoG), Drucksache 563/1/20

Bundesvereinigung Deutscher Arbeitgeberverbände (BDA), Einführung einer Identifikationsnummer ist wichtig, aber noch nicht ausreichend. Stellungnahme zum Referentenentwurf des BMI zum Registermodernisierungsgesetz, 2020, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/registermodernisierungsgesetz/bda.pdf?__blob=publicationFile&v=1

Bundesrechtsanwaltskammer (BRAK), Stellungnahme, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/registermodernisierungsgesetz/bundesrechtsanwaltskammer.pdf?__blob=publicationFile&v=3

Databund, Stellungnahme zum Registermodernisierungsgesetz, 2020, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/registermodernisierungsgesetz/databund.pdf?__blob=publicationFile&v=3

Datenethikkommission der Bundesregierung, Gutachten, 2019, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/it-digitalpolitik/gutachten-datenethikkommission.pdf?__blob=publicationFile&v=6

Deutscher Anwaltverein (DAV), Stellungnahme, 2020, https://anwaltverein.de/de/newsroom/sn-75-20-zum-registermodernisierungsgesetz

Deutsche Rentenversicherung (DRV), Stellungnahme, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/registermodernisierungsgesetz/rentenversicherung.pdf?__blob=publicationFile&v=2

Ehmann, Eugen/Selmayr, Martin (Hrsg.), DSGVO. Kommentar, 2. Auflage München 2018 (zitiert als *Bearbeiter*, in: Ehmann/Selmayr)

Gola, Peter (Hrsg.), DSGVO, 2. Auflage, München 2018 (zitiert als: *Bearbeiter* in: Gola)

Gesellschaft für Informatik, Stellungnahme des Fachbereichs Informatik in Recht und Öffentlicher Verwaltung und des Präsidiums-Arbeitskreises Datenschutz und IT-Sicherheit der Gesellschaft für Informatik e.V. (GI)zum Referentenentwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz–RegMoG) des Bundesministeriums des Innern, für Bau und Heimat (BMI), 2020, https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/registermodernisierungsgesetz/gfi.pdf?__blob=publicationFile&v=3

Hornung, Gerrit, Die digitale Identität, Baden-Baden 2005

Humanistische Union (HU), Stellungnahme der Humanistischen Union zum Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat: Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz – RegMoG), 2020, http://www.humanistische-union.de/typo3/ext/naw_securedl/secure.php?u=0&file=uploads/media/2020-09-04_HU-StN_Registermodernisierungsgesetz.pdf&t=1599569825&hash=932c9fa5b37c6dd7f8fcf46228653b3e

IT-Planungsrat 2020: Eckpunkte für die Registermodernisierung – Bestehende Anforderungen, vorläufige Architekturskizze sowie sich daraus ergebende Maßnahmen im Rahmen des IT-Planungsratsprojekts Registermodernisierung, 2020, https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/32_Sitzung/TOP_06_Anlage_1_Eckpunkte.pdf?__blob=publicationFile&v=3

Katz, Jonathan/Lindell, Yehuda, Introduction to Modern Cryptography, 2. Auflage, London 2014

Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Entschließung Registermodernisierung verfassungskonform umsetzen, 2020, https://www.datenschutzkonferenz-online.de/media/en/20200828_entschlie%C3%9Fung_pkz_final_1.pdf

Körner, Thomas/Krause, Anja/Ramsauer, Katharina, Anforderungen und Perspektiven auf dem Weg zu einem künftigen Registerzensus, in: WISTA – Wirtschaft und Statistik, Sonderheft Zensus 2021, Statistisches Bundesamt, Wiesbaden 2019, https://www.destatis.de/DE/Methoden/WISTA-Wirtschaft-und-Statistik/2019/07/anforderungen-perspektiven-registerzensus-072019.pdf?__blob=publicationFile

Kühling, Jürgen/Buchner, Benedikt, DSGVO und BDSG. Kommentar, 3. Auflage München 2020 (zitiert als *Bearbeiter*, in: Kühling/Buchner)

Martini, Mario/Wagner, David/Wenzel, Michael, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, 2017, https://www.normenkontrollrat.bund.de/resource/blob/72494/476034/eebab686008cfec0a7919ca03e51abe3/2017-10-06-download-nkr-gutachten-2017-anlage-untersuchung-datenschutz-data.pdf?download=1

Martini, Mario/Wenzel, Michael, »Once only« versus »only once«: Das Prinzip einmaliger Erfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit, DVBl. 2017, S. 749 ff.

Maunz-Dürig, Grundgesetz Kommentar, 91. Auflage, München 2020 (zitiert als: *Bearbeiter*, in: Maunz-Dürig)

Nationaler Normenkontrollrat, Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren, 2017, https://www.normenkontrollrat.bund.de/resource/blob/300864/476004/12c91fffb877685f4771f34b9a5e08fd/2017-10-06-download-nkr-gutachten-2017-data.pdf

Nationaler Normenkontrollrat und McKinsey & Co, Ergänzende Dokumentation zu „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren.", Nationaler Normenkontrollrat, Berlin 2017, https://www.normenkontrollrat.bund.de/resource/blob/72494/476010/b6c476acd8bac8d1a81c1f7b7212cabd/2017-10-06-download-nkr-gutachten-2017-anlage-dokumentation-data.pdf?download=1.

Paal, Boris/Pauly, Daniel A. (Hrsg.), DSGVO und DSG. Kommentar. 2. Auflage, München 2019

Roßnagel, Alexander, Kontinuität oder Innovation? Der deutsche Spielraum in der Anpassung des bereichsspezifischen Datenschutzrechts, DuD 2018, S. 477 ff.

Schaar, Peter, Steuer-ID darf kein allgemeines Personenkennzeichen werden!, ZD 2011, 49 f.

Simitis, Spiros/Hornung, Gerrit/Spiecker genannt Döhmann, Indra (Hrsg.), Datenschutzrecht. Kommentar, Baden-Baden, 2019 (zitiert als *Bearbeiter*, in: Simitis/Hornung/Spiecker gen. Döhmann)

Smith, Sean, Hardware Security Modules, in Rosenberg, Burton (Hrsg.), Handbook of Financial Cryptography and Security, London 2010, S. 257 ff.

Sorge, Christoph/Leicht, Maximilian, Registermodernisierungsgesetz – eine datenschutzgerechte Lösung?, ZRP 2020, S. 242 ff.

Stallings, William, Cryptography and Network Security, 7. Auflage, Pearson India 2017

Statistisches Bundesamt, Ein Blick in die Registerlandschaft in Deutschland. Beistellung zum Gutachten „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren." im Auftrag des Nationalen Normenkontrollrates, 2017, https://www.normenkontrollrat.bund.de/resource/blob/72494/476024/04a6019c945895d3587136ff2ce46b73/2017-10-06-download-nkr-gutachten-2017-anlage-untersuchung-staba-register-data.pdf?download=1

Stocksmeier, Dirk/Hunnius, Sirko, OZG-Umsetzungskatalog – Digitale Verwaltungsleistungen im Sinne des Onlinezugangsgesetzes,]init[AG, Berlin 2018, https://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/26_Sitzung/TOP2_Anlage_OZGUmsetzungskatalog.pdf?__blob=publicationFile&v=4.

Voßkuhle, Andreas, Grundwissen Öffentliches Recht: Der Grundsatz des Vorbehalts des Gesetzes, Juristische Schulung (JuS) 2001, S. 118 f.

Wissenschaftlicher Dienst des Bundestages, Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines RegistermodernisierungsgesetzesDSGVO und Recht auf informationelle Selbstbestimmung, 2020 https://cdn.netzpolitik.org/wp-upload/2020/09/WD-Registermodernisierung.pdf (zitiert als Wiss. Dienst BTag)

Über die Autoren

Prof. Dr.-Ing. Christoph Sorge

war nach seinem Studium der Informationswirtschaft und seiner Promotion in Informatik am KIT zunächst als Research Scientist bei den NEC Laboratories Europe tätig. Von 2010 bis 2014 war er Juniorprofessor für Sicherheit in Netzwerken an der Universität Paderborn. Anschließend wechselte er an die rechtswissenschaftliche Fakultät der Universität des Saarlandes, wo er Inhaber des Lehrstuhls für Rechtsinformatik ist. Gleichzeitig ist er als kooptierter Professor Mitglied der Fachrichtung Informatik der Universität, assoziiert mit dem CISPA Helmholtz-Zentrum für Informationssicherheit sowie Senior Fellow des Deutschen Forschungsinstituts für öffentliche Verwaltung Speyer. Mit seinem interdisziplinären Team forscht er an der Schnittstelle von Informatik und Recht, insbesondere im Bereich des Datenschutzes.

Prof. Dr. rer. publ. Jörn von Lucke

hat den Lehrstuhl für Verwaltungs- und Wirtschaftsinformatik am The Open Government Institute (TOGI) an der Zeppelin Universität Friedrichshafen inne. Seine aktuellen Forschungsschwerpunkte liegen in E-Government (Hochleistungsportale), Open Government (offenes Regierungs- und Verwaltungshandeln), offenen Daten, offener gesellschaftlicher Innovation, Smart Government (Internet der Dinge und Internet der Dienste im öffentlichen Sektor; Verwaltung 4.0, Smarte Stadt), Realtime Government und Künstlicher Intelligenz im öffentlichen Sektor. Zugleich vertritt er die Interessen der Gesellschaft für Informatik e.V. im Rahmen der deutschen Aktivitäten zur Open Government Partnership.

Prof. Dr. iur. Indra Spiecker
gen. Döhmann

hat Rechtswissenschaften in Bonn, Mainz und Washington studiert und war wissenschaftliche Mitarbeiterin an den Universitäten Bonn und Heidelberg sowie am Max-Planck-Institut für Gemeinschaftsgüter, Bonn. Von 2008 bis 2013 war sie Professorin für öffentliches Recht, Telekommunikationsrecht und Datenschutzrecht am Institut für Informations- und Wirtschaftsrecht des Karlsruher Instituts für Technologie. Seit 2013 ist sie Professorin für öffentliches Recht, Informationsrecht, Umweltrecht und Verwaltungswissenschaften an der Goethe-Universität Frankfurt. Dort ist sie auch Direktorin der Forschungsstelle Datenschutz. Sie wurde als erste Juristin in die Akademie der Technikwissenschaften (acatech) aufgenommen. Indra Spiecker ist Herausgeberin des Kommentars zum Datenschutzrecht (Simitis/Hornung/Spiecker genannt Döhmann).

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)667 D

Kompetenzzentrum Öffentliche IT

An:
Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin
an: innenausschuss@bundestag.de

Kompetenzzentrum Öffentliche IT
Kaiserin-Augusta-Allee 31
10589 Berlin
E-Mail: info@oeffentliche-it.de
Telefon: +49 (0) 30 3463-7173
Fax: +49 (0) 30 3463-997173

Analyse der rechtlich-technischen Gesamtarchitektur des Entwurfs des Registermodernisierungsgesetzes

von Peter Parycek[1,2], Verena Huber[2], Simon S. Hunt[1], Anna-Sophie Novak[2] & Basanta E.P. Thapa[1]

Fraunhofer FOKUS

[1] Kompetenzzentrum Öffentliche IT (ÖFIT) am Fraunhofer-Institut FOKUS
[2] Department für Electronic Governance an der Donau-Universität Krems

Inhaltsverzeichnis

Thesen

1. *Eine datenschutzkonforme Registerlandschaft ist eine Grundvoraussetzung für das Erreichen der bestehenden gesetzlich verpflichtenden Digitalisierungsziele des Onlinezugangsgesetzes (OZG) und der europäischen Verordnung zum Single Digital Gateway (SDG-VO).*

   Für das Ziel der gesetzlich verpflichtenden Umsetzung von digitalen Verwaltungsdienstleistung nach OZG[3] und SDG-VO[4] und dem Ziel des elektronischen Zensus sind harmonisierte Register die Grundvoraussetzung. Als harmonisiert gelten Register, wenn ihre Datensätze mit Identifikationsnummern versehen sind, so dass Datensätze über eine Person über fachlich und dezentral gehaltene Register hinweg zweifelsfrei einer Person zugeordnet werden können und übereinstimmen. Dabei wird die Identifikationsnummer zentral verwaltet, während die Inhaltsdaten der jeweiligen Fachmaterie möglichst dezentral bei den zuständigen Behörden gespeichert und verarbeitet werden.

   Der Zugang und die Nutzung der Daten sind - wie bisher - nur mit gesetzlicher Grundlage möglich. Eine vielfach diskutierte Suchfunktion über die fachlich getrennten Register hinweg ist weder vorgesehen noch wäre es aufgrund der logischen Trennung der Register technisch möglich. Die dezentral verteilte Architektur des RegMoG ist im Steuerbereich und Meldewesen entwickelt, erfolgreich etabliert und seit mehreren Jahren im Einsatz.

2. *Zur Verhinderung der Erstellung eines digitalen Persönlichkeitsprofils ist die Sicherung der Datenabfrage bei den Registern entscheidend und nicht das Verbot einer Identifikationsnummer.*

   Bei den historisch nachvollziehbaren Bedenken eines Datenmissbrauches steht insbesondere die personenbezogene Identifikationsnummer in der Kritik. Die Kritik verweist meist auf das Volkszählungsurteil[5], welches in einer Personenkennziffer die Grundlage für eine umfassende Profilbildung gesehen hat.[6] Zudem ist eine Personenkennziffer auch aufgrund historischer und zeitgenössischer Negativbeispiele zu einem Tabubegriff geworden, wie der wissenschaftliche Dienst des Bundestages darlegt.[7] Diese Sichtweise ist jedoch zu kurz gegriffen.[8] Mit den beschränkten Rechenleistungen und den geringen Datenpunkten war das Verbot einer einheitlichen Personenkennziffer 1983 eine wirksame Schutzmaßnahme zur Profilbildung, speziell im thematischen Zusammenhang der Volkszählung.[9] Im 21. Jahrhundert ist fraglich, inwieweit eine Identifikationsnummer als eine notwendige technische Befähigung bewertet werden kann, um digitale Persönlichkeitsprofile zu erstellen. Die umfassende Anzahl an

[3] Onlinezugangsgesetzes (OZG) verpflichtet Bund und Länder ihre Verwaltungsleistungen bis Ende 2022 online anzubieten.
[4] Verordnung (EU) 2018/1724 zum Single Digital Gateway (SDG), bis 12.12.2023 sind 17 Verfahren für Bürgerinnen und Bürger und in 4 Verfahren für die Wirtschaft grenzüberschreitend online zur Verfügung zu stellen, zwingend wenn die Verfahren auch im jeweiligen Mitgliedsstaat angeboten werden; aber auch asymmetrische Verpflichtungen sind denkbar.
[5] BVerfG 15.12.1983, 1 BvR 209/83.
[6] BVerfG 15.12.1983, 1 BvR 209/83, Rn 169.
[7] Deutscher Bundestag – Wissenschaftliche Dienste, Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes - DSGVO und Recht auf informationelle Selbstbestimmung, bundestag.de/resource/blob/793658/c8c9c4a28cf88a2ae31f81887ec293d9/WD-3-196-20-pdf-data.pdf (07.12.2020).
[8] BVerfG 15.12.1983, 1 BvR 209/83, Rn 152.
[9] *Martini/Wagner/Wenzel,* Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, 2017, 38.

Datenpunkten in den staatlichen Registern ist ausreichend, um die überwiegende Mehrheit der Bürger und Bürgerinnen eindeutig zuordnen zu können. In der datenbasierten Verwaltungslandschaft sind die Sicherungsmaßnahmen für den Zugang zu Daten entscheidend, die im RegMoG-E vorgesehen sind: Minimierung der Zugriffsmöglichkeiten durch örtlich verteilte Register, revisionssichere Protokollierung aller Datenabrufe in den durch das RegMoG umfassten Register, eine damit verbundene Ex-Post-Prüfung durch die Bürgerin und den Bürger und einer Ex-Ante-Prüfung im Fall von sensiblen und bereichsübergreifenden Transaktionen mit dem 4-Corner-Modell. Für den Schutz der personenbezogenen Daten in den Registern des RegMoG ist der Zugang zu den Registern entscheidend, nicht das Vorhandensein einer Identifikationsnummer.

3. *Privacy-by-Design durch Separierung der Datenbearbeitung und -speicherung ist ein effektiver Schutz vor einem bundesweiten Datenmissbrauch.*

   Die dezentrale verteilte Speicherung und Bearbeitung der Daten auf Länder- und kommunaler Ebene bedeutet Privacy-by-Design durch Separierung der Daten. Die Verteilung der Datenbestände erzeugt einen höherwertigen Schutz gegen missbräuchliche Zugriffe. Zentrale Register auf Bundesebene wie beispielsweise in Österreich oder Estland haben ein wesentlich höheres Schadenspotential im Fall eines unberechtigten Zugangs und das Angriffsrisiko ist aufgrund der Menge an Daten ebenfalls als wesentlich höher einzustufen. Die vorliegende Architektur folgt der Privacy-by-Design Empfehlung der Europäischen Agentur für Netz- und Informationssicherheit (Separate-Prinzip)[10].

4. *Das 4-Corner-Modell ist aktuell der wirksamste Schutz gegen die Erstellung von digitalen Persönlichkeitsprofilen durch Prüfung der Rechtmäßigkeit vor einer bereichsübergreifenden Übermittlung der Daten.*

   Datenübermittlungen zwischen verschiedenen Bereichen - wie potenziell 'Inneres' und 'Soziales' - werden vor der Übermittlung der Daten auf ihre Zulässigkeit durch das 4-Corner-Modell geprüft (Ex-Ante-Prüfung der Zulässigkeit der Datenabfrage). Zusätzlich werden sowohl durchgeführte als auch abgelehnte Abfragen protokolliert. Die Protokolle sind nicht nur für die Datenschutzbeauftragten zugänglich, sondern sollen zukünftig auch durch die betroffene Person mit Hilfe des Datencockpits überprüfbar gemacht werden. Die Kontrolle der Datennutzung wird damit erheblich erweitert. Das 4-Corner-Modell ist eine europäische Entwicklung zur datenschutzkonformen Übermittlung von Daten, die für die grenzüberschreitende Übermittlung von Daten zwischen EU-Mitgliedsländer über das Single Digital Gateway (SDG) genutzt werden soll.

5. *Das vorgesehene Datencockpit soll nach dem RegMoG-E den betroffenen Personen eine Übersicht über alle Datenübertragungen ermöglichen und eine Datenauskunft zu den Inhaltsdaten nach Art. 15 DSGVO wird empfohlen.*

   Ein zentrales Element in der Gesamtarchitektur des RegMoG ist die Einrichtung eines Datencockpit, welches den betroffenen Personen die Übersicht alle Übermittlungen ihrer persönlichen Daten innerhalb der Registerlandschaft ermöglicht. Diese Protokollierungs-daten werden nicht zentral im Datencockpit gespeichert, sondern weiterhin bei den Quellregistern, die durch die betroffene Person geprüft werden können. Auch bei dieser

[10] ENISA, Privacy by design in Big Data, enisa.europa.eu/publications/big-data-protection/at_download/fullReport (9.12.2020).

Funktion wird das technische Datenschutzprinzip der verteilten Speicherung genutzt. Zusätzlich könnte das Datencockpit den betroffenen Personen auch die Möglichkeit der Auskunft nach der Art. 15 DSGVO über ihre Inhaltsdaten gewährleisten. Die Einsicht in die Protokollierungsdaten und die Inhaltsdaten stärkt maßgeblich den datenschutzrechtlichen Grundsatz der Transparenz nach Art 5 lit a DSGVO, daher wird empfohlen diese Funktionalität explizit im RegMoG vorzusehen.

6. *Die Einführung der Identifikationsnummer kann die Datenschutzgrundsätze nach Art 5 DSGVO maßgeblich stärken.*

   Die aktuelle Datennutzungspraxis im öffentlichen Sektor steht teilweise im Spannungsverhältnis mit den Grundsätzen des Art 5 der Datenschutzgrundverordnung (DSGVO). Aktuelle werden zum Zweck der Identifikation der Person, aufgrund einer fehlenden Identifikationsnummer, zusätzliche personenbezogene Daten (z.B. aktuelle Anschrift, Geburtsdatum und -ort, Mädchenname der Mutter) verarbeitet, gespeichert und zwischen den Behörden übermittelt.[11] Diese Verwaltungspraxis führt zu Datenmaximierung und entspricht nicht dem Grundsatz der Datenminimierung nach Art 5 lit c DSGVO. Aufgrund von Transkriptionsfehlern, Namensverwechslungen, unterschiedlichen Aktualisierungs-frequenzen und verschiedene fachliche Anforderungen besteht dringender Handlungsbedarf die Datenqualität in den Fachregistern zu erhöhen.[12] Die aktuelle Datenqualität in den Registern steht im starken Spannungsverhältnis zum Grundsatz der Richtigkeit und Integrität der Daten nach Art. 5 Abs. 1 lit d DSGVO und führt im Fall von Namensverwechslungen bis zum Bruch der Vertraulichkeit. Die Registerlandschaft und im Besonderen die Identifikationsnummer werden maßgeblich zur Verbesserung der Datenqualität beitragen und somit die Datenschutzgrundsätze nach Art. 5 Abs. 1 lit c und d der DSGVO stärken.

7. *Eine beliebige Kombination von Modellen ist in der Theorie denkbar, in der Praxis zum Scheitern verurteilt.*

   Das durch das RegMoG determinierte Architekturmodell ist komplex in der Zusammenwirkung der ausgewählten Elemente, die in ihrer Kombination den technischen Datenschutz gewährleisten sollen: 4-Corner-Modell, dezentral verteilte Speicherung und Bearbeitung sowie das Datencockpit. Diese Komponenten sind bereits im Einsatz oder im Testbetrieb und bilden daher eine ausgezeichnete Grundlage für eine erfolgreiche Umsetzung. In der Debatte zum RegMoG-E werden unterschiedliche zusätzliche Kombinationen internationaler Modelle diskutiert und vorgeschlagen, beispielsweise eine Mischung der bereichsspezifischen Personenkennzeichen aus dem österreichischen Modell mit dem 4-Corner-Modell und/oder mit einer dezentralen Speicherung. In der Theorie sind diese Modelle eventuell auch kombinierbar, wenn auch nicht immer zweckmäßig oder zielführend. In der Praxis ist aufgrund der steigenden Komplexität des Gesamtsystems eine funktionale Umsetzung eines kombinierten Modells mit einer so hohen Anzahl von Beteiligten von Bund über Länder bis zu den Kommunen fraglich bzw. so gut wie auszuschließen. Dies kann in weiterer Folge auch die Sicherheit aufgrund der steigenden Komplexität des Gesamtsystems reduzieren. Prof. Mertens empfiehlt die Machbarkeit von IT-Großprojekten

[11] Gesetzentwurf der Bundesregierung, Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (RegMoG-E), Drucksache 19/24226, 1.
[12] RegMoG-E, Drucksache 19/24226, 1.

im Gesetzesentstehungsprozess als Kriterium zu berücksichtigen, auf Basis seiner Misserfolgsforschung zu gescheiterten IT-Großprojekten in der öffentlichen Verwaltung.[13] Diese Empfehlung ist in Anbetracht der notwendigen datenschutzrechtlichen Abwägungen und der Informationssicherheit von besonderer Bedeutung.

8. Der internationale Vergleich macht sicher.

In der Debatte wird häufig das österreichische Modell mit den bereichsspezifischen Personenkennzeichen (bPK) angeführt, dabei dürfte nicht bekannt sein, dass das bPK-Modell von den Bundesländern aufgrund der hohen Komplexität und eines geringen Mehrwerts nur in wenigen Verfahren genutzt wird. Seit mehr als einem Jahrzehnt fordern die Länder ein bereichsspezifisches Kennzeichen für die Landesverwaltung. Die bPK sind erfolgreich in den Bundesregistern im Einsatz, die allerdings aus Sicht des Datenschutzes den Nachteil der zentralen Speicherung vorweisen. Im direkten internationalen Vergleich ist der datenschutzfreundlichere Weg der dezentralen Speicherung des RegMoG-E hervorzuheben, weder Dänemark, Österreich, noch Estland verfügen über so einen Ansatz. Die Kombination des dezentral verteilten Ansatzes in Kombination mit dem 4-Corner-Modell ist einzigartig und kann weltweit zu einem Vorzeigemodell werden. Neben den technischen Sicherungsmaßnahmen sind auch die rechtlichen Sicherungsmaßnahmen bis hin zum Straftatbestand mit Freiheitsstrafe als führend zu beurteilen.

[13] *Mertens*, Fehlschläge bei IT-Großprojekten der Öffentlichen Verwaltung – ein Beitrag zur Misserfolgsforschung in der Wirtschaftsinformatik, 2008.

I. Nutzen einer harmonisierten Registerlandschaft

Eine harmonisierte Registerlandschaft ist der Schlüssel für eine wirkungsvolle digitale Verwaltung. Dies verdeutlicht auch der Blick zu europäischen E-Government-Spitzenreitern wie Dänemark, Estland und Österreich mit ihren unterschiedlichen Registermodellen (siehe Kapitel IV). Die richtigen Daten mit Vertrauen in ihre Korrektheit bei Bedarf über verschiedene föderale Ebenen und Fachbehörden hinweg abrufen zu können, ist sowohl die Voraussetzung für (halb-)automatisierte Verwaltungsprozesse, holistische Planungsprozesse sowie Analysen und Vorhersagen für die Politikentwicklung.[14]

Datenqualität in der öffentlichen Verwaltung

Korrektes Verwaltungshandeln hängt auch an der Qualität der verfügbaren Daten, sowohl im Einzelfall als auch bei der Planung. Doubletten, veraltete, nicht zuordenbare oder falsch zugeordnete Datensätze erhöhen nicht nur den Prüfaufwand, sondern können sogar zu fehlerhaften Entscheidungen oder der Zustellung an die falsche Person führen. Allein die der öffentlichen Verwaltung vorliegenden Adressdaten sind in über 25 % der Fälle falsch.[15] Dabei können falsch zugestellte Verwaltungsschreiben bis zur Offenlegung vertraulicher Informationen führen. Dies ist insbesondere im Kontext des Grundsatzes der Datenintegrität und Vertraulichkeit der Daten als kritisch zu beurteilen (Art. 5 Abs. 1 lit. f DSGVO).

Mangelhafte Datenqualität kann in aggregierter Form auch leicht zu Fehlplanungen führen, indem etwa Bedarfe über- oder unterschätzt werden. Aufsehenerregend waren beispielsweise die Ergebnisse des registergestützten Zensus 2011, der die amtliche Einwohnerzahl der Bundesrepublik um 1,5 Millionen und Berlins um 180.000 Menschen nach unten korrigierte.[16] Dabei hatte im Vorfeld des Zensus 2011 bereits die Einführung der Steueridentifikationsnummer zu merklichen Korrekturen der Melderegister geführt.[17]

Eine Registerharmonisierung bedeutet durch eine höhere Datenqualität in der Verwaltung also auch weniger fehlerhafte Entscheidungen, eine geringere Wahrscheinlichkeit versehentlicher Datenschutzbrüche und eine bessere Planungsgrundlage.

Eindeutige Daten für (halb-)automatische Verwaltungsprozesse

Routineaufgaben in der Verwaltung zu automatisieren, birgt Zeit- und Kostensparnisse für die Verwaltung sowie für Bürgerinnen und Bürger. Bereits das Zusammensuchen der notwendigen Informationen für die Prüfung eines Antrags beschäftigt schnell Sachbearbeitende in mehreren Behörden und auch die antragstellenden Bürgerinnen und Bürger selbst. Mithilfe eines registerübergreifenden Identitätsmanagements können derartige Prozesse beschleunigt werden, da die für den Antrag relevanten Informationen ohne weiteres menschliches Zutun aus den betreffenden Fachregistern abgefragt werden können.[18] So sehen sich Sachbearbeitende vollständigen Informationsgrundlagen gegenüber.

In einigen Anwendungsfällen können Verwaltungsentscheidungen auch vollautomatisch gefällt werden. Ein einfaches Beispiel hierfür ist die automatische Vergabe von Bewohnerparkausweisen, die

[14] *Thapa/Parycek,* Data Analytics in Politik und Verwaltung in M*ohabbat Kar/Thapa/Parycek*,(Un)berechenbar? Algorithmen und Automatisierung in Staat und Gesellschaft, 2018, 40-75.
[15] *Deutsche Post*, „Adress-Studie 2018: Untersuchung zur Qualität von Kundenadressen in Deutschland", 2018.
[16] Statistische Ämter des Bundes und der Länder, Zensus 2011: Zensus Kompakt, 2014.
[17] taz, Neue Steuernummer lässt Berlin schrumpfen, 14.9.2010.
[18] *Mohabbat Kar/Thapa/Hunt/Parycek*, Recht Digital: Maschinenverständlich und automatisierbar - Impuls zur digitalen Vollzugstauglichkeit von Gesetzen", Kompetenzzentrum Öffentliche IT, 2019.

bereits in zahlreichen deutschen Kommunen praktiziert wird.[19] Dabei werden die angegebene Adresse und das Kraftfahrzeugkennzeichen mit dem Melde- und dem Fahrzeughalterregister abgeglichen. In mehr als der Hälfte der Fälle laufen die Anträge vollautomatisch durch das System und die Bürgerinnen und Bürger können sich ihre Bewohnerparkausweise nach Zahlung der Gebühr zuhause ausdrucken. Mangels eindeutiger Identifikationsnummer ist jedoch auch bei der Arbeit mit den bereits bestehenden Registern noch in vielen Fällen menschliches Eingreifen nötig.

Auch die Umsetzung der Grundrente illustriert die Vorteile harmonisierter Registerlandschaften. Bereits die organisationsübergreifende Ermittlung von Lebenspartnerschaften und Einkommen stellt hier eine beachtliche Herausforderung für den digitalen Vollzug dar.[20]

Für (halb-)automatische Verwaltungsprozesse sind Register mit eindeutigen Identifikationsnummern also eine Erfolgsbedingung.

Umsetzung des Once-Only-Prinzips

Das Once-Only-Prinzip ist im E-Government-Aktionsplan der EU 2016-2020[21] verankert und besagt, dass Bürgerinnen und Bürger Informationen der öffentlichen Verwaltung grundsätzlich nur einmal mitteilen sollen.[22] Falls diese Informationen noch an anderer Stelle in der Verwaltung benötigt werden, sollen diese zwischenbehördlich ermittelt werden.

Das Once-Only-Prinzip wird in Deutschland beispielsweise mit der vorausgefüllten Steuererklärung bereits umgesetzt, bei der dem Finanzamt bereits von Arbeitgebern und Sozialversicherungen übermittelte Daten in die Maske der Steuererklärung gespeist werden, so dass Bürgerinnen und Bürger diese Daten nicht ihrerseits bei den zuständigen Stellen erfragen und eintragen müssen.[23]

Bei der Datenerhebung für Verwaltungsverfahren ist der Umweg über Bürgerinnen und Bürger erst dann weitgehend auszuschließen, wenn die relevanten Informationen zuverlässig und in gesicherter Qualität eindeutig zuordenbar in Fachregistern ermittelt werden können. Der vorliegende Gesetzesentwurf ist daher ein wichtiger Schritt zur Umsetzung des Once-Only-Prinzips.

Teilhabewirkung proaktiver Verwaltungsverfahren

Eine automatisierte Anspruchsermittlung kann insbesondere in der Leistungsverwaltung inklusive Wirkung erzielen. So liegt die Nicht-Inanspruchnahme von Sozialleistungen etwa bei Hartz IV bei um die 50 Prozent und bei der Grundsicherung bei ungefähr 60 Prozent.[24] Diese zentralen sozialpolitischen Instrumente erreichen also weniger als die Hälfte der berechtigten Bürgerinnen und Bürger. Als Gründe gelten Unwissenheit über die Anspruchsberechtigung, geringe Ansprüche,

---

[19] Siehe beispielsweise hier: https://ozg.kdn.de/umsetzungsprojekte/details/parkausweise-gesamtprojekt (10.12.2020).

[20] Deutsche Rentenversicherung Bund, Stellungnahme der Deutschen Rentenversicherung Bund anlässlich der Öffentlichen Anhörung vor dem Ausschuss für Arbeit und Soziales des Deutschen Bundestages am 25. Mai 2020 zu dem Gesetzentwurf der Bundesregierung „Entwurf eines Gesetzes zur Einführung der Grundrente für langjährige Versicherung in der gesetzlichen Rentenversicherung mit unterdurchschnittlichem Einkommen und für weitere Maßnahmen zur Erhöhung der Alterseinkommen (Grundrentengesetz)“, BT-Drucksache 19/18473.

[21] Mitteilung der Kommission COM (2016) 179 final, EU-eGovernment-Aktionsplan 2016-2020.

[22] Bundesministerium für Wirtschaft und Energie, Top 100: Wirtschaft Die wichtigsten und am häufigsten genutzten Verwaltungsleistungen für Unternehmen, 2017, 50.

[23] *Stocksmeier/Wimmer/Führer/Essmeyer*, Once-Only in Deutschland und Europa: Eine Roadmap grenzüberschreitender Vernetzung im Bereich Steuern. Digitalisierung von Staat und Verwaltung, 2019.

[24] *Friedrichsen/Schmacker*, Die Angst vor Stigmatisierung hindert Menschen daran, Transferleistungen in Anspruch zu nehmen, DIW Wochenbericht 26, 2019, 455-461.

Stigmatisierung, insbesondere bei öffentlicher Antragsstellung, und die Komplexität der Inanspruchnahme.[25] Eine proaktive Anspruchsermittlung und folgendes Leistungsangebot an Bürgerinnen und Bürger durch die Verwaltung hätte also eine teilhabe- und sozialpolitisch signifikante Wirkung. Die hierfür nötigen Prüfvorgänge sind ohne harmonisierte Register kaum leistbar.

Antragslose Verfahren

Als besonders bürgerorientiert gelten antragslose Verwaltungsverfahren. In Österreich zeigt die antragslose Familienbeihilfe seit 2015 die Vorteile registergestützter Verfahren. In Deutschland verdeutlicht das Pilotprojekt "Einfach Leistungen für Eltern" (ELFE) die vielen Hürden ohne modernisierte Register.

Österreichische Eltern erhalten anlässlich der Geburt eines Kindes ohne Antrag automatisiert die Familienbeihilfe nach § 10a des Familienlastenausgleichsgesetzes.[26] Nach der Geburt werden die Daten von Kind und Eltern durch das Standesamt im Zentralen Personenstandsregister erfasst und automatisch an Sozialversicherung und Finanzamt weitergeleitet. Liegen alle notwendigen Daten vor, erfolgt mit einem Informationsschreiben über den Familienbeihilfenanspruch an die Eltern gleichzeitig die Überweisung des Familienbeihilfenbeitrags - die Bankverbindung liegt dem Finanzamt meist bereits vor.

Das deutsche ELFE-Projekt will auf ähnliche Weise die Kontaktpunkte der Eltern bei der Gewährung von Familienleistungen reduzieren. Im Idealfall sollen Eltern nur noch ihre Einwilligung für den zwischenbehördlichen Datenaustausch sowie die gewünschte Aufteilung der Elternzeit angeben. Die beteiligten Einrichtungen tauschen die nötigen Daten autonom und digital untereinander aus, bis schlussendlich Urkunden und Leistungen die Eltern erreichen. Mangels harmonisierter Register währen allein die informationstechnischen und rechtlichen Vorbereitungen für das auf Bremen beschränkte Pilotprojekt bereits seit 2018.[27] Erst im November 2020 stimmte der Bundesrat notwendigen Gesetzesänderungen für erste Teilanwendungen von ELFE zu.[28]

Die breite Umsetzung antragsloser Verfahren zum Vorteil der Bürgerinnen und Bürger ist erst mithilfe von harmonisierten Registern und verbindender Identifikationsnummer realistisch.

Registerbasierter Zensus

In einer immer stärker auf Daten basierenden Gesellschaft müssen auch die Grundinformationen höhere Anforderungen erfüllen. Entsprechend plant die Europäische Kommission, ab 2024 jährliche Berichtszeiträume für Bevölkerungszahlen und gegebenenfalls weitere Merkmale wie gewöhnlicher Aufenthalt, Alter oder Geschlecht innerhalb des Europäischen Statistischen Systems.[29] Derart kurze Zensus-Zyklen sind nur mit einem registerbasierten Zensus auf Grundlage einer "verknüpfbaren Registerinfrastruktur" realistisch einzuhalten, wie der Rat für Sozial- und Wirtschaftsdaten

[25] *Buslei,/Geyer/Haan/Harnisch*, Starke Nichtinanspruchnahme von Grundsicherung deutet auf hohe verdeckte Altersarmut, DIW Wochenbericht 49/2019, 909-917.
[26] Familienlastenausgleichsgesetz BGBl 1967/376 idF BGBl I 2019/104.
[27] Freie Hansestadt Bremen "ELFE - Einfach Leistungen für Eltern", https://www.finanzen.bremen.de/digitalisierung/digitalisierungsbuero/elfe einfach leistungen fuer eltern -60128 (10.12.2020)
[28] Gesetz zur Digitalisierung von Verwaltungsverfahren bei der Gewährung von Familienleistungen, Bundesrat Drucksache 664/20.
[29] Working Group on Population and Housing Censuses, Post-2020 Census-Strategy, 2014.

empfiehlt.[30] Dabei werden die zensusrelevanten Merkmale in verschiedenen Verwaltungsregistern mithilfe einer einheitliche Identifikationsnummer ermittelt.[31] Hierbei ist ein ”Rückspielverbot” sicherzustellen, also dass der Staat die Daten, die zu statistischen Zwecken erhoben werden, nicht anschließend zum Verwaltungsvollzug verwendet.[32]

Verordnung zum Single Digital Gateway EU (SDG-VO)

Neben den nationalen OZG Zielen bestehen mit der Verordnung zum Single Digital Gateway europarechtliche Verpflichtungen zur grenzüberschreitenden Übermittlung von Registerdaten. Die SDG-VO[33] verpflichtet Mitgliedstaaten zur digitalen Bereitstellung von Verwaltungsverfahren und Hilfsdienste auf eine grenzüberschreitende und diskriminierungsfreie Art und Weise. Grundsätzlicher Maßstab ist die Online-Verfügbarkeit der Verfahren in den jeweiligen EU-Mitgliedsstaaten, der Geburtsnachweis muss jedenfalls mit 12.12.2023 online angeboten werden. Wird ein Verfahren in beiden Mitgliedsstaaten online angeboten, haben beide Mitgliedsstaaten einen digitalen Datentransfer beispielsweise von digitalen Nachweisen aus den jeweiligen nationalen Registern über das Single-Digital-Gateway bis Ende 2023 sicherzustellen. Die Verfahren sind im Anhang 2 der SDG-VO definiert, davon sind 17 Verfahren für Bürgerinnen und Bürger und 4 für die Wirtschaft. Aufgrund der nationalen OZG-Verpflichtung, alle Verwaltungsleistungen bis 2023 online anzubieten, sind diese auch gegenüber EU-Bürgerinnen und -Bürgern online anzubieten und deren digitalen Nachweise über das Single-Digital-Gateway entgegenzunehmen bzw. Nachweise aus Registern von in Deutschland lebenden Personen über das Gateway in andere Mitgliedsstaaten zu transferieren.

Fazit

Ein modernes Registerwesen ist für den Digitalisierungserfolg eines Landes von zentraler Bedeutung. Harmonisierte Register erlauben der Verwaltung die Etablierung vollständig digitaler und zunehmend automatisierter Angebote für Bürgerinnen und Bürger.[34] Erst so werden bürgerfreundliche und effiziente Verfahren wie (halb-)automatische und antragslose Verwaltungsprozesse, die Umsetzung des Once-Only-Prinzips, die Teilhabeeffekte proaktiver Verwaltungsverfahren und die Durchführung registerbasierter Zensus realisierbar. Dabei ist entscheidend, die Datenschutzkonformität der Registerlandschaft bereits durch ihren technischen Aufbau zu sichern. Neben den nationalen Potentialen und rechtlichen Vorgaben des OZG bestehen auch europarechtliche Verpflichtungen durch die SDG-VO, die bereits 2023 erfüllt werden müssen.

[30] Rat für Sozial- und Wirtschaftsdaten, Empfehlungen des RatSWD zum Zensus 2021 und zu späteren Volkszählungen, 2016.
[31] Rat für Sozial- und Wirtschaftsdaten, Empfehlungen des RatSWD zum Zensus 2021 und zu späteren Volkszählungen, 2016, Output, No. 2 (5).
[32] *Martini/Wagner/Wenzel*, 34.
[33] Verordnung (EU) 2018/1724.
[34] *Martini/Wagner/Wenzel,* 42.

II. Datennutzungspraxis im öffentlichen Sektor

Für den Datenschutz gelten in Deutschland die DSGVO, das Bundesdatenschutzgesetz (BDSG) und weitere deutsche Datenschutzregelungen. Maßgebliches Grundrecht ist für den Datenschutz vor allem die informationelle Selbstbestimmung als Konkretisierung des allgemeinen Persönlichkeitsrechts.[35] Neben dem diskutierten datenschutzrechtlichen Eingriff durch eine mögliche Einführung einer Identifikationsnummer, ist in einer Gesamtbetrachtung die aktuelle Verwaltungspraxis und das damit verbundene Spannungsverhältnis zu den Datenschutzgrundsätzen nach Art. 5 DSGVO zu berücksichtigen.

Derzeitige Verwaltungspraxis im Spannungsverhältnis zum Grundsatz der Datenminimierung

Datenminimierung geht als Grundsatz aus Art 5 Abs 1 lit c DSGVO[36] hervor. Demnach müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Personenbezogene Daten sind dem Zweck angemessen, wenn sie der Kontrollfrage 'Sind die Daten erforderlich, um den zuvor festgelegten, eindeutigen Zweck zu erreichen?', standhalten können.[37] Im derzeitigen Verwaltungsalltag werden häufig zusätzliche personenbezogene Daten übermittelt, welche für die eigentliche Aufgabenwahrnehmung nicht notwendig sind. Informationen wie aktuelle Anschrift, Geburtsdatum und -ort sowie der Mädchenname der Mutter dienen ausschließlich der eindeutigen Identifikation, obwohl sie für die eigentliche Aufgabenwahrnehmung nicht notwendig sind.[38] Mit einer solchen unzweckmäßigen Erhebung und Speicherung von Daten, steht die aktuelle Verwaltungspraxis im Spannungsverhältnis zum Grundsatz der Datenminimierung nach Art. 5 Abs. 1 lit c DSGVO.

Ein registerübergreifendes Identitätsmanagement mit einer eindeutigen Identifikationsnummer stellt im Vergleich zur aktuellen Verwaltungspraxis eine erhebliche Verbesserung dar. Dies verdeutlichen die Austauschprozesse zwischen Finanzämtern und beispielsweise den Rentenversicherungen gemäß § 22a Abs. 1 Nr. 1 EStG i.v.m. § 93c Abs. 1 Nr. 2 lit. c AO, wonach einmalig Datensätze ausgetauscht werden, die Folgendes enthalten: den Familiennamen, den Vornamen, den Tag der Geburt, die Anschrift des Steuerpflichtigen und dessen Identifikationsnummer nach § 139 AO. Mit zunehmender Nutzung einer Identifikationsnummer nimmt die Qualität der Daten in den Registern zu, da die Daten aktuell gehalten und regelmäßig berichtigt werden und die übermittelnden Attribute zukünftig noch weiter reduziert werden können. Denkbar und technisch machbar wäre eine Reduktion bis hin zu einem ausschließlich auf die Identifikationsnummer reduzierten Austausch von Daten.

Derzeitige Verwaltungspraxis im Spannungsverhältnis zum Grundsatz der Transparenz

Der Grundsatz der Transparenz in Art 5 Abs 1 lit a DSGVO[39] setzt voraus, dass eine bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist.[40] Diese Information kann in elektronischer Form bereitgestellt werden, insbesondere wenn Bürgerinnen und Bürger nur schwer erkennen und nachvollziehen können, ob, von wem und zu

[35] *Roßnagel*, Kein „Verbotsprinzip" und kein „Verbot mit Erlaubnisvorbehalt" im Datenschutzrecht, NJW 2019,1.
[36] Verordnung (EU) 2016/679.
[37] *Paal/Pauly/Frenzel*, DS-GVO[2] Art. 5 Rz 35.
[38] RegMoG-E, Drucksache 19/24226, 1.
[39] Verordnung (EU) 2016/679.
[40] ErwG 58 Verordnung (EU) 2016/679.

welchem Zweck sie betreffende personenbezogene Daten erfasst werden. Gründe dafür können etwa die große Zahl der Datenverarbeitenden oder die Komplexität der benötigten Technik sein.

Da Bürgerinnen und Bürgern nicht dargelegt werden kann, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden, steht die aktuelle Verwaltungspraxis im Spannungsverhältnis zum datenschutzrechtlichen Grundsatz der Transparenz. Mit dem im vorliegenden Entwurf geplanten Datencockpit hingegen kann die vorgeschriebene Transparenz umgesetzt werden. Das Datencockpit soll den Bürgerinnen und Bürgern einen Überblick bieten, welche sie betreffenden Datenverarbeitungen wann, durch welche Einrichtung und zu welchem Zweck stattgefunden hat. So wird ein nachträglicher Rechtsschutz möglich. Neben den bestehenden Datenschutzbeauftragten werden so in Zukunft auch die Betroffenen selbst die Kontrolle der Rechtmäßigkeit der Datennutzung stärken.

Mangelnde Richtigkeit und Integrität der Datennutzung in der Verwaltungspraxis

Der Grundsatz der Datenrichtigkeit, wie ihn Art 5 Abs 1 lit[41] festschreibt, kann im derzeitigen System nicht garantiert werden.[42] Die Verarbeitung der personenbezogenen Daten steht im Spannungsverhältnis mit dem Grundsatz der Richtigkeit der Daten nach Art. 5 Abs. 1 lit d DSGVO und im Falle der Weitergabe an Dritte dem Grundsatz der Integrität und Vertraulichkeit Art. 5 Abs. 1 lit. f DSGVO. Derzeit können Personenverwechslungen nicht ausgeschlossen werden, da vorhandene Registerdatensätze den Bürgerinnen und Bürgern nicht immer zweifelsfrei zugeordnet werden können.[43] Aufgrund von Transkriptionsfehlern, Namensverwechslungen, unterschiedlichen Aktualisierungsfrequenzen und verschiedenen fachlichen Anforderungen liegen derzeit in den einzelnen Fachregistern bisweilen mehrere Datensätze zu den gleichen Bürgerinnen und Bürgern vor.[44] Dadurch kommt es zu Trefferlisten, in denen auch die Daten unbeteiligter Personen enthalten sein können, oder zu einem Abbruch des Vorgangs, da die Bürgerinnen und Bürger nicht in allen nötigen Registern auffindbar sind.[45] Eine Identifikationsnummer verhindert derartige Fehler und erhöht somit die Datenqualität sowie die Integrität und Vertraulichkeit durch korrekte Datenweitergabe. Die Identifikationsnummer stellt durch die korrekte Zuordnung von Datensätzen also langfristig die Einhaltung der Grundsätze der Richtigkeit der Daten und der Vertraulichkeit der Daten sicher.

Verwaltung muss Auskunft geben können

Bürgerinnen und Bürger haben laut Art. 15 DSGVO ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten. Um von der Datenverarbeitung Kenntnis zu erlangen und deren Rechtmäßigkeit prüfen zu können, soll das Auskunftsrecht problemlos und in angemessenen Abständen wahrnehmbar sein.[46] Nach enger Auslegung des Begriffs des Verantwortlichen im Sinne der datenverarbeitenden Stelle müsste die betroffene Person hierzu bei der jeweiligen Behörde eine Auskunft der Datenverarbeitung beantragen. Der öffentliche Sektor kann aber auch als eine verantwortliche Stelle auslegt werden, solch einem Auskunftsbegehren kann derzeit nicht nachgekommen werden. Erst der Überblick über alle dem Staat vorliegenden Daten mithilfe der

[41] Verordnung (EU) 2016/679.
[42] RegMoG-E, Drucksache 19/24226, 1.
[43] RegMoG-E, Drucksache 19/24226, 1.
[44] RegMoG-E, Drucksache 19/24226, 1.
[45] RegMoG-E, Drucksache 19/24226, 1.
[46] ErwG 63 Verordnung (EU) 2016/679.

Identifikationsnummer schafft Datensouveränität für Bürgerinnen und Bürger und fördert das Vertrauen in den öffentlichen Sektor.

Datenschutzfreundliche Technikgestaltung (Privacy by Design)

Mit einer datenschutzfreundlichen Technikgestaltung sollen die Grundsätze in Art 5 Abs 1 DSGVO[47], etwa die oben angeführte Datenminimierung, zu einem möglichst frühen Zeitpunkt realisiert werden.[48] Indem von vornherein in geringerem Umfang Daten verarbeitet werden, ist auch das Ausmaß unrechtmäßiger Datenverarbeitungen unwahrscheinlicher.[49] Konkrete Maßnahmen oder Instrumente führt die DSGVO nicht an.[50]

Wie die systematische Umsetzung von Privacy by Design aussehen kann, legt die Europäische Agentur für Netz- und Informationssicherheit (ENISA) in einem Bericht[51] dar.[52] Demnach sollten personenbezogene Daten unter anderem auf ein Minimum reduziert (Minimise) und in getrennten Systemen verarbeitet, ausgewertet und gespeichert werden (Separate). Der vorliegende Entwurf entspricht durch eine Verringerung der für die eindeutige Identifikation notwendigen Attribute - bis hin zur Identifikationsnummer alleine - einerseits dem Minimise-Prinzip. Andererseits folgt die föderal und fachlich verteilte dezentrale Datenverarbeitung und -speicherung dem Separate-Prinzip.

Fazit

Im derzeitigen System werden entgegen dem Grundsatz der Datenminimierung häufig zusätzliche personenbezogene Daten (z.B. aktuelle Anschrift, Geburtsdatum und -ort, Mädchenname der Mutter) nicht für die eigentliche Aufgabenwahrnehmung, sondern ausschließlich zu Zwecken der Identifikation übermittelt.[53]

Die aktuelle Verwaltungspraxis steht im Spannungsverhältnis zum datenschutzrechtlichen Grundsatz der Transparenz, da Bürgerinnen und Bürgern keine Auskunft dazu gegeben werden kann, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden.

Transkriptionsfehler, Namensverwechslungen, unterschiedlichen Aktualisierungsfrequenzen und verschiedene fachliche Anforderungen führen derzeit bisweilen zu Doubletten in den Fachregistern.[54] Dadurch wird dem Grundsatz der Richtigkeit und Integrität der Daten nicht entsprochen.

Ziel der datenschutzfreundlichen Technikgestaltung ist die Umsetzung der datenschutzrechtlichen Grundsätze zu einem möglichst frühen Zeitpunkt. Der vorliegende Entwurf entspricht mit dem Minimise-Prinzip bei der Verringerung der allein für die Identifikation übermittelten Attribute und dem Separate-Prinzip durch dezentrale verteilte Register den durch die Europäische Agentur für Netz- und Informationssicherheit anerkannten Privacy-by-Design-Ansätzen.

---

[47] Verordnung (EU) 2016/679.
[48] *Kühling/Buchner*, Datenschutzgrundverordnung, Art 25 Rz 14.
[49] *Kühling/Buchner*, Datenschutzgrundverordnung, Art 25 Rz 14.
[50] *Kühling/Buchner*, Datenschutzgrundverordnung, Art 25 Rz 17.
[51] ENISA, Privacy by design in Big Data, enisa.europa.eu/publications/big-data-protection/at_download/fullReport (9.12.2020).
[52] *Schütze,* EU: ENISA veröffentlicht Bericht zu Privacy by Design in Big Data, ZD-Aktuell 2016, 05015.
[53] RegMoG-E, Drucksache 19/24226, 1.
[54] RegMoG-E, Drucksache 19/24226, 1.

III. Architektur der Registerlandschaft nach dem Entwurf des RegMoG

Der technische Aufbau des Registermodernisierungsgesetzes strebt einen Ausgleich zwischen den gesellschaftlichen Zielsetzungen, technischen Voraussetzungen und datenschutzrechtlichen Vorgaben an. Das gewählte System zielt dabei auf eine Kombination von verschiedenen Maßnahmen, die unterschiedliche Aspekte des Datenschutzes zum Ziel haben und sich gegenseitig ergänzen.

Die dezentrale verteilte Datenhaltung wird aufrechterhalten und erzeugt weiterhin eine analoge Distanz zwischen den Datenbeständen des Gesamtsystems. Dieser dezentrale Aufbau mit seinen bestehenden Sicherungsmechanismen wird mit dem Gesetz zusätzlich in Bereiche eingeteilt, die bestimmte Datenbestände voneinander trennen. Über das 4-Corner-Modell wird für diese Bereiche eine übergreifende Kommunikation mit hohem Schutzstandart ermöglicht. Zugriffe und Verarbeitungen können auf tatsächlich rechtlich berechtigte Personen und Stellen beschränkt, protokolliert und über ein Portal, dem Datencockpit, den Betroffenen transparent gemacht werden. Das System ermöglicht somit, ex-ante Zugriffe auf einen tatsächlich berechtigten Kreis zu beschränken und ex-post unberechtigte Versuche einer Kontrolle durch die Betroffenen und der Strafverfolgung zu eröffnen. Die zentrale IDNr ermöglicht in diesem System den bereichsübergreifenden Abgleich von Daten und die Transparenz der Verarbeitung. Sie legt den Grundstein für eine digitale Verwaltung. Ihre Einführung wird besonders kritisch gesehen, da nun alle Daten einer Person verknüpfbar sein sollen. Unter Berücksichtigung der Möglichkeiten moderner Datenverarbeitung ist jedoch nicht mehr die theoretische Verknüpfbarkeit ausschlaggebend, diese ist oft schon aufgrund weniger übereinstimmender Datenpunkte möglich, sondern der praktische Zugang. Die im RegMoG-E vorgesehenen Schutzmechanismen, wie Protokollierung der Zugriffe und Zugriffsversuche, Vorabprüfung der Zulässigkeit der Datenübermittlung und dezentraler verteilter Datenhaltung sind zumindest gleichwertig mit bereichsspezifischen Kennzeichen. Diese einzelnen Maßnahmen ließen sich theoretisch noch weiter kombinieren. So entsteht der Eindruck, dass mehr Schichten und Schutzmechanismen auch weiter die Sicherheit steigern, jedoch kann die Sicherheit mit steigender Komplexität auch wieder abnehmen, da eine Kontrolle und Funktionsgarantie des Gesamtsystems immer schwerer zu gewährleisten ist.

In der Gesamtschau legt das Gesetz einen sinnvollen technischen Grundstein für ein zeitgemäßes System der Datenhaltung und Verarbeitung, das traditionelle Anforderungen an den Datenschutz erfüllt und modernen Verarbeitungsmöglichkeiten Rechnung trägt.

Architektur: 4-Corner-Modell und weitere Sicherungsmaßnahmen

Im 4-Corner-Modell werden die Verwaltungsregister nach fachlichen Kriterien in mindestens sechs Bereiche geteilt, wie beispielsweise Inneres, Justiz, Wirtschaft und Finanzen, Arbeit und Soziales, Gesundheit, Statistik. Diese Bereiche bilden eine zusätzliche Sicherungsschicht mit Zugriffskontrolle sowie Protokollierung, welche die Datenschutzwirkung der bestehenden dezentralen verteilten Datenhaltung ergänzt. Im Fall einer bereichsübergreifenden Transaktion wird vorab über Intermediäre die Zulässigkeit der Datenabfrage geprüft.

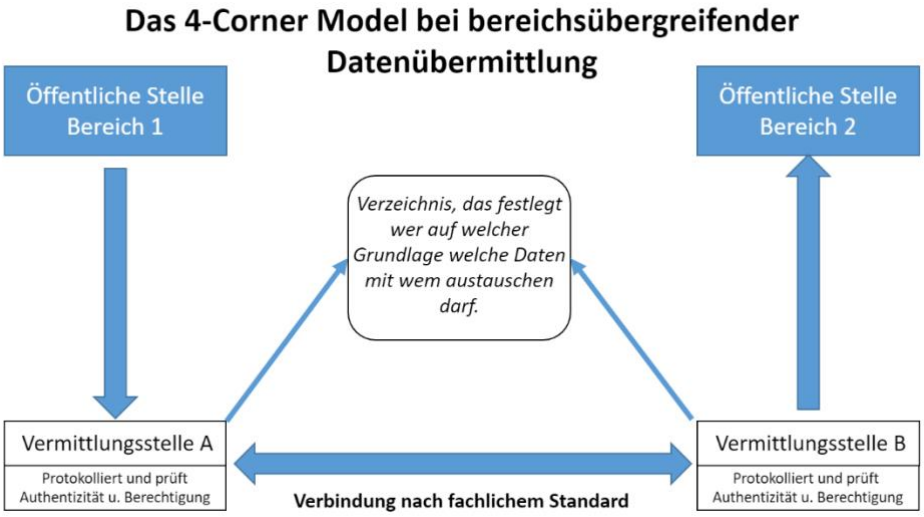
Die bestehenden Standards innerhalb der Bereiche und Bundesländer für Beweissicherung und Revisionsfestigkeit werden nicht geschwächt. Clearingstellen der Länder überwachen bereits die Datenbewegungen unter Einbindung der Datenschutzbeauftragten.[55] Diese Verfahren müssen gem. §

[55] RegMoG-E, Drucksache 19/24226, 51.

7 Abs. 2 S.1 ivm. S. 7 IDNrG-E ebenfalls dem aktuellen Stand von Sicherheit und Technik entsprechen.[56]

Kontrollierte Datenübermittlung

Kernelement des 4-Corner-Modells ist die Kontrolle der Datenübermittlung. So werden Daten im 4-Corner-Modell ausschließlich über neutrale dritte Stellen übertragen. Diese kontrollieren den Zugang und protokollieren die Übermittlung. Im Deutschen Verwaltungsdienstverzeichnis (DVDV) werden die Dienste mit ihren jeweiligen Berechtigungen geführt.[57] So können die Vermittlungsstellen prüfen, welche öffentlichen Stellen auf welcher Rechtsgrundlage miteinander welche Daten austauschen dürfen.



Die Vermittlungsstellen selbst können dabei nicht in die übertragenen Datenpakete hineinschauen, sondern prüfen die Voraussetzungen für den Datenaustausch. Liegen diese Voraussetzungen nicht vor, wird die Anfrage verwehrt und es werden keine personenbezogenen Daten übermittelt. Abfrageversuche mit fehlender Berechtigung oder ohne ein-eindeutige Zuordnung zu einer berechtigten Stelle werden nicht durchgeführt und sind später nachvollziehbar, da sämtliche Datenübermittlungen zwischen öffentlichen Stellen unter Verwendung der IDNr gem. § 9 Abs. 1 IDNrG-E protokolliert werden müssen. Die Datenübermittlungen selbst erfolgen gem. § 7 Abs. 2 IDNrG-E verschlüsselt, nach einem dem aktuellen Stand von Sicherheit und Technik entsprechenden Verfahren. Das genaue Verfahren wird im Rahmen der Vorgaben des § 7 Abs. 2 IDNrG-E durch das gem. § 7 Abs. 2 IDNrG-E BMI in Einvernehmen mit dem Bundesministerium der Finanzen und im Benehmen mit dem IT-Planungsrat durch Rechtsverordnung gem. § 12 Abs. 2 Nr. 6 IDNrG-E bestimmt. Das 4-Corner-Modell wird in der Innenverwaltung bereits eingesetzt und ist auch im IT-Architekturmodell für den EU-weiten Datenaustausch nach der SDG-VO vorgesehen.

Verhinderung umfassender digitaler Persönlichkeitsprofile

Zur Absicherung des Einsatzes einer Identifikationsnummer sind geeignete technisch-organisatorische und rechtliche Mittel entscheidend, wie Martini et al. dargelegt haben.[58] Sie nennen beispielhaft das Risiko einer späteren Profilbildung oder das Risiko für nachhaltige Persönlichkeitsverletzungen bei Schadensfällen. Zur Absicherung dieser Risiken sind mögliche Maßnahmen zu entwickeln, um einem

[56] RegMoG-E, Drucksache 19/24226, 51.
[57] RegMoG-E, Drucksache 19/24226, 51.
[58] *Martini/Wagner/Wenzel*, 44 und 52.

potentiellen Missbrauch vorzubeugen, wie rechtliche Sanktionsmaßnahmen, Maßnahmen zur Datensicherheit, den Datenbestand selbst oder Vorgaben zum Stand der Technik.[59] Das 4-Corner-Modell prüft mithilfe von technischen Prozessen vor der Übermittlung der Daten die Rechtmäßigkeit und sichert zusätzlich mit strafrechtlichen Sanktionen.

In der Gesamtwirkung erscheint das 4-Corner-Modell eine geeignete rechtliche technische Maßnahme darzustellen. Trotz der kombinierten Maßnahmen wird das 4-Corner-Modell als unzureichend kritisiert und bereichsspezifische Identifikationsnummern gefordert. Diese Kritik ist schwer nachvollziehbar, da das Schutzniveau des 4-Corner-Modells mit dem einer bereichsspezifischen Kennziffer als ebenbürtig einzustufen ist bzw. geht es mit der zwingenden Vorabprüfung und Protokollierung noch darüber hinaus. Zusätzlich ermöglicht das Architekturmodell eine dezentral verteilte Führung der Register sowie Kontroll- und Protokollierungsmechanismen, die Datenzugriffe im Gesamtsystem über das Datencockpit transparent und nachverfolgbar machen. Aktuell ist dem AutorInnen-Team keine rechtlich-technische Architektur bekannt, die in ihrer Gesamtwirkung ein ähnlich hohes Schutzniveau vorweisen kann.

Anzahl und Auswahl der Bereiche im 4-Corner-Modell

Damit das 4-Corner-Modell in seiner Schutzfunktion greifen kann, dürfen die einzelnen Bereiche keine Register umfassen, die zu einem Persönlichkeitsprofil verknüpft werden können. Demnach ist zu prüfen, ob das Minimum von sechs Bereichen ausreichend ist. Die tatsächliche Zahl der einzurichtenden Bereiche wird unter Berücksichtigung der jeweils enthaltenen Datenfelder und ihrer Sensibilität festzustellen und der Verordnung gem. § 12 Abs. 1 Nr. 2 IDNrG-E zugrunde zu legen sein.

Zum Teil wird kritisch angemerkt, dass die Einteilung auf Verordnungsebene nach § 12 IDNrG-E problematisch sei. Eine Definition der Bereiche auf Gesetzesebene nähme die Flexibilität gegebenenfalls auch mehr als sechs Bereiche festzulegen, falls dies aus der Perspektive des Datenschutzes notwendig sein sollte. Begrüßenswert wäre es jedoch, eine stärkere, auf Kriterien gestützte Zielsetzung für die Bereichseinteilung in das Gesetz bzw. in die Erläuterungen aufzunehmen. Die vorgeschriebene Mindestzahl von sechs Bereichen deutet bereits an, dass die bestehenden großen Fachbereiche wie Inneres, Justiz, Steuern oder Gesundheit voraussichtlich definiert werden sollen.

Fazit und Ausblick

In der Gesamtschau ist zu beachten, dass das 4-Corner-Modell nicht die einzige Schutzebene ist, die das unberechtigte und unkontrollierte Auslesen und Verknüpfen von Datenbeständen verhindert. Auch innerhalb der Bereiche ist kein beliebiger Datenaustausch möglich. Das 4-Corner-Modell ist bereichsintern zwar nicht verpflichtend vorgeschrieben, kann aber dennoch, wie etwa in der Innenverwaltung bereits zum Einsatz kommen. Ebenso bestehen innerhalb der Bereiche Sicherheitsstandards und Protokollierungspflichten.

Das 4-Corner-Modell ist im Tandem mit dem Datencockpit zu betrachten, auf das noch eingegangen wird. Gemeinsam ermöglichen sie Zugriffskontrollen sowohl ex-ante, indem das Vorliegen der gesetzlichen Zugriffsvoraussetzungen geprüft wird, sowie ex-post durch die Protokollierung der Zugriffsversuche, dadurch wäre erstmals Transparenz der Datenverarbeitung für Bürgerinnen und Bürger garantiert. Darüber hinaus sind über die bestehenden Sanktionsmaßnahmen der DSGVO weitere die Sanktionierung unberechtigter Datenverarbeitungsversuche vorgesehen.

[59] *Martini/Wagner/Wenzel,* 43 ff.

Kern und Stärke der Gesamtarchitektur ist die dezentrale und verteilte Haltung der Inhaltsdaten bei Ländern und Kommunen. Die führenden E-Government-Nationen setzen alle auf zentrale Bundesregister, die ein ungleich höheres Risiko mit sich bringen, weil eine analoge räumliche Trennung fehlt und ein einzelner Angriffsvektor geboten wird.

Identifikationsnummer

Informationelle Selbstbestimmung

Die primäre Kritik am vorgeschlagenen System speist sich aus zwei Befürchtungen: Einerseits die umfassende Profilbildung zu Bürgerinnen und Bürgern mithilfe der Identifikationsnummer, andererseits ein mangelnder Schutz des Systems vor Angriffen von innen oder außen. [60]

Als zentrales Argument in der Debatte gegen die Einführung einer Identifikationsnummer wird das Volkszählungsurteil des Bundesverfassungsgerichts aus 1983 angeführt: [61]

> *„Das Erhebungsprogramm vermag zwar einzelne Lebensbereiche, zum Beispiel den Wohnbereich des Bürgers, jedoch nicht dessen Persönlichkeit abzubilden. Etwas anderes würde nur gelten, 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; denn eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebensdaten und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger ist auch in der Anonymität statistischer Erhebungen unzulässig* […]."

Mit den beschränkten Rechenleistungen und spärlichen Datenpunkten der 1980er war das Verbot eines einheitlichen Personenkennzeichens 1983 ein wirksamer Schutz vor Profilbildung. Im 21. Jahrhundert ist ein einheitliches Personenkennzeichen jedoch nicht mehr notwendig, um Datenbestände zu einem Profil zusammenzuführen. Auf Basis der zahlreichen Datenpunkte in Registern und Anwendungen können aktuelle marktübliche IT-Systeme auch ohne eindeutige Identifikationsnummer mit einer hohen Trefferquote zusammengehörige Datensätze zu Personenprofilen bzw. Persönlichkeitsprofilen verbinden.[62] Eine Suche nach Datenpunkten oder eine Verknüpfung von Datenpunkten mit Hilfe der Identifikationsnummer über alle Register ist weder vorgesehen noch aufgrund der logischen Trennung der Register technisch möglich. Eine Profilbildung erfolgt daher nicht über die Identifikationsnummer, sondern über die unrechtmäßige Zusammenführung von Daten zu einer Person. Hierfür muss auf die jeweiligen dezentralen Register und Datenbanken tatsächlich zugegriffen werden können. Dies ist bereits heute nicht der Fall und wird durch die Einführung einer dezentral harmonisierten Registerlandschaft auch nicht ermöglicht. Selbst wenn der Zugang an einem Zugangspunkt kompromittiert wird, kann, aufgrund der dezentralen Struktur nur auf die lokal gespeicherten Daten des jeweiligen Registers zugegriffen werden. Die technischen Voraussetzungen für eine Profilbildung schafft somit nicht erst eine Identifikationsnummer, sondern allein der umfassende Zugriff auf die Register. Entscheidend sind daher die Sicherungsmaßnahmen, die im RegMoG-E vorgesehen sind: Minimierung der

[60] *Kelber*, Stellungnahme des BfDI an den Innenausschuss, bfdi.bund.de/DE/Infothek/Transparenz/Stellungnahmen/2020/StgN_InnenA-Registermodernisierungsgesetz.pdf?__blob=publicationFile&v=1 (10.12.2020).
[61] BVerfG 15. 12. 1983, 1 BvR 209/83.
[62] *Martini/Wagner/Wenzel,* 38.

Zugriffsmöglichkeiten durch fachlich und örtlich verteilte Register, revisionssichere Protokollierung aller Zugriffe, eine damit verbundene Ex-Post-Prüfung durch den Bürger und die Bürgerin mit Hilfe des Datencockpits und eine Ex-Ante-Zugriffsberechtigungsprüfung im Fall von sensiblen und bereichsübergreifenden Transaktionen. Die dezentrale verteilte Architektur, die mit dem RegMoG etabliert werden soll, ist auch im internationalen Vergleich eine der Stärken, siehe dazu auch letztes Kapitel.

Steuer-Identifikationsnummer

Die Verwendung der Steuer-Identifikationsnummer als registerübergreifende einheitliche Identifikationsnummer ermöglicht für natürliche Personen die eindeutige Zuordnung in den relevanten Registern der öffentlichen Verwaltung. Dabei kann auf die bereits vorhandenen Strukturen der Steueridentifikationsnummer nach § 139b der Abgabenordnung aufgesetzt werden: So besteht bereits eine Stelle, die den Identifikator fortlaufend betreuen, weiterentwickeln und beaufsichtigen kann. Diese bestehenden Organisationsstrukturen können zeitnah für ein registerübergreifendes Identitätsmanagement aufgerüstet werden.

Derzeit ist die Verwendung der Steuer-Identifikationsnummer auf den steuerlichen Bereich beschränkt. Die Bereiche, in denen die Steuer-ID bereits genutzt wird, reichen von Meldebehörden, Arbeitgebern im Rahmen des Lohnsteuerabzugsverfahrens über Banken, Gerichte und Notare (gemäß § 139b Abs. 2 AO, § 154 Abs. 2a AO, § 93c Abs. 1 Nr. 2 lit. a-c AO, § 26 Abs. 4 u. 5 EGAO, § 22a Abs. 1 Nr. 1 EStG i.v.m. § 93c Abs. 1 Nr. 2 lit. c AO).[63] Die Entwürfe des RegMoG und des IDNrG bauen auf diesen technischen und organisatorischen Erfahrungen auf und stellt damit aus dem Blickwinkel der Informationssicherheit eine geprüfte Grundlage dar.

Registermodernisierungsbehörde

Die nach RegMoG-E einzurichtende Registermodernisierungsbehörde wird keinen dauerhaften Datenbestand aufbauen (vgl. § 11 IDNrG-E). Die Behörde darf nach § 11 IDNrG-E die vom Bundeszentralamt für Steuern übermittelten Basisdaten zum Zweck der Datenübermittlung und Protokollierung zwischenspeichern. Danach sind sie jedoch zu löschen.[64]

Die Basisdaten sind die zur Identifizierung einer natürlichen Person erforderlichen personenbezogenen Daten. Dazu zählen die Identifikationsnummer nach § 139b der Abgabenordnung, Familienname, frühere Namen, Vorname, Doktorgrad, Tag und Ort der Geburt, Geschlecht, Staatsangehörigkeiten, gegenwärtige oder letzte bekannte Anschrift, Sterbedatum sowie Tag des Einzugs und des Auszugs.[65]

Datencockpit als Datenschutzkontrollinstrument für Bürgerinnen und Bürger

Das Datencockpit wird in § 10 Abs. 1 OZG als IT-Komponente im Portalverbund beschrieben, in der sich Betroffene Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen, die unter Verwendung der Identifikationsnummer erfolgt sind, anzeigen lassen können. Das Datencockpit fungiert also als Mittler zwischen datenverarbeitenden Stellen und der betroffenen Person. Sinn und

[63] Abgestimmter BLAG-Abschlussbericht, 13.
[64] Deutscher Bundestag - Wissenschaftliche Dienste, Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes, 17.
[65] § 4 Abs 2 IDNrG-E.

Zweck des Datencockpits ist, aus dem Zusammenhang des Entwurfs genommen, die Stärkung der informationellen Selbstbestimmung und, aus der Perspektive des BVerfG, die Minderung der Eingriffsintensität. Denn durch den Zugang zu den Protokollen der Datenübermittlung nach § 9 IDNrG können Bürgerinnen und Bürger die Rechtmäßigkeit der Nutzung der sie betreffenden Daten prüfen. So wird eine heimliche Datenverarbeitung erschwert, die für Betroffene grundsätzlich gravierender als eine offene Verarbeitung ist.[66]

Zugang zu und Funktionsweise des Datencockpits

Das Datencockpit soll durch eine noch durch Rechtsverordnung zu bestimmende öffentliche Stelle bereitgestellt werden.[67] Die Registrierung für das Datencockpit hat mit dem Vertrauensniveau "hoch" gem. der eIDAS-VO zu erfolgen. Alternativ sollen Bürgerinnen und Bürger auch ihr Nutzerkonto des Portalverbundes für den Zugang verwenden können.[68] Auch hier ist ein Identifizierungsmittel des Vertrauensniveaus hoch bzw. eines gem. § 3a Abs.2 S.5 VwVfG vorausgesetzt.[69] Ein drei Jahre lang ungenutztes Datencockpit wird automatisch gelöscht. Nutzerinnen und Nutzer können das Konto auch jederzeit selbst löschen und beeinflussen, in welchem Umfang welche Protokolldaten das Datencockpit anzeigen darf.[70] Diese Protokolldaten werden gem. § 10 Abs. 2 OZG nur für jeweils einen Nutzungsvorgang auf den Endgeräten der Nutzerinnen und Nutzer gespeichert. Dauerhaft liegen die Protokolldaten dezentral bei den Registern. Diese sind gemäß § 2 S.1 Nr.3 IDNrG für die Protokollierung zuständig. Vorteil dieses "Quellmodells" ist, dass weder bei den Nutzerinnen und Nutzern noch in einem zentralen Protokollregister eine Ansammlung sensibler Datenbestände entsteht. Dieses Modell lässt sich zeitnah umsetzen und ist offen für einen weiteren Ausbau einer datenschutzkonformen Informationsbereitstellung. Zur Stärkung der Ex-Post-Kontrolle wäre langfristig ein kurzer Beschwerde-/Meldeweg über das Datencockpit bei Zweifeln an der Rechtmäßigkeit einer Datenübermittlung zu begrüßen.

Pflicht der Protokollierung

Die Protokollierungspflicht umfasst nach § 2 S.1 Nr.3 IDNrG-E alle Datenübermittlungen zwischen verschiedenen Rechtsträgern und unterschiedlichen Bereichen. Nach § 9 IDNrG-E sind zudem alle Übermittlungen zwischen öffentlichen Stellen zu protokollieren.

Die Protokolldaten sind gem. § 9 Abs. 3 IDNrG-E zwei Jahre aufzubewahren und anschließend zu löschen. Von der Protokollierung dürften derzeit alle Übermittlungen unter Verwendung der IDNr erfasst sein, da keine Zugangsberechtigungen für nicht-öffentliche Stellen ersichtlich sind. Datenschutzbeauftragte äußerten bereits dahingehende Befürchtungen im Rahmen der Zweckbindung.[71] Sinnvoll wäre daher eine präzise Formulierung der Protokollierungspflichten, sodass sämtliche Datenverarbeitungen und -abrufe auf Grundlage der IDNr zu protokollieren sind. Dies schließt eine mögliche Regulierungslücke.

Protokollierungsstandard

Offen ist nach den Ausführungen im Gesetzentwurf, welche Datenpunkte für die Protokollierung gespeichert werden sollen. § 9 Abs. 1 S. 1 Hs. 2 IDNrG schreibt lediglich eine Weise der Protokollierung

[66] BVerfG 11.03.2008, 1 BvR 2074/05, Rn 79.
[67] § 10 Abs. 5 Neu OZG.
[68] Vgl § 10 Abs. 3 Neu OZG.
[69] RegMoG-E, 128 f.
[70] Vgl § 10 Abs. 4 Neu OZG.
[71] BfDI, Stellungnahme des BfDI zum Entwurf des RegMoG, 6.

vor, die die Kontrolle der Zulässigkeit von Datenabrufen technisch unterstützt. Hierbei entsteht ein Spielraum möglicher gesetzeskonformer Umsetzungen.

Dem Wortlaut von § 12 Abs. 2 Nr. 6 IDNrG-E folgend, besteht eine Verordnungsermächtigung des BMI lediglich für die Ausgestaltung der Protokollierung bei der Registermodernisierungsbehörde, bzw. für Datenübermittlungen zwischen dieser und dem Zentralamt für Steuern.[72] Hier besteht das Risiko, dass sich ein uneinheitlicher Protokollierungsstandard verfestigt, der im Datencockpit zu Darstellungsproblemen führt. Entsprechend ist sicherzustellen, dass die jeweiligen lokalen Protokollierungen vom Datencockpit verarbeitet werden können. Dies sollte mit einer standardisierten technischen Schnittstelle lösbar sein, welche die länderspezifischen Protokollierungen für die standardisierte Abfrage über das Datencockpit übersetzt.

Umfang der Protokollierung

Die Eingriffsintensität des Gesetzentwurfs ergibt sich in Teilen auch aus dem Umfang der Protokollierung. Die Protokollierung muss tatsächlich eine Nachvollziehbarkeit der Verarbeitung ermöglichen. Auch muss die Darstellung im Datencockpit die Nachvollziehbarkeit (Transparenz) der Datenverarbeitung gemäß Art. 5 Abs. 1 lit. a DSGVO sicherstellen. Ebenso sind die Anforderungen an Beweissicherheit und Revisionsfestigkeit zu erfüllen, wobei diese Daten nicht zwingend alle im Datencockpit angezeigt werden müssen, bzw. sollten. Hier ist der Maßstab stärker auf die Nachvollziehbarkeit der Verarbeitung zu setzen und nicht die absolut betrachtete Vollständigkeit aller Protokolldaten.

Zur Beweissicherheit und Revisionsfestigkeit stehen zwei Punkte im Konflikt: Einerseits darf die Protokollierung keine automatisierte Leistungs- und Verhaltenskontrolle der datenverarbeitenden Personen ermöglichen. Andererseits sollte sie möglichst datensparsam eingerichtet werden.[73] Insgesamt sollte auf eine Weise protokolliert werden, die ein Nachvollziehen der einzelnen Verarbeitungsschritte, Anwendungen, Maschinen und Personen mit Zeitbezug erlaubt und diese Daten unveränderlich mit beschränktem Zugang ablegt. Nach § 8 Abs. 2 IDNrG-E ist auf Ebene der Registermodernisierungsbehörde vorgeschrieben, dass durch technische und organisatorische Maßnahmen Daten nicht unbefugt verarbeitet werden können. Ebenso haben abrufende Stellen, die das automatisierte Abrufverfahren nutzen, sicherzustellen, dass nur befugte Personen dieses nutzen können.

Der vorliegende Gesetzesentwurf lässt offen, ob die Protokolle aus Metadaten, Inhaltsdaten oder beidem bestehen. In die Protokolle personenbezogene Inhaltsdaten aufzunehmen, ist nicht empfehlenswert. Metadaten sind für das Nachvollziehen der Datenverarbeitung ausreichend, also beispielsweise Angaben zu Zeitpunkt, Verarbeitungszweck, Verarbeitungsgrundlage sowie der verarbeitenden Stelle. Inhaltsdaten sollten hingegen über das Auskunftsrecht abrufbar sein, die Trennung von Inhaltsdaten und Metadaten ist ein Schutzmechanismus für den Fall einer Kompromittierung des Datencockpits. Das Datencockpit könnte in Zukunft neben der Auskunft über die Datenverarbeitung auch eine Datenauskunft nach Art. 15 DSGVO ermöglichen. Die hier etablierte Infrastruktur könnte ebenso die Grundlage für einen datenschutzkonformen Kontakt zum Staat

[72] Der § 12 Abs. 2 Nr. 6 IDNrG-E nennt explizit nur § 9 Abs. 1 S. 2 IDNrG-E.

[73] Arbeitskreis „Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten der Bundes und der Länder, Orientierungshilfe „Protokollierung, 2009, 3. https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2009-OH-Protokollierung.pdf (10.12.2020).

bieten, eine gesetzliche Verankerung einer Funktion zur Datenauskunft nach Art. 15 DSGVO ist empfehlenswert. Zusätzlich sollte ein zukünftiger grenzüberschreitender Datenverkehr nach SDG-VO im Datencockpit abgebildet werden.

IV. Internationale Architekturmodelle von Registerlandschaften

Internationale Übersicht von Registerlandschafen

Im E-Government führende Länder haben funktionierende Registerlandschaften als Basis für digitale Verwaltungsverfahren gemein. Basierend auf der europaweiten Datenschutzdebatte und zur Wahrung der Datensicherheit besitzen diese Registerlandschaften Schutzmechanismen, um Datenmissbrauch zu verhindern.

Schutzmechanismen	**Deutschland (RegMoG)**	**Österreich**	**Estland**	**Dänemark**
System bereichsspezifischer Personenkennzeichen	-	x	-	-
Ex-Ante-Berechtigungsprüfung durch Intermediär (4 Corner)	x	(x) auf Bundesebene	x	x
Ex-Post Kontrollierbarkeit der Datenzugriffe, Datencockpit	x	(x) teilweise in Planung	x	-
Dezentrale verteilte Register	x	-	-	-
Datenschutz als Verfassungsrecht, strenge Datenschutzaufsicht, Evaluierung und Berichtswesen ans Parlament, Straftatbestand mit Freiheitsstrafe	x	-	-	-

[74]

Österreich

In der Debatte wird häufig das österreichische Modell und die bereichsspezifischen Personenkennzeichen (bPK), die aus Stammzahlen gebildet werden, als eine der wirksamsten datenschutzrechtlichen Maßnahmen angeführt. In Österreich kann die Stammzahl als allgemeines Personenkennzeichen gewertet werden.[75] Allerdings ist die Stammzahl nur der Stammzahlenregisterbehörde bekannt, sie wird nicht zwischen den Behörden übermittelt und damit nicht verbreitet.[76] Mit der Einführung der Kombination aus Stammzahl und bPK wird grundsätzlich eine grundrechtsschonende Lösung gewählt und dem Gedanken “Privacy by Design” Rechnung getragen, da die Möglichkeiten von Datenabfragen und Zusammenführungen nicht erweitert werden.[77] Allerdings wird die fortlaufend notwendige bPK-Berechnung für Datenübermittlungen an einer zentralen Stelle vorgenommen, sodass theoretisch die Gefahr der Datensammlung an der sensiblen Stelle besteht. In Diskussion ist eine Verschlüsselung der Inhaltsdaten und der Protokolldaten.

[74] Vgl Stellungnahme Nationaler Normenkontrollrat (NKR), 12/2020.
[75] *Martini/Wagner/Wenzel*, 38.
[76] *Martini/Wagner/Wenzel*, 38.
[77] *Martini/Wagner/Wenzel,* 40.

Das bPK-System wurde Anfang 2000 entwickelt und auf Bundesebene in mehr als 30 Registern realisiert, die Daten werden, selbst wenn lokale Register vorliegen, zentrale auf Bundesebene harmonisiert, gespeichert und verarbeitet. Das Angriffs- und Missbrauchsrisiko beim österreichischen Zentralen-Melderegister (ZMR) ist im Vergleich zur aktuellen dezentral verteilten Lösung des deutschen Meldewesens höher einzustufen. Im Fall eines unberechtigten Zugangs oder eines Missbrauchs durch Zugangsberechtigte kann im österreichischen Melderegister grundsätzlich auf alle Daten zugegriffen werden. In Deutschland ist im gleichen Fall nur das jeweilige lokale Melderegister betroffen, das nur einen Ausschnitt der Meldedaten enthält. Das Risiko wurde beim österreichischen Ergänzungsregister für Sonderfälle natürlicher und juristischer Personen sichtbar, bei welchem über Jahre persönliche Daten von mindestens einer Million Bürger und Bürgerinnen öffentlich zugänglich waren.[78]

Das österreichische System bietet keine Kontrollfunktion der Datennutzung. Ein Zugriff auf die Protokolldaten durch die betroffene Person ist nicht vorgesehen. Geplant ist hingegen die Weitergabe von staatlichen Daten durch Bürgerinnen und Bürger an die Wirtschaft. Durch die dazu notwendigen bPK-Berechnungen sind die Metadaten der Datentransaktionen während der Transaktion bzw. im Anschluss theoretisch in einem dafür vorgesehenen Datencockpit einsehbar. Der Fokus liegt dabei auf die Protokollierung der Datenübermittlung, die durch den Bürger oder die Bürgerin initiiert wurde. Ein zukünftiger Vorteil des österreichischen Datencockpits wird ein automatisiertes Auskunftsrecht über die bPK-geführten Register. Nicht dazu zählen aufgrund der fehlenden Ausstattung mit bereichsspezifischen Personenkennzeichen die Register und Datenanwendungen auf der Landesebene. Die Landesverwaltungen, die um ein Vielfaches mehr Verfahren führen, haben die bPK nicht oder nur für vereinzelte Verfahren eingeführt. Dadurch mangelt es an der durchgehend praktischen Umsetzung und Wirkung des Systems, trotz einer Einführung vor über 15 Jahren.

Estland

Das X-Road-System in Estland ermöglicht den Datenaustausch zwischen autorisierten Datenbanken, wobei streng geregelt ist, wer was speichern und worauf zugreifen darf. Ähnlich dem 4-Corner-Modell erfolgt eine Ex-Ante-Prüfung. Daten werden zum überwiegenden Teil auf nationaler Ebene gespeichert. Gemeinsamer Grundsatz ist, dass die Daten dort gespeichert werden, wo sie entstehen.[79] Bürgerinnen und Bürger können auf all ihre Inhaltsdaten zugreifen und diese auch für von ihnen verantwortete Prozesse nutzen. Zusätzlich können Bürgerinnen und Bürger ex-post nachvollziehen, wer die Daten wann verarbeitet hat. Zur Harmonisierung der Daten wird wie im RegMoG-E eine Identifikationsnummer in den Registern geführt.

Dänemark

In Dänemark werden von Behörden die Basisdaten, zum Beispiel Informationen über Personen, Unternehmen oder Orte, registriert und im gesamten öffentlichen Sektor wiederverwendet.[80] Die Basisdaten müssen zuverlässig und von hoher Qualität sein. Um Behörden, Unternehmen und Bürgerinnen und Bürgern einen leichten Zugang zu den Daten zu ermöglichen, sind sie über den ”Data Distributor” teilweise frei zugänglich.[81]

[78] https://epicenter.works/content/groesster-datenskandal-der-republik-ueber-eine-million-wohnadressen-oeffentlich (10.12.2020).
[79] https://thedigitalarchitects.de/x-road-estland/ (10.12.2020).
[80] The Danish Government/Local Government Denmark, Good basic data for everyone – a driver for growth and efficiency, 2012.
[81] The Government/Local Government Denmark/Danish Regions: A stronger and more secure digital Denmark, Digital Strategy 2016-2020, 2016.

Kombination von Schutzmechanismen der internationalen Registerlandschaften

In den aktuellen Gutachten und Stellungnahmen zum RegMoG-E wird eine Kombination von Schutzmechanismen der beschriebenen internationalen Modelle vorgeschlagen. Beispielswiese eine Mischung der bereichsspezifischen Personenkennzeichen aus dem österreichischen Modell mit dem 4-Corner-Modell und/oder mit einer dezentralen Speicherung. In der Theorie sind diese Modelle kombinierbar, wenn auch nicht immer zweckmäßig. In der Praxis ist aufgrund der steigenden Komplexität des Gesamtsystems eine erfolgreiche Umsetzung von kombinierten Schutzmechanismen so gut wie auszuschließen. Der Vorschlag, das österreichische bereichsspezifische Kennzahlsystem mit dem Modell einer dezentralen verteilen Datenhaltung und -verarbeitung des deutschen RegMoG-E zu kombinieren, übersteigt in seiner technischen und seiner organisatorischen Komplexität angesichts der föderal verteilten Organisationen des Bundes, der Länder und der Kommunen eine Schwelle der Machbarkeit. Eine dadurch verzögerte Umsetzung hätte zum Ergebnis, dass die aktuellen datenschutzrechtlichen Spannungsfelder der Datenminimierung, Transparenz und Datenintegrität über das nächste Jahrzehnt nicht auflösbar wären. In Folge wären auch die Ziele des Gesetzes nicht erreichbar, weil eine datenschutzkonforme Registerlandschaft die Grundlage sowohl für digitale Verwaltungsverfahren in Deutschland als auch für die europarechtlich zwingend vorgesehenen grenzüberschreitende Verwaltungsverfahren bildet.

Eine andere diskutierte Variante sind zentrale Register nach dem österreichischen Modell. Die dezentrale Registerstruktur in Deutschland - im Gegensatz zur zentralen Struktur in Österreich - müsste unter großem Aufwand zurückgebaut und die gesamte etablierte Datenkommunikation reorganisiert werden.[82] Technisch wäre dieses Vorgehen mit großem finanziellem und zeitlichem Aufwand möglich. Die Speicherung der fachlichen Daten auf Bundesebene löst jedoch das Privacy-by-Design-Prinzip der Separierung der Daten durch dezentrale lokale Speicherung auf und verliert so eine zentrale Stärke des RegMoG-E auf. Durch die zentrale Speicherung und Verarbeitung wäre zwar das bPK-Modell anwendbar, aber die Motivation für Angriffe und das Datenmissbrauchspotential generell würden dadurch steigen. Aufgrund der wesentlich höheren Komplexität des Architekturmodells, der hohen Anzahl der Beteiligten und der fehlenden Erfahrungen mit den bPK-Komponenten ist eine erfolgreiche und vor allem zeitnahe Umsetzung bis Ende 2023 so gut wie auszuschließen.

In Abwägung dieser beiden Modelle ist die vorgeschlagene Architektur des RegMoG-E mit dezentraler verteilter Speicherung und Verarbeitung, der Vorabprüfung (ex-ante) der bereichsübergreifenden Kommunikation durch das 4-Corner-Modell und einer nachträglichen Prüfung der Protokolldaten durch die Bürgerinnen und Bürger (ex-post) nach Einschätzung des AutorInnen-Teams eine größere Stärkung der informationellen Selbstbestimmung und somit ist auch aus der Perspektive des Datenschutzes dem RegMoG-E im Vergleich zu anderen Varianten der Vorzug zu geben.

[82] Deutscher Bundestag - Wissenschaftliche Dienste, Einführung einer registerübergreifenden einheitlichen Identifikationsnummer nach dem Entwurf eines Registermodernisierungsgesetzes, 11.

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.

Überblick

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

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)667 F

Deutscher Bundestag
Ausschuss für Inneres und Heimat Platz der Republik 1
11011 Berlin

Per eMail an: innenausschuss@bundestag.de

Stellungnahme
zum
Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze
(Registrierungsmodernisierungsgesetz - RegMoG-E)

vorgelegt
von
Rechtsassessorin Kirsten Bock

Zusammenfassung

- Die Modernisierung der Deutschen Verwaltung ist legitim und überfällig.
- Im Zentrum der Registermodernisierung muss die Gewährleistung von moderner, demokratiefester und grundrechteverträglicher Verwaltung stehen.
- Die Einführung eines allgemeinen Personenkennzeichens ist für die Registermodernisierung nicht erforderlich, weil weniger eingriffsintensive Alternativen bestehen.
- Selbst wenn die Erforderlichkeit eines allgemeinen Personenkennzeichens bejaht würde, sind die vorgesehenen Schutzmaßnahmen nicht ausreichend.
- Allein die Verkettungsmöglichkeiten der Lebensbereiche der Bürgerïnnen führt in ihrer Gesamtheit zu einer Eingriffsintensität, die verfassungsrechtlich nicht zu rechtfertigen ist.
- Auch die Ausgestaltung des Datencockpits als reine Transparenzmaßnahme ist nicht geeignet, die durch die Verkettungsmöglichkeiten intensivierte Machtasymmetrie zwischen Bürgerïnnen und staatlicher Verwaltung auszugleichen.
- Mit dem Identifikationsnummerngesetz wird das informationelle Trennungsprinzip unterlaufen.
- Die bereichsspezifischen Alternativen lassen sich ohne wesentlichen Mehraufwand und passgenauer in die bestehenden Strukturen der deutschen Verwaltung einbinden.
- Der Verzicht auf ein allgemeines Personenkennzeichen macht moderne Verwaltung nicht unmöglich, sondern macht Verwaltung demokratiefest und hat einen sicherheitspolitischen Mehrwert.

Einleitung

Die Bundesregierung plant mit dem Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registrierungsmodernisierungsgesetz - RegMoG-E)[1] die - seit langem erforderliche - Modernisierung der deutschen Verwaltung. Nicht nur Gründe der Effizienzverbesserung, sondern auch der IT-Sicherheit sprechen dafür, die bislang heterogenen Lösungen auf allen Ebenen der Verwaltung zu modernisieren. Grundlage dafür wären Vorgaben für Standards und Schnittstellen für die Fachverfahren, die Interoperabilität ermöglichen. Stattdessen konzentriert sich der Entwurf in seinem wesentlichen Regelungsgegenstand auf die Einführung einer registerübergreifenden Identifikationsnummer als einem eindeutigen und veränderungsfesten Ordnungsmerkmal. Deren Einführung wird durch das Identifikationsnummerngesetz (IDNrG-E) geregelt, das in § 1 drei Ziele ausweist:

1. „Daten einer natürlichen Person in einem Verwaltungsverfahren eindeutig zuzuordnen [Identifizierungsfunktion],
2. die Datenqualität der zu einer natürlichen Person gespeicherten Daten zu verbessern sowie
3. die erneute Beibringung von bei öffentlichen Stellen bereits vorhandenen Daten durch die betroffene Person zu verringern.“ (sog. Once-Only-Prinzip)

Zur Erreichung dieser Ziele soll die Identifikationsnummer nach § 139b der Abgabenordnung (SteuerID) genutzt und in den für die Umsetzung des Onlinezugangsgesetzes relevanten Fachregistern gespeichert werden. Weitere registerführenden Stellen sollen innerhalb von fünf Jahren diese Identifikationsnummer als zusätzliches Ordnungsmerkmal zu den Personendaten in ihren jeweiligen Registern aufnehmen.
Die Bürgerïnnen sollen über ein sog. Datencockpit eine einfache, transparente und zeitnahe Übersicht über die zwischen Behörden vorgenommenen Datenübermittlungen erhalten.
Eine detailliertere Ausgestaltung des Datencockpits einschließlich der Möglichkeiten der Bürgerïnnen, den Zugriffen der Verwaltung zuzustimmen oder sie zu initiieren, ist in dem Gesetzentwurf noch nicht vorgesehen, wäre aber wünschenswert.

1 RegMoG-E: Gesetz zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung, Bundestagsdrucksache 19-24226, Deutscher Bundestag, Berlin 2020. Abrufbar unter: https://dip21.bundestag.de/dip21/btd/19/242/1924226.pdf.

A. Weichen für das E-Government verfassungskonform und zukunftsgerichtet gestalten

Deutschland hinkt im E-Government im internationalen Vergleich hinterher. Zudem machen neue Lebensgewohnheiten der Bürgerïnnen eine Veränderung der Verwaltung erforderlich, wenn der Mensch im Zentrum der staatlichen Verwaltung stehen soll. Mit den Möglichkeiten die Digitalisierung bietet, können Verwaltungsleistungen bedarfsgerechter und effizienter erbracht werden. Es ist aber ein Missverständnis, wenn angenommen wird, eine Modernisierung erfordere eine Digitalisierung um jeden Preis. Allein die Zunahme von Cyberangriffen auf staatliche Verwaltung macht deutlich, dass bei der Modernisierung der Verwaltung die Digitalisierung nur einen Teilaspekt darstellt. Vor diesem Hintergrund ist eine Registermodernisierung legitim und angezeigt, aber mit Bedacht zu planen und umzusetzen.

Auffällig ist bei dem vorgelegten Entwurf zur Registermodernisierung, dass er nur vordergründig eine vorausschauende, an den Bedürfnissen der Bürgerïnnen ausgerichtete Digitalisierung gestaltet, sich jedoch primär um eine Vernetzung der Systeme und möglichst effiziente Verwaltung bemüht, bei der der einzelne Mensch nur noch als Nummer verwaltet wird. Die Bildung von umfassenden Persönlichkeitsprofilen wird damit zum digitalen Kinderspiel. Diesen Ansatz sollte die Bundesregierung überdenken, um einerseits tatsächlich die Bürgerïnnen und ihre Rechte im Blick zu haben und andererseits nicht in das offene Messer der Verfassungswidrigkeit zu laufen.

Für einen verfassungskonformen Weg hat das Bundesverfassungsgericht in wegweisenden Entscheidungen schon wesentliche Ankerpunkte und Maßgaben vorbereitet, an der sich die Bundesregierung mit ihrem Entwurf orientieren sollte. Insbesondere das Volkszählungsurteil (Urteil v. 15. Dezember 1983 – 1 BvR 209/83 - BVerfGE 65, 1) spielt für die Gestaltung des E-Governments eine zentrale Rolle.

Der Schutz der Menschenwürde und das Grundrecht auf informationelle Selbstbestimmung als Garant für die Möglichkeit des Individuums, sich innerhalb der Gemeinschaft frei entwickeln zu können, stehen im Zentrum einer Verwaltung, deren Sinn und Zweck es ist, den Bürgerïnnen als freiheitsgarantierende Exekutive des Staates gegenüberzutreten. Die Möglichkeit einer vollständigen Katalogisierung und Registrierung der Persönlichkeit von Bürgerïnnen muss darum ausgeschlossen sein, damit ein beobachtungsfreie Kernbereich gewahrt bleibt (s. BVerfGE 27, 1, 6; 65, 1, 169 f.).

Das E-Government als Ausdruck moderner Verwaltung lebt davon, dass die staatlichen, datenhaltenden Stellen „miteinander-reden-können“. Im Mittelpunkt der Diskussion stehen dabei die Register, die Fachverfahren und die Interoperabilität ermöglichenden Schnittstellen. Sie sollen es der Verwaltung erlauben, ihre Aufgaben als Exekutive im Rahmen der Eingriffs-, Lenkungs- und Leistungsverwaltung zu erfüllen. Dabei sollte die Einbindung eines Registers in ein vernetztes System sachorientiert und vergleichbar dem Need-to-know-Prinzip[2] organisiert sein. Es ist insofern vor der Einbindung jeweils zu fragen, ob ein Register im Hinblick auf die mit ihm verbundene Aufgabenerfüllung z.B. auf die Richtigkeit der Personenangaben angewiesen ist und eine Abfrage der SteuerID dafür erforderlich ist.

B. Funktionen und Wirkweisen der Identifikationsnummer

Eine Identifikationsnummer soll die eindeutige Zuordnung eines Datensatzes zu einer Person ermöglichen (Identifizierungs- und Ordnungsfunktion) und steht damit gleichsam für die Person (Repräsentationsfunktion).[3] Wird dieselbe Identifikationsnummer für eine Person in allen Registern verwendet, erfüllt es die Funktionen registerübergreifend. Ist ein Wechsel der Identifikationsnummer nicht vorgesehen, wird sie lebenslang vergeben. Einer einfachen Identifikationsnummer wird durch diese Attribute Persistenz verliehen. Damit ändert sich die Wirkweise beträchtlich.

Die Aufgabenteilung ist ein wesentliches Merkmal der verfassungsrechtlich festgeschriebenen funktionalen Differenzierung, die sich besonders in der Gewaltenteilung manifestiert. Letzterer kommt eine, historisch bedingte, besondere Schutzfunktion zu. Mit Hilfe einer registerübergreifenden Identifikationsnummer wird dieser Schutzmechanismus durchbrochen, indem an sich getrennte Bereiche in Verbindung gebracht werden. Für das Individuum bedeutet diese Möglichkeit ein Verlust an Sicherheit im sowieso schon ausgeprägten Machtgefälle zum Staat. Konkret kann sich dadurch die Gefahr der Erstellung eines umfassenden Persönlichkeitsprofils realisieren, aber auch die Fortsetzung kleiner Fehler, wie beispielsweise eine fehlerhafte Transkription, zu deren Behebung das System

2 Auf der Zugriffsebene z.B. im Rahmen eines Discretionary-Access-Control-Modells. Dieses Sicherheitskonzept aus der Informationstechnik findet im Datenschutzrecht sein Pendant im Grundsatz der Erforderlichkeit aus Art. 5 Abs. 1 lit. c DSGVO.

3 Vgl. Martini/Wagner/Wenzel, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, Speyer, 2017, S. 1.

eigentlich dienen soll, kann sich schnell in alle Bereiche übertragen und damit die Betroffenen in die Situation versetzen, dem Staat gegenüber Fehler nachweisen zu müssen. Dies ist schon unter herkömmlichen Bedingungen schwierig. In einer digitalen Verwaltungsumgebung wird dies für die betroffenen Personen zur Herkulesaufgabe.

C. Datenschutzrechtliche Betrachtung

Die Datenschutz-Grundverordnung (DSGVO) schützt gem. Art. 1 Abs. 2 natürliche Personen, indem sie ihre Rechte und Freiheiten und insbesondere ihr Recht auf Datenschutz aus Art. 8 Charta der Grundrechte der Europäischen Union (GRCh) gewährleistet. Dafür stellt sie die Verarbeitung personenbezogener Daten gem. Art. 1 Abs. 1 DSGVO unter Bedingungen. Die DSGVO stellt damit nicht das Datum, sondern die Gewährleistung der Rechte und Freiheiten der natürlichen Person bei der Verarbeitung in den Mittelpunkt der Betrachtung.

I. Zulässigkeit eines Kennzeichens gem. Art 87 DSGVO

Die im IDNrG-E vorgesehene Identifikationsnummer für natürliche Personen ist eine Kennnummer im Sinne des Art. 4 Nr. 1 DSGVO, für die in Art. 87 eine Öffnungsklausel für spezifische Regelungen durch die Mitgliedstaaten vorgesehen ist. Insbesondere stellt Art. 87 DSGVO klar, dass sowohl nationale Kennziffern als auch Kennzeichen von allgemeiner Bedeutung „nur unter Wahrung geeigneter Garantien für die Rechte und Freiheiten der betroffenen Person gemäß dieser Verordnung verwendet werden“ dürfen. Insofern kann dahinstehen, ob es sich bei der Identifikationsnummer um eine nationale Kennziffer oder ein Kennzeichen von allgemeiner Bedeutung handelt. Bedeutender ist, dass weder die Schaffung einer solchen Kennzahl noch deren Nutzung ohne weiteres zulässig sind. Von einer generellen Vereinbarkeit eines Kennzeichens mit dem europäischen Datenschutzrecht kann insofern nicht ausgegangen werden.

Es kommt damit für die datenschutzrechtliche Beurteilung auf die konkrete Ausgestaltung der Kennziffer oder des Kennzeichens und der zur Nutzung verbundenen Verfahren, etwa zum Austausch oder der Korrektur von Basisdaten einer Behörde mit und beim Zentralamt für Steuern oder der Registermodernisierungsbehörde, an. Die vom Austausch mit Hilfe der SteuerID verbundenen Daten fallen selbst nicht unter Art. 87 bzw. deren mitgliedstaatlicher Ausgestaltung, sondern bedürfen für ihre Verarbeitung eigener Rechtsgrundlagen nach Art.

6 Abs. 1 S. 1 lit. b DSGVO. Neben den Vorgaben der Charta der Grundrechte der Europäischen Union ist auch das deutsche Verfassungsrecht zu beachten.

Steuer ID als registerübergreifendes Kennzeichen

Mit der Entscheidung für die SteuerID wird aus einem bereichsspezifischen ein allgemeines, eindeutiges Personenkennzeichen. Bereits die verfassungsrechtliche Zulässigkeit der SteuerID war problematisch und wurde nur für den eingeschränkten Zweck, der Verwendung im Rahmen der Steuerverwaltung, als gegeben erachtet (vgl. § 139a Abs. 1 S. 1 AO).[4] Das Bundesverfassungsgericht hat in den Entscheidungen zum Mikrozensus (BVerfGE 27,1) und zur Volkszählung (BVerfGE 65, 1) immer wieder auf die Unvereinbarkeit einer umfassenden Registrierung und Katalogisierung der Persönlichkeit hingewiesen. So wurde z.B. im Volkszählungsurteil die Gefahr der Erstellung von Persönlichkeitsprofilen durch die Nutzung von Daten aus verschiedenen Registern als verfassungswidrig qualifiziert und als „entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren“(Rn. 110) gesehen.

Die Verwendung eines allgemeinen, übergreifenden Kennzeichens macht alle, bei der Verwaltung vorhandenen Informationen über eine Person auffindbar und verknüpfbar. Ob dabei tatsächlich über jede Person ein Verwaltungsprofil erstellt wird, das weitreichende Auskünfte über die Lebensumstände einer Person gibt, ist dabei nicht maßgeblich. Denn das Bundesverfassungsgericht erachtet bereits ein Verfahren, durch das die „Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal möglich wäre,“ als verfassungswidrig (BVerfGE 65, 1 Rn. 171). Wird, und dafür mehren sich die Indizien, das Kennzeichen auch im Wirtschaftsleben aufgegriffen, die Erstellung von umfassenden Persönlichkeitsprofilen nicht nur möglich, sondern Realität werden. Die Schnittstellen sind schon jetzt über die Krankenkassen, Arbeitgeber und die Geldinstitute vorhanden.

4 Vgl. Kleinert, et al., Stellungnahme zum Referentenentwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz) der Humanistischen Union, in: vorgänge Nr. 230 (2/2020), S. 125-134, abrufbar unter http://www.humanistische-union.de/nc/aktuelles/aktuelles_detail/back/aktuelles/article/stellungnahme-zum-referentenentwurf-eines-gesetzes-zur-einfuehrung-einer-identifikationsnummer-in-di/

II. Eingriff in Rechte und Freiheiten

Jede Verarbeitung personenbezogener Daten und damit auch die Einführung und Nutzung einer registerübergreifenden, einheitlichen Identifikationsnummer stellen Eingriffe in das Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und des Rechts auf Datenschutz nach Art. 8 GRCh dar.

In dem vom IDNrG-E geregelten Verfahren, sind mindestens die folgenden grundlegenden Verarbeitungen personenbezogener Daten zu unterscheiden:

Beim Bundeszentralamt für Steuern (BZSt)

- Generierung und Zuordnung der SteuerID als allgemeines Identifikationskennzeichen und
- Speicherung der SteuerID, des Datums des letzten Verwaltungskontakts sowie der Validitätswerte und Bereithaltung zum Abruf durch die Registermodernisierungsbehörde.

Bei der Registermodernisierungsbehörde beim Bundeverwaltungsamt (BVA)

- Übermittlung der Identifikationsnummer sowie der übrigen Daten nach § 4 Abs. 2 und 3 IDNrG-E an registerführende Stellen in Bund und Ländern zur Erfüllung der Aufgaben nach § 2 sowie öffentliche Stellen nach § 6 Absatz 2 IDNrG-E und
- Abruf der unter einer SteuerID gespeicherten Daten beim BZSt.

Bei den Registerbehörden und registerführende Stellen zur Erfüllung der Aufgaben nach § 2 IDNrG-E sowie öffentliche Stellen zum Zwecke der Erbringung von Verwaltungsleistungen nach dem Onlinezugangsgesetz (OZG)

- Übermittlung der unter der SteuerID erhobenen Daten an die Registerbehörde,
- Empfang und Speicherung der von der Registermodernisierungsbehörde übermittelten Daten und
- Abgleich mit und ggfs. Korrektur des vorhandenen Datenbestands.

Diese Schritte erfolgen auch bei einem automatisierten Abgleich der Einzelregister mit den beim BZSt gespeicherten Daten. Dazu erfolgt eine automatisierte Übernahme der beim BZSt in der SteuerID-Datenbank gespeicherten Daten in das Einzelregister.

Mittels der SteuerID kann zudem eine Verbindung zwischen allen, die SteuerID als Ordnungsmerkmal nutzenden Registern erfolgen. Der Nutzung der SteuerID als einheitliches Identifikationsmerkmal kommt damit eine hohe Eingriffsintensität zu.

III. Fehlende Rechtfertigung der Eingriffe

1. Geeignetheit und legitimer Zweck

Dem Registermodernisierungsgesetz liegen die folgenden, legitimen Zwecke zugrunde:

- Effizienzsteigerung der Verwaltung durch Verknüpfung von Registern,
- Bereinigung der Register von Fehlern und Dubletten, Richtigkeit der Daten,
- Umsetzung des Once-Only-Prinzips und
- Vorbereitung eines registerbasierten Zensus.

Ob die Nutzung der SteuerID geeignet ist, insbesondere die Fehlerbehebung zu unterstützen, bleibt angesichts der dezentralen Registerstruktur und zahlreicher möglicher Änderungen allein im Personenstand einer Person zweifelhaft und wird auch aus der Gesetzesbegründung kaum deutlich.

2. Erforderlichkeit

Zwei wesentliche Gründe sprechen gegen die Erforderlichkeit der Einführung der SteuerID als registerübergreifendes Ordnungsmerkmal.
In vielen Fällen ist eine eindeutige Identifizierung der Person gar nicht zwingend erforderlich. Vielmehr geht es in diesen Fällen primär um die Zuordnung von Sachverhalten zu einer Person. In diesen Fällen, wäre allenfalls eine schrittweise Identifizierung erforderlich. Das dem Entwurf zugrundeliegende System sieht eine solche nicht vor.

Hinzu kommt, dass die Daten des § 4 Abs. 2 IDNrG-E fast ausnahmslos im Personaldokument hinterlegt sind und somit zum Anstoßen eines Verwaltungsverfahrens von den Betroffenen selbst beigesteuert werden könnten. Es wird insofern aus dem Entwurf nicht deutlich, welchen konkreten Mehrwert bzw. welche Erleichterungen die SteuerID gegenüber anderen Verfahren für Bürgerïnnen bringen wird. Verwechslungen von Bürgerïnnen dürften sich auch hinsichtlich bestehender Merkmale wie bisher nur in einem sehr geringen Maße ergeben. Dazu finden sich auch in der Gesetzesbegründung keine Hinweise.

Zudem steht mit der bereichsspezifischen Kennzahl ein weniger eingriffsintensives Verfahren zur Verfügung, das in anderen Staaten, z.B. Österreich, erfolgreich eingesetzt wird. Der Aufwand für die Einführung einer bereichsspezifischen Kennzahl dürfte mit dem Aufwand bei der Integration der SteuerID vergleichbar sein. Aufgrund der föderalen und dezentralen Registerstrukturlandschaft in Deutschland wäre die Einführung einer bereichsspezifischen Kennzahl auch kein Fremdkörper, sondern trüge dem Grundsatz der Aufgabentrennung sogar stärker Rechnung.

Eine „größere rechtliche, technische und organisatorische Komplexität“5 und ein außerordentlicher Kosten- und Zeitaufwand soll der Grund gewesen sein, warum ein bereichsspezifisches Modell für das RegModG-E nicht in Frage gekommen sei. Weitere Gründe werden nicht angeführt. Natürlich wäre eine Eins-zu-eins-Übertragung des Österreichischen Modells schon wegen der unterschiedlichen Verwaltungsstruktur nicht in Frage gekommen, aber das Grundprinzip der Berechnung einer bereichsspezifischen Kennziffer wäre ohne weiteres auch auf andere Verwaltungsstrukturen anwendbar.

Grundriss des Alternativverfahrens mit bereichspezifischen Kennzeichen

Auch das RegModG-E sieht mit der Registermodernisierungsbehörde einen Intermediär vor, der die Kommunikation zwischen den Behörden managt. Eine solche Funktion besteht auch beim bereichsspezifischen Verfahren. Nur sorgt der Intermediär in diesen Verfahren dafür, dass für die Kommunikationspartner die jeweiligen bereichsspezifischen Kennzeichen unbekannt bleiben.

Zur Errechnung der bereichsspezifischen Personenkennziffer wird zunächst aus der Stammzahl und dem Verfahrensbereich eine Zeichenkette gebildet. In einem weiteren Schritt berechnet dann ein Hash-Algorithmus aus dieser Zeichenkette eine sichere kryptografische Einwegableitung, das dann über eine Base64-Standard-Kodierung lesbar gemacht wird. Die Berechnung der verschlüsselten bereichsspezifischen Personenkennziffer erfolgt mithilfe eines asymmetrischen kryptographischen Verfahrens so, dass nicht auf die betroffene Person geschlossen werden kann. Maßgeblich ist, dass Behörden in diesem Verfahren die Stammzahl natürlicher Personen nicht als Ordnungskriterium speichern dürfen.

5 Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze, BT-Drucksache 19/24226, S. 35.

Benötigt eine Behörde zur Identifikation einer Person eine bereichsspezifische Personenkennziffer von einer anderen Behörde, wird es durch die Stammzahlenregisterbehörde berechnet. Diese Aufgabe kann durch die Registermodernisierungsbehörde, aber beispielsweise auch Landesbehörden wahrgenommen werden. Die Stammzahlregisterbehörde übermittelt die bereichsspezifische Personenkennziffer ausschließlich verschlüsselt an die anfragende Behörde. Die verschlüsselte bereichsspezifische Personenkennziffer kann so nur durch jene Behörden entschlüsselt und verarbeitet werden, die für den Fachbereich zuständig ist, für den die bereichsspezifische Personenkennziffer errechnet worden ist.

Der Verwaltungsaufbau in Deutschland steht der Einführung bereichsspezifischer Kennzeichen als weniger eingriffsintensive Alternative nicht entgegen, sondern begünstigt diese sogar durch deren dezentrale Organisation der datenhaltenden Stellen. Die Komplexität einer bereichsspezifischen Kennziffer entsteht anders als bei einer einheitlichen Personenkennzahl nicht bei den datenhaltenden Stellen, sondern in der Einrichtung einer Interoperabilität herstellenden Vermittlungsstelle (Intermediär). Ein erheblicher Mehraufwand ist dadurch nicht zu erwarten, aber die Bundesregierung erbringt auch für das Gegenteil keinen Nachweis[6]. Der Unterschied der Systeme liegt allein in den Zugriffs- und Nutzungsmöglichkeiten bei der Registermodernisierungsbehörde. Bereichsspezifische Kennzeichen verhindern einen unkontrollierten Austausch zwischen Behörden, weil eine Zuordnung der Datensätze zu einer Person nicht ohne weiteres möglich ist. Der damit gewährleistete grundrechtliche Schutz kann dadurch technisch gewährleistet werden, während bei einer einheitlichen Personenkennziffer dieser Schutz nur normativ organisatorisch gewährleistet werden kann. Allein die Nutzbarmachung der SteuerID entgegen den Zusicherungen bei deren Einführung, diese ausschließlich für steuerliche Zwecke nutzen zu wollen, zeigt, dass normativ organisatorische Regelungen vergleichsweise leichter geändert werden können als technische Schutzmaßnahmen, die eine Verkettung der Informationen erschweren. Allein vor dem Hintergrund der historischen Verantwortung gilt es, die Trennung der datenhaltenden Stellen auch informationell umzusetzen. Die Entwicklungen hin zu autokratischen Systemen der jüngeren Zeit zeigen, dass der freiheitlich-demokratische Rechtsstaat keine dauerhafte Selbstverständlichkeit ist, sondern

6 Antwort des Parlamentarischen Staatssekretärs Dr. Günter Krings vom 2. Oktober 2020, BT- Drucksache 19/23238.

aktiv gelebt werden muss. Die Bundesregierung hat eine Verpflichtung auch gegenüber zukünftigen Generationen, die Verwaltungsstruktur auch im E-Government demokratiefest und krisensicher zu gestalten.

Auch steht der Grundsatz der Datenminimierung aus Art. Abs. 1 lit. c DSGVO der Grunddatenhaltung in den Fachregistern und bereichsspezifischen Lösungen nicht entgegen. Das Prinzip der Datenminimierung stellt eine Ausprägung des Erforderlichkeitsgrundsatzes im Datenschutzrecht dar, der die obere und untere Grenze der rechtfertigungsfähigen Verarbeitung personenbezogener Daten bestimmt. Nach Maßgabe des Art. 5 Abs. 1 lit. b und c DSGVO ist die zur Erfüllung eines festgelegten, eindeutigen und legitimen Zwecks erforderliche Verarbeitung so auszugestalten, dass die personenbezogenen Daten auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden. Ein Erfordernis für eine zentrale Datenhaltung oder einfache Zugriffsmöglichkeiten für den behördlichen Gebrauch ergeben sich daraus nicht. So bedeutet das Prinzip der Datenminimierung nicht, erforderliche Daten schnell wieder zu löschen, sondern sie (nur) solange zu speichern, wie sie für den zu erfüllenden Zweck erforderlich sind. Dies ist insbesondere bei der Protokollierung von Verarbeitungsvorgängen zu beachten. Auf Protokollierung kann nicht mit dem Hinweis auf Datenminimierung verzichtet werden.

Es hätte erwartet werden können, dass der Gesetzgeber in der Begründung des Entwurfs des Registermodernisierungsgesetzes von seiner Einschätzungsprärogative im Hinblick auf die Erforderlichkeit einer bereichsübergreifenden Identifikationsnummer zu den mit der Registermodernisierung verfolgten Zwecken tatsächlich Gebrauch macht und die Alternative einer bereichsspezifischen Kennziffer hinreichend sachlich erörtert. Denn je stärker der Gesetzgeber in grundrechtlich geschützte Freiheiten eingreift, desto größer ist seine Verpflichtung, den gesetzgeberischen Gestaltungsspielraum angemessen zu prüfen. Angesichts der hohen Bedeutung einer einheitlichen Identifizierungsnummer und den Ausführungen des Bundesverfassungsgerichts zur Einführung einer Personenkennziffer hätte der Gesetzgeber daher nachvollziehbar darlegen müssen, warum eine bereichsspezifische Kennziffer nicht in Betracht kommt.

4. Angemessenheit

Angesichts der erheblichen Risiken, die mit der Einführung eines lebenslangen, einheitlichen Identifikationskennzeichen einhergehen und denen nur unzureichend mit effektiven Schutzmaßnahmen begegnet wird, erscheint die Einführung auch als nicht angemessen.

Die hohe Eingriffsintensität ergibt sich aus der absoluten Verkettbarkeit der bei den einzelnen datenhaltenden Stellen verfügbaren Datensätzen zu einer Person. Über den Portalverbund und die Registermodernisierungsbehörde als zentralem Intermediär zu einem zentralen Grunddatenbestand, wird ein virtueller Zugriff auf alle, eine Person betreffenden Daten ermöglicht. Zwar besteht im Hinblick auf Informationen, die über den Grunddatenbestand hinausgehen, eine dezentrale Datenhaltung, es kann aber mit Hilfe des Intermediärs oder aber auch direkt, z.B. im Rahmen von automatisierten Abfragen, ohne hohen Aufwand, ein umfassendes Persönlichkeitsprofil zu einer Person erstellt werden.

5. Kein Aufweichung der Zweckbindung

Schon jetzt ist abzusehen, dass Behörden die SteuerID nicht nur zu Authentifizierungszwecken nutzten werden, sondern umfangreiche Zugriffsrechte sowohl auf den zentralen Datenbestand, als auch auf Informationen, die aufgabentypisch bei anderen Behörden vorhanden sind, fordern werden. Dieses Einfallstor ist erheblich, da z.T. vertreten wird, dass der für das Datenschutzrecht schlechthin konstituierende Zweckbindungsgrundsatz „nicht ohne weiteres auf eine Personenkennziffer übertragen werden könne“7. Zweck eines registerübergreifenden Identifikationsmerkmals ist die Verkettung von Informationen. Doch ist ihr hohes Verkettungspotential kein Grund, den Zweckbindungsgrundsatz aufzugeben. Denn Sinn und Zweck der DSGVO und ihrem Schutzgedanken ist es gerade, Verkettung unter Bedingungen zu stellen. Der Umstand, dass eine Verkettung stattfindet, macht damit die Zweckbindung nicht obsolet. Im Gegenteil, je höher das Verkettungspotential, desto höher sind auch die Anforderungen, die das Datenschutzrecht an die Verarbeitungsbedingungen stellt (vgl. z.B. die Anforderungen an die Verarbeitung biometrischer Merkmale, die ein ähnliches Verkettungspotential aufweisen können). Bei der Bemessung der Anforderungen, ist stets das gesamte Verarbeitungsverfahren zu betrachten und nicht nur das Kennzeichen als solches. Liegt ein

7 BeckOK DatenschutzR/von Lewinski, 34. Ed. 1.11.2020, DS-GVO Art. 87 Rn. 45.

hohes Verkettungspotential vor, sind die Schutzmaßnahmen entsprechend des Art. 25 DSGVO möglichst nicht nur organisatorisch, sondern technisch in das Verfahren einzubinden. Verfassungsrechtliche Maßgaben beschreibt das Bundesverfassungsgericht (Urteil v. 24. April 2013 – BvR 1215/07 BVerfGE 133,277 ff – Antiterrordateigesetz I) beispielsweise für die Auswertung der gemeinsamen Verbunddatei im Antiterrordateigesetz (ATDG). Eine erweiterte, projektbezogene Datennutzung (Data-Mining) auch zur operativen Aufgabenwahrnehmung, d.h. der Generierung neuer Erkenntnisse aus den Querverbindungen der gespeicherten Datensätze oder nur der Austausch von Daten, unterliegen hinsichtlich des Grundrechts auf informationelle Selbstbestimmung gesteigerten verfassungsrechtlichen Anforderungen. „Aus den Grundrechten folgt ein informationelles Trennungsprinzip, das diesen Austausch nur ausnahmsweise zulässt“ (BVerfG Urt. v. 24.04.2013, Az. 1 BvR 1215/07).

Hierfür wären Kontrollmechanismen und besondere Regelungen zu schaffen. Dies gilt umso mehr, als dass die Möglichkeit, zukünftig komplexe Algorithmen wie etwa künstliche Intelligenz (KI), die per se eine hohe Eingriffsintensität haben, einsetzen zu können, Berücksichtigung finden muss, um den Schutz auch im Hinblick auf sich erweiternde technische Möglichkeiten zu gewährleisten.

6. Schutzmaßnahmen unzureichend

Die nach Art. 87 S. 2 DSGVO gesetzlich zu normierenden Schutzmaßnahmen müssen denen der DSGVO entsprechen. Dabei darf das Schutzniveau weder unterschritten noch im Hinblick auf den freien Verkehr personenbezogener Daten innerhalb der Union überschritten werden. Maßgeblich sind dafür für den für die Verarbeitung Verantwortlichen nach Maßgabe des Art. 24 DSGVO die Grundsätze aus Art. 5, die Umsetzung der Rechte der Betroffenen im Hinblick auf Auskunft (Intervenierbarkeit und Transparenz), Löschung und Widerspruch (Nichtverkettung), Vertraulichkeit, Korrektur (Integrität und Intervenierbarkeit) und Verfügbarkeit.

8. Strafbewährung als Schutzmaßnahmen

Die Option der Strafbewehrung als Schutzmaßnahme bietet nur einen - vergleichsweise - geringen Schutz, um die Erstellung von umfassenden Persönlichkeitsprofilen und andere,

unerwünschte Verarbeitungen zu verhindern. Einerseits ist hierbei die schwere Verfolgbarkeit bei Straftaten, die aus dem Ausland verübt werden, zu berücksichtigen und andererseits das Bedürfnis, eine komplexe Registerlandschaft demokratiefest zu gestalten, d.h. technische Systeme so zu bauen, dass allein legislative Änderungen die Gewährleistung des grundrechtlichen Wesensgehaltsschutzes nicht gefährden können.

9. Datencockpit

Zur Gewährleistung von Transparenz gem. Art. 5 Abs. 1 lit. a DSGVO über weitestgehend ohne Zustimmung des Betroffenen erfolgenden Datenzugriffe durch Behörden soll durch Ergänzung eines § 10 Onlinezugangsgesetzes (Art. 2 RegModG-E) ein sog. Datencockpit geschaffen werden. Der Betroffene soll in die Lage versetzt werden, die auf der SteuerID basierenden Datenabrufe, nachverfolgen zu können. Über die Anzeigefunktion sind derzeit keine weiteren Funktionalitäten vorgesehen, die das Recht auf informationelle Selbstbestimmung durch Eingreifbarkeit (sog. Intervenierbarkeit) in Verwaltungsabläufe umsetzen. Aufgrund der hohen Zugangsvoraussetzungen ist zu befürchten, dass dieses Angebot nur von einer kleinen Zahl von Betroffenen genutzt wird und damit nur eine bedingte Milderung der informationellen Machtasymmetrie zwischen Bürgerïnnen und Verwaltung schafft.

Protokolldaten nicht vorzeitig löschen

Zwar sind personenbezogene Daten zu löschen, sobald sie für die festgelegten Zwecke nicht mehr benötigt werden (vgl. BVerfGE 150, 1, 106 Rn. 221 f). Doch ist bei Protokolldaten zu beachten, dass sie bspw. auch für den gerichtlichen Rechtsschutz der Betroffenen erforderlich werden können. Die Löschfristen müssen sich demnach an den Fristen der Rechtsschutzmöglichkeiten, bei lebenslangen Auswirkungen von Änderungen aber auch daran, orientieren. Diese müssen nachvollziehbar für die Dauer des Lebens der betroffenen Person bleiben. Eine Löschfrist von generell zwei Jahren, wie dies für die Protokolldaten gilt, erscheint als generelle, undifferenzierte Löschfrist zu kurz.

IV. Kontrolle kaum möglich

Auch die Implementierung von technischen Maßnahmen zur Gewährleistung von Vertraulichkeit und Integrität wird nicht in der Lage sein, Angriffe aus den datenhaltenden

Stellen selbst zu verhindern. Solche Eingriffe in die Grundrechte aus Art. 7 und 8 GRCh müssen nicht einmal in der Erstellung umfassender Persönlichkeitsprofile bestehen. Es reicht dafür bereits die stetige Erfassung der Daten aus § 4 Abs. 3 Nr. 2 IDNrG-E, um Schlüsse auf die Lebensumstände (etwa den Bezug von Sozialleistungen) zu ziehen.

Bereits bei Einführung der lebenslangen SteuerID warnte der damalige Datenschutzbeauftragte des Landes Schleswig-Holstein davor, dass es den für die Aufsicht zuständigen Datenschutzbehörden „praktisch nicht möglich sein“ werde, die Nutzung zu kontrollieren und einen Missbrauch zu verhindern.[8] An der Situation der Aufsichtsbehörden im Hinblick auf hinreichende Ausstattung und Kompetenz hat sich in den meisten Behörden kaum etwas geändert. Um eine Kontrolle der Verarbeitung einer lebenslangen, einheitlichen Identifikationsnummer zu garantieren, müssten die Aufsichtsbehörden erheblich besser ausgestattet werden, um auch anlassunabhängige Kontrollen durchführen zu können. Allein die Möglichkeiten des Datencockpits reichen für einen wirksamen Schutz nicht aus, da sie lediglich die Protokolldaten von Behördenabrufen anzeigen und zudem die Kontrollfunktion allein den überforderten Bürgerïnnen überlässt.

V. Datenschutzfolgenabschätzung (DSFA)

Für die Einführung eines Identifikationsmerkmals als einheitliches Kennzeichen ist aufgrund der Eingriffsintensität und der mit einem lebenslangen einheitlichen Kennzeichen verbundenen erheblichen Risiken stets eine Datenschutzfolgenabschätzung nach Art. 35 DSGVO durchzuführen. Idealerweise erfolgt die Datenschutzfolgenabschätzung als sog. Gesetztes-DFSA nach Art. 35 Abs. 10 DSGVO. Vor dem Hintergrund, dass wesentliche technische Details erst per Verordnung geregelt werden sollen, wäre spätestens eine Fertigstellung mit Verordnungserlass anzuraten. Mit Hilfe der Datenschutzfolgenabschätzung können die Risiken und Schutzmaßnahmen, die mit der geplanten Registermodernisierung einhergehen, angemessen beurteilt werden können.

8 Krempl; Stefan, Warnung vor Überwachungspotenzial der neuen Bürger-Identifikationsnummer, heise.de, 29.6.2007, abrufbar unter: https://www.heise.de/newsticker/meldung/Warnung-vor-ueberwachungspotenzial-der-neuen-Buerger-Identifikationsnummer-145643.html

D. Fazit

Der Verzicht auf die SteuerID als allgemeines Personenkennzeichen bei der Registermodernisierung ist aus verfassungs- und datenschutzrechtlichen Gründen geboten. Dadurch entginge die Bundesregierung der hohen Gefahr weiterer Verzögerungen, Kosten und Vertrauensverlusten, die bei einer hoch wahrscheinlichen Verfassungswidrigkeit der Verwendung der SteuerID als allgemeines Personenkennzeichen entstünden. Der Verwaltungsaufbau der Bundesrepublik Deutschland steht einer bereichspezifischen Lösung zur verbesserten Interoperabilität zwecks Gewährleistung moderner Verwaltung nicht entgegen, ja ist sogar dafür prädestiniert. Die Bundesregierung könnte aus der Not eine Tugend machen und richtungsweisend zeigen, dass moderne, zukunftsgerichtete Verwaltung Rechte und Freiheiten der Bürgerïnnen in einer digitalisierten Welt gewährleisten und schützen kann. Dieses staatliche Interesse besteht nicht nur im Hinblick auf die Gewährleistung der informationellen Selbstbestimmung der einzelnen Bürgerïn als Teil ihres Grundrechts auf Datenschutz, sondern setzt auch die informationelle Gewaltenteilung um, die einen wesentlichen Beitrag zur Demokratiefestigkeit des Staates leistet. Mit einer föderierten Struktur wird nicht nur der leichte Aufbau eines Profilbildungs- und Überwachungssystems erschwert, sondern sie ermöglicht zudem auch einen verbesserten Schutz und eine Verringerung der Angriffsfläche gegenüber feindlichen Angriffen aus Drittstaaten.

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Prof. Ulrich Kelber
Bundesbeauftragter
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Vorsitzende des Ausschusses
für Inneres und Heimat
des Deutschen Bundestages
Frau Andrea Lindholz, MdB
Platz der Republik 1
11011 Berlin

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)612

HAUSANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
FON (0228) 997799-5000
FAX (0228) 997799-5550
E-MAIL referat11@bfdi.bund.de
INTERNET www.bfdi.bund.de
DATUM Bonn, 21.10.2020
GESCHÄFTSZ. 11-100/010#0157

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

Nachrichtlich:
Sekretariat des Innenausschusses

Nur per E-Mail:
innenausschuss@bundestag.de

BETREFF **Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz)**

HIER Stellungnahme des BfDI an den InnenausschussStellungnahme des BfDI an den Innenausschuss

Sehr geehrte Frau Vorsitzende,

zum Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz) übersende ich Ihnen im Anhang meine Stellungnahme. Ich würde mich freuen, wenn meine Vorschläge und Anregungen im weiteren Gesetzgebungsverfahren Berücksichtigung fänden. Für Ihre Fragen stehe ich Ihnen gerne zur Verfügung. Ich bitte Sie darum, meine Stellungnahme auch an die übrigen Ausschussmitglieder zu verteilen.

Mit freundlichen Grüßen

[redacted]

Prof. Ulrich Kelber

97403/2020

ZUSTELL- UND LIEFERANSCHRIFT Graurheindorfer Straße 153, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61 und 65, Innenministerium
Bus 550 und SB60, Innenministerium

Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Bonn, den 21.10.2020

Stellungnahme

des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zum Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz - RegMoG)

Graurheindorfer Str. 153
53117 Bonn

FON +49 (0)228-997799-0
FAX +49 (0)228-997799-5550

E-MAIL poststelle@bfdi.bund.de
INTERNET www.bfdi.bund.de

Kernforderungen:

1. **Kein Ausbau der Steuer-ID zu einem einheitlichen bereichsübergreifenden Personenkennzeichen**

   Die Steuer-ID allein ist kein tragfähiges Fundament für den geplanten Einsatz als Personenkennzeichen. Ein Personenkennzeichen, das in dieser Art sowohl bereichsübergreifend als auch einheitlich gestaltet ist, ist mit der Verfassung nicht vereinbar. Es schafft ein system-inhärentes, übermäßiges Risiko der Katalogisierung der Persönlichkeit und bietet, auch mit den im Gesetzentwurf geplanten Maßnahmen zur technischen Absicherung, keinen ausreichend Schutz vor Missbrauch sowohl nach innen als auch nach außen. Mit bereichsspezifischen Kennzeichen gibt es eine moderne Alternative.

2. **Eine starke Zweckbindung zur Identitätsfeststellung**

   Der aktuelle Entwurf bindet den neuen Identifikator nur unzureichend an den Zweck der Identitätsfeststellung zur Erbringung von digitalen Verwaltungsdienstleistungen. Nach den allgemeinen Regelungen der Datenschutz-Grundverordnung (DSGVO) können so schnell weitere zweckändernde Verwendungen gefunden werden und der Identifikator verbreitet sich unkontrolliert.

3. **Moderne Transportsicherheit in allen Bereichen**

   Der aktuelle Entwurf nutzt das sog. „4-Corner-Modell" mit kryptographischen doppelten Umschlägen und dem Versand über eine dritte Stelle, die auch die Berechtigung prüft. Dieses Modell soll allerdings ausschließlich bei bereichsübergreifenden Übermittlungen angewendet werden. Dies entspricht weder dem Koalitionsbeschluss noch dem Stand der Technik. Das Modell soll für jede Übermittlung mit dem Identifikator eingesetzt werden.

4. **Keine Aussparung des Steuerbereichs**

   Mit Einführung des geplanten Identifikators wird auch der Steuerbereich ein allgemeines Personenkennzeichen verwenden. Die Steuer-ID im bisherigen Sinn hört auf zu bestehen. Darum muss auch der Steuerbereich an den neuen Sicherheits- und Transparenzmaßnahmen teilnehmen.

5. **Die Fortentwicklung der Transparenz mitdenken**

   Das im Entwurf aufgenommene Datencockpit ist ein wichtiger und guter erster Schritt bei der Schaffung von Transparenz. Die Weiterentwicklung dieses Instruments sollte aber von Anfang mitgedacht werden, um am Ende den Bürger mit dem Staat gleichzustellen. Auch die zukünftige Möglichkeit des Registerabrufs durch den Bürger sollte sich im Entwurf wiederfinden.

Begründung:

Zu 1. Verfassungsrechtliche Probleme bei der Schaffung eines einheitlichen, bereichsübergreifenden Personenkennzeichens durch Ausbau der Steuer-ID

Betreffend Art. 1 RegMoG, § 1 Identifikationsnummerngesetz (IDNrG)

a) Einleitung

Gemäß § 1 IDNrG-E soll die Steuer-ID als einheitliches Personenkennzeichen für große Teile der Verwaltung eingesetzt und in vielen bereits bestehenden Registern als zusätzlicher Datenpunkt eingespeichert werden. Zudem sollen die beim Bundeszentralamt für Steuern (BZSt) gespeicherten Identifikationsdaten zum größten Teil die bisher in die übrigen Register vorhandenen Daten ersetzen. Beide Datensätze wurden bisher ausschließlich für Steuerzwecke verwendet – auch dann, wenn die Steuer-ID ausnahmsweise bereits in anderen Registern aufgenommen wurde.

b) Verfassungsrechtliche Grundproblematik

Die Verwendung eines derartigen einheitlichen Personenkennzeichens ist nach Auffassung des BfDI verfassungswidrig, da in diesem System keine hinreichenden strukturellen und systematischen Hemmnisse vorgesehen sind, die einen Missbrauch des Systems sowohl von innen heraus, als auch nach außen effektiv verhindern. Dieses System gefährdet so bereits durch seine Implementierung den besonders geschützten geistigen Innenraum des Bürgers.

Schon im Mikrozensus-Urteil des BVerfG (Az. 1 BvL 19/63) wurde ein unangreifbarer geistiger Innenraum als notwendiger Baustein für die Entfaltung der Persönlichkeit, Meinungs- sowie Versammlungsfreiheit gesehen, ohne den eine freiheitliche Demokratie nicht vorstellbar sei. Dieser Innenraum muss frei staatlicher Beobachtung sein. Dabei erkannte das BVerfG ebenfalls, dass eine Katalogisierung der Persönlichkeit diesen Innenraum zwangsweise angreift, da eine solche ihrer Gesamtheit nach zwangsweise auch Teile eben jenes Innenraums umfasst und er dann nicht mehr frei von staatlicher Beobachtung ist. Zudem reicht bereits der subjektive Eindruck der Bürgers, dass die Persönlichkeit in dieser Art und Weise durch den Staat und ohne sein Wissen erfasst werden kann(!), um ebenfalls den geistigen Innenraum in seiner Unverletzlichkeit zu berühren. Es käme zur berüchtigten „Schere im Kopf", einer vorauseilenden Anpassung des Verhaltens und langfristig auch des Denkens des Bürgers hierdurch.

Auf Grundlage dieser Gedanken formte das BVerfG im Volkszählungsurteil (Az. 1 BvR 209/83 u. a.) das Recht auf informationelle Selbstbestimmung. Eine Gefahr für den Innenraum ist nicht gegeben, so lange der Bürger selbstbestimmt über seine Daten walten und Einfluss nehmen kann. Vor diesem Hintergrund erwähnte das BVerfG die Einführung eines

Personenkennzeichens ausdrücklich als Negativbeispiel für eine verfassungswidrige Rechtslage. Aus Sicht des BfDI spielten hierfür wohl mehrere Gründe eine Rolle.

Die Einführung eines zentralen Personenkennzeichens ist unweigerlich mit schwerwiegenden Eingriffen in das Recht auf informationelle Selbstbestimmung verbunden. Mit seiner Hilfe und angesichts der intendierten breiten Verwendung steht dem Staat sodann ein einfaches Mittel zur Verfügung, um übergreifend Daten einer natürlichen Person zusammenzuführen, die aus völlig unterschiedlichen Bereichen stammen. Insbesondere sind dem Personenkennzeichen zugeordnete Daten ohne weiteres verkettbar. Sowohl innerhalb als auch außerhalb eines Systems mit einem solchen Kennzeichen, können alle Daten, die eine Person betreffen, anhand dieses Merkmals verknüpft werden.

Allein die Schaffung eines derart absolut zuverlässigen, rasanten Systems zum Datenaustausch ist ein Umstand, der wenigstens den Eindruck einer totalen Erfassbarkeit der Persönlichkeit hinterlässt. Eben jener Eindruck reicht wie dargelegt bereits aus, um den besonders geschützten geistigen Innenraum zu gefährden. Dieser Eindruck wird verstärkt durch die besondere Niedrigschwelligkeit des Systems. Eine Zusammenführung einer Vielzahl an personenbezogenen Daten ist prinzipiell ohne Schwierigkeiten möglich. Dadurch erhöht sich das Risiko eines Miss- oder Fehlgebrauchs. Wie die Erfahrungen zeigen, werden nicht selten Begehrlichkeiten an anderer Stelle geweckt, die den Eingriff in das Recht auf informationelle Selbstbestimmung noch verstärken könnten. Ein System, das ein Personenkennzeichen verwendet, egal welcher Natur, ist also inhärent gefährlich.

Dies gilt dabei nicht nur für den öffentlichen Bereich. So zeigen Beispiele aus anderen Ländern, dass eine zentrale ID-Nr. mit hoher Wahrscheinlichkeit im Laufe der Zeit von der gesamten Privatwirtschaft als zentrales Ordnungsmerkmal genutzt wird. Darüber hinaus birgt die Verwendung eines einheitlichen Personenkennzeichens an sich besondere Risiken der Kompromittierung der Register durch Angriffe oder Fehlgebrauch. Fehlgeleitet ist auch der Versuch, die Steuer-ID als erwiesen verfassungskonforme Grundlage darzustellen. Dabei legte der Bundesfinanzhof (BFH) großen Wert auf die sehr strenge Zweckbindung für den Steuerbereich. Ein Umstand, der sich gerade durch das IDNrG-E ändern wird. Mit Einführung dieser neuen Funktion ist jedwedes Präjudiz aus der BFH-Entscheidung verloren.

c) Moderne Ausgleichsmöglichkeiten - Bereichsspezifische Kennzeichen

Um diese inhärente Gefahr für den geistigen Innenraum durch das System selbst auf ein verfassungsrechtlich erträgliches Maß zu verringern, bedarf es bereits dort des Einsatzes von modernen Mitteln zum Erhalt der Selbstbestimmtheit. Da vor allem die perfekte Verkettbarkeit, die Geschwindigkeit sowie die besondere Niedrigschwelligkeit die größten abstrakten Gefahrenquellen darstellen, bedarf es bereits im System angelegter Hemmnisse, die dort abfedernd wirken. Hier kommt es auf die technische und architektonische Ausgestaltung an.

Derartige Ausgleichsmaßnahmen müssen gleichermaßen nach innen wie auch nach außen wirken, da die inhärente Gefahr ebenfalls in beide Richtungen ausstrahlt. Aus der Innensicht beziehen sich die Maßnahmen dabei sowohl auf die bereichsübergreifende Identifikation als auch auf den bereichsübergreifenden Datenaustausch zwischen Behörden. In der Außensicht geht es dagegen insbesondere darum, eine Kompromittierung durch Angreifer, die unbefugt Zugriff erlangen wollen, zu verhindern.

Eine Architektur, die auf bereichsspezifischen Kennzeichen (bPKZ) beruht, kann diese Risiken auf ein verfassungsrechtlich erträgliches Maß reduzieren. Bei einem System mit bPKZ wird jedem Verwaltungsbereich für jeden Bürger ein eigenes Kennzeichen zugeordnet. In Österreich wird beispielsweise ein solches System eingesetzt. Eine Alternative, die im Entwurf mit einem nur kurzen Hinweis auf ein Beratergutachten schnell beiseitegeschoben wird, obwohl die Berechnungsgrundlagen im Gutachten selbst große Lücken haben. Das System basiert letztlich auf einem kryptographischen Vorgang, bei dem eine dritte Stelle die jeweiligen bPKZ ausgibt und zudem Schlüssel für die Datenübermittlung bereitstellt. Die bPKZ werden dabei nicht-rückrechenbar aus einer virtuellen Stammzahl generiert, die wiederum nicht-rückrechenbar aus der in Österreich eingesetzten Meldenummer ad hoc, also nur für den Moment, jeweils berechnet wird.

Dieses System erhöht durch die nachprüfbare Beteiligung einer dritten Stelle, die bereits beim Abruf eines entsprechenden bPKZ und des Schlüssels stattfindet, die Hemmschwelle für einen Missbrauch oder einen leichtfertigen Fehlgebrauch durch die staatlichen Institutionen oder einzelne Beschäftigte. Insbesondere sinkt das Risiko einer Umgehung dieses Systems erheblich, da für eine bereichsübergreifende Identifizierung kein eineindeutiger Identifikator mehr zur Verfügung steht. Die Implementierung kann dabei ohne Verluste für das eigentliche Ziel der Registermodernisierung automatisiert erfolgen. Im Entwurf wird dagegen ausschließlich auf das sog. 4-Corner-Modell als besondere architektonische Gestaltung zurückgegriffen. Dabei werden kryptographische doppelte Umschläge genutzt und der Versand erfolgt über eine dritte Stelle (Verzeichnisdienst), die auch die Berechtigung prüft. Diese Sicherungen wirken im Gegensatz zur bPKZ nur nach innen in das System selbst. Das Modell bietet aber letztlich keine Sicherung gegen die vorgenannten Szenarien einer missbräuchlichen Zusammenführung der Daten einer Person durch Angreifer von außen oder eine Umgehung des Systems. Naturgemäß kann es auch eine Verbreitung des Personenkennzeichens in die Öffentlichkeit nicht verhindern. Das 4-Corner-Modell ist insofern also nur eine Ergänzung für die Architektur.

Der BfDI hält daher den flächendeckenden Einsatz von bereichsspezifischen Kennzeichen für verfassungsrechtlich geboten. Eine Lösung für die sich ursprünglich auch der Normenkontrollrat in seinen Gutachten zur Registermodernisierung aussprach. Der Bürger würde so auch zusätzliches Vertrauen in das System gewinnen, da er um die zusätzlichen Schwellen der Sicherung wüsste.

Zu 2. Zweckbindung zur Identitätsfeststellung

Betreffend Art. 1 RegMoG, § 5 Identifikationsnummerngesetz (IDNrG)

In § 5 IDNrG-E wird lediglich der Zweck der Identifikationsnummer nach diesem Gesetz beschrieben. Eine gesetzliche Begrenzung auf den Einsatz der Identifikationsnummer als Werkzeug zur sicheren Identitätsfeststellung bei der Erbringung von digitalen Verwaltungsleistungen ist nicht vorgesehen, obwohl es gemäß § 3 IDNrG-E alleine darum gehen soll. Es muss klar geregelt sein, dass andere Datenverarbeitungen unter Verwendung der Steuer-ID unzulässig sind. Anderenfalls würden nämlich die allgemeinen Bestimmungen in Art. 5 Abs. 1 lit. b), Art. 6 Abs. 4 DSGVO und § 23 Bundesdatenschutzgesetz (BDSG) gelten, die in einem nicht unerheblichen Umfang Zweckänderungen zulassen. Die Unkontrollierbarkeit des Systems aus Bürgersicht würde hierdurch noch verstärkt werden. Die Verarbeitung durch nicht-öffentliche Stellen außer zu gesetzlich zugelassenen Zwecken muss vollkommen unterbleiben, um ein Durchsickern in die zivile Gesellschaft zu verhindern.

Für eine derart strenge Zweckbindung gibt es beispielsweise eine Präzedenz-Regelung im Bundesfernstraßenmautgesetz. Dort dürfen bestimmte Daten (u. a. Name des Fahrers, Kennzeichen) ausschließlich zur Überwachung der Einhaltung des Gesetzes verarbeitet werden. Jedwede zweckändernde Weiterverarbeitung ist ausgeschlossen.

Der BfDI hält hier eine Regelung für eine sehr strenge Zweckbindung geboten, die vergleichbar ist mit der Regelung aus dem Bundesfernstraßenmautgesetz. Dies erscheint auch nur schlüssig, da die Risiken, die von der Identifikationsnummer ausgehen, weit über die Risiken durch die genannten Daten aus der Mautverwaltung hinausgehen.

Zu 3. Moderne Transportsicherheit in allen Bereichen

Betreffend Art. 1 RegMoG, § 7 Identifikationsnummerngesetz (IDNrG)

In § 7 Abs. 2 IDNrG-E ist unter anderem geregelt, dass Datenübermittlungen unter Nutzung der Identifikationsnummer nach diesem Gesetz zwischen öffentlichen Stellen verschiedener Bereiche verschlüsselt über Vermittlungsstellen stattzufinden haben. Dabei handelt es sich letztlich um die Festlegung auf das 4-Corner-Modell, das ich bereits zuvor unter Zu 1. kurz dargestellt habe.

Die Festlegung im Entwurf, das Modell nur bei bereichsübergreifenden Übermittlungen einzusetzen, entspricht dabei nicht dem datenschutzrechtlich gebotenen Stand der Technik. Die Verwendung des 4-Corner-Modells ist bereits für viele Übermittlungen schon heute eine etablierte technische Lösung, um gewisse Risiken innerhalb eines Datenaustausch-

systems zu mindern. Ein weiterer Ausbau auf diese Anwendungen wäre ohne weiteres möglich.

Außerdem entspricht diese Regelung nicht dem Ergebnis des Koalitionsausschusses vom 03.06.2020, der in Rn. 40 ausdrücklich erwähnt, dass registerübergreifender Datenaustausch nicht direkt zwischen den Behörden stattfinden solle, sondern als zusätzliche Sicherung immer über eine dritte Stelle zu erfolgen hat. Diese Absicht bestätigte die Bundesregierung auch bei der Beantwortung einer kleiner Anfrage der Fraktion Bündnis 90/Die Grünen (BT Drs. 19/19784).

Insofern ist es schon unverständlich, warum der Entwurf hier zulasten der Bürger vom Ergebnis des Koalitionsausschusses abweicht. Der BfDI hält daher den flächendeckenden Einsatz des 4-Corner-Modells bei allen Übermittlungen, also auch bei Übermittlugen zwischen öffentlichen Stellen innerhalb des jeweiligen Bereiches, die sich der Identifikationsnummer bedienen, für datenschutzrechtlich geboten.

Zu 4. Keine Aussparung des Steuerbereichs
Betreffend Art. 1 RegMoG, §§ 7, 9 Identifikationsnummerngesetz (IDNrG)

In den §§ 7, 9 IDNrG-E sind einerseits die Anforderungen an die Transportsicherheit (s. o. zu 3.) geregelt und andererseits die Pflicht zur Protokollierung des Einsatzes der Identifikationsnummer, damit diese im Transparenzwerkzeug/Datencockpit (siehe Art. 2 RegMoG) für den Bürger zugänglich gemacht werden können. Dabei verwendet der Entwurf bewusst die Formulierung „Identifikationsnummer nach diesem Gesetz", um eine Trennung zur bisherigen Steuer-ID vorzunehmen. Diese soll diesen neuen Regelungen nicht unterfallen.

Dies erscheint nicht schlüssig. Mit Einführung des IDNrG würde die Steuer-ID als ausschließlich steuerliches Identifikationsmittel aufhören zu existieren. Stattdessen wäre sie ab dann zugleich ein allgemeines Personenkennzeichen, das zwar weiterhin der Steuerverwaltung, aber eben auch der allgemeinen Verwaltung im Zusammenhang mit OZG-Leistungen dienen würde. Beide sind im Grunde identisch miteinander und verschmelzen so dann.

Ein allgemeines Personenkennzeichen und das dazugehörige Datenaustauschsystem haben aber eben jene, bereits unter 1. erwähnten, höheren Risiken. Dieses höhere Risiko und damit der verstärkte Eingriff müssen durch ausreichende strukturelle Maßnahmen eingedämmt werden. Ob der Einsatz (weiterhin) in der Steuerverwaltung oder in neuen Verwaltungsbereichen erfolgt, spielt dann keine Rolle mehr, da sich das System als Ganzes verändert hat. Auch die bisherige Rechtsprechung des BFH zur Steuer-ID hilft in diesem Fall nicht mehr weiter. Insofern muss die Steuer-ID auch in ihrer alten Verwendung alle neuen Sicherungs- und Transparenzmaßnahmen der Identifikationsnummer erfahren.

Der BfDI hält daher die Gleichstellung des Steuerbereichs, der dann ebenfalls das allgemeine Personenkennzeichen einsetzt, mit den übrigen Verwaltungsbereichen bei Sicherheit und Transparenz für verfassungsrechtlich geboten.

Zu 5. Fortentwicklung der Transparenz
Betreffend Art. 2 RegMoG, § 10 Onlinezugangsgesetz (OZG)

In § 10 OZG-E wird das Datencockpit geregelt. Es soll allen Bürgern Auskünfte über die Datenübermittlungen zwischen öffentlichen Stellen ermöglichen, die sich der Identifikationsnummer bedient haben. Das Datencockpit greift hierfür auf die Protokolldaten gemäß § 9 IDNrG-E zurück. Anhand ihres Nutzerkontos im Portalverbund können Bürgerinnen und Bürger dann auf das Datencockpit digital zugreifen.

Der BfDI begrüßt die Schaffung des Datencockpits. Es ist ein wichtiger Baustein bei der Schaffung der notwendigen Transparenz, um den Bürger technologisch auf die gleiche Stufe zu stellen wie die Verwaltung. Der nun in § 10 OZG-E normierte Funktionsumfang ist dabei die eigentliche Kernaufgabe des Datencockpits. Es dient in dieser Konzeption als Teil einer verfassungsgemäßen architektonischen Gestaltung dieses mit der ID-Nr. vereinfachten Datenaustauschsystems. Es ist insofern notwendiger Teil der Bauweise und kein subjektives Recht im engeren Sinne. Es dient in dieser Funktion daher auch nicht der Umsetzung des datenschutzrechtlichen Auskunftsrechts, welches unabhängig vom Datencockpit gegenüber allen beteiligten Behörden unverändert besteht.

Allerdings bietet die technische Einrichtung des Datencockpits natürlich ein gut geeignetes Fundament für die Fortentwicklung datenschutzrechtlicher Transparenz. Das eingerichtete System kann bei datenschutzgerechter Ausgestaltung ebenso für den Abruf bereits vorhandener Daten des Bürgers genutzt werden. Dieser Bestandsdatenabruf wäre dann eine echte Erfüllung des Art. 15 DSGVO. Das Datencockpit wäre so ein zukunftsgerichteter Baustein für eine moderne Verwaltung, die dem Bürger offen gegenüber steht.

Aus der Begründung zu Absatz 4 des § 10 OZG-E geht jedoch hervor, dass der erweiterte Anwendungsbereich des Datencockpits vor allem aus Gründen der technischen Komplexität wohl auch mittelfristig nicht verfolgt werden soll. Der BfDI wirbt hier dafür, dass die Möglichkeiten und Chancen des Datencockpits konsequent genutzt werden sollen, um eine vollständige Informationsgleichstellung von Bürger und Staat zu erreichen.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)657

Bundessteuerberaterkammer, KdöR, Postfach 02 88 55, 10131 Berlin

Frau
Andrea Lindholz, MdB
Vorsitzende des Ausschusses für Inneres und Heimat
Deutscher Bundestag
Platz der Republik 1
11011 Berlin

E-Mail: innenausschuss@bundestag.de

Bundessteuerberaterkammer
KÖRPERSCHAFT DES ÖFFENTLICHEN RECHTS

Abt. Steuerrecht und Rechnungslegung

Unser Zeichen: Gs/Gr
Tel.: +49 30 240087-68
Fax: +49 30 240087-77
E-Mail: steuerrecht@bstbk.de

23. November 2020

113. Sitzung des Ausschusses für Inneres und Heimat am 25. November 2020; Stellungnahme der BStBK zum Regierungsentwurf eines Gesetzes zur Einführung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz – RegMoG), Drs. 19/24226 vom 11. November 2020

Sehr geehrte Frau Lindholz,

auf der am 25. November 2020 anstehenden 113. Sitzung des Ausschusses für Inneres und Heimat wird als TOP 2 der o. g. Gesetzentwurf diskutiert. Aus Sicht des Berufsstandes der Steuerberater besteht wesentlicher Änderungsbedarf an dem Gesetzentwurf.

Bevor wir im Folgenden auf einzelne Punkte explizit eingehen, möchten wir einige grundsätzliche Anmerkungen vorausschicken.

I. Vorbemerkung

Die Identifikationsnummer ist als registerübergreifendes Ordnungskriterium nach § 139b AO grundsätzlich nur geeignet, sofern das Register lediglich natürliche Personen umfasst. Werden auch Gesellschaften in das Register eingetragen, bedarf es – etwa mit der geplanten Wirtschafts-IdNr – eines weiteren Kriteriums. Erforderlich wäre von vornherein ein Ansatz, der sowohl natürliche Personen als auch Gesellschaften in gleicher Weise erfasst.

Durch die Integration der Steuerberater als natürliche Person als auch die Erfassung der Steuerberatungsgesellschaften als juristische Personen im Berufsregister bietet sich die Perspektive, einen Weg für die Prüfung der Berufsträgereigenschaft im Verwaltungsverfahren vorzunehmen. Hintergrund ist, dass Gesellschaften im gleichen Umfang wie Steuerberater Mandanten vertreten können, diese aber bisher nicht im Berufsregister eingetragen sind, weil in elektronischer Hinsicht dazu bisher kein Bedarf bestand. Die BStBK arbeitet daher derzeit an einer Lösung zur Identifizierung und Authentifizierung von Steuerberatern und Steuerberatungsgesellschaften mit Bestätigung der Berufsträgereigenschaft.

Die Sonderstellung des steuerberatenden Berufsstandes fließt derzeit auch in die Weiterentwicklung des Nutzerkontos Bund (NKB) ein und hat sich insbesondere bei der Beantragung von Überbrückungshilfen gezeigt, deren Beantragung nur über einen Berufsträger ermöglicht

wird. Es muss zudem gesehen werden, dass der Steuer-Id über ihre ursprüngliche Zweckbestimmung hinaus eine viel weitreichendere Bedeutung zu Teil wird. Entsprechend hoch müssen vor dem Hintergrund des Grundrechts auf informationelle Selbstbestimmung die Anforderungen an den Datenschutz sein. Die faktische Möglichkeit zur Bildung umfassender Persönlichkeitsprofile ist überaus kritisch einzuordnen und muss ausgeschlossen werden.

Unsere Anmerkungen zu dem Regierungsentwurf im Einzelnen entnehmen Sie bitte den nachfolgenden Ausführungen.

II. Zum Regierungsentwurf

Das RegMoG soll die Möglichkeit schaffen, eine Person betreffende Daten aus einem Register – mittels der Identifikationsnummer nach § 139b AO als registerübergreifendes Ordnungsmerkmal – denen auf einem anderen Register zuzuordnen oder im Rahmen eines Verwaltungsverfahrens auf Registerdaten einer Person zugreifen zu können.

Die regionalen Steuerberaterkammern sind als Betreiber von zwei in Anlage 1 des Gesetzes genannten Registern direkt betroffen; dem Berufsregister der Steuerberater (§ 45 ff. Verordnung zur Durchführung der Vorschriften über Steuerberater, Steuerbevollmächtigte und Steuerberatungsgesellschaften (DVStB)) sowie dem Verzeichnis der Berufsausbildungsverhältnisse (§ 34 Berufsbildungsgesetz (BBiG)).

1. Berufsregister

Ausweislich der Gesetzesbegründung wird das Berufsregister der Steuerberater bei der BStBK geführt (vgl. S. 43). Das ist so nicht richtig. Die BStBK führt gem. § 86b StBerG das Gesamtverzeichnis aller Mitglieder der Steuerberaterkammern (Amtliches Steuerberaterverzeichnis). Das Verzeichnis dient der Information der Behörden und Gerichte, der Rechtsuchenden sowie anderer am Rechtsverkehr Beteiligter. Datenquelle für das Gesamtverzeichnis sind die Berufsregister, die von den örtlich zuständigen Steuerberaterkammern eigenständig geführt werden (§ 76 Abs. 5, § 86b Abs. 1 Satz 3 StBerG).

Der RegMoG-E macht nicht hinreichend deutlich, ob er sich auf das von der BStBK geführte Gesamtverzeichnis der Steuerberater oder auf die von den regionalen Steuerberaterkammern geführten Verzeichnisse der Berufsregister bezieht.

a. Amtliches Steuerberaterverzeichnis

Sofern sich die Verpflichtung zur Speicherung der Steuer-IdNr auf das Gesamtverzeichnis der Steuerberaterkammern (§ 86b StBerG) bezieht, muss gesehen werden, dass dessen Inhalt öffentlich zugänglich ist. Der Abruf der gespeicherten Daten ist jedermann unentgeltlich möglich. Die Veröffentlichung der Steuer-IdNrn der in dem Verzeichnis geführten Mitglieder ist jedoch datenschutzrechtlich problematisch und wird – sofern vorgesehen – von der BStBK abgelehnt.

b. Berufsregister

Verpflichtet das geplante Gesetz hingegen die regionalen Steuerberaterkammern als Betreiberinnen der Berufsregister der Steuerberater dazu, zu jedem Personeneintrag die Steuer-IdNr zu speichern, wird diese nicht vom Betreiber des Registers selbst erhoben, sondern über die Registermodernisierungsbehörde abgefragt. Datenabrufe bei der Registermodernisierungsbehörde erfolgen gem. § 6 Abs. 3 IDNrG-E in einem automatisierten Verfahren anhand eines Abgleichs von Name, Wohnort und Geburtsdatum der jeweiligen Person. Allerdings wird der Wohnort aktuell nicht im Berufsregister gespeichert. Erfasst wird vielmehr die berufliche Niederlassung, die regelmäßig nicht mit der Wohnadresse übereinstimmen wird.

Dabei ergeben sich rechtliche und praktische Folgeprobleme:

- **Rechtsgrundlage für die Erweiterung der Berufsregister**

Die Berufsregister müssen um Datenfelder für Wohnort und Steuer-IdNr erweitert werden. Hierzu bedarf es einer datenschutzrechtlichen Rechtsgrundlage. Paragraf 46 DVStB, der die in das Berufsregister einzutragenden Daten regelt, sieht eine Eintragung des Wohnortes und der Steuer-IdNr bisher nicht vor. Im Gegensatz etwa zu den Industrie-, Handels- und Handwerkskammern, für die der Entwurf in Art. 17 und 18 die normative Grundlage zur Speicherung der Steuer-Id schafft, ist dies für § 46 DVStB nicht vorgesehen. Diese Inkonsistenz sollte vor der Einbringung in den parlamentarischen Gesetzgebungsprozess behoben werden.

- **Übereinstimmung der Meldedaten**

Um einen zuverlässigen automatisierten Abgleich von Name, Geburtsdatum und Wohnort mit der Registermodernisierungsbehörde zu gewährleisten, müssen die zu erfassenden Personendaten exakt mit den Meldedaten der Person übereinstimmen. Dies ist in zuverlässiger Weise nur durch eine Identifizierung der Kammermitglieder mittels der eID im Personalausweis (oder anderer geeigneter elektronischer Identifizierungsmittel) möglich. Bislang besteht allerdings keine flächendeckende Pflicht der Ausweisinhaber, von der eID Gebrauch zu machen oder die für den Einsatz des nPA geeignete technische Infrastruktur vorzuhalten. Es besteht daher die Gefahr, dass die Nacherfassung der Wohnorte aller bestehenden Kammermitglieder die Steuerberaterkammern mit einem erheblichen manuellen Aufwand belasten wird.

- **Regelung für den Schwebezustand bis zur Vergabe einer Steuer-IdNr**

Soweit Personen im Berufsregister erfasst werden sollen, die weder deutsche Staatsbürger sind, noch zuvor ihren Wohnsitz in Deutschland hatten oder hier aus anderem Grund steuerpflichtig waren, verfügen diese zum Zeitpunkt der Erfassung im Berufsregister womöglich (noch) nicht über eine Steuer-IdNr. Die geplante Fassung des § 139a AO sieht vor, dass nicht nur die Steuerpflicht die Vergabe einer Steuer-IdNr auslöst, sondern auch die Führung eines Verwaltungsverfahrens bei einer öffentlichen Stelle. Sobald eine Steuerberaterkammer also für eine Person nach der Steuer-IdNr bei der Registermodernisierungsbehörde anfragt, für die eine solche noch nicht existiert, sollte das Bundeszentralamt für Steuern dies zum Anlass nehmen, eine Steuer-IdNr zu erzeugen.

Es ist jedoch nicht davon auszugehen, dass dies unmittelbar, binnen weniger Sekunden erfolgt. Der RegMoG-E enthält jedoch keine Regelungen, wie in der Zwischenzeit während des Schwebezustandes mit der Person zu verfahren ist. Paragraf 6 IDNrG-E regelt nur den Fall einer nicht eindeutig zu identifizierenden Person, nicht jedoch den Fall einer identifizierbaren Person, für die (noch) keine Steuer-IdNr existiert. Sollte ein Abschluss des Zulassungsverfahrens ohne die Steuer-IdNr nicht möglich sein, besteht die Gefahr, dass sich das Zulassungsverfahren betroffener Personen unangemessen verlängert und diese in ihrer Berufsausführungsfreiheit einschränkt.

- **Keine Steuer-IdNr für Steuerberatungsgesellschaften**

Die Berufsregister der Steuerberater enthalten nicht nur personenbezogene Einträge zu Steuerberatern als natürliche Personen. In den Berufsregistern erfasst werden auch Steuerberatungsgesellschaften (u. a. AG, GmbH, OHG, KG, Partnerschaftsgesellschaft). Es können daher nicht alle Einträge einer Steuer-IdNr zugeordnet werden.

Die Berufsregister enthalten Daten zu wirtschaftlich tätigen natürlichen Personen sowie Steuerberatungsgesellschaften und deren Vertretern. Die Register sind daher keine Personenregister im engeren Sinne, sondern entsprechen eher den der Wirtschaft zuzuordnenden Registern wie dem Handels- oder Genossenschaftsregister. Diese sind laut Entwurf von der Umsetzung des RegMoG bis zur Einführung der Wirtschafts-IdNr zunächst ausgenommen. Aus Sicht der BStBK muss dies ebenso für die Berufsregister gelten.

Es besteht (dennoch) die Befürchtung, dass die Umsetzung des RegMoG zu einer Gemengelage in den Berufsregistern der Steuerberater führt. Steuerberatungsgesellschaften wird zukünftig eine Wirtschafts-IdNr zugeteilt, selbstständige Steuerberater erhalten eine Steuer-IdNr und zukünftig zusätzlich eine Wirtschafts-Id, angestellte Steuerberater bekommen voraussichtlich nur eine Steuer-IdNr, Partnerschaftsgesellschaften mit beschränkter Berufshaftung erhalten zukünftig wohl eine Wirtschafts-IdNr, werden aber nicht im Register geführt. Zumindest bei selbstständigen Steuerberatern oder solchen, die neben einer Tätigkeit als angestellte Steuerberater selbstständig tätig sind, besteht die Gefahr von einander widersprechenden Daten aus den zwei Quellen der IDs. Aus Sicht der BStBK sollte dem Entstehen einer Gemengelage von vornherein entgegengewirkt werden, indem ein in sich schlüssiges und widerspruchsfreies Erfassungskonzept für natürliche Personen und Gesellschaften entwickelt wird.

2. Berufsausbildungsverzeichnis

Im Berufsausbildungsverzeichnis werden nicht nur die Auszubildenden nachgewiesen, sondern auch deren Ausbilder. Paragraf 2 IDNrG-E sieht grundsätzlich eine Speicherung der IdNrn zu allen zu einer natürlichen Person gespeicherten Daten vor. Demnach müsste die Steuer-IdNr jeweils auch für die Person des Ausbilders erhoben werden. Laut Art. 16 des RegMoG-E wird die Pflicht, zusätzlich die Steuer-IdNr zu speichern jedoch nur für den Auszubildenden vorgesehen. Hier ist aus Sicht der BStBK eine Klarstellung erforderlich.

Insofern ergibt sich eine gewisse Unsicherheit, ob es sich hierbei nur um eine nicht gewollte Inkonsistenz des Entwurfs oder um eine gewollte Unterscheidung handelt. Im ersten Fall wäre die Erfassung der privaten Wohnadresse des Ausbilders zum Abgleich der Daten erforderlich. Unseres Erachtens ist hier eine Klarstellung des Gesetzgebers erforderlich.

Mit freundlichen Grüßen

Claudia Kalina-Kerschbaum
Geschäftsführerin

i. A. Oliver Glückselig
Referent

Nationaler
Normenkontrollrat

eu2020.de

Dr. Johannes Ludewig
Vorsitzender des Nationalen Normenkontrollrates

Prof. Dr. Sabine Kuhlmann
Stellv. Vorsitzende des Nationalen Normenkontrollrates

Bundeskanzleramt, 11012 Berlin

Frau Andrea Lindholz, MdB
Vorsitzende des Ausschusses für Inneres und Heimat
Deutscher Bundestag
Platz der Republik 1
11011 Berlin

HAUSANSCHRIFT Bundeskanzleramt
Willy-Brandt-Straße 1, 10557 Berlin

TEL +49 (0)30 18 400-1300
FAX +49 (0)30 18 400-1848
E-MAIL nkr@bk.bund.de

Berlin, 11. Dezember 2020

Sehr geehrte Frau Vorsitzende,

aus Anlass der Anhörung zum Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz) möchten wir Ihnen, zusätzlich zur bereits dem Gesetzentwurf beigefügten Stellungnahme des NKR, weitere beratungsrelevante Informationen zukommen lassen, die sich aus der langjährigen Beschäftigung des NKR mit dieser Thematik ergeben und auf der inzwischen erworben Expertise beruhen.

Ich würde mich freuen, wenn Sie unsere ergänzende Stellungnahme auch den anderen Ausschussmitgliedern zur Verfügung stellen könnten.

[redacted]

[redacted]

Dr. Ludewig

Prof. Dr. Kuhlmann

Nationaler
Normenkontrollrat

Berlin, 11. Dezember 2020

Ergänzende Stellungnahme des Nationalen Normenkontrollrats zum Entwurf eines Gesetzes zur Einführung und Verwendung einer Identifikationsnummer in der öffentlichen Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz)

Einleitung

Zum überragenden Nutzen und zur Bedeutung der Registermodernisierung für eine leistungsfähige, digitale Verwaltung und für den Bürokratieabbau hat sich der NKR in der Vergangenheit wiederholt geäußert – so auch in seiner förmlichen Stellungnahme (NKR-Nr. 5253) zum vorliegenden Gesetzentwurf. Obgleich es zum Nutzen und zur strategischen Notwendigkeit der Registermodernisierung grundsätzlich keinen Disput gibt, fällt die datenschutzrechtliche Bewertung sehr unterschiedlich aus. Dies bezieht sich insbesondere auf die geplante Nutzung der Steuer-Identifikationsnummer als bereichsübergreifendes, ein-eindeutiges Identifikationsmerkmal für natürliche Personen. So gibt es neben der kritischen Einschätzung des Bundesbeauftragten für den Datenschutz noch verschiedene andere Stellungnahmen, die die Einführung eines solch bereichsübergreifenden Personenkennzeichens für verfassungswidrig halten und die Existenz leistungsfähigerer Alternativen behaupten.

Gesamtbewertung

Aufgrund der langjährigen Beschäftigung mit der Thematik[1] und der zwischenzeitlich erworbenen Expertise möchte der NKR im Folgenden darlegen, warum er den vorgelegten Gesetzentwurf als verfassungskonform bewertet und aus denselben Erwägungsgründen seine Umsetzung sogar als verfassungsrechtlich geboten ansieht. Zugleich soll erläutert werden, warum der NKR die vermeintliche Überlegenheit des österreichischen Modells nicht als gegeben ansieht, sondern das im Gesetzentwurf vorgesehene Konzept als valide, im Kontext der bestehenden deutschen Registerlandschaft und deren Absicherungsmechanismen, datenschutzrechtlich sogar als besser geeignete Lösung bewertet. Eine grafische Darstellung des vorliegenden Lösungskonzeptes findet sich im Anhang.

[1] McKinsey & Company (2017) „Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren“, Gutachten im Auftrag des NKR; abrufbar unter: https://www.normenkontrollrat.bund.de/nkr-de/service/presse/pressemitteilungen/nationaler-normenkontrollrat-veroeffentlicht-gutachten-759036

Begründung

1. Das Volkszählungsurteil des Bundesverfassungsgerichts wendet sich nicht gegen ein einheitliches Personenkennzeichen als solches

Das Urteil wendet sich vielmehr gegen eine zum Zeitpunkt der Urteilsverkündung gesehene mögliche Folge des Einsatzes eines solchen Personenkennzeichens: Die Erstellung von Persönlichkeitsprofilen der Bürgerinnen und Bürger. Insofern muss der Gesetzgeber alle Anstrengung darauf richten, eine Profilbildung zu verhindern. Der Zwang zum Verzicht auf ein einheitliches Personenkennzeichen ergibt sich daraus jedoch nicht. Der Gesetzgeber ist im Grunde frei in der Wahl seiner Mittel, so lange er adäquate strukturellen Hemmnisse vorsieht, die eine Profilbildung unterbinden:

> *„Mit Blick auf die veränderten technischen Möglichkeiten entspricht es einer zeitgemäßen und am geschützten Rechtsgut der informationellen Selbstbestimmung orientierten Deutung, die Aussagen des Volkszählungsurteils nicht als an das Instrument „PKZ" anknüpfendes pauschales Verbot zu begreifen. Vielmehr verstößt eine PKZ nur insoweit gegen die Verfassung, als von ihr die nicht hinnehmbare Gefahr ausgeht, dass der Staat sie zur umfassenden Verknüpfung vorhandener Datenbestände nutzt und so einer persönlichkeitsfeindlichen Katalogisierung des Einzelnen den Weg ebnet.*
>
> *Lassen sich die Gefahren für das informationelle Selbstbestimmungsrecht hingegen durch wirksame technische, organisatorische und rechtliche Maßnahmen effektiv bannen, so bewegt sich ihre Nutzung innerhalb der Zulässigkeitsgrenzen des Grundgesetzes. Insofern deckt sich die Wertung des deutschen Verfassungsrechts im Grundsatz weitgehend dem normativen Wertungsprogramm des Art. 87 DSGVO.*
>
> *Welche organisatorischen, technischen und rechtlichen Maßnahmen der Gesetzgeber in concreto vorsehen muss, sagt die Verfassung nicht. Insoweit verfügt der Gesetzgeber über einen Handlungsspielraum."*[2]

2. Der Gesetzgeber ist frei in der Wahl seiner Mittel, so lange er adäquate strukturellen Hemmnisse gegen eine Profilbildung vorsieht

Der vorliegende Gesetzentwurf trägt diesem Grundsatz Rechnung, auch wenn er auf die Einführung eines Systems bereichsspezifischer Personenkennzeichen verzichtet. Der Gesetzgeber macht insofern von seinem Bewertungs- und Handlungsspielraum Gebrauch, indem er folgende strukturellen Hemmnisse berücksichtigt:

a. Beibehaltung einer fachlich ausdifferenzierten sowie dezentral organsiert- und verantworteten Registerlandschaft

---

[2] Martini M., Wagner D., Wenzel M. (2017) Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, Speyer, S. 33; abrufbar unter: https://www.normenkontrollrat.bund.de/resource/blob/72494/476034/eebab686008cfec0a7919ca03e51abe3/2017-10-06-download-nkr-gutachten-2017-anlage-untersuchung-datenschutz-data.pdf

b. Ex ante Berechtigungsprüfung durch Intermediäre (4 Corner Modell), die den Abruf der Steuer-ID bei der Registermodernisierungsbehörde und deren Einsatz beim Datenaustausch zwischen abgrenzbaren Politikbereichen kontrollieren (zusätzlich zu bestehenden Berechtigungsprüfungen)
c. Ex post Kontrollierbarkeit durch Protokollierung der Datenaustausche und Transparentmachung über ein Datencockpit
d. Unzulässigkeit der widerrechtlichen Nutzung der Steuer-ID durch öffentliche Stellen und Private und Einführung eines Straftatbestandes mit Freiheitsstrafe
e. Evaluierungs- und Berichtspflichten ans Parlament

3. Im internationalen Vergleich setzt Deutschland auf eine große Anzahl struktureller Hemmnisse

Im Vergleich zu anderen Staaten würde Deutschland bei Umsetzung des vorliegenden Gesetzentwurfs über ein öffentliches Datenmanagementsystem mit den meisten strukturellen Hemmnissen gegen eine Profilbildung verfügen (vgl. Abb. 1) und würde sich auch gegenüber dem aktuellen Ist-Zustand deutlich verbessern. Eine „Datenzusammenführung auf Knopfdruck“, wie es einige befürchten, ist weder heute möglich, noch würde sie in Zukunft erleichtert – das Gegenteil ist der Fall.

Strukturelle Hemmnisse gegen Profilbildung	Deutschland (RegMod)	Österreich	Estland	Schweiz	Frankreich	Dänemark
System bereichsspezifischer Personenkennzeichen	-	X	-	-	-	-
Ex ante Berechtigungsprüfung Durch Kontrollmechanismen wie 4-Corner, Intermediäre o.ä.	X	(X)	X	X	X	X
Ex post Kontrollierbarkeit der Datenzugriffe, Transparenz durch Datencockpit	X	(X)	X	-	X	-
Fachlich ausdifferenzierte, dezentral organisiert und verantwortete Register	X	-	-	(X)	-	-
Datenschutz als Verfassungsrecht, strenge Datenschutzaufsicht, Evaluierung und Berichtswesen ans Parlament, Straftatbestand mit Freiheitsstrafe	X	-	(X)	-	-	-
Summe	**4**	**3**	**3**	**2**	**2**	**1**

Abb. 1: Strukturelle Hemmnisse gegen eine Profilbildung im Ländervergleich

4. Das österreichische Modell verknüpfter, bereichspezifischer Personenkennzeichen bietet nur eine bedingte Sicherheit gegen eine Profilbildung

Zum einen basiert das österreichische Modell auf zentralen Registern, die – sofern unerlaubte Zugriffe gelingen – ein viel größeres Schadenspotential aufweisen, als dezentrale Register. Zum anderen sind die sprechenden Stammdaten der Bürgerinnen und Bürger weiterhin Bestandteil dieser Register und eine Profilbildung auch ohne einheitliches Personenkennzeichen – einfach auf Basis der genauso identifizierenden persönlichen Stammdaten – möglich. Zum dritten beschränkt sich das österreichische Modell auf die zentralen Registerbestände des Bundes; die Landes- und Kommunalebene sind nicht umfasst.

5. So lange persönliche Stammdaten in den Registern vorkommen, können bereichsübergreifende Persönlichkeitsprofile genauso erstellt werden wie mit einem numerischen Personenkennzeichen

Es ist wichtig zu verstehen, dass Personen mit Hilfe ihrer persönlichen Stammdaten (Name, Geburtsdatum, Wohnort, etc.) eindeutig identifiziert werden können. Insofern existiert auch jetzt schon in Deutschland für einen Großteil der Bevölkerung de facto ein einheitliches, wenn auch nicht numerisches Personenkennzeichen, das – die bestehende Kritik konsequent zu Ende gedacht – bereits den Ist-Zustand in Deutschland verfassungswidrig erscheinen ließe. Daher verwundert es, dass der Ist-Zustand in Deutschland von einigen als vorzugswürdiger erachtet wird, zumal er datenschutzrechtlich am Ende kein besseres Ergebnis erzielt und seine Wirksamkeit allein vom „Zufall schlechter Datenhaltung“ abhängt, d.h. z.B. von den zufällig auftretenden Fehlern in der Namensschreibweise oder einer zu langsamen Aktualisierung von persönlichen Stammdaten nach Namenswechseln. In jedem System, auch dem österreichischem und solchen, die z.B. von Sorge et al.[3] vorgeschlagen werden, findet die Zuordnung der Datensätze zu einer Person immer mit Hilfe dieser persönlichen Stammdaten statt. Gerade Österreich nutzt sein System auch dafür, diese persönlichen Stammdaten über die Register hinweg qualitätszusichern und aktuell zu halten. So lange also persönliche Stammdaten in den Registern vorkommen, können bereichsübergreifende Persönlichkeitsprofile genauso erstellt werden, wie mit einem numerischen Personenkennzeichen. Für einen effektiven Schutz sind daher dezentrale Datenhaltungsstrukturen, Zugriffskontrollmechanismen (4-Corner-Modell), Protokoll- und Transparenzmechanismen (Datencockpit) sowie ein konsequentes Strafverfolgungsregime die geeignetere Wahl.

[3] Sorge Ch., von Lucke J., Spiecker I. (2020) Registermodernisierung. Datenschutzkonforme und umsetzbare Alternativen, Friedrich-Naumann-Stiftung.

6. Die ganz überwiegende Zahl der europäischen Länder verwendet ein einheitliches Personenkennzeichen

Deutschland bildet bisher eine der wenigen Ausnahmen, die kein einheitliches Personenkennzeichen nutzen (vgl. Abb. 2). Viele der im europäischen und internationalen Kontext genutzten Kennzeichen sind sprechend, d.h. sie beinhalten das Geburtsdatum, einen Zahlencode für das Geschlecht oder auch den Geburtsort und sind auf einem Ausweisdokument abgedruckt. Dies ist mit dem vorliegenden Gesetzentwurf nicht geplant.

Land	Einheitliches Personenkennzeichen vorhanden	Einheitliches Personenkennzeichen steht auf dem Ausweis	Einheitliches Personenkennzeichen ist sprechend
Belgien	X	X	X
Bulgarien	X	X	X
Dänemark	X	X	X
Deutschland	-	-	-
Estland	X	X	X
Finnland	X	X	X
Frankreich	X	-	X
Griechenland	-	-	-
Irland	X	-	-
Italien	X	X	X
Kroatien	X	X	-
Lettland	X	X	-
Litauen	X	X	X
Luxemburg	X	-	X
Malta	X	X	X
Niederlande	X	X	-
Österreich	(X) geheim	-	-
Polen	X	X	X
Portugal	-	-	-
Rumänien	X	X	X
Schweden	X	X	X
Slowakei	X	X	X
Slowenien	X	X	X
Spanien	X	X	-
Tschechien	X	X	X
Ungarn	-	-	-
Zypern	-	-	-
Summe	**22**	**18**	**16**

Abb. 2: Einheitliche Personenkennzeichen im europäischen Vergleich

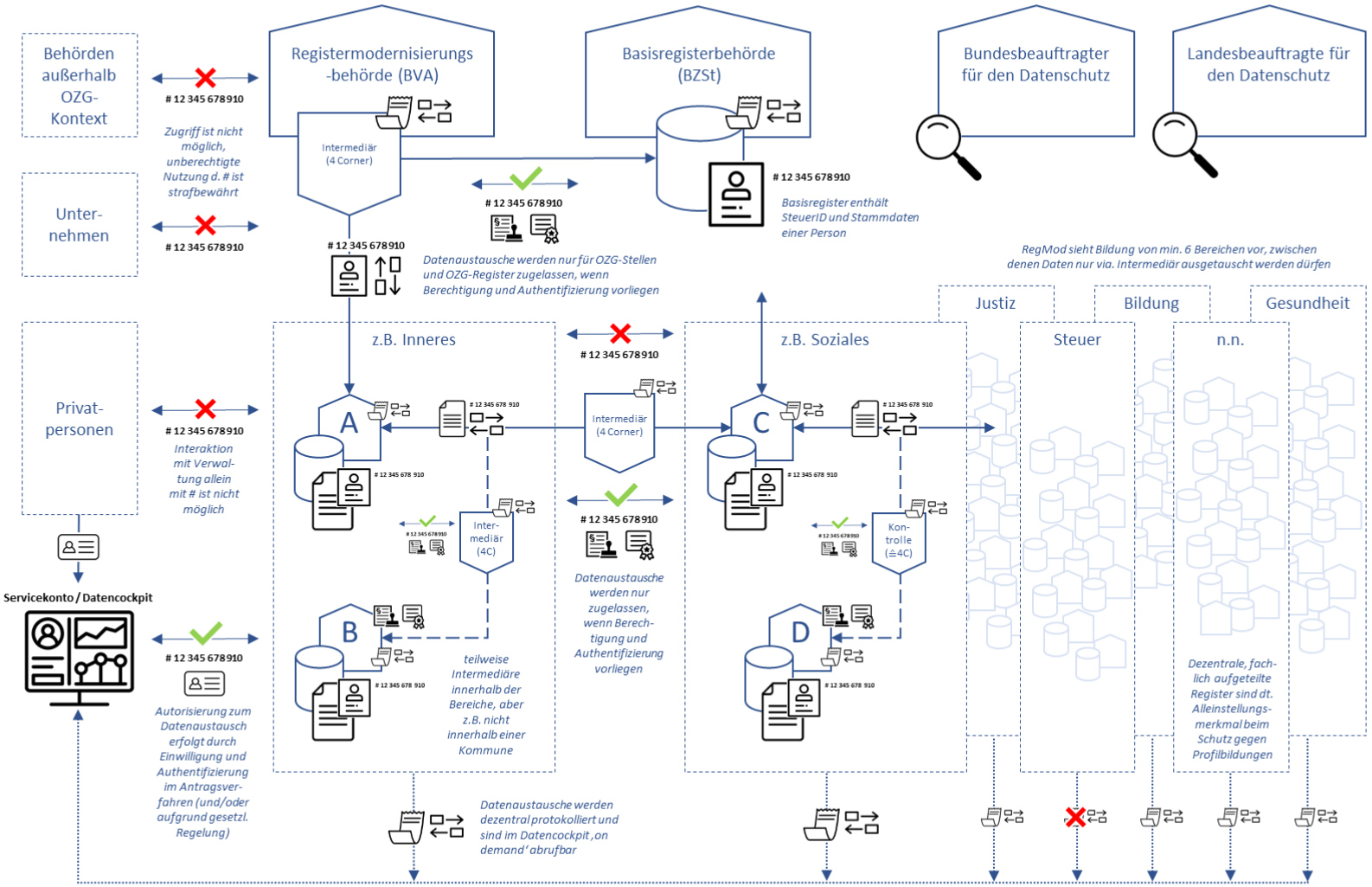
7. Von der Umsetzungskomplexität und Beherrschbarkeit eines Systems hängt auch seine datenschutzrechtliche Wirkung und Kontrollierbarkeit ab

Bei aller Unsicherheit einer ex ante Schätzung möglicher Umsetzungsaufwände und dem darauf basierenden Vergleich der beiden Umsetzungsszenarien „bereichsspezifische vs. einheitliches Personenkennzeichen", zeigt die vorgelegte Schätzung eine klare Tendenz. Aus einer datenschutzrechtlichen Bewertung heraus sind dabei nicht der höhere Aufwand und die längeren Umsetzungszeiträume entscheidend, sondern die dahinter liegende Einsicht, dass die Einführung bereichspezifischer Personenkennzeichen im deutschen System dezentraler Register und etablierter Sicherungsmechanismen ein äußerst komplexes Unterfangen wäre. Angesichts des zweifelhaften datenschutzrechtlichen Mehrwertes erscheint es unangemessen, dafür die erheblichen Umsetzungsrisiken in Kauf zu nehmen und ein System zu riskieren, dessen Funktionstüchtigkeit, Beherrschbarkeit und Kontrollierbarkeit fraglich sind.

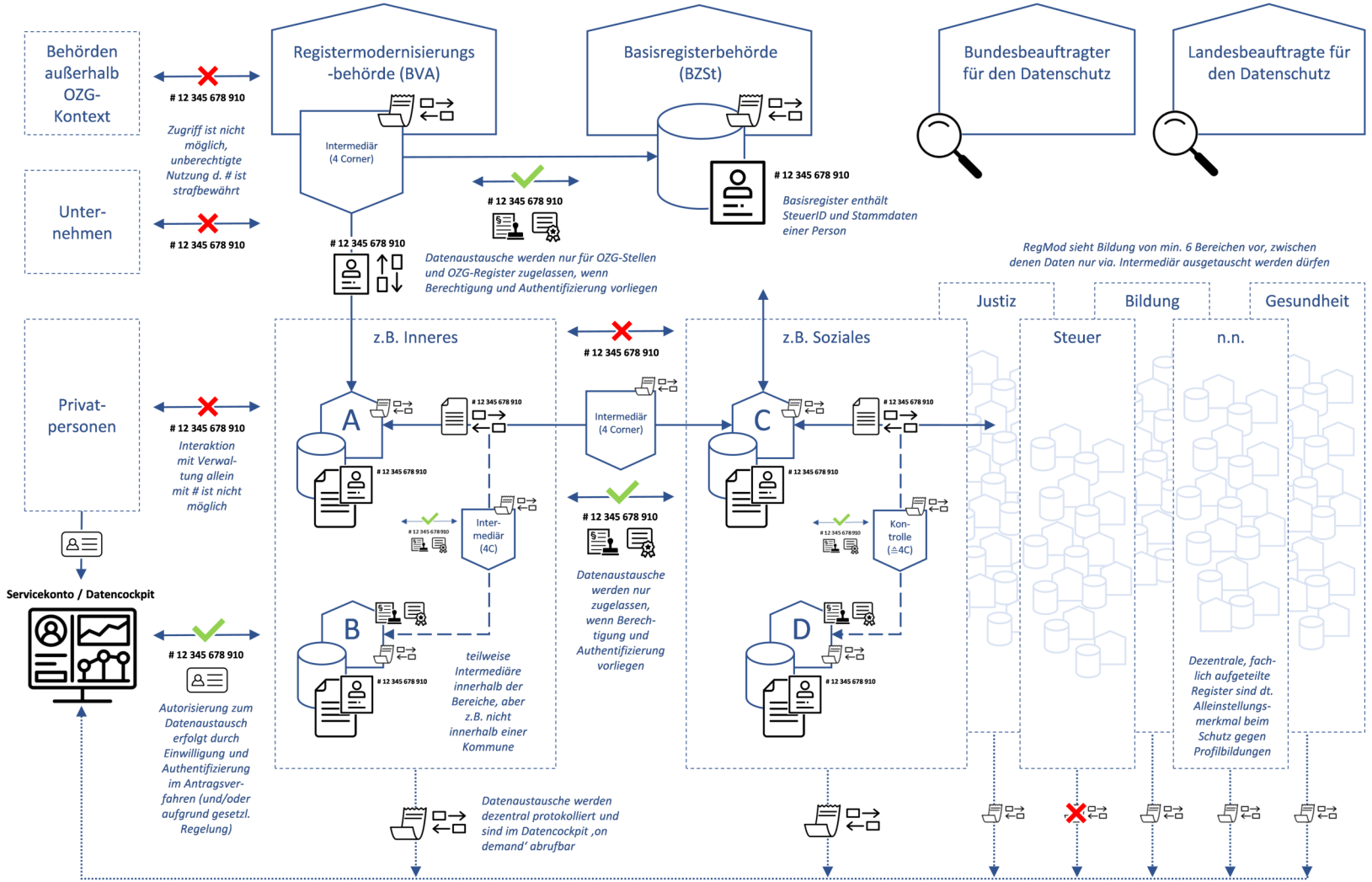
Aus dieser Perspektive heraus ist es auch verständlich, dass sich die Bundesregierung für eine „Nachnutzung" der Steuer-ID entschieden hat, da sie ein etabliertes Personenkennzeichen nutzen und auf bewährte IT-Strukturen aufbauen möchte. Dass die Steuer-ID unter anderen Prämissen eingeführt worden ist, mag kommunikativ problematisch sein. Datenschutzrechtlich macht es am Ende aber keinen Unterschied, ob formal gesehen eine neue Nummer etabliert wird, die dann von der Steuer genutzt wird oder ob die Genese andersherum erfolgt. In vergleichbarer Weise sind auch andere Länder vorgegangen, zuletzt die Schweiz mit ihrem Beschluss vom 8.12.2020, die Sozialversicherungsnummer (AHV-Nummer) zum einheitlichen Personenkennzeichen zu erklären[4].

[4] ttps://www.vbs.admin.ch/de/home.detail.news.html/vbs-internet/parlament/2020/201210.html#dossiers

Datenverarbeitung gemäß Registermodernisierungsgesetz (und bestehender Regelungen)



Datenverarbeitung gemäß Registermodernisierungsgesetz (und bestehender Regelungen)



Nationaler Normenkontrollrat 12/2020