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]).