

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

Per eMail an: innenausschuss@bundestag.de

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)667 F

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 Bürgerinnen 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 Bürgerinnen 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 Bürgerinnen 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 Bürgerinnen, 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 Bürgerinnen 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 Bürgerinnen 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 Bürgerinnen 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 Bürgerinnen als freiheitsgarantierende Exekutive des Staates gegenüberzutreten. Die Möglichkeit einer vollständigen Katalogisierung und Registrierung der Persönlichkeit von Bürgerinnen muss darum ausgeschlossen sein, damit ein beobachtungsfreier 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-Prinzip² 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 Bundesverwaltungsamt (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 Bürgerinnen bringen wird. Verwechslungen von Bürgerinnen 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 bereichsspezifischen 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 Personenkenziffer 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 Personenkenziffer 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 Personenkenzahl 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 Nachweis⁶. 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 Personenkenziffer 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 nutzen 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 Ur. 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 Strafbewährung 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 Bürgerinnen 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 Bürgerinnen 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 Krempf; 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 bereichsspezifischen 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 Bürgerinnen in einer digitalisierten Welt gewährleisten und schützen kann. Dieses staatliche Interesse besteht nicht nur im Hinblick auf die Gewährleistung der informationellen Selbstbestimmung der einzelnen Bürgerin 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.