Der Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

POSTANSCHRIFT Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Postfach 1468, 53004 Bonn

Bundesministerium des Innern, für Bau und Heimat
Referat V II 2

Nachrichtlich:
Bundesressorts

HAUSANSCHRIFT Husarenstraße 30, 53117 Bonn
FON (0228) 997799-1100
FAX (0228) 997799-5550
E-MAIL referat11@bfdi.bund.de
BEARBEITET VON Herr Hermerschmidt
INTERNET www.datenschutz.bund.de
DATUM Bonn, 04.05.2020
GESCHÄFTSZ. 11-100/010#0157

Bitte geben Sie das vorstehende Geschäftszeichen bei allen Antwortschreiben unbedingt an.

BETREFF **Entwurf eines Gesetzes zur Einführung einer Identifikationsnummer in die öffentliche Verwaltung und zur Änderung weiterer Gesetze (Registermodernisierungsgesetz - RegMoG)**
HIER Stellungnahme des BfDIStellungnahme des BfDI
BEZUG E-Mail des BMI vom 20.04.2020E-Mail des BMI vom 20.04.2020

Sehr geehrte Damen und Herren,

für den BfDI nehme ich zu dem o. g. Gesetzentwurf wie folgt Stellung:

1. Vorbemerkung

Der Gesetzentwurf wurde den Ressorts mit E-Mail des BMI vom 9. April 2020 zugesandt und damit die Ressortabstimmung eingeleitet. Der BfDI war ebenso wenig im Empfängerkreis dieser E-Mail wie in dem einer weiteren E-Mail des Referates V II 2 des BMI. Ich habe den Gesetzentwurf erstmals mit der Einladung zur Ressortbesprechung mit E-Mail vom 20. April 2020 erhalten, mithin elf Tage später als die Ressorts.

Ich habe diesen Verstoß gegen §§ 21 Abs. 1, 45 Abs. 3 GGO sowie gegen Art. 36 Abs. 4 DSGVO bei einem der aus datenschutzrechtlicher Sicht wichtigsten Gesetzgebungsverfahren der laufenden Legislaturperiode bereits beim Bundesminister des Innern, für Bau und Heimat sowie beim Chef des Bundeskanzleramtes gerügt.

ZUSTELL- UND LIEFERANSCHRIFT Husarenstraße 30, 53117 Bonn
VERKEHRSANBINDUNG Straßenbahn 61, Husarenstraße

Im Ergebnis bedeutet dies, dass mir eine deutlich kürzere Zeit für die Stellungnahme zur Verfügung steht, obwohl der Gesetzentwurf eine eingehende verfassungsrechtliche und datenschutzrechtliche Würdigung erfordert.

2. Grundsätzliche Fragen zur Konzeption der Registermodernisierung

Mit dem vorliegenden Gesetzentwurf ist die Einführung eines registerübergreifenden Identitätsmanagements für die öffentliche Verwaltung in Deutschland geplant. Konzeptionell beruht dieses Identitätsmanagement auf der registerübergreifenden Nutzung eines eindeutigen und veränderungsfesten Ordnungsmerkmals. Hierfür soll die Identifikationsnummer nach § 139b AO (im Folgenden: Steuer-ID) verwendet werden. Der Gesetzentwurf verfolgt dabei im Wesentlichen den Ansatz, die Identifikationsnummer (im Folgenden ID-Nr.) in allen Registern zum Zwecke der eindeutigen Identifizierung einer natürlichen Person zu verarbeiten. Alternative Modelle sind im Vorfeld des Gesetzgebungsverfahrens erörtert worden, worauf sowohl im Vorblatt des Gesetzentwurfs als auch in der Begründung näher eingegangen wird.

Die dem Gesetzentwurf zugrundeliegende Gesamtkonzeption lehne ich aus verfassungsrechtlichen und datenschutzrechtlichen Gründen ab. Die auf der Grundlage der Konzeption vorgesehenen Eingriffe in das Recht auf informationelle Selbstbestimmung und in das durch die EU-Grundrechtecharta garantierte Grundrecht auf Datenschutz genügen nicht den verfassungsrechtlichen Anforderungen. Der Gesetzentwurf greift erheblich in zentrale datenschutzrechtliche Prinzipien – insbesondere das Gebot der Zweckbindung und dessen technische Umsetzung – ein und verstößt damit gegen den Grundsatz der Verhältnismäßigkeit.

Bereits in den intensiven Vorberatungen, bei denen ich mich einbringen konnte, wurden Alternativen zu der nunmehr geplanten Konzeption erörtert. Es hat sich jedoch sehr bald gezeigt, dass das federführende BMI zunehmend einseitig auf das dem Gesetzentwurf zugrundeliegende Modell festgelegt war und die in die Diskussion hauptsächlich eingebrachte Alternative nicht ernsthaft in Betracht gezogen wurde.

2.1. Zur Zielsetzung und der Notwendigkeit der Regelungen

In der Begründung (S. 27) wird konstatiert, dass in der gegenwärtigen Registerorganisation staatliche Register jeweils die für den jeweiligen Fachbereich erforderlichen Daten enthielten und der Kreis der zugriffsberechtigten Behörden eng begrenzt sei. Diese Organisation wird sodann dahingehend kritisiert, dass sie zu einer vielfach redundanten, häufig widersprüchlichen und inkonsistenten Datenhaltung führe. Diese Kritik ist nur dann nachvoll-

ziehbar, wenn man die verfassungsrechtlichen Gründe, die zur Entstehung dieser Organisation geführt haben, ausblendet. Das verfassungsrechtliche Gebot der Zweckbindung (BVerfGE 65, 1, 46) erfordert es, dass die Verwendung personenbezogener Daten jeweils auf den gesetzlich bestimmten konkreten Zweck begrenzt ist und dass es entsprechende Weitergabe- und Verwertungsverbote gibt. Darüber hinaus bedarf es entsprechender Sicherungen in dem Sinne, dass die Bürger wissen müssen, wer was bei welcher Gelegenheit über sie weiß (BVerfGE 65, 1, 43).

Die hier als redundant und widersprüchlich kritisierte Datenhaltung ist daher zumindest auch ein Ergebnis der datenschutzrechtlich gebotenen Zweckbegrenzung und der zu deren Unterstützung notwendigen Transparenz. Mit der sehr heterogenen Landschaft wird sichergestellt, dass der Einzelne grundsätzlich nachvollziehen kann, welche Behörde welche Daten über ihn zu welchem Zweck speichert. Durch die bestehenden Hemmnisse bei der registerübergreifenden Kommunikation kann er sich einigermaßen darauf verlassen, dass der Staat nicht ohne weiteres seine Daten zusammenführen und zweckwidrig verwenden kann. Der datenschutzrechtliche Wert der gegenwärtigen Situation wird im Gesetzentwurf nicht gewürdigt und daher auch nur unzureichend der verfassungsrechtlichen Rechtfertigung zugrunde gelegt.

Die verfassungs- und datenschutzrechtlichen Anforderungen stehen dabei selbstverständlich einer Modernisierung und einer Qualitätsverbesserung der Register nicht im Wege. Es ist mir jedoch wichtig zu betonen, dass die datenschutzrechtlichen Vorzüge der gegenwärtigen Situation bei der Modernisierung in der gebotenen Weise berücksichtigt und in die digitale Verwaltung „übersetzt“ werden.

2.2. Zur verfassungsrechtlichen Rechtfertigung

In der Begründung (S. 31 ff.) finden sich die Ausführungen zur Vereinbarkeit mit den grundrechtlichen Anforderungen des Grundgesetzes. Als Zweck des Entwurfs wird dabei zunächst das hohe Bedürfnis der Verwaltung für eine eineindeutige Zuordnung von Datensätzen zu der jeweils richtigen Person angegeben. Dies diene der Funktionsfähigkeit und Effektivität der Verwaltung. Zudem sei die Einführung der ID-Nr. auch ein ebenso hohes Bedürfnis der betroffenen Personen, die einen Anspruch auf die Richtigkeit und Aktualität der über sie verarbeiteten Daten hätten. Weiterhin sollten die Leistungsgerechtigkeit staatlichen Handelns gesteigert, die Bürger von Nachweispflichten entlastet und dem Leistungsmissbrauch vorgebeugt werden. Schließlich sei die Einführung der ID-Nr. für den registerbasierten Zensus von Bedeutung.

Die genannten Zwecke als solche sind durchaus nachvollziehbar und legitim, sofern sie sich ausschließlich auf die eindeutige Identifizierbarkeit bei zulässigen Datenverarbeitungsprozessen beziehen und nicht auf eine leichtere Verknüpfbarkeit getrennt zu haltender Datenbestände. Letzteres wäre angesichts des Gebots der Zweckbindung kein legitimer Zweck. Es bestehen allerdings erhebliche Zweifel, ob der Gesetzentwurf eine dem Grundsatz der Verhältnismäßigkeit entsprechende Basis ist, um die genannten Zwecke zu erreichen. Insbesondere habe ich erhebliche Bedenken im Hinblick auf die Erforderlichkeit und die Verhältnismäßigkeit im engeren Sinne, d. h. die Angemessenheit der Regelungen.

2.2.1. Erforderlichkeit

Die Begründung (S. 32) stellt hierzu fest, dass kein gleich geeignetes, aber weniger eingriffsintensives Mittel vorhanden sei, das ein registerübergreifendes Identitätsmanagement sicherstellen könne.

Diese Feststellung trifft nach meiner Ansicht nicht zu. Das in der Begründung als theoretische Möglichkeit angesprochene Modell „eines anderen EU-Mitgliedstaates“ (gemeint: Österreich) ist aus hiesiger Sicht ebenso geeignet, die Ziele zu erreichen und ist durch die eingebauten Hemmnisse bei der registerübergreifenden Kommunikation von geringerer Eingriffstiefe.

In der Begründung wird dazu ausgeführt, dass das österreichische Modell nicht gleichermaßen geeignet sei. Begründet wird dies mit der dezentralen Registerlandschaft in Deutschland und der netzartigen Verarbeitungsprozesse. Diese Begründung überzeugt nicht. Es ist unbestritten, dass eine Übertragung des österreichischen Modells auf Deutschland komplexer wäre, als dies in Österreich der Fall war. Sie ist jedoch nicht ausgeschlossen und eine 1-zu-1-Übertragung wäre auch nicht zwingend notwendig. Eine Architektur mit bereichsspezifischen Identitätskennzeichen (bPK-Modell) wäre jedoch durchaus möglich. Es bestand in den Expertengruppen nach meinem Eindruck auch Einigkeit, dass beide Modelle (4-Corner-Modell und Modell mit bereichsspezifischen Kennzeichen) gleichermaßen geeignet seien. Unter „Alternativen“ (S. 28 der Begründung) wird zudem der immense Aufwand des bPK-Modells hervorgehoben. Allerdings liegt mir bis heute keine belastbare Betrachtung der Aufwände für die beiden Modelle vor. In den Expertengruppen wurde insoweit kommuniziert, dass eine detaillierte Kostenbetrachtung aufgrund des zeitlichen Drucks eher nicht mehr zu erwarten sei. Vor diesem Hintergrund halte ich es für nicht sachgemäß, den Aufwand als Argument heranzuziehen, zumal auch die Umsetzung des 4-Corner-Modells und die notwendige Registerbereinigung einen Aufwand verursachen werden.

Darüber hinaus wird in der Begründung (S. 32 f.) der datenschutzrechtliche Mehrwert des bPK-Modells als nicht nennenswert angesehen. Das 4-Corner-Modell sei eine ausreichende Sicherung gegen unzulässige Datenzusammenführungen. Zudem diene das dem Gesetzentwurf zugrundeliegende Modell dem Datenschutz, indem es die Datenqualität verbessere und das Prinzip der Datensparsamkeit konsequent umsetze und die Datenschutzkontrolle verbessert werde.

Auch gegen diese aus meiner Sicht einseitigen Feststellungen sind erhebliche Zweifel angebracht. Die datenschutzrechtlichen Vorzüge des bPK-Modells werden marginalisiert, während hinsichtlich des vom Gesetzentwurf verfolgten Modells entweder Vorzüge dargestellt werden, die bei beiden Modellen gelten (bessere Datenqualität, Datenschutzkontrolle) oder die bei näherer Betrachtung keine Vorteile sind. Letzteres trifft vor allem auf die Datensparsamkeit zu. Datenminimierung oder Datensparsamkeit bedeutet nicht, dass man nur dadurch in den einzelnen Registern weniger Daten verarbeitet, indem ein registerübergreifender Identifier gewissermaßen als Schlüssel mittels einer zentralen Speicherung von Basisdaten die Zusammenführung der Daten erleichtert. Mit Blick auf die Gesamtarchitektur ist dies eher das Gegenteil von Datenminimierung. Datenminimierung bedeutet vielmehr, dass die Datenverarbeitung bereits auf technischem Wege auf das für den jeweiligen Zweck notwendige Maß beschränkt werden muss. Dies wird eher erreicht, wenn auf die Verwendung einer registerübergreifenden ID-Nr. verzichtet wird.

Der entscheidende datenschutzrechtliche Vorteil des bPK-Modells besteht m. E. darin, dass dieses gegen Angreifer von außen sowie bei einem Szenario, bei dem sich der Staat selbst als feindlicher Akteur betätigt, die besseren Sicherungen aufweist. Aufgrund der unterschiedlichen bPKs könnten Daten einer natürlichen Person aus unterschiedlichen Registern jedenfalls nicht so leicht zusammengeführt werden wie bei der Verwendung eines registerübergreifenden Identifiers, da im ersteren Falle der „Schlüssel“ fehlt.

Beim 4-Corner-Modell befinden sich die Sicherungen im Wesentlichen innerhalb des Systems. Das 4-Corner-Modell stellt grundsätzlich sicher, dass nur autorisierte Behörden miteinander kommunizieren dürfen und diese auch nur die zugelassenen Daten austauschen. Darüber hinaus erfolgt eine Ende-zu-Ende-Verschlüsselung und die bereichsübergreifende Kommunikation erfolgt über einen vertrauenswürdigen Intermediär, der keinen Zugriff auf die Inhalte der Kommunikation hat. Das Modell bietet aber letztlich keine Sicherung gegen die vorgenannten Szenarien einer missbräuchlichen Zusammenführung der Daten einer Person. Die bestehenden Vorzüge des 4-Corner-Modells können auch im bPK-Modell genutzt werden, nur dass durch die bPKs eine zusätzliche Sicherung gegen die missbräuchliche und rechtswidrige Zusammenführung der personenbezogenen Daten einer natürlichen Person enthält.

Vor diesem Hintergrund betrachte ich das bPK-Modell – ggf. in Kombination mit dem 4-Corner-Modell – als ebenso geeignetes, aber weniger eingriffsintensives Mittel.

2.2.2. Angemessenheit

Das dem Gesetzentwurf zugrundeliegende Modell ist aus meiner Sicht auch nicht angemessen, da die Schwere des Eingriffs nicht in einem angemessenen Verhältnis zu dem angestrebten Zweck steht.

Die Einführung eines zentralen Personenkennzeichens ist mit schwerwiegenden Eingriffen in das Recht auf informationelle Selbstbestimmung verbunden, da mit seiner Hilfe angesichts der intendierten breiten Verwendung ein einfaches Mittel zur Verfügung steht, um übergreifend Daten einer natürlichen Person zusammenzuführen, die aus völlig unterschiedlichen Bereichen stammen. Dies stellt eine enorme Herausforderung für die Gewährleistung der Zweckbindung dar, die durch den Grundsatz der Nichtverkettbarkeit personenbezogener Daten auch technisch gesichert werden muss.

Bedauerlicherweise werden diese Risiken im Gesetzentwurf nicht angesprochen und eine Risikobewertung wird dementsprechend nicht vorgenommen. Bereits in den letzten Sitzungen der Expertengruppen wurde signalisiert, dass eine eingehende Risikobetrachtung wegen des Zeitdrucks bei der Registermodernisierung nicht mehr vorgenommen werden könne. Dies ist angesichts der weitreichenden Folgen der Einführung einer zentralen ID-Nr. nicht akzeptabel und erschwert zudem die seriöse Bewertung des Gesetzesvorschlags.

Wie bereits angesprochen wurden etwa die Risiken der Kompromittierung der Register durch bestimmte Angriffsszenarien nicht bewertet. Darüber hinaus wurden die Folgen nicht betrachtet, die die geplante umfassende Verbreitung der ID-Nr. mit sich bringen wird. Beispiele in anderen Ländern zeigen, dass eine zentrale ID-Nr. am Ende in der gesamten Privatwirtschaft als zentrales Ordnungsmerkmal genutzt wird. Auch in Deutschland wird damit zu rechnen sein. Der Gesetzentwurf unternimmt nicht einmal den Versuch, die Verarbeitung der ID-Nr. einer adäquaten Zweckbindung zu unterwerfen (siehe dazu die Anmerkungen zu Art. 1 § 3).

Das durch eine zentrale ID-Nr. deutlich erhöhte Risiko einer unzulässigen Profilbildung durch Zusammenführung der Daten aus verschiedenen Registern wird ebenfalls unzureichend adressiert. In der Begründung (S. 33) finden sich dazu nur wenige Sätze, deren Inhalt sich darauf beschränkt, dass eine Profilbildung rechtlich und technisch ausgeschlossen sei, wobei zu den technischen Sicherungen nur auf die durch das Deutsche Ver-

waltungsdiensteverzeichnis (DVDV) ermöglichten Sicherungen und die Protokollierung verwiesen wird. Dies bleibt letztlich diffus und ist den Risiken nicht angemessen.

An dieser Stelle ist es erforderlich, noch einmal die vom BVerfG aufgestellten Grundsätze in Erinnerung zu rufen, an deren Maßstab der vorliegende Gesetzentwurf zu prüfen ist.

Kern des Datenschutzrechts ist das Recht auf informationelle Selbstbestimmung, dessen wesentliche Elemente bereits im Mikrozensus-Urteil des BVerfG beschrieben wurden (BVerfGE 27, 1). Danach hat jede Person das Recht auf einen persönlichen Innenraum, in dem sie sich besitzt und in den sie sich zurückziehen kann. Sie ist dort frei von Beobachtung. Dieser Innenraum ist zwingende Voraussetzung für die Entfaltung der Persönlichkeit und das Ausleben der Handlungsfreiheit. Eingriffe in diese Bereiche könnten die Personen bei der (öffentlichen) Inanspruchnahme dieser Freiheiten hemmen. Dabei reicht schon ein gewisser psychischer Druck auf die Person aus, um diesen Effekt zu erzielen.

Da schon ein psychischer Druck beim Bürger ausreichen kann, um diesen Innenraum in seiner Unverletzlichkeit anzugreifen, entsteht der Eindruck bereits durch das Risiko einer vollständigen Registrierung und Katalogisierung der Persönlichkeit. Eine tatsächliche Vollkatalogisierung ist nicht notwendig, um einen derartigen subjektiven Eindruck entstehen lassen zu können. Auf Grundlage dieser Gedanken formte das BVerfG im Volkszählungsurteil (BVerfGE 65, 1) das Recht auf informationelle Selbstbestimmung. Eine Gefahr für den Innenraum ist so lange nicht gegeben, so lange der Bürger selbstbestimmt über seine Daten walten und Einfluss nehmen kann. Zudem bedarf es einer Vielzahl weiterer Sicherungen, von denen im vorliegenden Kontext den notwendigen technischen und organisatorischen Maßnahmen die entscheidende Bedeutung zukommt.

Vor diesem Hintergrund ist es weiterhin aktuell, dass das BVerfG im Volkszählungsurteil beispielhaft ein einheitliches verwaltungsübergreifendes Personenkennzeichen als entscheidenden Schritt des Staates wertet, den Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren (BVerfGE 65, 1, 57). Die Schaffung dieses Systems ist also bereits problematisch, da das Risiko einer verlässlichen Zusammenführung der Daten über eine Person besteht, die ggf. Gegenstand der Bewertung und weiterer staatlicher Maßnahmen werden kann.

Aus diesen Gründen bedarf es struktureller Hemmnisse, die eine registerübergreifende Zusammenführung der Daten einer Person verhindern. Während Transparenz, Rechtsschutz und die übrigen Mittel zur Gewährleistung der informationellen Selbstbestimmtheit auch bei einer einheitlichen ID-Nr. gewährleistet werden können, trifft der Gesetzentwurf jedoch keine befriedigenden Aussagen, mit welcher effektiven technischen und organisa-

torischen Ausgestaltung das Risiko einer vollständigen Zusammenführung und Katalogisierung auf das verfassungsrechtlich notwendige Maß reduziert werden soll. Hier fehlt es an strukturellen Hemmnissen.

Insgesamt ist daher festzustellen, dass der Gesetzentwurf auch nicht den Ansprüchen an eine verhältnismäßige Regelung genügt.

2.2.3. Nutzung der Steuer-ID als Identifikator

Der Gesetzentwurf begründet die Verwendung der Steuer-ID zunächst mit (nicht belegten) Kostengesichtspunkten und Nützlichkeitserwägungen. Vor allem wird die Verwendung der Steuer-ID aber auf datenschutzrechtliche Gesichtspunkte gestützt, da deren Konformität mit dem Recht auf informationelle Selbstbestimmung durch den BFH bereits bestätigt sei (Begründung S. 33).

Diese Begründung ist besonders abwegig, da der BFH ausschließlich über die Verwendung der Steuer-ID für steuerliche Zwecke befunden hat. Auch der Hinweis auf die Verarbeitung der Steuer-ID in anderen Registern ändert daran nichts, da es auch dann bei der Begrenzung auf die steuerlichen Zwecke bleibt. Das Urteil des BFH (II R 49/10) weist eher in eine gegenteilige Richtung.

So verweist der BFH bereits im Obersatz seiner Begründetheitsprüfung (Rn. 33 des Urteils) darauf, dass die Steuer-ID aufgrund ihrer Zielsetzung sowie der zweckentsprechenden Ausgestaltung nicht gegen das Recht auf informationelle Selbstbestimmung verstößt. Diese strenge Zweckbindung, die sich auf einen gut abgrenzbaren Bereich der Verwaltung bezieht, würde durch den Vorschlag aufgelöst werden.

Weiterhin geht der BFH (Rn. 35ff. im Urteil) in seiner Entscheidung darauf ein, dass die Gefährdungslage für das Recht auf informationelle Selbstbestimmung bereits im Vorfeld konkreter Bedrohungen entsteht. Dies geschieht durch die unbegrenzte Speicherbarkeit, den sekundenschnellen Abruf sowie vielfältige Nutzungs- und Verknüpfungsmöglichkeiten. All dies führt zu einer gefährdenden Zusammenführbarkeit, die bis zu einem Persönlichkeitsprofil reichen kann. Bei der Eingriffsintensität spielt darüber hinaus eine Rolle, ob der Bürger einen ihm zurechenbaren Anlass für die Datenverarbeitung gegeben hat oder ob sie anlasslos erfolgt. Letzteres wäre für viele Verarbeitungen im Rahmen der Registermodernisierung der Fall.

Ein besonderes Rechtfertigungselement für die Verfassungsmäßigkeit der Steuer-ID war unter anderem die besondere Verpflichtung zur Wahrung des Steuergeheimnisses der mit

der Verarbeitung betrauten Personen (§§ 30 AO, 355 StGB). Dieses wäre bei der Einrichtung der Steuer-ID als allgemeine ID-Nr. so nicht mehr gegeben. Zudem ergibt sich aus der bereits erwähnten strengen Zweckbindung, dass in den Fällen, in denen keine gesetzliche Grundlage zur Verarbeitung der Steuer-ID gegeben ist, der klar umgrenzte Bereich der Steuerverwaltung nicht verlassen werden darf. Dies ist beim Gesetzesvorschlag in dieser Form so nicht mehr gegeben, da die öffentliche Verwaltung als Ganzes sich auch neue Tätigkeitsfelder erschließen kann und darf (vgl. Rn. 67ff. im Urteil). Übermittlungen der Steuer-ID über den Bereich der Steuerverwaltung hinaus benötigen laut BFH (Rn. 75-77) stets eine eindeutige Rechtsvorschrift.

Der Stammdatensatz ist laut BFH (Rn. 82 im Urteil) zulässig, da dieser für sich kein Persönlichkeitsprofil darstellt und auch die Bildung eines solchen aufgrund der strengen Zweckbindung und des ebenso strengen Gesetzesvorbehalts für eine Verarbeitung, die sich alleine auf die Steuerverwaltung bezieht, nicht zulässt. Sobald also der klar abgrenzbare Bereich der Steuerverwaltung verlassen wird, sieht der BFH die Gefahr einer Katalogisierung und schließt diese Möglichkeit daher aus.

Vor diesem Hintergrund kann aus der Rechtsprechung keineswegs der Schluss gezogen werden, die Verwendung der Steuer-ID sei ganz allgemein datenschutzrechtlich unproblematisch. Es ist vielmehr so, dass gerade die Begrenzung auf die steuerlichen Zwecke die Verfassungskonformität begründet. Es wird bedauerlicherweise nicht einmal die Möglichkeit erwogen, aus der Steuer-ID bspw. mittels eines Hashwertverfahrens eine neue, nicht in die Steuer-ID rückrechenbare ID zu errechnen, um wenigstens die Steuerverwaltung weiterhin angemessen abzuschotten. Dies hatte das BMI bereits im Vorfeld als nutzlos abgelehnt.

Insofern werden die erheblichen Bedenken gegen den Gesetzentwurf durch die Verwendung der Steuer-ID noch verstärkt.

3. Zu den Vorschriften im Einzelnen

Ungeachtet der grundsätzlichen Ablehnung des Gesetzentwurfs nehme ich hilfsweise zu den einzelnen Vorschriften wie folgt Stellung:

3.1. Zu Art. 1 (Entwurf des Identifikationsnummerngesetzes – IDNrG-E)

3.1.1. Zu § 1 IDNrG-E

Zu Absatz 1 Nr. 3 erlaube ich mir die Anmerkung, dass die dort genannten Ziele mit genau dem Mittel erreicht werden sollen, das die Risiken erst verursacht hat. Die Zweckbindung der Daten ließe sich viel besser sicherstellen, wenn es erst gar keine zentrale ID-Nr. gäbe.

In Absatz 2 findet sich die Verpflichtung, die ID-Nr. innerhalb von fünf Jahren in allen Registern zu speichern. In Absatz 3 wird dann zwar definiert, was ein Register ist, allerdings ergibt sich im Übrigen weder aus der Begründung noch bspw. aus der Verordnungsermächtigung, welche Register hiervon erfasst sein sollen.

In Absatz 2 Nr. 3 findet sich die Verpflichtung, die Personendaten in den Registern in jedem Falle durch die qualitätsgesicherten Basisdaten zu ersetzen. Dies dürfte in der Regel unkritisch und im Sinne der Qualitätssicherung in den meisten Fällen auch wünschenswert sein. Allerdings kann es je nach der konkreten Zweckbestimmung eines Registers auch im Interesse der betroffenen Person sein, mit anderen Basisdaten gespeichert zu sein als im BZSt. Insofern sollte bei fachlicher Notwendigkeit davon abgewichen werden können. In der Begründung wird hier der Abbau von Redundanzen hervorgehoben, die nach der Regelung m. E. jedoch erhalten bleiben. Die Daten werden lediglich vereinheitlicht.

3.1.2. Zu § 3 IDNrG-E

Wie bereits in meinen grundsätzlichen Ausführungen angemerkt, fehlt eine konkrete Ausgestaltung der Zweckbindung. In Absatz 1 wird lediglich eine Zweckbeschreibung vorgenommen, Anforderungen an die Zweckbindung finden sich nicht.

Für zweckändernde Weiterverarbeitungen gelten somit die allgemeinen Bestimmungen in Art. 5 Abs. 1 lit. b) und Art. 6 Abs. 4 Datenschutz-Grundverordnung (DSGVO). Damit wären in einem nicht unerheblichen Umfang Zweckänderungen möglich. Eine Weiterverarbeitung für statistische Zwecke wäre bspw. uneingeschränkt möglich.

Dies wird den oben beschriebenen Risiken der Einführung einer zentralen ID-Nr. in keiner Weise gerecht. Art. 6 Abs. 3 lit. b) DSGVO würde es dem deutschen Gesetzgeber durchaus ermöglichen, eine sehr viel striktere Zweckbindung vorzusehen. Auch wenn rein rechtliche Begrenzungen die grundsätzlichen verfassungsrechtlichen Bedenken gegen die Gesamtkonzeption nicht zu beseitigen vermögen, wäre es zumindest ein Schritt, um die zweckwidrige Verwendung der ID-Nr. – bspw. durch nichtöffentliche Stellen – zu begrenzen.

3.1.3. Zu § 4 IDNrG-E

In Absatz 2 wird angeordnet, die ID-Nr. als Ordnungsmerkmal zu verwenden. Hierfür kann ich keine Notwendigkeit erkennen, die Begründung führt dazu bedauerlicherweise nichts aus. Darüber hinaus erhöht sich auf diese Weise das Risiko für die Gewährleistung der Datensicherheit, da insbesondere bei Angriffen von außen eine noch leichtere Zugänglichkeit zu den Daten einer Person besteht, da die ID-Nr. selbst ohnehin flächendeckend bekannt sein wird.

3.1.4. Zu § 8 IDNrG-E

In Absatz 1 Satz 1 ist festgelegt, dass die Basisdaten nur von öffentlichen Stellen im Rahmen und im Umfang ihrer gesetzlichen Aufgaben und Befugnisse abgerufen und weiterverarbeitet werden dürfen. Die Formulierung macht das bei der Verarbeitung personenbezogener Daten durch öffentliche Stellen zentrale Erforderlichkeitsprinzip nicht ausreichend deutlich. Es sollte daher folgende Formulierung verwendet werden:

> *„Die Basisdaten dürfen von einer öffentlichen Stelle nur abgerufen und weiterverarbeitet werden, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist.“*

In der Begründung (S. 41) wird richtigerweise darauf hingewiesen, dass sich die Befugnisse aus Art. 6 DSGVO und auf der Basis gesetzlicher Grundlagen ergeben, wobei noch zu ergänzen ist, dass auch solche Stellen abrufberechtigt sind, die nicht in den Anwendungsbereich der DSGVO fallen, sodass ggf. andere Rechtsgrundlagen gelten. Darüber hinaus wird in der Begründung festgestellt, dass auch Verarbeitungen auf der Basis von Einwilligungen umfasst seien. Dieser Verweis auf die Einwilligung ist zu streichen. Zum einen ergibt sich aus der Formulierung des Absatzes 1, dass Daten nur zur Erfüllung der gesetzlichen Aufgaben und Befugnisse abgerufen werden dürfen. Dies erfasst gerade keine Einwilligungen. Zudem weise ich darauf hin, dass die Einwilligung bei Verarbeitungen zur Erfüllung gesetzlicher Aufgaben ohnehin grundsätzlich nicht in Betracht kommt, vgl. EG 43 der DSGVO.

3.1.5. Zu § 9 IDNrG-E

Vorab möchte ich betonen, dass es wünschenswert wäre, einen einheitlichen datenschutzrechtlichen Standard für das zu verarbeitende Datum im Gesetz zu verankern, anstatt gemäß Absatz 3 je nach verarbeitender Behörde individuelle Standards gelten zu lassen. Ergänzend erscheinen mir Klarstellungen für erforderlich, um mit Blick auf Wortlaut von Norm und Gesetzbegründung Rechtssicherheit beim Verwaltungshandeln zu gewährleisten. Näheres zu den Standards und Verantwortlichkeiten der Protokollierung ist ausweislich der Gesetzesbegründung einer Rechtsverordnung vorbehalten, so dass eine abschließende datenschutzrechtliche Würdigung an dieser Stelle nicht möglich ist.

Im Einzelnen:

Absatz 2 enthält die Zweckbestimmung für die Verwendung der Protokolldaten. Ausweislich der Begründung (S. 42) seien die Zwecke auf die datenschutzrechtliche Prüfung sowie die Gewährleistung der Betroffenenrechte aus den Art. 13 ff. DSGVO beschränkt. Dies wäre aus meiner Sicht eine notwendige und zugleich ausreichende Zweckbestimmung. Allerdings lässt der Wortlaut von Absatz 2 die Verwendung der Protokolldaten auch für Zwecke der Überprüfung der Rechtmäßigkeit des Verwaltungshandelns zu. Diese Zweckbestimmung lehne ich ab und die Worte *„sowie zur Überprüfung der Rechtmäßigkeit des Verwaltungshandelns“* sollten gestrichen werden. Die Speicherung von Protokolldaten ist eine technische Maßnahme, die i. S. v. Art. 5 Abs. 2, 24 Abs. 1 DSGVO allein der notwendigen Dokumentation der Einhaltung der datenschutzrechtlichen Bestimmungen dient. Weitere Verarbeitungszwecke sind bei Protokolldaten auch in anderen Fällen nicht intendiert. Eine über die datenschutzrechtliche Kontrolle hinausgehende Überprüfung der Rechtmäßigkeit des Verwaltungshandelns ist nicht der Sinn einer Protokollierung. Dies halte ich für unverhältnismäßig. Dabei ist auch zu bedenken, dass die eigentlich zum Schutz der betroffenen Personen erfolgende Verarbeitung personenbezogener Daten zum Zwecke der Protokollierung ihrerseits mit Eingriffen in das Recht auf informationelle Selbstbestimmung verbunden sind, die deshalb so gering wie möglich gehalten werden müssen. Zudem rege ich aus redaktionellen Gründen an, in Absatz 2 das Wort „datenschutzrechtlichen“ vor das Wort „Zulässigkeit“ zu verschieben. Absatz 2 sollte daher wie folgt lauten:

> *„(2) Die Protokolldaten nach Absatz 1 dürfen nur zur Prüfung der datenschutzrechtlichen Zulässigkeit sowie zur Gewährleistung der datenschutzrechtlichen Rechte der betroffenen Person verwendet werden.“*

Schließlich möchte ich zur Begründung zu Absatz 2 anmerken, dass es den Begriff „Beauftragter für den Datenschutz“ nicht gibt. Ich gehe davon aus, dass hier der Datenschutzbeauftragte i. S. v. Art. 37 DSGVO bzw. § 5 BDSG gemeint ist.

Der Verweis in Absatz 3 Nr. 6 auf § 6 Abs. 3 Satz 2 bis 5 BVerfSchG hebt die Standards für die Protokollierung und Speicherung, die nach § 9 Absatz 2 und 4 gelten sollen, auf und setzt an deren Stelle die Standards aus dem BVerfSchG. Dies gilt auch für die Löschfrist. Die Löschfrist wird durch die Verweisung verkürzt. Zugleich werden die Möglichkeiten des Bürgers aus § 9 Absatz 2 ausgehebelt.

Damit bleiben bei Verarbeitung der an die genannten Nachrichtendienste des Bundes übermittelten Daten sowohl die Protokollierungsstandards als auch die Aufbewahrungsstandards unbegründet hinter denjenigen von Verarbeitungen bei anderen Behörden zurück. Ein Sachgrund aus der Natur der Behörde besteht nicht und wird dem Umgang mit den sensiblen Daten aus der Steuernummer nicht gerecht. Auszugehen ist regelmäßig vom für das in Rede stehenden Datum erforderlichen Schutzstandard. Angesichts des Umgangs mit einer Datenkategorie sind ein einheitlicher Schutzstandards sowie einheitliche Voraussetzungen für die Prüfung und Durchsetzung von Betroffenenrechten zu gewährleisten.

Ich rege deshalb eine Ergänzung des Wortlauts von Absatz 3 Nr. 6 an, der sicherstellt, dass die Vorgaben der Absätze 1, 2, und 4 erfüllt sind.

Die in Absatz 4 normierte Erforderlichkeitsprüfung bedarf für die datenschutzrechtliche Kontrolle der Dokumentation. Die Dokumentation muss ermöglichen, bei der Kontrolle erkennen zu können, ob länger aufbewahrte Daten in der Folge zweckgebunden verwendet wurden. Entsprechend der schon im Zusammenhang mit Absatz 3 eingeforderten einheitlichen Schutzniveaus sowie eines einheitlichen Regimes zur Prüfung und Durchsetzung der Betroffenenrechte für dieselbe Datenkategorie ist der Verweis aus Absatz 4 Satz 2 zu streichen.

Ich rege daher für Absatz 4 eine Fassung an, die in Satz 1 ergänzt, dass die Erforderlichkeitsprüfung und ihre Erwägungen sowie der Zweck, für den die längere Aufbewahrung erfolgt, zu dokumentieren sind. Weiter rege ich an, Satz 2 mit Blick auf Satz 1 und Absatz 3 zu streichen. Meine Anregung zu Absatz 3 Nr. 6 bezieht sich sowohl auf die vorgelegte Fassung des Gesetzentwurfs als auch auf die hier neu angeregte Fassung des Absatzes 4 gleichermaßen.

3.1.6. Zu § 11 IDNrG-E

Die Vorschrift enthält eine Einschränkung des Auskunftsrechts nach Art. 15 DSGVO. Ausweislich der Begründung (S. 44) stützt sich diese Ausnahme auf Art. 23 DSGVO.

Diese Einschränkungen lehne ich insgesamt ab; die Regelung sollte daher gestrichen werden.

Zunächst bleibt unklar, um welchen Adressaten es bei der Norm überhaupt gehen soll. Geht es um Auskünfte bei der Registermodernisierungsbehörde, beim BZSt oder bei den Fachregisterbehörden? Aus Absatz 1 Nr. 1 könnte man schließen, dass tatsächlich alle Fachregisterbehörden gemeint sein sollen. Diese unterliegen allerdings nicht alle dem Anwendungsbereich der DSGVO. Zudem gelten bei ihnen ohnehin zum Teil schon unterschiedliche Einschränkungen des Auskunftsrechts, sodass es insoweit widersprüchliche Regelungen für die einzelnen Behörden geben wird. Insgesamt ist der sachliche Anwendungsbereich der Norm völlig unklar.

Darüber hinaus ist die Regelung auch inhaltlich überflüssig und schränkt das Auskunftsrecht unangemessen ein. § 34 BDSG enthält bereits Einschränkungen, die in dessen Absatz 1 Nr. 1 tatbestandlich mit § 11 IDNrG-E identisch sind. Der entscheidende Unterschied ist allerdings, dass letzterer die in § 34 Abs. 1 BDSG enthaltene Abwägungsklausel nicht enthält. Damit wirkt die hier vorgesehene Einschränkung des Auskunftsrechts deutlich stärker zu Lasten des Betroffenen. Es ist überhaupt kein Grund ersichtlich, warum gewöhnliche Behörden, nur weil sie Registerbehörden sind, deutlich stärkere Beschränkungen des Auskunftsrechts für sich in Anspruch nehmen können als außerhalb der Registerlandschaft. Die Begründung schweigt hierzu.

Gerade der Tatbestand der Gefährdung der ordnungsgemäßen Aufgabenerfüllung ist ohne weiteres Korrektiv nahezu uferlos und es ist zu befürchten, dass dieser immer schon dann herangezogen wird, sobald dem Verantwortlichen der Aufwand für die Auskunftserteilung zu groß erscheint.

Beschränkungen der Betroffenenrechte sind nach Art. 23 Abs. 1 DSGVO nur zulässig, wenn diese den Wesensgehalt der Grundrechte achten und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellen. Die vorliegende Regelung setzt sich mit diesen Anforderungen nicht auseinander und auch dazu finden sich in der Begründung keine Anhaltspunkte. Die bloße Aufzählung der einzelnen Tatbestände des Art. 23 Abs. 1 DSGVO genügt keineswegs den Anforderungen, um eine derart weitgehende Einschränkung der Grundrechte zu rechtfertigen. Die in der Begründung (S. 44) für Nr. 1

genannten Buchstaben c, d und h des Art. 23 Abs. 1 DSGVO deuten zwar darauf hin, dass die Beschränkung des Auskunftsrechts dann doch nur bei bestimmten Gefährdungen der Aufgabenerfüllung (öffentliche Sicherheit, Strafverfolgung und -prävention, Aufsichtsfunktionen) gelten soll. Dies spiegelt sich allerdings im Wortlaut des Gesetzestextes nicht wider, sodass in der Praxis deutlich weitergehende Beschränkungen zu befürchten sind.

Im Ergebnis verstößt § 11 Abs. 1 IDNrG-E gegen die DSGVO, da er nicht den Anforderungen des Art. 23 DSGVO entspricht, und ist daher zu streichen.

3.1.7. Zu § 12 IDNrG-E

Die in Satz 2 vorgesehene Löschungsfrist sieht eine sehr weite Spanne vor. Zwischen „unverzüglich“ und 20 Jahre nach dem Tod der betroffenen Person können ggf. mehrere Jahrzehnte liegen. Hier wird angeregt, eine Verkürzung der Maximalfrist zu prüfen.

Der in Satz 3 vorgesehene Löschungstatbestand ist nicht notwendig, da sich diese Anforderung bereits unmittelbar aus der DSGVO ergibt. Sofern er aus Klarstellungsgründen enthalten bleiben sollte, sollte dann aber auch als Löschungsfrist „unverzüglich“ – wie in Art. 17 Abs. 1 DSGVO – festgelegt werden.

3.1.8. Zu § 13 IDNrG-E

In Nr. 1 wird die Bestimmung der Registermodernisierungsbehörde einer Rechtsverordnung überlassen. Hierzu sollte m. E. geprüft werden, ob diese wesentliche Entscheidung nicht unmittelbar im Gesetz getroffen werden muss. Da sich die Bestimmung der Behörde voraussichtlich auch nicht permanent ändern dürfte, wäre dies auch aus dieser Hinsicht unproblematisch.

Naturgemäß kann auf Basis einer Verordnungsermächtigung im Übrigen noch keine inhaltliche Bewertung vorgenommen werden, wenngleich diese aufgrund der erheblichen Datenschutzimplikationen vorliegend zwingend angezeigt ist. Um die datenschutzrechtliche Expertise bei der Schaffung der Verordnung möglichst frühzeitig und möglichst wirksam einzubinden, halte ich es für notwendig, nicht nur den IT-Planungsrat, sondern auch den BfDI bei der Schaffung der Rechtsverordnung zu beteiligen. Ich schlage daher für den Eingangssatz von § 13 IDNrG-E folgende Formulierung vor:

> *„Das Bundesministerium des Innern, für Bau und Heimat wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach dem Benehmen mit*

der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und dem IT-Planungsrat Näheres zu bestimmen…“

3.2. Zu Art. 2 (Änderung des Onlinezugangsgesetzes)

Mit dem Änderungsbefehl Nr. 2 soll das Onlinezugangsgesetz (OZG) um eine weitere Vorschrift ergänzt werden, mit der ein Datencockpit geregelt werden soll. Aufgabe des Datencockpits ist laut Gesetzesbegründung die Information, welche personenbezogenen Daten grundsätzlich zwischen öffentlichen Stellen auf der Grundlage des Identitätsnummerngesetzes (IDNrG) oder des OZG wann und zu welchem Zweck über Betroffene ausgetauscht werden.

Grundsätzlich ist das Anliegen begrüßenswert, für mehr Transparenz gegenüber den Betroffenen durch den Aufbau eines Datencockpits, das eine einfache, nachvollziehbare und zeitnahe Wahrnehmung der Betroffenenrechte nach der DSGVO ermöglichen soll, zu sorgen. Allerdings wirft die vorgesehene Regelung erhebliche Fragen auf.

Mit dem Datencockpit soll die Auskunftsgewährung nach Art. 15 DSGVO digital sichergestellt werden, sofern ein Betroffener dies verlangt. Allerdings räumt Art. 15 DSGVO das Auskunftsrecht der betroffenen Person gegenüber einem (datenschutzrechtlich) Verantwortlichen ein. Aus dem Gesetzentwurf wird nicht ersichtlich, welche öffentliche Stelle das Datencockpit bereitstellt. Hat jede öffentliche Stelle, die Daten über Betroffene nach dem OZG verarbeitet bzw. nach dem IDNrG übermittelt, ein Datencockpit bereitzustellen oder richtet sich die Vorschrift nur an die Registermodernisierungsbehörde nach § 1 Abs. 4 IDNrG-E? Zwar ist in § 1 Abs. 1 Nr. 4 IDNrG-E die Rede davon, allen natürlichen Personen zu ermöglichen, Auskünfte zu Datenübermittlungen zwischen öffentlichen Stellen im Rahmen ihres Auskunftsrechts nach Art. 15 DSGVO auch digital über eine zentrale Stelle zu erhalten. Eine entsprechende Aussage fehlt jedoch in § 10 OZG-E, so dass nicht deutlich wird, ob es nur ein zentrales Datencockpit oder viele dezentrale geben wird.

Einhergehen diese vorstehenden Fragen mit der Frage der datenschutzrechtlichen Verantwortung für das Datencockpit selbst.

Auch wird aus dem Gesetzentwurf noch nicht deutlich, ob das Datencockpit auf Dauer oder nur temporär bereitgestellt wird, d. h. ob eine dauerhafte Speicherung von allen Übermittlungsvorgängen, die sich auf die Betroffenen beziehen, erfolgt oder ob bei jeder einzelnen Auskunftsanfrage die Daten „zusammengesammelt“ und nach Auskunftserteilung sofort gelöscht werden. Damit verbunden ist auch die Frage nach einer doppelten Datenhaltung, die es zu vermeiden gilt, da ansonsten gegen den datenschutzrechtlichen

Grundsatz der Datenminimierung verstoßen würde. Mir ist bewusst, dass über die konkrete Ausgestaltung des Datencockpits noch auf Arbeitsebene beraten wird. Auch dort habe ich mich für eine Lösung ausgesprochen, die auf eine zentrale Datenhaltung verzichtet, da anderenfalls neue Risiken für die Grundrechte bestehen und letztlich eine Vorratsdatenspeicherung erfolgen würde. Angesichts der technischen Schwierigkeiten bei einer Broadcastabfrage aller Register in Echtzeit sollte ein Modell geprüft werden, bei dem die Metadaten von Datenübermittlungen nicht an zentraler Stelle, sondern dezentral in der Verantwortung der registerführenden Behörden gespeichert werden. Die grundsätzlichen Rahmenbedingungen sollten sich dabei so weit wie möglich aus dem Gesetz selbst ergeben.

Zudem sind die wesentlichen Kernelemente zur Ausgestaltung des Datencockpits aufgrund der Wesentlichkeitstheorie gesetzlich zu regeln. Hierzu gehören Regelungen über Verarbeitungsbefugnisse, Zugriffsberechtigungen, Informationspflichten, Zuständigkeiten für die Einrichtung eines Datencockpit, etc.. Die vorgesehene Verordnung, in der die technische Ausgestaltung des Datencockpits im Einvernehmen mit dem IT-Planungsrat festgelegt werden soll, ist hierfür nicht ausreichend.

Das Auskunftsrecht nach Art. 15 DSGVO soll mit dem Datencockpit digital „bedient“ werden. Offen ist, in welcher Form durch das Datencockpit die Anforderungen des Art. 15 DSGVO, insbesondere die Zurverfügungstellung von Kopien nach dessen Absatz 3, erfüllt werden.

Es besteht also erheblicher Nachbesserungsbedarf zu § 10 OZG-E. Ohne eine Beantwortung der hier aufgeworfenen Fragestellungen ist eine abschließende datenschutzrechtliche Bewertung von Art. 2 des Gesetzentwurfs nicht möglich.

3.3. Zu Art. 3 (Änderung der Abgabenordnung)

3.3.1. Allgemeines

Durch die vorgesehenen Änderungen sollen in die Abgabenordnung als Mantelgesetz des Steuerrechts steuerrechtsferne Regelungen zur Vergabe einer Identifikationsnummer für die gesamte öffentliche Verwaltung eingefügt werden. Dies begegnet bereits grundsätzlichen Bedenken im Hinblick auf eine klare, nachvollziehbare und konsistente Regelung, da die Abgabenordnung sich im Übrigen auf steuerliche Regelungen, die für alle oder mehrere Steuerarten gemeinsam gelten, beschränkt (siehe auch oben 2.2.3).

Das BZSt vergibt bisher für steuerliche Zwecke (ganz im Sinne der Abgabenordnung) ein einheitliches Identifikationsmerkmal (Steuer-ID) und ist selbst Finanzbehörde im Sinne des § 6 Abs. 2 AO. Die Steuer-ID soll in erster Linie der Steuerverwaltung ermöglichen, Steuerpflichtige eindeutig zu identifizieren und im Ergebnis die steuerliche Belastungsgleichheit sicherstellen. Diese Regelung ist in sich konsistent und nachvollziehbar.

Nunmehr ist angedacht, dass eine Finanzbehörde (BZSt) die Steuer-ID auch für nicht steuerliche Zwecke vergibt, speichert und weiterverarbeitet. Abgesehen von den verfassungsrechtlichen Bedenken halte ich die Regelung auch insoweit für verfehlt, als dass damit eine Finanzbehörde explizit nicht-steuerliche Zwecke erfüllen soll. Es sollte insbesondere berücksichtigt werden, dass für Datenverarbeitungen der Finanzbehörden spezielle Regelungen in der Abgabenordnung gelten (z.B. § 2a; §§ 29b ff. AO). Die diesen Regelungen zu Grunde liegenden gesetzgeberischen Entscheidungen mit ggf. grundrechteinschränkendem Charakter sind vorrangig vor dem Hintergrund der steuerlichen Zwecke entstanden.

Ich halte daher die Führung der Datenbank zum Zwecke der Schaffung eines einheitlichen ressortübergreifenden Identifikationsmerkmals beim BZSt für systemwidrig. Abgesehen von meinen grundsätzlichen Vorbehalten gegen ein einheitliches Identifikationsmerkmal wäre es konsequenter, dieses von der steuerlichen Regelungssystematik zu trennen. Damit würde die Trennung steuerrechtlicher Verfahren von den übrigen Registerverfahren auch für den Bürger klar erkennbar.

Zumindest müsste klargestellt werden, wann das BZSt als Finanzbehörde tätig wird und wann nicht, da in diesen Fällen unterschiedliche Regelungen zur Verarbeitung personenbezogener Daten zur Anwendung kommen. Außerdem müssten die Zugriffe der Finanzbehörden auf Informationen, die das BZSt für steuerliche Zwecke verarbeitet, begrenzt werden. Es muss sichergestellt werden, dass die Finanzbehörden durch die Ausweitungen der Datenbank keinen erleichterten Zugriff auf Daten erhalten, die für die Besteuerung grundsätzlich nicht erforderlich sind (z. B. Staatsangehörigkeit).

Ausdrücklich wiederum hilfsweise nehme ich zu den geplanten Änderungen der AO im Einzelnen wie folgt Stellung:

3.3.2. Zu Art. 3 Nr. 1

Das BZSt soll nunmehr neben den Steuerpflichtigen „jeder sonstigen natürlichen Person mit Kontakt zu öffentlichen Stellen im Sinne von § 6“ das Identifikationsmerkmal zuteilen. Die Regelung ist zu unkonkret. Zunächst ist unklar, was mit „Kontakt“ gemeint sein soll. Gilt dies u.a. nur für willentlich von der Person vorgenommenen Kontakt oder erfolgt eine

Zuteilung auch ohne Wissen der betroffenen Person. Ggf. sollte hier eine Definition im IDNrG eingefügt werden und darauf verwiesen werden. Außerdem bleibt unklar, welchen Umfang der Verweis auf § 6 AO haben soll. Sollen damit auch Stellen i. S. d. § 6 Abs. 1c, 1d S. 2 und 1e AO gemeint sein? Ich bitte insoweit um Klarstellung.

3.3.3. Zu Art. 3 Nr. 2

Der Datenkranz, der derzeit gemäß § 139b Abs. 3 AO beim BZSt gespeichert wird, soll um die Daten Staatsangehörigkeiten, Datum des letzten Verwaltungskontakts (Monat, Jahr) und Validität der Daten erweitert werden. In der Gesetzesbegründung findet sich dazu die Erläuterung, „soweit diese neuen Daten nicht für die Finanzverwaltung relevant sind, werden sie in diesem Bereich nicht verarbeitet“. Dieser Aussage ist zuzustimmen, jedoch ist dies zwingend in das Gesetz selbst aufzunehmen. In diesem Zusammenhang ist außerdem eine Einschränkung der § 139b Abs. 4 und 5 AO vorzunehmen, da diese bisher unterschiedslos eine Verarbeitung der in § 139b Abs. 3 AO gespeicherten Daten, mithin des gesamten Datenkranzes, zulassen.

3.4. Zu Artikel 6 (Änderung des Ausländerzentralregistergesetzes)

Mit dem Änderungsbefehl Nr. 4 soll ein neuer § 6a eingefügt werden, der die Übermittlung der ID-Nr. regeln soll. Demnach sollen die Meldebehörden die ID-Nr. an die Registermodernisierungsbehörde übermitteln. Sie sollen zu allen Ausländern, die sich bereits im Geltungsbereich dieses Gesetzes befinden, neben der Identifikationsnummer die Grundpersonalien und zum Zwecke der eindeutigen Zuordnung die AZR-Nummer in einem automatisierten Verfahren übermitteln. Diese Regelung scheint systemfremd zu sein, da es sich um eine Übermittlungspflicht der Meldebehörden handelt. Zudem sieht das IDNrG soweit ersichtlich nur einen Datenabruf bei der Registermodernisierungsbehörde vor und keine Datenlieferung durch andere Stellen.

Weiterhin ist nicht erkennbar, welche Regelung mit Satz 1 verfolgt werden soll. So soll nach Satz 1 eine generelle Übermittlung von ID-Nummern erfolgen. Erst in Satz 2 wird eine Beschränkung auf Ausländer vorgenommen. Ist also mit Satz 1 eine generelle Übermittlungspflicht beabsichtigt? Zudem ist nicht klar, wie und wozu die Registermodernisierungsbehörde diese Daten verarbeiten soll. Schließlich ist nicht ersichtlich, wozu die Registermodernisierungsbehörde die AZR-Nummer benötigt.

3.5. Zu Art. 12 (Änderung des SGB VI)

Die in Änderungsbefehl Nr. 2 vorgesehene Einfügung einer Nr. 9 in § 150 Abs. 2 SGB VI wird abgelehnt, da sie überflüssig ist. Das Geburtsdatum wird bereits durch § 150 Abs. 2 Nr. 1 SGB VI erhoben, da sie Teil der RV-Nummer ist.

3.6. Zu Ar. 14 (Änderung des SGB X)

Mit der vorgesehenen Ergänzung eines Absatzes 4 in § 67d SGB X soll die ID-Nr. als Personenkennziffer generell im Bereich des Sozialrechts eingeführt werden. Bislang gab es im Sozialrecht mehrere eindeutige Kennzeichen in den Sozialversicherungsnummern nach dem § 290 SGB V (Krankenversicherungsnummer), § 101 SGB XI (Pflegeversichertennummer) und vor allem nach § 146 SGB VI (Rentenversicherungsnummer). Diese Nummern, die nicht identisch sein durften, wenn auch die Krankenversichertennummer aus der Rentenversicherungsnummer herausgerechnet wird, sind bislang in ihrer Nutzung deutlich durch §§ 18f und 18g SGB IV eingeschränkt.

Diese Einschränkung der Sozialversicherungsnummern wird durch den vorgesehenen § 67d Absatz 4 SGB X nahezu ad absurdum geführt. Es stellt sich die Frage, wozu noch einschränkende Regelungen für Sozialversicherungsnummern erforderlich sind, wenn auch im Sozialrecht die ID-Nr. verwendet werden wird.

Die Änderung lehne ich daher ab.

Mit freundlichen Grüßen

Im Auftrag

Hermerschmidt

Dieses Dokument wurde elektronisch versandt und ist nur im Entwurf gezeichnet.