Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern

PROF. DR. MARIO MARTINI/DAVID WAGNER/ MICHAEL WENZEL*

Lektorat:
Michael Kolain

Lehrstuhl für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer; Deutsches Forschungsinstitut für öffentliche Verwaltung

Version 1.0

Stand: 17.9.2017

ANSCHRIFT:
PROF. DR. MARIO MARTINI
DEUTSCHE UNIVERSITÄT FÜR VERWALTUNGSWISSENSCHAFTEN SPEYER
LEHRSTUHL FÜR VERWALTUNGSWISSENSCHAFT, STAATSRECHT, VERWALTUNGSRECHT UND EUROPARECHT
http://www.uni-speyer.de/de/lehrstuehle/martini.php
FREIHERR-VOM-STEIN-STRAßE 2
67346 SPEYER

DEUTSCHES FORSCHUNGSINSTITUT FÜR ÖFFENTLICHE VERWALTUNG SPEYER
PROGRAMMBEREICH: „TRANSFORMATION DES STAATES IN ZEITEN DER DIGITALISIERUNG“
http://www.foev-speyer.de/de/forschung/digitalisierung.php
FREIHERR-VOM-STEIN-STRAßE 2
67346 SPEYER

Mario Martini ist Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften Speyer (DUV) und Leiter des Programmbereichs „Digitalisierung“ am Deutschen Forschungsinstitut für öffentliche Verwaltung Speyer (FÖV).
David Wagner und *Michael Wenzel* sind Forschungsreferenten im Programmbereich.

Die Autoren danken *Renana Braun* und *Jonas Ganter* für ihre wertvolle Unterstützung sowie *Michael Kolain* für das sehr gute Lektorat.

Das Gutachten beruht nicht auf einem entgeltlichen Auftrag des Nationalen Normenkontrollrats, sondern ist Teil der allgemeinen Forschungstätigkeit, welche die Deutsche Universität für Verwaltungswissenschaften sowie der FÖV-Programmbereich „Digitalisierung“ als Teil der staatlichen Förderung ihrer Träger wahrnehmen.

Zitierempfehlung:

Martini/Wagner/Wenzel, Rechtliche Grenzen einer Personen- bzw. Unternehmenskennziffer in staatlichen Registern, Speyer, 2017.

Gliederung

Die deutsche Verwaltung schöpft die Potenziale des digitalen Zeitalters noch nicht aus. Nicht nur der Föderalismus, sondern auch datenschutzrechtliche Bedenken erweisen sich oftmals als Hemmschuh.[1] Ein Vergleich mit anderen Ländern, die eine Vorreiterrolle bei der Digitalisierung ihrer staatlichen Leistungen einnehmen, legt für Deutschland Entwicklungsperspektiven offen.[2] Als Ausgangsbasis für die Erfolge vieler Länder im E-Government identifiziert der Nationale Normenkontrollrat ein „modernes, digitales und vernetztes Registerwesen“[3]. Damit trifft er einen neuralgischen Punkt: Register sind eine wichtige Grundlage für automatisierte digitale Verwaltungsverfahren[4] – allerdings nur, wenn die bestehenden unterschiedlichen Register bestmöglich vernetzt und ihre Datenbestände miteinander verzahnt sind.

Zu diesem Ziel können eine allgemeine Personen- (PKZ; unten A.) und Unternehmenskennziffer (UKZ; unten B.) beitragen, sofern sie den datenschutzrechtlichen Anforderungen genügen, welche das nationale Recht und das Unionsrecht an die Datenverarbeitung öffentlicher Stellen richten. Die Potenziale und Risiken einer allgemeinen Kennzahl – insbesondere für den Datenabgleich staatlicher Register und für Datenabfragen für statistische Zwecke in den Blick zu nehmen, macht sich dieses Werk zur Aufgabe.

A. Zulässigkeit einer Personenkennziffer

I. Gesellschaftlicher, staatspolitischer und historischer Hintergrund

1. Funktionen und Vorteile einer Personenkennziffer

Eine PKZ ermöglicht den Behörden, Verwaltungsvorgänge eindeutig einer bestimmten Person zuzuordnen (Identifizierungsfunktion); sie repräsentiert den einzelnen Bürger innerhalb eines Systems, etwa einer Datenbank (Repräsentationsfunktion), und trifft eine Aussage über seine Einordnung in ein bestimmtes Bezugssystem (Ordnungsfunktion).[5] Aufgrund dieser Eigenschaften kann die PKZ entscheidend dazu beitragen, Erfassungs-, Übertragungs- und Zuordnungsfehler in staatlichen Registern zu vermeiden.[6] Andere Ordnungsmerkmale (z. B. eine Kombination aus Name und Adresse) lassen für sich genommen eine eindeutige Identifizierung hingegen nicht stets zu, da sie mehrfach vorkommen oder wechseln können.

---

[1] Dazu bspw. *Martini*, DÖV 2017, 443 ff.
[2] Ausführlich hierzu *Martini* (Fn. 1), 443 ff. m. w. N.
[3] *Nationaler Normenkontrollrat*, Leistungsbeschreibung NKR Gutachten 2017, 2017, S. 1.
[4] Vgl. *McKinsey & Company Inc.*, Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren, Okt. 2017, S. 14 f.; vgl. dazu auch das estnische Registerverknüpfungsverfahren der „X-Road“, *Beck/Hilgers et al.*, Digitale Transformation der Verwaltung, 2017, S. 16 ff.
[5] *von Lewinski*, in: Wolff/Brink (Hrsg.), BeckOK DatenschutzR, 19. Ed., Stand: 2017, Art. 87 DSGVO, Rn. 3 ff. Siehe auch *Gola*, in: ders. (Hrsg.), DS-GVO, 2017, Art. 87, Rn. 1.
[6] *Weichert*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2017, Art. 87, Rn. 5.

Die Vorzüge einer allgemeinen PKZ prädestinieren sie als zentralen Baustein einer Registermodernisierung in der Bundesrepublik Deutschland:[7] Sie ermöglicht es, Datensätze aus verschiedenen Registern[8] miteinander zu vernetzen und deren Inhalte für konkrete Verwaltungsverfahren zu synchronisieren. Mit Hilfe einer PKZ kann die öffentliche Verwaltung Register abgleichen und Fehler in einzelnen Registern identifizieren. Dadurch schafft sie Korrekturmöglichkeiten und steigert die Registerqualität.[9] Ein Registerabgleich kann bspw. offenbaren, dass die Informationen, die eine Behörde zur Durchführung eines Fachverfahrens benötigt, bei der anderen Behörde entweder bereits vorhanden und dort zum Abruf direkt aus dem betreffenden staatlichen Register[10] zur Verfügung stehen – oder dort fehlerhaft gespeichert sind und daher einer Anpassung bedürfen. Gerade bei automatisierten Datenabrufen wirkt die PKZ aufgrund ihrer Eignung, die betreffende Person in binären Prozessen eindeutig zu identifizieren und zu repräsentieren, vereinfachend und fehlerminimierend. Von inhaltlich richtigen Informationen in staatlichen Registern profitieren im Ergebnis alle Stellen, die darauf zugreifen. Hinzu kommen nachhaltige Einsparpotenziale für das Gemeinwesen.[11]

Die PKZ lässt sich aber nicht nur zum Registerabgleich und zum punktuellen Datenaustausch einsetzen. Das zeigt das Beispiel des registergestützten Zensus[12]: Die Ordnungsnummer, welche § 13 ZensG 2011 etabliert hat, ermöglicht – im Interesse der amtlichen Statistik – die Zusammenführung der Daten aus verschiedenen Registern zu einer neuen Erkenntnisquelle (vgl. insofern bereits § 13 Abs. 2 i. V. m. § 9 ZensG 2011). Der Zensus schöpft somit im doppelten Sinne aus einer Ordnungsnummer: Zum einen optimiert sie die erforderliche Registerqualität; zum anderen erleichtert sie dessen Durchführung.

2. Spannungslagen zum Persönlichkeitsschutz

Eine allgemeine PKZ verheißt zwar, dass eine Behörde Daten, die bei verschiedenen Stellen verstreut vorhanden sind, effizient für ein bestimmtes Fachverfahren abrufen kann. Zugleich löst sie Registerdaten unweigerlich aus ihrem bisherigen Verwendungskontext: Tauschen staatliche Stellen Daten aus, so führen sie Daten, die für bestimmte Zwecke erhoben wurden, neuen Nutzungszwecken zu, nutzen diese also für unterschiedliche Kontexte. Dies gleicht im

---

[7] Sie ist im föderalen Deutschland freilich kein Allheilmittel. Vgl. *Statistisches Bundesamt*, Beistellung zum Gutachten "Registermodernisierung" im Auftrag des Nationalen Normenkontrollrats, 2017, S. 68: „Unabhängig von der Führung der Register im technischen Sinn erwies sich sowohl in Österreich als auch in der Schweiz die Harmonisierung von Merkmalen, Ausprägungen und Definitionen der verschiedenen Register als zentraler Erfolgsfaktor".

[8] Für den Austausch von Basisdaten bedarf es keiner zentralisierten Registerlandschaft. Vgl. *McKinsey & Company Inc.* (Fn. 4), S. 36: „Das Beispiel der Schweiz zeigt, dass auch dezentrale Führung mit gemeinsamen Standards für Inhalte und Form bei hoher Qualität möglich ist."

[9] Vgl. *McKinsey & Company Inc.* (Fn. 4), S. 24.

[10] Zur Idee, für bestimmte Daten – etwa Meldeadresse oder Informationen über Betriebsinhaber – jeweils ein „Leitregister" zu definieren *McKinsey & Company Inc.* (Fn. 4), S. 44.

[11] Ausführlicher hierzu S. 22.

[12] Das ZensG 2011 definiert den Zensus in § 1 Abs. 1 legal als Durchführung einer Bevölkerungs-, Gebäude- und Wohnungszählung durch die Statistikbehörden.

Ergebnis einer Direkterhebung für eine Mehrzahl an Zwecken und löst dadurch Spannungslagen mit dem datenschutzrechtlichen Zweckbindungsgrundsatz[13] aus.

Ein großflächiger Einsatz der PKZ in der deutschen Verwaltung ebnet einer Vielzahl von Zuordnungsmöglichkeiten persönlicher Daten, die in den verschiedenen Registern gespeichert sind, den Weg – darunter auch besonders sensiblen Daten, wie ethnischer Herkunft oder Gewerkschaftszugehörigkeit (vgl. Art. 9 DSGVO). Dass die PKZ nach ihrem inneren Anspruch künftig alle bei der Verwaltung vorrätigen personenbezogenen Bürgerdaten potenziell verknüpfbar macht, birgt ein erhebliches Risiko für das informationelle Selbstbestimmungsrecht: Auf ihrer Grundlage könnte die Verwaltung schlimmstenfalls umfassende Persönlichkeitsprofile erstellen und die Bevölkerung umfassend überwachen. Im Extremfall droht eine datengestützte Vermessung der Persönlichkeit jedes einzelnen Bürgers, die tief in seine grundrechtlich geschützte Freiheitssphäre hineinwirkt.[14]

3. Historischer Hintergrund und internationaler Stand der Entwicklung

Ein Blick über den „nationalen Tellerrand“ zeigt: In anderen westlichen Industriestaaten ist der Einsatz allgemeiner Personenkennziffern üblich.[15] In Deutschland kommt eine PKZ demgegenüber bislang nur in bestimmten administrativen Teilbereichen zum Einsatz.[16] Denn die Sensibilität einer Ordnungsnummer, die einzelne Menschen für den Staat individuell erfassbar macht, ist tief im kollektiven Bewusstsein der Deutschen verankert. Als „Häftlingsnummer“ in Konzentrationslagern während der NS-Zeit sowie als „Personenkennzahl“ in der DDR hat sie traurige Berühmtheit erlangt.[17] Vor diesem Hintergrund werden viele Betroffene die Einführung einer PKZ mit dem Versuch assoziieren, den Menschen zu einem reinen Objekt staatlicher Machtausübung zu degradieren.

Die Diskussion um die Einführung einer PKZ ist in Deutschland nicht neu. Bereits in den 70er Jahren stand das Thema auf der Agenda des Bundesministeriums des Innern und des Parlaments.[18] Schon zur damaligen Zeit beherrschten aber verfassungsrechtliche Bedenken

---

[13] Dazu aus unionsrechtlicher Sicht näher unten S. 11 ff.
[14] Vgl. dazu auch *Schaar*, ZD 2011, 49 (49 f.).
[15] Siehe *Weichert* (Fn. 6), Art. 87, Rn. 12; *Ehmann*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2017, Art. 87, Rn. 2.
[16] Etwa die Steueridentifikationsnummer (Steuer-ID) im Rahmen des Steuerverfahrens (§ 139a. 139b AO), die Krankenversicherungsnummer (§ 290 SGB V) und die Rentenversicherungsnummer (§ 147 SGB VI), vgl. *von Lewinski*, in: Wolff/Brink (Hrsg.), BeckOK DatenschutzR, 20. Ed., Stand: 1.5.2017, Art. 87 DSGVO, Rn. 54 ff. Als solche bezeichnete „Personenkennziffern“ vergibt die Wehrverwaltung, um Soldaten eindeutig zu identifizieren – ebenso das Bundesamt für Migration und Flüchtlinge bei der Antragstellung zum Integrationskurs. Um eine *allgemeine* PKZ handelt es sich in diesen Fällen aber nicht. Denn die Kennziffern kommen dort nur bereichsspezifisch zum Einsatz. Ausführlicher zu solchen bereichsspezifischen Personenkennziffern (bPKZ) – im Kontext des österreichischen PKZ-Modells – unten S. 36 ff.
[17] *Weichert* (Fn. 6), Art. 87, Rn. 13.
[18] Das Bundesministerium des Innern veröffentlichte sogar eine ausführliche Informationsbroschüre, um das Thema in die Bevölkerung zu tragen. Bundesinnenminister *Genscher* schrieb im Vorwort: „Die vorliegende Schrift will über die Planungen der Bundesregierung im Zusammenhang mit der Einführung eines Personenkennzeichens aufklären. Sie soll zum Verständnis verhelfen, daß diese Maßnahme nicht nur der

gegen eine Datenverarbeitung mittels PKZ die Diskussion, die – befeuert durch die Aussagen des BVerfG im Volkszählungsurteil[19] – bis heute aktuell geblieben sind. 1976 waren sie der Grund dafür, dass das bereits angelaufene Gesetzgebungsverfahren zur Einführung einer PKZ im Meldegesetz ein abruptes Ende fand. Prominent artikuliert hatte die Einwände seinerzeit der Rechtsausschuss des Bundestages im Zuge der parlamentarischen Beratung des Bundesdatenschutzgesetzes.[20]

Auf diese Weise mutierte die PKZ im Laufe der Jahre schleichend zum rechtspolitischen Tabubegriff. Mit ihr verknüpft sich die (unserer freiheitlich-demokratischen Rechtsordnung fremde) Vorstellung, dass Behörden Daten über Bürger systematisch zusammenführen, um auf dieser Grundlage gezielt in deren Sphäre privater Lebensgestaltung vorzudringen und das Innerste ihrer Persönlichkeit auszuleuchten. Das Verfahren, mit dessen Hilfe die chinesische Regierung in ausgewählten Regionen die soziale Zuverlässigkeit anhand eines Score-Wertes misst, entwirft insoweit – neben den Erinnerungen aus der NS-Zeit und der DDR – eine abschreckende Kontrastfolie: Es greift zur Identifikation der Betroffenen auf eine Kennziffer zurück.[21]

Der schwere Stand, den die Idee einer PKZ in Deutschland normativ hat, ist vor diesem Hintergrund auch im digitalen Zeitalter nicht weiter verwunderlich.

4. Überblick über den normativen Handlungsrahmen

Der Handlungsrahmen des deutschen Gesetzgebers, eine PKZ einzuführen, ist aus normativer Sicht von zwei Seiten her begrenzt: durch die Datenschutz-Grundverordnung (DSGVO)[22] einerseits (dazu unter II.) und das nationale Verfassungsrecht andererseits (dazu unter III.).

Das Datenschutzrecht ist fest in der Hand des Unionsgesetzgebers (vgl. Art. 16 Abs. 2 AEUV[23]): Er ist es, der über die Reichweite des Persönlichkeitsschutzes bei der Verarbeitung personenbezogener Daten befindet. Die DSGVO füllt die abstrakten Vorgaben des Art. 16 Abs. 1 AEUV sowie des Art. 8 GRCh[24] ab dem 25.5.2018 grundsätzlich abschließend aus (vgl. Art. 99 Abs. 2 DSGVO). Als Verordnung gilt sie in den Mitgliedstaaten unmittelbar und bedarf grundsätzlich keines Umsetzungsaktes des nationalen Gesetzgebers (Art. 288 Abs. 2 AEUV).

Verwaltung nützt, sondern daß sie im allgemeinen Interesse liegt und jeden Bürger angeht, ihm unmittelbar oder mittelbar Vorteile bringt.“, *Bundesministerium des Innern*, Personenkennzeichen, 1971, S. 3.

[19] BVerfGE 65, 1 ff.

[20] Vgl. dazu *Weichert* (Fn. 6), Art. 87, Rn. 21; *Zelyk*, Das einheitliche steuerliche Identifikationsmerkmal, 2012, S. 7 f.

[21] Siehe dazu *Hanfeld*, Punkte für gefälliges Verhalten, faz.net vom 10.10.2015; *Warislohner*, Dystopia wird Wirklichkeit: Was ist dran an Chinas „Social Credit System“?, netzpolitik.org vom 9.10.2015.

[22] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) v. 27.4.2016, ABl. Nr L. 119/1.

[23] Vertrag über die Arbeitsweise der Europäischen Union in der Fassung der Bekanntmachung v. 9.5.2008, ABl. Nr. C 115/47.

[24] Charta der Grundrechte der Europäischen Union v. 12.12.2007, ABl. Nr. C 303/1.

Der Persönlichkeitsschutz im Mehrebenensystem verlagert sich damit maßgeblich auf die Grundrechtskontrollmacht des EuGH. Das BVerfG verzichtet im Rahmen eines „Kooperationsverhältnisses“[25] zum EuGH grundsätzlich auf eine eigene verfassungsrechtliche Überprüfung abgeleiteten Unionsrechts.[26] Die Konformität mit deutschen Grundrechten prüft das BVerfG allerdings dann detailliert, wenn das Unionsrecht dem Mitgliedstaat einen eigenen (Umsetzungs-)Spielraum belässt: Der parlamentarische Gesetzgeber muss diesen ausfüllen, ohne die Grenzen der nationalen Verfassung zu überschreiten.[27] Zugleich ist der eigene Handlungsbereich des Mitgliedstaats bei Verordnungen aufgrund ihrer unmittelbaren Wirkung aber wesensgemäß sehr schmal. Die deutschen Grundrechte sind bei Verordnungen daher grundsätzlich kein maßgeblicher Prüfungsmaßstab.[28]

Die DSGVO ist aber materiell keine Verordnung reinsten Wassers. Bei genauer Betrachtung ihrer Regelungstechnik präsentiert sie sich, gerade in Bezug auf den öffentlichen Bereich, als ein Handlungsformenhybrid.[29] Sie hält zahlreiche Öffnungsklauseln vor, die den nationalen Gesetzgeber zum eigenen Handeln, etwa zur Abweichung von den Vorgaben der Verordnung (z. B. Art. 12-22 i. V. m. Art. 23 DSGVO), ermächtigen.[30] Das eröffnet dem deutschen Gesetzgeber in vielen Fällen einen Spielraum, in dessen Rahmen er selbstständig regelnd tätig werden darf. Das gilt auch für die Vorschrift der DSGVO, die für die Implementierung einer PKZ maßgeblich ist: die Vorschrift des Art. 87 DSGVO. Insoweit muss sich daher auch die Einführung und Nutzung einer PKZ am deutschen Verfassungsrecht messen lassen.[31]

II. Unionsrechtliche Grenzen

Ebenso wie die Daten, auf die sie Bezug nimmt, ist die PKZ ihrerseits ein personenbezogenes Datum i. S. d. Art. 4 Nr. 1 DSGVO (vgl. auch ErwGr. 30 S. 2 DSGVO).[32] Ihre Einführung und Verarbeitung bewegt sich daher innerhalb des Bereichs, für den die DSGVO einen Regelungsanspruch reklamiert.

---

[25] BVerfGE 89, 155 (175).
[26] Siehe die Rekapitulation der eigenen Judikatur des BVerfG in BVerfGE 102, 147 (161 ff.).
[27] BVerfGE 121, 1 (15), st. Rspr.
[28] Vgl. *Augsberg*, DÖV 2010, 153, 155.
[29] Vgl. dazu *Kühling/Martini*, EuZW 2016, 448 (449); die Europäische Kommission scheint indes davon auszugehen, dass vermeintliche Öffnungsklauseln allenfalls Raum für nationale Spezifizierungen lassen, siehe *Greis*, EU-Kommission lehnt deutschen Sonderweg ab, golem.de vom 21.4.2017.
[30] Ausführlich hierzu *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 1 ff.
[31] Dazu unten S. 19.
[32] *von Lewinski* (Fn. 16), Art. 87 DSGVO, Rn. 19. Zwar lässt die Ziffernfolge nicht unmittelbar auf eine bestimmte Person rückschließen (es sei denn, es handelt sich um eine sog. sprechende Nummer, vgl. *Weichert* (Fn. 6), Art. 87, Rn. 16; siehe auch unten S. 9), sodass die PKZ isoliert betrachtet zunächst kein tauglicher Anknüpfungspunkt datenschutzrechtlicher Regulierung ist. Durch die Verknüpfung der PKZ mit dem Namen bzw. der Identität der jeweiligen Person wird sie gleichwohl zu einem personenbezogenen Datum (und damit Regelungsgegenstand der DSGVO). Dann ist die PKZ selbst ein personenbezogenes Datum, das Objekt eines Verarbeitungsvorgangs sein kann.

1. Spezifische unionsrechtliche Vorgaben: Grenzen für die Mitgliedstaaten zur Verarbeitung einer nationalen Kennziffer – Art. 87 DSGVO

a) Regelungsinhalt

Art. 87 S. 1 DSGVO erlaubt es den Mitgliedstaaten, nähere Regelungen zur Verarbeitung einer nationalen Kennziffer (Art. 87 S. 1 Alt. 1 DSGVO) oder anderer Kennzeichen von allgemeiner Bedeutung (Art. 87 S. 1 Alt. 2 DSGVO) zu erlassen. *Expressis verbis* ermächtigt Art. 87 S. 1 DSGVO die Mitgliedstaaten zur Konkretisierung („können näher bestimmen"). Implizit räumt er ihnen zugleich die Befugnis ein, Kennziffern beizubehalten oder einzuführen,[33] verpflichtet sie hierzu aber nicht[34]. Von der Warte des Unionsrechts aus betrachtet, steht es jedem Mitgliedstaat also frei, ob er überhaupt rechtsetzend aktiv werden möchte.

Zwar kennt die Bundesrepublik aktuell noch kein alle Lebensbereiche umspannendes Kennzeichen von allgemeiner Bedeutung; Verwendung finden lediglich sektorielle Personenkennzeichen.[35] Sollte der nationale Gesetzgeber eine registerübergreifende PKZ einführen, entstünde ein solches Kennzeichen jedoch – mitsamt der ihm anhaftenden persönlichkeitsrechtlichen Sensibilität. Denn eine allgemeine PKZ soll gerade für eine möglichst große Vielzahl von Verarbeitungszusammenhängen Verwendung finden.[36]

Führt der Staat eine allgemeine PKZ ein, muss er sie jedoch durch Vorschriften flankieren, welche die Voraussetzungen festlegen, unter denen der Staat sie rechtmäßig verarbeiten darf.[37] Art. 87 S. 2 DSGVO gibt den Mitgliedstaaten insofern – ähnlich wie die Öffnungsklausel des Art. 22 Abs. 2 lit. b – auf, geeignete Garantien bzw. Maßnahmen bei der Ausgestaltung des gesetzlichen Verarbeitungsrahmens vorzusehen, welche die Rechte und Freiheiten der Betroffenen schützen.

Ob Garantien „geeignet" sind, ist autonom unionsrechtlich zu bestimmen, ergibt sich also nicht aus Traditionen und Verständnissen des nationalen Rechts.[38] Die ergriffenen Maßnahmen dürfen jedenfalls nicht hinter dem Schutzniveau zurückbleiben, welches die DSGVO mit Blick auf Art. 8 Abs. 1 GrCh sowie Art. 16 Abs. 1 AEUV als Mindestgewährleistung des Schutzes für den Schutz des informationellen Selbstbestimmungsrechts unionsweit

---

[33] *Grages*, in: Plath (Hrsg.), BDSG/DSGVO, 2. Aufl., 2016, Art. 87 DSGVO, Rn. 1.
[34] *von Lewinski* (Fn. 16), Art. 87 DSGVO, Rn. 39.
[35] Vgl. *von Lewinski* (Fn. 16), Art. 87 DSGVO, Rn. 53 sowie bereits Fn. 16. Gemessen am unionsrechtlichen Maßstab „von allgemeiner Bedeutung" (Art. 87 S. 1 DSGVO) können aber auch sektorielle PKZ unter den Begriff „Kennzeichen von allgemeiner Bedeutung" fallen; in diesem Sinne *Ehmann* (Fn. 15), Art. 87, Rn. 5.
[36] Zu der Abgrenzung der beiden Tatbestandsalternativen siehe *von Lewinski* (Fn. 16), Art. 87 DSGVO, Rn. 26 ff. sowie *Weichert* (Fn. 6), Art. 87, Rn. 8 ff. Da an die Einordnung eines Kennzeichens als „nationale Kennziffer" oder als „Kennzeichen von allgemeiner Bedeutung" keine unterschiedlichen Rechtsfolgen geknüpft sind, ist eine Abgrenzung grundsätzlich auch lediglich von akademischem Interesse.
[37] *Grages* (Fn. 33), Art. 87 DSGVO, Rn. 2.
[38] *von Lewinski* (Fn. 16), Art. 87 DSGVO, Rn. 44. Laut *Gola* (Fn. 5), Art. 87, Rn. 5 müssen die Garantien in der Lage sein, die vom BVerfG im Volkszählungsurteil beschriebenen Gefahren zu bannen.

etablieren will.[39] Diese normative Forderung der DSGVO treibt die Sorge um, dass die unionale Datenschutzlandschaft eine (weitere) Fragmentierung erfährt, wenn die Mitgliedstaaten in sehr unterschiedlicher Weise von Öffnungsklauseln Gebrauch machen. Art. 87 DSGVO gibt den Mitgliedstaaten daher – im Duktus einer Richtlinie – ein zu erreichendes Ziel vor und überlässt ihnen die Wahl der Mittel.[40]

b) Das Schutzniveau der DSGVO als Grenze des mitgliedstaatlichen Spielraums

Das Schutzniveau, das zu gewährleisten, Art. 87 S. 2 DSGVO den Mitgliedstaaten aufgibt, speist sich primär aus den einzelnen Verarbeitungsvorgaben der DSGVO, insbesondere den allgemeinen Grundsätzen des Art. 5 DSGVO (vor allem dem Gebot der Datenminimierung als spezieller Ausprägung des Verhältnismäßigkeitsprinzips, dem Gebot der Zweckbindung und der Transparenz) sowie ihren spezialgesetzlichen Ausformungen, in Verbindung mit den Rechten Betroffener (Art. 12-22 DSGVO) sowie den Verpflichtungen der Datenverarbeiter (Art. 24 ff. DSGVO).[41]

2. Allgemeine Vorgaben der DSGVO für die Verarbeitung einer Personenkennziffer

Für die Zuteilung der PKZ (a) sowie für deren Nutzung im Rahmen des interbehördlichen Datenaustauschs (b) hält die DSGVO jeweils unterschiedliche allgemeine Maßgaben bereit, welche den Verarbeitungsvorgang determinieren.

a) Zuteilung der Personenkennziffer und Verknüpfung mit personenbezogenen Daten

Den Startpunkt zur Einführung einer PKZ markiert ihre Zuteilung an jeden Bürger. Verbindet die Verwaltung bereits vorhandene personenbezogene Daten mit der PKZ als neuer zusätzlicher Information, verarbeitet sie jene Daten im Sinne der DSGVO (vgl. die Legaldefinition von „Verarbeitung“ in Art. 4 Nr. 2 DSGVO[42]).[43] Finden später weitere Daten zur

---

[39] Vgl. *Pauly*, in: Paal/Pauly (Hrsg.), DS-GVO, 2017, Art. 87, Rn. 3.
[40] Vgl. auch *Ehmann* (Fn. 15), Art. 87, Rn. 6.
[41] Berücksichtigung müssen aber auch die normativen Vorgaben sie betreffender Öffnungsklauseln (in Gestalt von Abweichungsmöglichkeiten) finden. Das wichtigste Beispiel hierfür markiert Art. 23 DSGVO. Zwar verbürgt die DSGVO in ihren Art. 12 bis 22 verschiedene Betroffenenrechte sowie Pflichten von Verantwortlichen und Auftragsverarbeitern. Das Mindestmaß an Datenschutz bestimmen jedoch nicht (nur) diese Vorschriften, sondern maßgeblich auch Art. 23 DSGVO, der durch spezifische Vorgaben die Grenze für mitgliedstaatliche Beschränkungen der in den Art. 12 bis 22 DSGVO genannten Rechte und Pflichten absteckt.
[42] Die umfangreiche Aufzählung des Art. 4 Nr. 2 DSGVO lässt sich als Beleg dafür verstehen, dass grundsätzlich „jede Form der Behandlung von personenbezogenen Daten“ eine Verarbeitung im Normsinne darstellt, vgl. *Schreiber*, in: Plath (Hrsg.), BDSG/DSGVO, 2. Aufl., 2016, Art. 4 DSGVO, Rn. 12.
[43] Jedenfalls der Auffangtatbestand einer „Verwendung personenbezogener Daten“ im Sinne eines „zweckgerichteten Gebrauchs“ (vgl. *Ernst*, in: Paal/Pauly (Hrsg.), DS-GVO, 2017, Art. 4, Rn. 29) ist einschlägig. Teilt der Staat jedem Bürger eine PKZ zu, beschafft er nicht im eigentlichen Sinne personenbezogene Daten, sodass sich nicht bereits aus Art. 13 Abs. 1 DSGVO eine Informationspflicht des Verantwortlichen ergibt. Stattdessen entsteht ein neues personenbezogenes Datum. In der Sache findet durch die Zuteilung lediglich eine Verarbeitung der bereits erhobenen personenbezogenen Daten statt, indem ihnen eine neue Information hinzugefügt wird. Jedoch führt die Verbindung mit der PKZ die bereits erhobenen Daten einem neuen Zweck zu.

betreffenden Person Aufnahme in ein Register, geht damit unweigerlich zugleich eine Verknüpfung dieser Daten mit der PKZ einher. Rechtstechnisch liegt dann eine erneute Datenverarbeitung im Sinne der DSGVO vor.

aa) Verarbeitungsgrundlage

Jede Form der Verarbeitung personenbezogener Daten bedarf einer gesetzlichen Erlaubnis: Art. 6 DSGVO statuiert – wie auch schon das deutsche BDSG (§ 4 Abs. 1 BDSG)[44] – ein sog. Verbot mit Erlaubnisvorbehalt.[45] Die Öffnungsklausel des Art. 87 S. 1 DSGVO eröffnet jedem Mitgliedstaat die Möglichkeit, die notwendige gesetzliche Verarbeitungsgrundlage selbst zu schaffen.

Nicht nur die Zuteilung der PKZ an jeden Bürger, sondern auch die Verarbeitung der für die Zuordnung der PKZ zu der betroffenen Person notwendigen (Stamm-)Daten darf der nationale Gesetzgeber auf der Grundlage der Öffnungsklausel des Art. 87 S. 1 DSGVO regeln – jedenfalls soweit es sich dabei um einen notwendigen Zwischenschritt zur Zuteilung der PKZ handelt.[46] Selbst wenn man dies anders sehen wollte, könnte der Mitgliedstaat eine Norm, welche die Verbindung vorhandener Daten mit der PKZ regelt, hilfsweise auch auf die allgemeinere Öffnungsklausel des Art. 6 Abs. 3 S. 1 DSGVO stützen. Sie ermächtigt die Mitgliedstaaten – verkürzt ausgedrückt – zu eigenen Regelungen für die Datenverarbeitung im öffentlichen Bereich.

bb) Vorgaben der DSGVO hinsichtlich der Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO)

Die Verarbeitung besonderer Kategorien personenbezogener Daten, wie etwa der ethnischen Herkunft, verbietet die DSGVO grundsätzlich (Art. 9 Abs. 1 DSGVO). Ausnahmen sind nur aufgrund der in Art. 9 Abs. 2 DSGVO normierten Tatbestände zulässig.[47]

Die Verbindung einer PKZ mit besonderen Kategorien personenbezogener Daten ist vor diesem Hintergrund besonders heikel. Will die Verwaltung solche Daten mit einer PKZ verknüpfen, muss sie genau prüfen, ob und inwieweit die Union dafür (ggf. im Verbund mit dem nationalen Recht) insbesondere „aus Gründen eines erheblichen öffentlichen Interesses“ (Art. 9 Abs. 2 lit. g DSGVO) den Weg freimacht.

Eine PKZ als solche zählt nicht zu den besonderen Kategorien personenbezogener Daten. Eine entsprechende Einordnung trifft die DSGVO in ihrem Art. 9 gerade nicht – anders als die

---

Die Verwaltung trifft daher eine Informationspflicht gemäß Art. 14 Abs. 4 DSGVO. Zudem verleiht Art. 15 DSGVO dem Betroffenen ein datenschutzrechtliches Auskunftsrecht. Auch hierüber kann er erfragen, ob die Verwaltung ihm eine PKZ zugewiesen hat und welche Daten ihr zugeordnet sind.

[44] Siehe nur *Gola/Klug et al.*, in: Gola/Schomerus (Hrsg.), BDSG, 12. Aufl., 2015, § 4, Rn. 3.

[45] Dazu *Buchner/Petri*, in: Kühling/Buchner (Hrsg.), DS-GVO, 2017, Art. 6, Rn. 11 ff.

[46] Vgl. auch unten S. 11 zur Übermittlung der PKZ.

[47] *Schulz*, in: Gola (Hrsg.), DS-GVO, 2017, Art. 9, Rn. 1.

bisherige Datenschutzrichtlinie, welche die Verarbeitung einer PKZ noch systematisch im Rahmen der „Verarbeitung besonderer Kategorien personenbezogener Daten" geregelt hat (vgl. Art. 8 Abs. 7 RL 95/46/EG). Nichtsdestotrotz verarbeitet eine PKZ aufgrund ihrer instrumentellen Funktion ein sehr sensibles personenbezogenes Datum,[48] lässt sie sich doch als Mittel zur Verknüpfung anderer personenbezogener Daten und ihrer eindeutigen Zuordnung zu einer Person nutzen.[49]

Die Gründe, welche die PKZ als Schlüsselelement der Registermodernisierung erscheinen lassen, sind also zugleich die Ursache für ihre persönlichkeitsrechtliche Sensibilität. Das damit einhergehende Gefahrenpotenzial für das informationelle Selbstbestimmungsrecht Betroffener fängt die DSGVO aber nicht über Art. 9 DSGVO ein. Art. 87 DSGVO adressiert es vielmehr in einer eigenständigen Regelung, welche die Zuständigkeit für die Regulierung der PKZ den Mitgliedstaaten zuweist.

cc) Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO)

Der Verwendung eines sog. sprechenden Kennzeichens, also einer PKZ, die sich aus personenbezogenen Daten der Person (z. B. den Initialen des Namens und dem Geburtsdatum) zusammensetzt[50], zieht der Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) Grenzen: [51] Verantwortliche dürfen personenbezogene Daten nur dann verarbeiten, wenn dies erforderlich ist, um den Verarbeitungszweck zu erreichen.[52] Darüber hinaus muss der Verarbeitungsvorgang zweckangemessen sein, d. h. die mit ihnen verbundene Beeinträchtigung des informationellen Selbstbestimmungsrechts darf nicht in einem Missverhältnis zu den legitimen Zwecken stehen, die er verfolgt.[53]

Aufgrund des in ihm angelegten Aussagegehalts erlaubt ein sprechendes Kennzeichen Rückschlüsse auf personenbezogene Sachverhalte, die über den originären Zweck der Verarbeitung hinausreichen können. Jedenfalls für Zwecke der Registeroptimierung ist dies nicht erforderlich. Wenn überhaupt, ist eine PKZ grundsätzlich nur in einer Weise zulässig, die keinen unmittelbaren Rückschluss auf die Identität des Betroffenen zulässt.[54]

---

[48] Vgl. auch *von Lewinski* (Fn. 16), Art. 87 DSGVO, Rn. 20, der ihr daher eine inhaltliche Nähe zu den besonderen Kategorien personenbezogener Daten attestiert.
[49] Zur Funktion der PKZ siehe oben S. 1 f.
[50] *Ehmann* (Fn. 15), Art. 87, Rn. 2; *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*, Verkettung digitaler Identitäten, 2007, S. 81. Eine solche ist etwa die Personenkennziffer der Bundeswehr (PK). Für den Bereich der Wehrverwaltung findet die DSGVO allerdings keine Anwendung, vgl. *von Lewinski* (Fn. 16), Art. 87 DSGVO, Rn. 34 ff.
[51] *Weichert* (Fn. 6), Art. 87, Rn. 16.
[52] Vgl. *Plath*, in: ders. (Hrsg.), BDSG/DSGVO, 2. Aufl., 2016, Art. 5 DSGVO, Rn. 10; *Schantz*, in: Wolff/Brink (Hrsg.), BeckOK DatenschutzR, 20. Ed., Stand: 1.5.2017, Art. 5 DSGVO, Rn. 25.
[53] Vgl. zu dieser normativen Vorgabe auch *Schantz* (Fn. 52), Art. 5 DSGVO, Rn. 26.
[54] Die normative Einschränkung des § 139a Abs. 1 S. 2 AO, dass Identifikationsmerkmale (namentlich die Steuer-ID sowie eine Wirtschafts-Identifikationsnummer) „nicht aus anderen Daten über den Steuerpflichtigen gebildet oder abgeleitet werden darf", ist daher normativ konsequent und sachgerecht.

Das Gebot der Datenminimierung entfaltet seine begrenzende Wirkung auch und insbesondere bei einem (ggf. durch eine PKZ unterstützten) Auskunftsersuchen einer Behörde bei einer anderen: Der Grundsatz der Begrenzung auf das notwendige Maß[55] gebietet es, Daten nur in dem Umfang abzufragen, wie es zur Bearbeitung der konkreten behördlichen Aufgabe notwendig ist. Die Behörde darf daher nur diejenigen Daten bei einer anderen Behörde automatisiert abrufen, die zur Durchführung des betreffenden Fachverfahrens (z. B. der Gewährung einer bestimmten staatlichen Leistung) vonnöten sind. Ein Datenabruf, der über dieses Maß hinausgeht, ist untersagt. Dies trägt zugleich dazu bei, zu verhindern, dass die abrufende Behörde nicht anlasslos Daten unter der PKZ sammelt. Ebenso wenig ist es mit dem Gebot der Datenminimierung zu vereinbaren, dass die empfangende Behörde abgerufene Daten länger speichert, als dies für ihre Aufgabenerfüllung erforderlich ist.

Den Anforderungen der Datenminimierung muss der Verantwortliche nicht nur durch technische Maßnahmen (Art. 25 Abs. 1 DSGVO[56]) genügen, sondern insbesondere auch durch die inhaltliche Ausgestaltung der konkreten Abfrage. Erfragt z. B. die Sozialbehörde A von Finanzbehörde B, ob das Einkommen des Bürgers über einem bestimmten Schwellenwert liegt, so entspräche es dem Grundsatz der Datenminimierung nicht mehr, nach der genauen Einkommenshöhe zu fragen. Regelmäßig reicht die mit „ja“ oder „nein“ zu beantwortende Frage, „unterschreitet das Einkommen des Inhabers der PKZ ABC12345 den Schwellenwert?“, aus.

b) Übermittlung der Personenkennziffer

Einen wichtigen Verwendungszweck findet die PKZ darin, dass eine öffentliche Stelle sie an eine andere übermittelt, um einen Datenaustausch herbeizuführen. Dabei lassen sich im Wesentlichen zwei Konstellationen unterscheiden:

Zum einen ist denkbar, dass eine Behörde mit Hilfe der PKZ bei einer anderen (Register-)Behörde anfragt, um (insbesondere zwecks Kontrolle der Richtigkeit des eigenen Datensatzes) zu erfragen, über welche Daten zu der übermittelten PKZ sie verfügt bzw. welche Daten sie mit der PKZ verknüpft hat („Registerabfrage“). So könnte die Meldebehörde einer rheinland-pfälzischen Gemeinde die eigenen Angaben des Melderegisters zum (Zweit-)Wohnsitzstatus eines Bürgers mit den Registerangaben einer schleswig-holsteinischen Behörde abgleichen und die PKZ mit weiteren personenbezogenen Daten übermitteln.

Denkbar ist zum anderen aber auch, dass eine PKZ dazu dient, bei einer anderen Behörde bereits vorhandene Daten für das jeweilige Fachverfahren abzurufen. Dadurch lässt sich sicherstellen, dass der Bürger personenbezogene Daten, die er der öffentlichen Verwaltung

---

[55] Vgl. *Heberlein*, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2017, Art. 5 DSGVO, Rn. 24 f.
[56] Insoweit gibt die Vorschrift die Datenminimierung noch ein weiteres Mal – zusätzlich zu dem allgemeinen Grundsatz des Art. 5 Abs. 1 lit. c DSGVO – spezifisch vor.

mitgeteilt hat, nur ein einziges Mal an die Verwaltung übermitteln muss (sog. Once-only-Prinzip)[57].

Wie alle übrigen Datenverarbeitungsvorgänge bedarf die Übermittlung der PKZ nicht nur einer Verarbeitungsgrundlage (aa). Sie unterliegt auch dem Zweckbindungsgrundsatz (bb).

aa) Verarbeitungsgrundlage für die Übermittlung (Art. 6 Abs. 1 DSGVO)

Während der nationale Gesetzgeber eine Verarbeitungsgrundlage für die *Übermittlung der PKZ* als solcher aufgrund des Art. 87 DSGVO selbst schaffen darf,[58] gilt für die *Übermittlung der mit der PKZ verbundenen Daten e*twas anderes: Art. 87 DSGVO gibt dem Mitgliedstaat – im Gegensatz zu vielen anderen Öffnungsklauseln – zwar einen recht unbestimmten und somit *a prima vista* recht weiten Spielraum an die Hand, die Bedingungen für eine Übermittlung der PKZ festzulegen.[59] Ließe Art. 87 DSGVO indes auch die Übermittlung der Daten zu, die mit der PKZ verbunden sind, könnte der Mitgliedstaat das fein austarierte System der Öffnungsklauseln, welches die DSGVO vorsieht, leicht unterlaufen, indem er alle von ihm gesammelten personenbezogenen Daten mit der PKZ verbindet.

Eine Verarbeitungsgrundlage für die Übermittlung der Daten, die mit der PKZ verbunden sind, ergibt sich daher lediglich aus der mitgliedstaatlichen Öffnungsklausel des Art. 6 Abs. 1 lit. e, Abs. 3 S. 1 lit. b DSGVO („für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde“).

bb) Zweckbindung als allgemeiner Grundsatz der DSGVO (Art. 5 Abs. 1 lit. b DSGVO)

Die behördliche Übermittlung der PKZ und anderer personenbezogener Daten, die mit ihr verknüpft sind, berührt vor allem den datenschutzrechtlichen Grundsatz der Zweckbindung. Ihn formuliert die DSGVO an prominenter Stelle in Art. 5 Abs. 1 lit. b DSGVO.[60] Er untersagt es Verantwortlichen, Daten zu verarbeiten, die mit dem ursprünglichen Erhebungszweck nicht vereinbar sind.

Bevor der Verantwortliche ein personenbezogenes Datum (erst)verarbeitet, muss er den damit verfolgten Zweck festlegen.[61] Seine Zweckfestlegung bindet ihn für weitere Verarbeitungsvorgänge.[62] Sie darf auch nicht zu vage formuliert sein, sondern muss möglichst

---

[57] Ausführlich hierzu *Martini/Wenzel*, DVBl 2017, 749 ff.
[58] Siehe oben S. 8.
[59] Siehe oben S. 4.
[60] Zur *Direkterhebung* personenbezogener Daten beim Betroffenen verpflichtet die DSGVO – anders als das alte BDSG (§ 4 Abs. 2 BDSG) – hingegen nicht. Über die Erhebung ist der Betroffene aber zu informieren (vgl. Art. 13 und 14 DSGVO).
[61] Siehe *Schantz* (Fn. 52), Art. 5 DSGVO, Rn. 12.
[62] Er darf die anvisierte (Weiter-)Verarbeitung insbesondere grundsätzlich nur dann vornehmen, wenn der Zweck mit demjenigen der Erstverarbeitung kompatibel ist.

konkret erfolgen.[63] Andernfalls liefe das Gebot der Zweckbindung faktisch leer: Ganz unterschiedliche, bewusst unklar oder mehrdeutig gehaltene Zwecke könnten dann als kompatibel durchlaufen.

(1) Ausnahmen vom Zweckbindungsgrundsatz

Bestimmte Zwecke des Gemeininteresses erklärt die Sonderregelung des Art. 5 Abs. 1 lit. b Hs. 2 DSGVO per gesetzlicher Fiktion für mit dem Primärzweck vereinbar:[64] Verfolgt die Verwaltung „im öffentlichen Interesse liegende Archivzwecke, […] wissenschaftliche oder historische Forschungszwecke oder […] statistische Zwecke“ [65], steht der Zweckbindungsgrundsatz der Weiterverarbeitung nicht entgegen.

(2) Kompatibilitätstest nach Art. 6 Abs. 4 DSGVO

Ob der ursprüngliche Zweck mit dem der beabsichtigten Weiterverarbeitung vereinbar ist, bestimmt sich anhand eines sog. Kompatibilitätstests.[66] Art. 6 Abs. 4 DSGVO zählt fünf unterschiedliche Wertungsmaßstäbe auf, anhand derer die Vereinbarkeit der Zwecke zu bestimmen ist; abschließend sind die Kriterien jedoch nicht.[67] Im Rahmen des Kompatibilitätstests findet insbesondere kein rein schematischer Abgleich beider Zwecke statt. Vielmehr ist die Zweckkompatibilität anhand einer umfassenden Interessenabwägung zu beurteilen.[68]

Erweisen sich die beiden Zwecke als nicht miteinander vereinbar, so zieht dies nicht zwangsläufig die Unzulässigkeit der anvisierten Weiterverarbeitung nach sich. Willigt der Betroffene in die Weiterverarbeitung ein (a) oder legitimiert sie ein Gesetz der Union oder des Mitgliedstaates (b), darf der Verantwortliche die Daten trotz Zweckwidrigkeit (weiter-)verarbeiten. Der Verordnungstext sieht insbesondere nicht ausdrücklich ein Rückspielverbot hinsichtlich statistischer Daten vor, wie es das BVerfG durch sein Volkszählungsurteil im deutschen Recht etabliert hat (c).

(a) Einwilligung des Betroffenen

Eine Einwilligung des Betroffenen überspielt das Zweckbindungsgebot. Das hat auch seinen guten Sinn: Datenschutz versteht sich nicht als Schutz *gegen* den Betroffenen, sondern *für* den

---

[63] Vgl. *Schantz* (Fn. 52), Art. 5 DSGVO, Rn. 15.
[64] *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 2017, Art. 5, Rn. 32.
[65] Welche Vorgaben die DSGVO für die Verarbeitung personenbezogener Daten zu statistischen Zwecken trifft, erlangt vor allem für die Durchführung eines registerbasierten Zensus an Bedeutung. Klärungsbedürftig ist insoweit insbesondere, ob eine Behörde zu statistischen Zwecken verarbeitete Daten später an andere Verwaltungsbehörden mit dem Ziel der Verwendung der Daten für den allgemeinen Verwaltungsvollzug weiterreichen darf. Hierzu ausführlich S. 15 ff.
[66] Dazu auch schon *Martini/Wenzel* (Fn. 57), 752.
[67] *Frenzel*, in: Paal/Pauly (Hrsg.), DS-GVO, 2017, Art. 6, Rn. 48.
[68] *Plath*, in: ders. (Hrsg.), BDSG/DSGVO, 2. Aufl., 2016, Art. 6 DSGVO, Rn. 38; zustimmend auch *Martini/Wenzel* (Fn. 57), 752.

Betroffenen. Die Aufgabe der DSGVO besteht gerade darin, das Recht des Einzelnen, selbst zu bestimmen, ob und innerhalb welcher Grenzen er persönliche Lebenssachverhalte offenbaren will, zu schützen. Um sicherzustellen, dass sich in einer Zustimmungserklärung des Betroffenen tatsächlich die autonome Selbstbestimmung des Einzelnen manifestiert, knüpft die DSGVO ihre Wirksamkeit aber an hohe Voraussetzungen. Sie ergeben sich aus Art. 4 Nr. 11 und Art. 7 DSGVO.[69]

Art. 4 Nr. 11 DSGVO begrenzt die Einwilligung auf „freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung[en] […], mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“. Auf den Betroffenen ausgeübter Druck oder Zwang, der Datenverarbeitung zuzustimmen, schließen die Freiwilligkeit aus.[70]

Die Gefahr, dass der Verantwortliche dem Betroffenen die Einwilligung abtrotzt, manifestiert sich vor allem in Abhängigkeitsverhältnissen: Selbst wenn der Betroffene mit der Verarbeitung zwar an sich nicht einverstanden ist, stimmt er ihr dann unter Umständen notgedrungen doch zu, weil er andernfalls mit Nachteilen rechnet. Eine solche Coactus-volui-Konfliktlage hat der Verordnungsgeber bei der Festlegung seiner normativen Anforderungen an die Einwilligung vor Augen (vgl. auch Art. 7 Abs. 4 DSGVO):[71] Ist zweifelhaft, ob eine Einwilligung tatsächlich freiwillig erteilt worden ist, soll die Zustimmung des Betroffenen im Interesse eines effektiven Bürgerschutzes den Verarbeitungsvorgang nicht legitimieren können, „wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht“ (ErwGr. 43 S. 1 DSGVO). Beispielhaft nennt ErwGr. 43 S. 1 DSGVO den Fall, dass es sich bei dem Verantwortlichen um eine Behörde handelt.

Gegenüber einer Behörde willigt der Bürger nach der Einschätzung des Unionsgesetzgebers also grundsätzlich nicht freiwillig ein.[72] Diese normative Wertung beruht auf der Vermutung, dass das Damoklesschwert des Machtgefälles zwischen Staat und Bürger, das dieses Verhältnis überschattet, die Freiwilligkeit einer Zustimmung typischerweise ausschließt. Im Falle der Einwilligung in eine Once-only-Datennutzung greift diese Erwägung freilich nicht durch, sofern der Bürger auf informierter Grundlage einen ihm angebotenen Servicevorteil kraft autonomer Entscheidung nutzen möchte: Die Zustimmung des Bürgers ertrotzt sich die Verwaltung in diesem Fall nicht auf der Grundlage ihrer eigenen Machtposition.[73]

---

[69] Aber auch die Erwägungsgründe enthalten ergänzende Informationen dahin gehend, wie die Einwilligung ausgestaltet sein muss, um den Vorgaben der DSGVO zu genügen, so etwa ErwGr. 43 DSGVO.
[70] *Ernst* (Fn. 43), Art. 4, Rn. 69; *Schild*, in: Wolff/Brink (Hrsg.), BeckOK DatenschutzR, 20. Ed., Stand: 1.5.2017, Art. 4 DSGVO, Rn. 127.
[71] Ausführlicher zu sog. „Abhängigkeitslagen“ siehe *Ernst* (Fn. 43), Art. 4, Rn. 71.
[72] Siehe dazu *Martini/Wenzel* (Fn. 57), 753.
[73] *Martini/Wenzel* (Fn. 57), 753.

(b) Dispens durch gesetzliche Regelung

Art. 6 Abs. 4 DSGVO ermächtigt die Mitgliedstaaten sowie die Union, das Zweckbindungserfordernis durch Gesetz zu lockern.[74] Zulässig ist dies jedoch nur unter strengen Voraussetzungen: Bei der dispensierenden Vorschrift muss es sich um eine „in einer demokratischen Gesellschaft […] notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele" handeln.

Die Ziele, zu deren Erreichung die DSGVO eine zweckinkompatible Verarbeitung gestattet, fasst die DSGVO nicht offen, sondern listet sie in Art. 23 Abs. 1 DSGVO abschließend auf.[75] Im Zuge eines Registermodernisierungsprozesses fällt insoweit lit. e („Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats") eine Schlüsselrolle zu. Konkretisierend erklärt ErwGr. 73 DSGVO „das Führen öffentlicher Register" ausdrücklich zu einem allgemeinen öffentlichen Interesse im Sinne der Norm.

Das neue BDSG[76] macht von der (fakultativen) Öffnungsklausel des Art. 6 Abs. 4 DSGVO Gebrauch: „Die Verarbeitung zu anderen Zwecken" gestattet § 23 BDSG-neu für öffentliche und § 24 BDSG-neu für nicht-öffentliche Datenverarbeiter.

Auch für die staatliche Registerführung hat der deutsche Gesetzgeber eine instruktive Regelung parat: § 23 Abs. 1 Nr. 2 BDSG befreit Datenverarbeitungen vom Zweckbindungsgebot, sofern „Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen". Dem Tatbestand können zwar einzelne Fälle eines Registerabgleichs mittels PKZ unterfallen, ein umfassender Registerabgleich lässt sich auf die neue Vorschrift aber nicht stützen. § 23 Abs. 1 Nr. 2 BDSG-neu gestattet vielmehr lediglich einen punktuellen Abgleich dort, wo der Betroffene Anlass für eine Überprüfung gegeben hat, etwa dadurch, dass er widersprüchliche Angaben gegenüber der Behörde gemacht hat;[77] eine Generalklausel, um Registersynchronisationen umfassend zu legitimieren, hält § 23 Abs. 1 Nr. 2 BDSG-neu mithin nicht vor.

Auch die Implementierung des Once-only-Prinzips ist auf Grundlage des neuen BDSG grundsätzlich nicht möglich.[78] Denn § 23 BDSG-neu befreit insoweit gerade nicht von dem Zweckbindungsgrundsatz – bemerkenswerterweise auch nicht für die ursprünglich (im

---

[74] *Kühling/Martini et al.* (Fn. 30), S. 38 ff. Allerdings besitzt der Mitgliedstaat diese Befugnis nur dann, wenn er selbst auch die Erstverarbeitung regeln kann.
[75] *Stender-Vorwachs*, in: Wolff/Brink (Hrsg.), BeckOK DatenschutzR, 20. Ed., Stand: 1.5.2017, Art. 23 DSGVO, Rn. 14.
[76] Bundesdatenschutzgesetz vom 30.6.2017 (Art. 1 DSAnpUG-EU; im Folgenden: BDSG-neu), BGBl. I S. 2097. Es wird am 25.5.2018 in Kraft treten (Art. 8 Abs. 1 DSAnpUG-EU).
[77] *Martini/Wenzel* (Fn. 57), 756.
[78] *Martini/Wenzel* (Fn. 57), 757.

Regierungsentwurf für ein neues BDSG angedachte) Privilegierung des Austauschs von Daten aus allgemein zugänglichen Quellen.[79]

De lege ferenda steht es dem deutschen Gesetzgeber aber – in den Grenzen des Art. 6 Abs. 4 DSGVO i. V. m. Art. 23 DSGVO – frei, über die in § 23 BDSG-neu enthaltenen Tatbestände hinaus auch andere Datenverarbeitungen vom Zweckbindungsgrundsatz freizustellen und so ggf. einen PKZ-gestützten Datenaustausch (etwa auch nach dem Grundsatz „once only") zu legitimieren.

(c) Zweckbindung bei Datenverarbeitungen zu statistischen Zwecken: Fortbestand des Rückspielverbots unter der DSGVO?

Als spezielle Ausprägung des Zweckbindungsgrundsatzes bei Verarbeitungen statistischer Daten kennt das deutsche Recht bislang das sog. Rückspielverbot. In der nationalen Rechtsordnung verbindet sich mit dem Terminus das Verbot, Daten, die der Staat im Rahmen einer statistischen Erhebung gewonnen hat, für Zwecke des Verwaltungsvollzugs zu verwenden (i). Es reagiert damit auf die Gefahr, dass im Rahmen einer statistischen Erhebung gewonnene (mithilfe einer Ordnungsnummer [vgl. § 13 ZensG 2011] verknüpfte) Informationen der amtlichen Statistik sich leicht dazu nutzen lassen, Korrekturen auf der Ebene des Verwaltungsvollzugs vorzunehmen (z. B. zum Erlass von Verwaltungsmaßnahmen), ohne dass die betroffenen Bürger Informationen für diese Zwecke zur Verfügung gestellt haben oder darum wussten.

In der DSGVO klingt eine Inkompatibilität solcher Verarbeitungszwecke zwar an; ein gänzliches *Verbot* Datenerhebungen, die ursprünglich zu statistischen Zwecken erfolgt sind, für Zwecke des Verwaltungsvollzugs zu nutzen, sieht die DSGVO aber nicht ausdrücklich vor (ii).

Das Rückspielverbot determiniert als spezielles rechtliches Schutzkonzept zwar nicht die generelle Zulässigkeit einer PKZ, aber doch ihre Nutzung für Zielsetzungen der amtlichen Statistik.

i. Das Rückspielverbot im nationalen Recht

Im nationalen Recht findet das Rückspielverbot seinen Ursprung im Volkszählungsurteil des BVerfG: Das Gericht erkennt dort zwar an, dass bei der Datenverarbeitung für statistische Zwecke eine enge und konkrete Zweckbindung der erhobenen Daten „dem Wesen der Statistik" nach nicht zu verlangen ist.[80]

---

[79] Vgl. BT-Drucks. 18/12144, S. 4. Zum ursprünglichen Entwurf des Gesetzes *Martini/Wenzel* (Fn. 57), 756 f.; allgemein zu einem Social Media Monitoring öffentlicher Stellen *Martini*, VerwArch. 107 (2016), 307 ff.
[80] BVerfGE 65, 1 (47). Denn die statistisch aufbereiteten Daten sollen „für die verschiedensten, nicht von vornherein bestimmbaren Aufgaben verwendet werden", BVerfG, ibid.

Eine solche Zwecklockerung hält das Gericht aber nur für hinnehmbar, wenn der Gesetzgeber in die normative Architektur Sicherungsmaßnahmen einzieht, welche das Persönlichkeitsrecht der Betroffenen hinreichend schützen.[81] Sie darf nach seiner Einschätzung nicht dazu führen, dass der Staat Daten, die er zu einem privilegierten Zweck erhebt, auch zu anderen Zwecken nutzt, die mit den Zielen ihrer ursprünglichen Erhebung unvereinbar sind.[82] Wenn Daten, die zu statistischen Zwecken erhoben werden, zugleich zu Zwecken des Verwaltungsvollzugs Verwendung finden sollen, nimmt das Gericht eine solche Unvereinbarkeit an.[83]

Diese verfassungsrechtliche Wertung hat insbesondere über § 16 BStatG Eingang in das einfache Recht gefunden. Die Vorschrift ist Ausdruck einer informationellen Funktionentrennung[84]: Daten, die der Staat zu statistischen Zwecken erhoben hat, an eine Funktionseinheit zu übermitteln, die auch mit dem Verwaltungsvollzug betraut ist, lässt sie nur unter eingeschränkten Voraussetzungen zu[85] – nämlich dann, wenn die Wahrung des Statistikgeheimnisses durch Organisation und Verfahren, insbesondere Trennung der mit der Statistik betrauten Stelle von den Stellen des Verwaltungsvollzugs sichergestellt ist (vgl. insbesondere § 16 Abs. 5 S. 2 und § 16 Abs. 8 S. 3 BStatG). Dies gilt nicht nur bei Zweckänderungen, sondern auch bei nicht zweckkompatiblen Datenverarbeitungen. Prominenten Ausdruck findet das Rückspielverbot auch in § 8 Abs. 2 S. 3 sowie § 15 Abs. 2 S. 4 ZensG 2011: Sie verbieten ausdrücklich eine Rückmeldung erhobener Daten an die Meldebehörden.

Das Rückspielverbot soll zum einen das informationelle Selbstbestimmungsrecht wahren und ist zum anderen mittelbar auch der Qualität amtlicher Erhebungen verschrieben. Es soll gewährleisten, dass der Bürger nicht fürchten muss, sich durch wahrheitsgemäße Angaben bei statistischen Erhebungen negativen Folgemaßnahmen der Verwaltung auszusetzen, oder die Verwaltung gar die Möglichkeit erhält, ein Persönlichkeitsprofil der Bürger zu erstellen; vielmehr soll es diese motivieren, bei statistischen Erhebungen wahrheitsgemäße und vollständige Angaben zu machen.[86]

ii. Das Rückspielverbot in der DSGVO

Ein explizites Rückspielverbot kennt der materielle Teil der DSGVO nicht. Weder Art. 89 DSGVO noch eine andere Vorschrift der Verordnung geben eine spezifische Antwort auf die Frage, ob öffentliche Stellen statistische Daten für den Verwaltungsvollzug weiternutzen

---

[81] BVerfGE 65, 1 (48).
[82] BVerfGE 65, 1 (62).
[83] BVerfGE 65, 1 (62).
[84] *Martini*, Der Zensus 2011 als Problem interkommunaler Gleichbehandlung, 2011, S. 26; an anderer Stelle werden diese Maßgaben auch unter dem Stichwort „informationelle Gewaltentrennung" behandelt, siehe etwa *Hornung*, Die digitale Identität, 2005, S. 155. Zum Rückspielverbot s. a. VG Ansbach, Urt. v. 21.6.2012 – AN 4 K 11.02441 –, juris, Rn. 69; vgl. auch VG Potsdam, Beschl. v. 21.4.2015 – 12 L 450/15 –, juris, Rn. 15 m. w. N.
[85] Dazu schon *Martini* (Fn. 84), S. 26.
[86] BVerfGE 65, 1 (50).

dürfen.[87] Auch die Privilegierung des Art. 5 Abs. 1 lit. b Hs. 2 DSGVO findet keine Anwendung. Denn sie regelt gerade die umgekehrte Konstellation: die Nutzung von Verwaltungsdaten für statistische Zwecke. Grundsätzlich bleibt es daher auch in diesem Fall bei den allgemeinen Vorgaben der Art. 5 Abs. 1 lit. b Hs. 1 und Art. 6 Abs. 4 DSGVO.[88]

In eine andere Richtung weist indes ErwGr. 162 S. 3 DSGVO. Dort klingt ein Rückspielverbot leise an: Der europäische Gesetzgeber will seine Sonderregeln für statistische Zwecke auf solche Fälle begrenzt wissen, in denen „die Ergebnisse der Verarbeitung zu statistischen Zwecken keine personenbezogenen Daten, sondern aggregierte Daten sind und diese Ergebnisse oder *personenbezogenen Daten nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden*“.[89] Die Einschränkung „nicht für Maßnahmen […] gegenüber einzelnen natürlichen Personen“ lässt sich als ein grundsätzliches (implizites) Übermittlungsverbot statistisch erhobener Daten lesen. Andernfalls wäre nicht in hinreichendem Maße sichergestellt, dass der Staat statistische Daten nicht doch für den Verwaltungsvollzug nutzt.

Wie sich die Aussage des ErwGr. 162 S. 3 DSGVO mit den Vorgaben des Verordnungstextes selbst verträgt, ist unklar.[90] Bei weiter Auslegung zwingt der ErwGr. zu einer teleologischen Reduktion des Art. 6 Abs. 4 DSGVO, namentlich zu einer Einschränkung der gesetzlichen Möglichkeit, in solchen Fällen vom Zweckbindungsgrundsatz zu dispensieren („Rechtsvorschrift der Union oder der Mitgliedstaaten“). Die mit sonstigen Verwaltungszwecken unvereinbaren statistischen Zwecke dürften dann grundsätzlich nicht mehr an die Verwaltungsbehörden übermittelt werden. Einzig mit der Einwilligung des Betroffenen wäre es dann weiterhin möglich, die Übermittlung der mit einer PKZ verbundenen Daten zu legitimieren.[91]

---

[87] Den Begriff „statistische Zwecke“ definiert der Verordnungsgeber in ErwGr. 162 S. 3 DSGVO („jeder für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderliche Vorgang der Erhebung und Verarbeitung personenbezogener Daten“).

[88] Statistische Daten dürfen somit zunächst nur dann weiterverarbeitet werden, wenn der Zweck der Weiterverarbeitung mit den statistischen Zwecken der Ersterhebung kompatibel ist. Eine solche Zweckvereinbarkeit liegt im Falle der Verwertung statistischer Daten für den Verwaltungsvollzug allerdings gerade nicht vor. Die Weiterverarbeitung wird dadurch jedoch nicht automatisch unzulässig. Sie bedarf allerdings einer sie legitimierenden Einwilligung der betroffenen Person oder muss sich auf ein Gesetz der Union oder der Bundesrepublik stützen, das „in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt“ (Art. 6 Abs. 4 DSGVO).

[89] Hervorhebung durch die Verfasser.

[90] Erwägungsgründe sind nicht rechtsverbindlich, haben also nicht an der unmittelbaren Wirkung der Norm teil; EuGH, Urt. v. 19.6.2014 – C-345/13 –, ECLI:EU:C:2014:2013, Rn. 31, st. Rspr. Sie unterstützen den Normanwender bei der teleologischen Auslegung der betreffenden Norm, indem sie versuchen, ihm bestimmte Vorstellungen des Gesetzgebers vom Normverständnis zu vermitteln, vgl. *Gaitanides*, in: von der Groeben/Schwarze/Hatje (Hrsg.), EU-Recht, 7. Aufl., 2015, Art. 19 EUV, Rn. 45 m. w. N. Zu den Grenzen der teleologischen Auslegung unter Zuhilfenahme eines ErwGr. siehe EuGH, ibid.

[91] Die Möglichkeit einer legitimierenden Einwilligung ergibt sich aus der Achtung des Selbstbestimmungsrechts im Hinblick auf die Entscheidung über die Zulässigkeit einer Datenverarbeitung.

Einen Ausschluss oder eine Einschränkung des Art. 6 Abs. 4 DSGVO für statistische Daten proklamiert ErwGr. 162 S. 3 DSGVO jedoch weder ausdrücklich noch seiner Rationalität nach. Naheliegender erscheint, dass der ErwGr. seine Wertung auf etwas „kleinerer Flamme kochen", nämlich besonders hervorkehren will, dass statistische Zwecke mit solchen des Verwaltungsvollzugs nicht vereinbar sind.[92] Die Privilegierungstatbestände, insbesondere des Art. 5 Abs. 1 lit. b Hs. 2 i. V. m. Art. 89 DSGVO, sollen mit anderen Worten nur in solchen Fällen greifen, in denen aggregierte Daten verarbeitet werden, die nicht unmittelbar für Maßnahmen des Verwaltungsvollzugs Verwendung finden. Im Übrigen findet Art. 6 Abs. 4 DSGVO auch auf statistische Daten uneingeschränkt Anwendung. Wird der nationale Gesetzgeber nicht aktiv, dürfen statistische Daten daher aufgrund Zweckinkompatibilität (Art. 5 Abs. 1 lit. b i. V. m. Art. 6 Abs. 4 DSGVO) grundsätzlich nicht für den Verwaltungsvollzug genutzt werden.

Aus Art. 6 Abs. 4 DSGVO folgt somit in der Sache ebenfalls ein Rückspielverbot. Die Entscheidung über dessen Aushebelung, d. h. über die Untersagung der Weitergabe statistischer Daten an die Verwaltung, liegt dann – via Öffnungsklausel des Art. 6 Abs. 4 DSGVO – im Grundsatz bei den Mitgliedstaaten. Art. 6 Abs. 4 lässt dafür Raum („oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten"). Die Entscheidung des nationalen Gesetzgebers unterliegt dabei jedoch den strengen Anforderungen, die Art. 23 Abs. 1 DSGVO an die Verhältnismäßigkeit und die Verarbeitungszwecke stellt. Die Zweckbindung aufzuheben und damit das gegenwärtig bestehende Rückspielverbot zu überspielen, steht dem nationalen Gesetzgeber unionsrechtlich nur frei, soweit sich die Weiterverwendungszwecke der Verwaltungsbehörden mit den in Art. 23 Abs. 1 lit. a bis j DSGVO genannten Belangen decken.

Bei der Ausfüllung der Öffnungsklausel des Art. 6 Abs. 4 DSGVO bleibt der nationale Gesetzgeber darüber hinaus an die verfassungsrechtlichen Vorgaben gebunden.[93] Die bundesverfassungsgerichtliche Dogmatik zum Rückspielverbot[94] ist deshalb – wenn auch in anderem normativen Gewand – weiterhin bedeutsam. Weder intendiert die DSGVO im Ergebnis eine Aufweichung des strengen (auch verfassungsrechtlich vorgezeichneten) Rückspielverbots noch untersagt sie ein entsprechendes Vorgehen des Gesetzgebers generell.

3. Aussagen der RL 2016/680/EU zu Personenkennziffern

Die für die öffentliche Verwaltung besonders wichtige und sensible Datenverarbeitung der Gefahrenabwehr- und Polizeibehörden begrenzt auf unionsrechtlicher Ebene die RL 2016/680/EU[95]. Die Richtlinie erstreckt ihren Geltungsanspruch auf die „Verarbeitung

[92] Hiervon geht in der Sache auch Art. 5 Abs. 1 lit. b Hs. 2 DSGVO aus, wenn er die Vereinbarkeit von Verwaltungs- und statistischen Zwecken fingiert.
[93] Zur Begründung der Prüfungsbefugnis des BVerfG bei fakultativen Öffnungsklauseln bereits oben auf S. 4.
[94] BVerfGE 65, 1 (61 f.)
[95] Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien

personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit" (vgl. Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 RL 2016/680/EU). Eine explizite unionsrechtliche Regelung zur Einführung einer allgemeinen (oder bereichsspezifischen) PKZ enthält sie jedoch nicht.

4. Zwischenfazit

Dass sich die öffentliche Verwaltung des Instruments einer PKZ für staatliche Register bedient, ist in der EU bereits heute eher Regel als Ausnahme.[96] Der etablierten Praxis, jedem Bürger zur Vereinfachung administrativer Abläufe eine bestimmte Kennziffer zuzuweisen, stellt die DSGVO keine unüberwindbaren Hürden in den Weg: Sie steht der Einführung einer PKZ nicht entgegen, sondern reicht mit Art. 87 DSGVO die Entscheidungsgewalt über ihre Einführung grundsätzlich an die Mitgliedstaaten weiter. Solange der nationale Gesetzgeber mittels geeigneter Garantien gemäß Art. 87 DSGVO die Rechte und Freiheiten der betroffenen Personen schützt, kann er unionsrechtlich weitgehend frei über das „Ob" und „Wie" der Implementierung einer PKZ befinden.

III. Verfassungsrechtliche Implikationen der Personenkennziffer

Soweit das unionale Recht die Verarbeitung personenbezogener Daten nicht unmittelbar determiniert, sondern der nationale Gesetzgeber von dem eigenen Gestaltungsspielraum Gebrauch macht, den ihm die DSGVO lässt, ist er keineswegs vollständig frei, den Verarbeitungsprozess zuzulassen. Die nationale Regelung muss sich dann vielmehr an dem Grundrecht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG) messen lassen. Aufgrund der in Art. 87 S. 1 DSGVO enthaltenen Öffnungsklausel gilt dies auch für die datenschutzkonforme Einführung einer PKZ.

1. Schutzbereich des Rechts auf informationelle Selbstbestimmung

Das Grundrecht auf informationelle Selbstbestimmung hat das BVerfG mit dem Volkszählungsurteil[97] im Jahr 1983 als der Verfassung eingeschriebene Gewährleistung aus der Taufe gehoben. Die neuen Gefahren für die individuelle Selbstbestimmung, die von Instrumenten der amtlichen Statistik im Gefolge der Fortentwicklung der Informationstechnologie einhergingen, gaben dem Gericht dazu Anlass: Neuere Verfahren der Datenverarbeitung eröffnen die Möglichkeit, Daten beliebig zu speichern, abzurufen und mit

---

Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates v. 27.4.2016, ABl. Nr. L 119/89. Sie begrenzt den Regelungsanspruch unmittelbarer Wirkung, den die DSGVO verfolgt (Art. 2 Abs. 2 lit. d DSVO).

[96] *Ehmann* (Fn. 15), Art. 87, Rn. 2 f.

[97] BVerfGE 65, 1 ff.

anderen Daten zu verknüpfen.[98] Damit geht auch das Risiko einher, einzelne Datenkonglomerate miteinander „zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammen[zuführen] […], ohne daß der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann[99]. Hat der Staat den Zugriff auf ein Persönlichkeitsbild seiner Bürger, kann das ein verhaltenssteuerndes Gefühl des Überwachtwerdens auslösen: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen."[100]

Seit der Herleitung des Grundrechts auf informationelle Selbstbestimmung im Volkszählungsurteil hat der Gesetzgeber es im einfachen Recht weiter präzisiert und verfestigt, bspw. durch das Steuergeheimnis gemäß § 30 AO[101] sowie das Sozialgeheimnis gemäß § 35 SGB I[102].[103]

Die Einführung und Verwendung einer PKZ berührt den Schutzbereich des Rechts auf informationelle Selbstbestimmung aus zwei unterschiedlichen Perspektiven: Sie kann zum einen ein Instrument sein, personenbezogene Daten der Bundesbürger unter einer übergreifenden Chiffre systematisch zu sammeln. Zum anderen lässt sich eine PKZ als Mittel zur Datensynchronisation[104] verwenden. In beiden Fällen verarbeitet der Staat personenbezogene Daten der betroffenen Personen. Berührt ist davon jeweils die individuelle Befugnis, grundsätzlich autonom darüber zu entscheiden, ob und in welchem Umfang persönliche Lebenssachverhalte offenbart werden.[105]

2. Eingriff

Jede Verarbeitung personenbezogener Daten, die ohne Einwilligung des Betroffenen erfolgt, greift in dessen Recht auf informationelle Selbstbestimmung ein.[106] Sowohl die Einführung einer PKZ als auch jede weitere Verwendung dieses neu geschaffenen personenbezogenen Datums[107] markiert demnach einen rechtfertigungsbedürftigen Eingriff.

---

[98] BVerfGE 65, 1 (42).
[99] BVerfGE 65, 1 (42).
[100] BVerfGE 65, 1 (42 f.). Dazu auch *Martini* (Fn. 79), S. 325 m. w. N. in Fn. 69.
[101] Dazu *Intemann*, in: Koenig (Hrsg.), AO, 3. Aufl., 2014, § 30 AO, Rn. 5.
[102] Dazu *Seewald*, in: Körner/Leitherer/Mutschler et al. (Hrsg.), KassKomm SozVersR, 95. Erg-Lfg. (2017), § 35 SGB I, Rn. 2 f.
[103] Die besondere Sensibilität dieser Daten zeigt sich darin, dass § 203 Abs. 1 Nr. 6 StGB und § 355 StGB die unbefugte Weitergabe oder Verwertung solcher Daten auch dann unter Strafe stellen, wenn die Weitergabe bzw. Verwertung nicht gegen Entgelt erfolgt.
[104] Denkbar ist eine Synchronisation zum einen im Rahmen eines Abgleichs verschiedener Register auf Übereinstimmung oder Abweichung der jeweils unter einer PKZ gespeicherten Daten und zum anderen bei der Zusammenführung bestimmter Registerdaten im Rahmen eines verwaltungsrechtlichen Fachverfahrens. Siehe dazu im Einzelnen S. 1 ff.
[105] BVerfGE 65, 1 (43).
[106] Vgl. BVerfGE 65, 1 (42 f.).
[107] Dazu bereits oben Fn. 32.

Für die Steuer-ID (vgl. §§ 139a und 139b AO) – eine bereichsspezifische PKZ (bPKZ) – hat das FG Köln einen grundrechtlichen Eingriff exemplarisch aus mehrerlei Gründen festgestellt.[108] Es bewegt sich damit auf der Rechtsprechungslinie des BVerfG, das „schon auf der Stufe der Persönlichkeits*gefährdung*“ [109] einen Eingriff in das Recht auf informationelle Selbstbestimmung annimmt:[110] Ihr hat der Gesetzgeber auf Ebene der verfassungsrechtlichen Rechtfertigung des Eingriffs Rechnung zu tragen.[111]

Wie schwer derartige Eingriffe wiegen, lässt sich abstrakt nur unzureichend bestimmen; die genaue Belastungswirkung einer allgemeinen PKZ ergibt sich erst aus ihrer gesetzlichen Ausgestaltung und der Art sowie dem Umfang der mit ihr verknüpften Daten. Die konkrete Eingriffsintensität „hängt“ in den Worten des BVerfG „von Art, Umfang und denkbaren Verwendungen der erhobenen Daten sowie der Gefahr ihres Missbrauchs ab“.[112] So kann auch die Verarbeitung solcher Daten, die – isoliert betrachtet – wenig sensibel sind, schwerwiegend in die informationelle Selbstbestimmung eingreifen, sobald eine Behörde sie mit anderen Daten verknüpft und für eine Vielzahl anderer Zwecke verwendet.[113] Eine besondere Schwere des Eingriffs kann sich auch aus dem „Grad an Persönlichkeitsrelevanz ergeben“, den „die betroffenen Informationen je für sich und in ihrer Verknüpfung mit anderen aufweisen,“ – ebenso aus der Art und Weise, wie die verantwortliche Stelle die Daten erlangt hat, etwa im Falle einer Verletzung besonderer Vertraulichkeitserwartungen des Betroffenen.[114]

Der Eingriff wiegt darüber hinaus besonders schwer, wenn der Staat personenbezogene Daten heimlich verarbeitet. Denn der Betroffene kann sich dann nicht angemessen präventiv gegen die Persönlichkeitsbeeinträchtigung zur Wehr setzen, sondern allenfalls nachträglichen Rechtsschutz erlangen – falls er von ihr erfährt. [115] Für das Maß seiner Grundrechtsbeeinträchtigung ist zudem relevant, ob die Datenverarbeitung weitere Eingriffe in seine Grundrechte durch Folgemaßnahmen, z. B. Sanktionen oder Rückforderungen der Verwaltung, nach sich ziehen kann. [116] Gibt der Betroffene selbst Anlass zur Datenverarbeitung, so nimmt umgekehrt die Schwere des Grundrechtseingriffs ab.[117]

---

[108] „Durch die dem Kläger zugeordnete Steueridentifikationsnummer wird ein Datum geschaffen, über dessen Verwendung der Kläger nicht bestimmen kann.“ Vgl. FG Köln, Urt. v. 7.7.2010 - 2 K 2999/08 –, juris, Rn. 75 f. Daneben untersucht das FG Köln auch die *Verwendung* der Steuer-ID auf ihre Eingriffsqualität, a. a. O, Rn. 75 ff.
[109] Hervorhebung durch die Verfasser.
[110] BVerfGE 120, 378 (397).
[111] Weitere Eingriffe markieren die Verknüpfung personenbezogener Daten mit der Steuer-ID sowie die Übermittlung der Steuer-ID an andere Behörden. FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 –, juris, Rn. 77 ff.
[112] Vgl. BVerfGE 65, 1 (46) mit Verweis auf BVerfGE 49, 89 (142); 53, 30 (61).
[113] BVerfGE 118, 168 (197), st. Rspr.
[114] Vgl. BVerfGE 115, 320 (348), st. Rspr.
[115] BVerfGE 120, 378 (402 f.).
[116] BVerfGE 120, 378 (403).
[117] Vgl. BVerfGE 120, 378 (402), st. Rspr.

3. Rechtfertigung

Das Recht auf informationelle Selbstbestimmung gewährleistet die Verfassung nicht vorbehaltlos. Art. 2 Abs. 1 GG etabliert vielmehr eine Schrankentrias: die Rechte anderer, die verfassungsmäßige Ordnung und das Sittengesetz.[118] Ihre Rechtfertigungswirkung erstreckt sich auch auf die Beschränkung des Rechts auf informationelle Selbstbestimmung.

Zur verfassungsmäßigen Ordnung gehören alle formell und materiell verfassungskonformen Rechtsnormen.[119] Sie müssen insbesondere dem *Verhältnismäßigkeitsprinzip* genügen, wenn sie einen Eingriff rechtfertigen sollen: Eine Beeinträchtigung des Rechts auf informationelle Selbstbestimmung, die keinen legitimen Zweck verfolgt oder nicht geeignet, erforderlich oder angemessen ist, um das Ziel zu erreichen, ist verfassungswidrig.[120]

a) Eignung zur Erreichung eines legitimen Zwecks

Zu den Aufgaben einer PKZ gehört es, staatliche Register besser und leichter miteinander abgleichen zu können: Sie soll eine inhaltliche Kongruenz der einzelnen Datenbanken sicherstellen und damit zugleich deren Funktion als Grundlage der amtlichen Statistik verbessern. Fehlerhafte Datensätze lassen sich mit ihrer Hilfe zuverlässiger erkennen und beseitigen als im Status Quo. Registerfehler, also Untererfassungen (Fehlbestand) sowie Übererfassungen („Karteileichen"), sind auch nicht nur eine Randerscheinung staatlicher Datenverwaltung. So wies bspw. der Zensustest im Jahr 2001 in Städten mit über 800.000 Einwohnern einen Karteileichenbestand und 7, 6 % aus.[121] Die Qualität der staatlichen Register hat seither keine grundlegende Bereinigung durch eine Verbesserung der Erfassungsqualität erfahren. Als eindeutiges Identifizierungsmerkmal kann eine PKZ dazu beitragen, Verwechslungen zu vermeiden und unbeabsichtigte Parallelstrukturen abzubauen. Sie kann insoweit ein wertvoller Baustein der Modernisierung des deutschen Registerwesens sein.[122] Von ihrer Einführung können insbesondere Kosteneinsparungen und die Steigerung der Effizienz der registernutzenden Verwaltung ausgehen.[123] Eine eindeutige PKZ macht eine manuelle zwischenbehördliche Kommunikation für die Mehrzahl der Fälle, in denen eine Behörde auf den Datenbestand einer anderen Behörde zugreifen möchte, überflüssig.[124] Ein solcher automatisierter Abruf benötigter Informationen ist die Grundlage dafür, dass die Verwaltung den Bürgern digitale Leistungen effizient und schnell anbieten kann. Davon

---

[118] Siehe nur *Hofmann*, in: Schmidt-Bleibtreu/Hofmann/Henneke (Hrsg.), GG, 13. Aufl., 2014, Art. 2, Rn. 16.
[119] BVerfGE 6, 32 (37 f.), st. Rspr.
[120] Vgl. BVerfGE 65, 1 (46).
[121] *Martini* (Fn. 84), S. 37 m. w N.
[122] Vgl. *McKinsey & Company Inc.* (Fn. 4), S. 12, 27, 29.
[123] *McKinsey & Company Inc.* (Fn. 4), S. 38 ff., speziell in Bezug auf den Zensus S. 41.
[124] Eine manuelle Bearbeitung ist auf Dauer aber nur entbehrlich, wenn auch eine hohe Datenqualität gewährleistet ist, vgl. *McKinsey & Company Inc.* (Fn. 4), S. 27. Sonst erhöht sich die Gefahr (ggf. unbemerkt) fehlerhafter Entscheidungen.

profitieren im Ergebnis alle Beteiligten – auch die Bürger als Nutzer digitaler Verwaltungsangebote.[125]

Entbürokratisierend wirkt der automatisierte Datenaustausch aber hauptsächlich auf Seiten des Staates.[126] Eine vereinfachte, automatisierte Bearbeitung erschließt finanzielles Einsparpotenzial, schont insbesondere Personalressourcen. Auch in anderen Bereichen sind Effizienzsteigerungen zu erwarten. So kann ein vernetztes Registerwesen etwa als Grundlage für eine once-only-basierte E-Government-Strategie dienen.[127]

Eine Steigerung der Registerqualität kommt dabei nicht nur den registernutzenden Fachbehörden zugute. Auch für die Durchführung eines registergestützten Zensus sind verlässliche Register von elementarer Bedeutung:[128] Ohne eine hinreichende Datenqualität kann die Registerzählung nicht gelingen. Indem die PKZ eine eindeutige Datenzuordnung ermöglicht, ist ihre Einführung ein geeigneter Schritt, um die erstrebte Daten- und mithin Registerqualität zu gewährleisten.

b) Erforderlichkeit einer Personenkennziffer

Eine PKZ erweist sich nur dann als verfassungsrechtlich tragfähig, wenn sich die legitimen Ziele, die sie erreichen soll, nicht in einer grundrechtsschonenderen Weise verwirklichen lassen.[129]

aa) Erforderlichkeit mit Blick auf die Qualität staatlicher Register

(1) Registerabgleich mit Hilfe eines Stammdatensatzes als milderes Mittel?

Statt den Registerabgleich mit Hilfe einer PKZ durchzuführen, ist auch ein anderes Vorgehen denkbar: Eine Behörde übermittelt an eine andere ein Bündel personenbezogener Daten, mit deren Hilfe sich eine Person ebenfalls identifizieren lässt – beispielsweise Name, Geburtsdatum und Anschrift (also die sog. Stammdaten). Diese Parameter gewährleisten aber nicht in jedem Fall eine eindeutige Zuordnung und können zudem auch wechseln (etwa der Name durch Heirat oder die Adresse durch Umzug). Sie sind fehleranfälliger als eine eindeutige und permanente PKZ. Die heterogene Registerstruktur im föderalen Deutschland potenziert diese Fehleranfälligkeit zusätzlich.[130] Gerade bei häufig vorkommenden Namen wie „Peter Müller aus Köln“, kann das klassische Verfahren die Übermittlung einer größeren

---

[125] Zum (finanziellen) Nutzen der Verankerung des Once-only-Prinzips *Martini/Wenzel* (Fn. 57), 750.
[126] *McKinsey & Company Inc.* (Fn. 4), S. 40 ff.
[127] Ausführlich zum Once-only-Prinzip: *Martini/Wenzel* (Fn. 57), 749 ff.
[128] Vgl. *Martini* (Fn. 84), S. 13: „Korrekte Einwohnerzahlen und statistische Informationen zur Zusammensetzung der Bevölkerung sind unverzichtbare Planungsgrundlagen eines modernen Staates. Volkszählungen sind ein wesentliches Fundament der nationalen Statistik.“
[129] Zur Erforderlichkeitsprüfung etwa BVerfGE 100, 313 (375).
[130] Zu dieser Problematik auch *von Lewinski*, Datenbanken sowie Ordnungs- und Personenkennzeichen, in: Seckelmann (Hrsg.), Digitalisierte Verwaltung – Vernetztes E-Government, 2017 (im Erscheinen).

Zahl personenbezogener Daten oder aufwändige Abgleichverfahren erforderlich machen, um Fehler und Missverständnisse auf ein Minimum zu reduzieren.

Übermittelt eine Behörde einen Stammdatensatz, gibt sie unterschiedliche personenbezogene Daten an eine andere Stelle weiter. Die Empfängerbehörde verfügt dann ebenfalls über die betreffenden Daten, ohne sie für die Durchführung des Fachverfahrens jedoch zwingend zu benötigen. Dieser Effekt verstärkt sich, je mehr personenbezogene Daten eine Behörde zur Identifikation des Betroffenen an die andere übermitteln muss, um eine zweifelsfreie Identifikation zu ermöglichen. Durch den Rückgriff auf eine (nicht-sprechende[131]) PKZ lässt sich die Menge der zu übermittelnden Daten hingegen auf das unbedingt Erforderliche reduzieren und so dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) entsprechen. Die Mitarbeiter der Empfangsbehörde erhalten dann neben der PKZ keine zusätzlichen personenbezogenen Daten des Bürgers. Die Identifikation des Betroffenen erfolgt in diesem Fall vielmehr anhand einer pseudonymisierenden Ziffern- bzw. Zahlenfolge.[132] Dem Persönlichkeitsrecht des Betroffenen drohen dann auch in dem Fall eines Datenlecks oder einer Kompromittierung der Daten beim Vorgang der Übermittlung grundsätzlich weniger Gefahren: Wer unbefugt auf die Daten zugreift, erhält nur eine Buchstaben- bzw. Ziffernfolge, mit der er grundsätzlich wenig anfangen kann. Je weiter die PKZ im Back-End (also im nicht unmittelbar sichtbaren Maschinenraum) der Datenverarbeitung verbleibt, desto vertretbarer ist ihr flächendeckender Einsatz.

Mit Blick auf die Aspekte „Fehleranfälligkeit“ und „Datenminimierung“ entpuppt sich ein Registerabgleich mittels Stammdaten im Vergleich zu einer PKZ im Ergebnis nicht als in gleicher Weise zur Registeroptimierung geeignetes und zugleich milderes Mittel.

(2) Temporäre Personenkennziffer als milderes Mittel?

Ein milderes Mittel im Verhältnis zu einer dauerhaft zugewiesenen PKZ könnte darin bestehen, eine PKZ nur temporär zu vergeben: Beteiligte Behörden müssten sie nach erfolgtem Abgleich wieder löschen. Eine (verfassungsrechtlich unzulässige) dauerhafte und umfassende Verknüpfung der Daten ist dadurch weitgehend ausgeschlossen; die Eingriffsintensität sinkt drastisch.[133]

Eine temporäre PKZ erzielt aber nicht die angestrebte Erleichterung des Abgleichs mittels eines eindeutigen Kennzeichens für eine Vielzahl von Fällen und Registern. Vielmehr müsste für jeden Vorgang jeweils eine neue PKZ für die Datensätze generiert werden. So entstünde eine neue Quelle für fehlerhafte Zuordnungen, Überschneidungen und Verknüpfungen. Zudem wäre ihre Neuvergabe für jeden Datenabgleich auch mit einem deutlich höheren

[131] Dazu bereits oben S. 9.
[132] Vgl. in diesem Kontext auch *von Lewinski* (Fn. 16), Art. 87 DSGVO, Rn. 19.
[133] Vgl. auch *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (Fn. 50), S. 81: je länger die PKZ gültig ist, desto verknüpfungsfreundlicher ist sie.

Verwaltungsaufwand verbunden, den es auf der Suche nach geeigneten Maßnahmen ja gerade zu minimieren gilt. Daher entpuppt sich ein temporäres Personenkennzeichen nicht mit hinreichender Gewähr als in gleichem Maße geeignet, um die Regulierungsziele zu erreichen wie eine dauerhaft vergebene PKZ.

bb) Erforderlichkeit mit Blick auf den Zensus

In Deutschland gibt es kein zentrales Register, das alle für eine registerbasierte Volkszählung erforderlichen Daten sammelt. Erst die Zusammenführung der unterschiedlichen Registerdaten für Zwecke der amtlichen Statistik generiert daher die für eine Registerzählung erforderliche Datenlage. Ebenso wie der Registerabgleich ist die Sammlung verschiedener Registerdaten für einen registerbasierten Zensus nur unter Nutzung einer statischen Kennziffer effizient möglich.[134]

So vermag es nicht zu verwundern, dass auch das Zensusgesetz 2011 nicht ohne eine dafür gesondert vergebene Kennziffer auskam. § 13 Abs. 1 ZensG sieht explizit die Vergabe von Ordnungsnummern vor, um eine Datenzusammenführung für statistische Zwecke zu ermöglichen (§ 13 Abs. 2 ZensG 2011).[135]

Die Ordnungsnummer des § 13 ZensG 2011 greift indes nicht auf Daten sämtlicher oder der meisten Verwaltungsbereiche zu, sondern lediglich auf einen spezifischen Ausschnitt wichtiger Erfassungsdaten.[136] Will der Staat eine Vielzahl unterschiedlicher Registerdaten zusammenführen, um sie als Grundlage eines Zensus heranzuziehen, wird die Ordnungsnummer in der Sache zu einer allgemeinen PKZ.[137] Die Erforderlichkeitsprüfung fokussiert sich dann auf die Frage, welche Registerdaten die zuständige Behörde zur Durchführung des Zensus im Einzelnen benötigt. Davon ist aber nur die gegenständliche Reichweite der genutzten PKZ betroffen, nicht aber die grundsätzliche Erforderlichkeit ihrer Einführung.

(1) Verzicht auf einen registergeschützten Zensus – Vollzählung als milderes Mittel?

In seinem Volkszählungsurteil hat das BVerfG das Bedürfnis nach einer PKZ als Teil eines registerbasierten Zensus nicht als Rechtfertigungsgrund dafür ausreichen lassen, eine solche zu nutzen. Vielmehr hat es die Vollzählung als milderes, gleich effektives und damit verfassungsrechtlich gebotenes Mittel im Verhältnis zu einem Registerzensus eingestuft. Denn ein solcher sei nur durch eine Verknüpfung der Registerdaten unter Rückgriff auf ein

---

[134] Vgl. *Martini* (Fn. 84), S. 25. Siehe auch *McKinsey & Company Inc.* (Fn. 4), S. 12. Zum Schutz des informationellen Selbstbestimmungsrechts darf der Staat Ordnungsnummern nur vergeben, sofern diese keine Angaben über persönliche und sachliche Verhältnisse enthalten, die über die Erhebungs- und Hilfsmerkmale hinausgehen (§ 9 Abs. 2 BStatG) – das impliziert ein grundsätzliches Verbot sprechender Kennzeichen.
[135] Dazu bereits auch oben S. 2.
[136] Dazu *Martini* (Fn. 84), S. 15 ff. sowie 25 ff.
[137] Gleichzeitig lässt sich die Verwendung der Ordnungsnummern im Rahmen des Zensus für Zwecke amtlicher Statistik nicht ohne Weiteres mit einer Ordnungsnummer für den allgemeinen Verwaltungsvollzug vergleichen.

einheitliches Personenkennzeichen realisierbar. Vor diesem Hintergrund sah das BVerfG eine PKZ seinerseits als entscheidenden Schritt zur (verfassungswidrigen) Katalogisierung des einzelnen Bürgers an.[138]

Amtliche Statistiken verfolgen ein wichtiges Gemeinwohlziel: Sie sollen bislang noch nicht kategorisierte Daten (aus Aktenbeständen) einer systematischen Aufarbeitung zuführen, um auf dieser Grundlage Planungsgrundlagen für gesamtgesellschaftliche Priorisierungsentscheidungen zu schaffen. Was physisch in unterschiedlichsten Archiven lag und sich schon aufgrund des hohen Aufwands kaum zu einem Profil verknüpfen ließe, sollte der Zensus zum Zwecke hoheitlicher Erkenntnis zusammentragen. Die Möglichkeiten elektronischer Datenverarbeitung steckten damals noch in ihren Kinderschuhen. Das Potenzial einer per Internet vernetzten Behördenlandschaft, digitaler Verwaltungsangebote sowie das gewandelte Bewusstsein der Bevölkerung zum Umgang mit ihren Daten gegenüber Big-Data-Anbietern, die über den Einzelnen bisweilen mehr wissen als das Individuum selbst, waren damals ein (fernes) Zukunftsszenario. Unterdessen haben sich die Vorzeichen geändert – auch die Möglichkeiten (zugleich aber auch die Gefahren) technischer Sicherung personenbezogener Daten gegen unbefugten Zugriff, z. B. durch Verschlüsselungsmechanismen und individualisierte Zugriffsrechte.

Für die Zukunft lässt sich zudem prognostizieren, dass die Belastungen, die für Bürger mit einer Vollerhebung einhergehen, jedenfalls dann steigen werden, wenn es die unionsrechtlichen Vorgaben gebieten, zensustypische Daten künftig in immer kürzeren zeitlichen Abständen und mit höherer Aktualität zu erheben.[139] So plant die EU, georeferenzierte Statistiken mit hoher Aktualität zu erheben.[140] Unter Beibehaltung des derzeitigen Systems der Bevölkerungsfortschreibung ist dies aber kaum sachgerecht möglich.[141] Die künftig geforderte hohe Aktualität der Statistiken ginge unter Rückgriff auf die Methodik der Vollerhebung wegen des damit für die Betroffenen verbundenen Zeitaufwands mit einer zunehmend stärkeren Beeinträchtigung ihrer allgemeinen Handlungsfreiheit einher. Allein der Zensus 2011 löste bei den Bürgern einen Zeitaufwand von 8,4 Millionen Stunden aus – und das, obwohl er bereits weitgehend registerbasiert erfolgte (namentlich durchschnittlich nur 10 % der Bevölkerung einer direkten Befragung ausgesetzt waren).[142] Geht man davon aus, dass der Zeitaufwand der Bevölkerung für statistische Erhebungen

---

[138] BVerfGE 65, 1 (56 f.): „Auch die Übernahme sämtlicher Daten aus bereits vorhandenen Dateien der Verwaltung ist keine zulässige Alternative zu der vorgesehenen Totalzählung. Denn die Nutzung von Daten aus verschiedenen Registern und Dateien würde voraussetzen, daß technische, organisatorische und rechtliche Maßnahmen getroffen werden, die es erst erlauben, diese Daten, bezogen auf bestimmte Personen oder Institutionen, zusammenzuführen. Eine solche Maßnahme wäre zum Beispiel die Einführung eines einheitlichen, für alle Register und Dateien geltenden Personenkennzeichens oder dessen Substituts. Dies wäre aber gerade ein entscheidender Schritt, den einzelnen Bürger in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren. Die Verknüpfung vorhandener Dateien wäre danach auch nicht das mildere Mittel."
[139] *Statistisches Bundesamt* (Fn. 7), S. 13.
[140] *Statistisches Bundesamt* (Fn. 7), S. 13.
[141] *Statistisches Bundesamt* (Fn. 7), S. 13.
[142] Vgl. *Statistisches Bundesamt* (Fn. 7), S. 14 Fn. 2; *Martini* (Fn. 84), S. 15 ff.

künftig weiter steigen wird, so steht zu erwarten, dass eine Vollerhebung nur auf wenig Akzeptanz in der Bevölkerung stoßen wird.[143] Die grundrechtliche Beeinträchtigungswirkung, die von einem persönlichen Aufsuchen eines staatlichen Beauftragten in der Wohnung eines zu Befragenden ausgeht, empfinden viele Bürger in der Summe als höher als die Belastung, die von einem Abgleich von Registerdaten ausgeht, welche die Verwaltung ohnehin über ihn zur Verfügung hat.[144] Nicht zuletzt weisen Vollerhebungen einen nicht unbeträchtlichen Fehlergrad auf, der auf einem Bündel vieler Faktoren beruht.[145]

Logische Folge wären Abstriche bei der empirischen Aussagekraft eines Zensus, die ab einer gewissen Grenze seine Sinnhaftigkeit gegenüber repräsentativen Umfragen in Frage stellt. Spätestens ab diesem Zeitpunkt spricht vieles dafür, dass die registerbasierte Ermittlung zensustypischer Daten – mit Blick auf die Belastungen, die von (ggf. mit Sanktionsmitteln flankierten) Personenbefragungen ausgehen – insgesamt im Vergleich zu einer Vollzählung das wirksamere Mittel ist, um die zensustypischen Daten zu erheben.[146]

Profiteur eines registergestützten Zensus mittels PKZ sind aber nicht nur die Bürger. Auch bei staatlichen Stellen zöge eine regelmäßig wiederkehrende Vollerhebung einen wachsenden Ressourcenaufwand nach sich.[147] Im Vergleich dazu bieten die Innovationen (voll-)automatisierter Datenverarbeitung mittels PKZ substanzielle Effizienzvorteile.

(2) Verzicht auf eine dauerhafte PKZ

Allein zu Zwecken des Zensus bedürfte es jedenfalls keiner *dauerhaften* PKZ. Nach Abschluss des Zensus hat die Nummer keine weitere Funktion; ihre Daseinsberechtigung hat sie dann bis auf Weiteres eingebüßt. Dieser Wertung folgt auch § 13 Abs. 3 S. 2 ZensG 2011: Er verpflichtet die Statistikbehörde im Interesse der Gebote der Datensparsamkeit und der Zweckbindung dazu, die Ordnungsnummer nach der Beendigung des Zensus zu löschen.

Soll eine neue, dauerhaft vergebene PKZ nur für die Zwecke eines Zensus Anwendung finden, ist sie jedenfalls zurzeit nicht erforderlich.[148] Die Durchführung des Zensus ist aber nur *ein* Anwendungsfeld der PKZ. Über allen ihren Zielsetzungen schwebt das zusätzliche Bedürfnis,

---

[143] *Statistisches Bundesamt* (Fn. 7), S. 13.
[144] Dazu auch *Martini* (Fn. 84), S. 23 f.
[145] *Martini* (Fn. 84), S. 27.
[146] *Martini* (Fn. 84), S. 24. Ob eine registerbasierte Volkszählung das Recht auf informationelle Selbstbestimmung hinreichend achtet, ist letztendlich eine Frage der Angemessenheit.
[147] *Statistisches Bundesamt* (Fn. 7), S. 13.
[148] Der Befund kann sich aber perspektivisch ändern. Eine PKZ kann ihren ursprünglichen Zweck beibehalten, wenn der Staat sie *auch* zur Durchführung eines neuen Zensus heranzieht. Im Vergleich zur Neuvergabe von Ordnungsnummern lässt sich umso eher Verwaltungsaufwand einsparen, je kürzer die zeitliche Periode zwischen zwei Zensusterminen ist. Es ist bereits heute abzusehen, dass diese Perioden – auch vor dem Hintergrund gesellschaftlicher Disruptionen, starker Migrationsbewegungen und zunehmend fragmentierter Lebensläufe – immer kürzer ausfallen werden; *Statistisches Bundesamt* (Fn. 7), S. 13. In diesem Fall wird die stetige Neuvergabe von Ordnungsnummern aufgrund des damit einhergehenden Verwaltungsaufwandes nicht mehr ebenso geeignet sein, die Effizienzpotenziale eines registerbasierten Zensus auszuschöpfen, wie die Nutzung einer dauerhaften PKZ.

die Registerqualität mit Hilfe eines PKZ-gestützten Abgleichs zu steigern – und dadurch generell zu vereinfachen und sowohl für Bürger als auch für Behörden belastungsärmer zu gestalten.

cc) Anreizmechanismen zur Registeroptimierung

Neben einer Kennziffer weist die Qualität staatlicher Register viele Stellschrauben auf, an denen sich drehen lässt, um die mit der Registerführung intendierte Aufgabenerfüllung zu gewährleisten.[149] Denn die Fehlerquellen staatlicher Register, insbesondere Untererfassungen (Fehlbestand) sowie Übererfassungen („Karteileichen“) der durch die Kommunen verwalteten Melderegister,[150] haben viele Ursachen. Zu ihnen gehören nicht nur die Komplexität der Lebensverhältnisse, welche die Register abbilden sollen, sondern auch die Anreizmechanismen, welche die Verwaltung bei der Pflege der Register steuert. So entfaltet bspw. eine Übererfassung von Einwohnern für Kommunen typischerweise grundsätzlich einen positiven Effekt. Denn jeder zusätzlich im Melderegister erfasste Einwohner schlägt für Kommunen mit mehreren tausend Euro positiv zu Buche – im Rahmen des kommunalen Finanzausgleichs, beim Zuschnitt der Wahlkreise, der Festsetzung der Zahl der Gemeinderäte oder der Verteilung der Straßenbaulast etc.[151] Die Meldebehörden unterliegen daher im Hinblick auf die Registerführung einem Motivationsdilemma:[152] Einerseits sind sie zur ordnungsgemäßen Registerführung bundesrechtlich verpflichtet, andererseits verbessert jede Übererfassung ihre finanzielle Ausgangslage spürbar. Das beeinträchtigt die Nachhaltigkeit der Anstrengungen, Meldefehlern der Bevölkerung, die in Übererfassungen münden, unter den Bedingungen knapper Personalressourcen durch Nachforschungen bei den betroffenen Bürgern mit Entschiedenheit entgegenzuwirken. Die staatlichen Register bilden in der Folge die Realität in den Gemeinden auch aus diesem Grund nicht vollständig ab.[153] Das strukturelle Dilemma ist Teil des föderalen Vollzugssystems einer dezentralen Ausführung des Melderechts durch die Gemeinden. Es ist von dem nachvollziehbaren Gedanken getragen, die Vollzugsnähe der Meldeverwaltung zur Bevölkerung durch eine ortsnahe Zuständigkeit zu gewährleisten. Einfach gestrickte Hausrezepte wirken dem damit verbundenen Grundproblem einer zwiespältigen Motivationslage nur bedingt effektiv entgegen.

Neben technischen Maßnahmen des Registerabgleichs sind aber strukturelle Verwaltungsmaßnahmen als milderes Mittel erwägenswert, welche den Behörden Anreize setzen, die Qualität der Register zu optimieren.

---

[149] Zu technischen Optimierungspotenzialen in der föderalen Registerlandschaft bereits Fn. 7.
[150] Siehe dazu bspw. *Martini* (Fn. 84), S. 37 f.
[151] Dazu *Martini* (Fn. 84), S. 13 ff.
[152] Dazu auch schon oben S. 28.
[153] Dazu ausführlich *Martini* (Fn. 84), S. 37 ff.

Insbesondere die gesetzlichen Kontrollpflichten der Ortsbehörden zu straffen sowie den Zeitturnus regulärer Kontrollen zu verkürzen und Sanktionierungen von Meldefehlern der Bevölkerung zu verschärfen, kann ein Weg sein, zur Qualität der Register beizutragen.

Solche Maßnahmen erreichen die Zielsetzungen der Registeroptimierung jedoch nur bis zu einem gewissen Grade. Denn Sanktionierungen von Meldefehlern der Bevölkerung und Verkürzungen des Kontrolltaktes gehen zum einen nicht ohne Weiteres mit Gewissheit mit einer faktischen Verbesserung der Meldetreue in der Bevölkerung einher: Die Ursachen für unterbleibende oder fehlerhafte Meldungen sind vielfältig (auch wenn Vergesslichkeit, Nachlässigkeit oder fehlendes Bewusstsein einer Meldepflicht eine häufige Ursache bilden, denen Verkürzungen des Kontrollzeitraums entgegenwirken können). Sanktionen können unerwünschtes Verhalten ihrer Natur nach nur ex post ahnden, das erwünschte Verhalten aber nicht immer garantieren. Zum anderen erschöpft sich die Zielsetzung einer PKZ nicht darin, *Melde*register zu optimieren. Vielmehr ist es ihr Bestreben gerade, Querverbindungen zwischen verschiedenen Sachbereichen, etwa Familienleistungen verschiedener zuständiger Behörden, herstellen zu können, die sachlich miteinander in Verbindung stehen, deren sachliche Verbindung zueinander zwar vorhanden, aber nicht ohne Weiteres auf der Grundlage eines händischen Abgleichs zu erkennen ist. Kontrollen sowie sonstige Maßnahmen der Registeroptimierung können die technischen Möglichkeiten eines Datenabgleichs durch PKZ zur Vermeidung von Fehlern in ihrer Funktionalität nicht vollständig ersetzen.

dd) Ergebnis

Nicht nur um Datensynchronisation und Registeraustausch zu erleichtern, sondern auch um im Vorfeld des Zensus eine valide Datengrundlage zu schaffen, die bestenfalls auch ohne – bzw. allenfalls mit einer äußerst geringfügigen – stichprobenbasierten Korrektur auskommt, ist eine dauerhafte PKZ nach derzeitigem Erkenntnisstand erforderlich. Eine temporäre PKZ sowie sonstige Maßnahmen erweisen sich nicht als in gleichem Maße geeignet.

c) Angemessenheit einer Personenkennziffer

Dreh- und Angelpunkt der verfassungsrechtlichen Zulässigkeit einer PKZ ist die Frage nach der Angemessenheit ihrer Einführung. Die Belastungen, die eine PKZ für das informationelle Selbstbestimmungsrecht auslöst, dürfen nicht außer Verhältnis zu den legitimen Zwecksetzungen stehen, die der Gesetzgeber mit ihr verfolgt.

aa) Aussagen des BVerfG im Volkszählungsurteil

Die rote Linie verfassungsrechtlicher Zulässigkeit überschreitet eine PKZ jedenfalls dann, wenn sie darin mündet, dass der Staat umfassende Persönlichkeitsprofile erstellt. Das ist der

Fall, wenn der Staat Einzeldaten unabhängig vom Zweck der Datenerhebung in einer Weise sammelt, die zu einer „persönlichkeitsfeindliche[n] Registrierung und Katalogisierung des Einzelnen“ führt.[154]

Wann ein Persönlichkeitsprofil „umfassend“ ist, lässt sich nicht ganz trennscharf bestimmen. Eine Profilbildung als solche beginnt bereits, wenn die Zusammenführung vorhandener Einzeldaten neue Rückschlüsse über die betroffene Person erlaubt und so zumindest ein (Teil-)Abbild der Persönlichkeit entsteht.[155] Umgekehrt ist nicht jedes Teilabbild der Persönlichkeit per se verfassungsrechtlich verfemt. Je mehr Lebensbereiche ein Profil aber erfasst und umso länger und lückenloser der Staat Daten zu diesen Lebensbereichen sammelt, desto eher verletzt das Abbild das Persönlichkeitsrecht der Betroffenen und tangiert ihre Menschenwürde.[156]

(1) Die Personenkennziffer – ein per se verfassungswidriges Instrument?

Einen Datenverbund sensibler Verwaltungsdaten „durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal“[157] zu erschließen, hat das BVerfG in seinem Volkszählungsurteil für unzulässig erklärt.

(a) Enge Deutung: Verbot jeglicher Anknüpfung an das Mittel „Personenkennziffer“; Zulässigkeit der Steuer-ID als bereichsspezifische Personenkennziffer

Die Passage im Volkszählungsurteil des BVerfG zu Personenkennzeichen lässt sich so interpretieren, dass das Gericht die Einführung (einer sowohl einheitlichen als auch bereichsspezifischen) PKZ als per se verfassungswidrigen Eingriff in das Recht auf informationelle Selbstbestimmung gebrandmarkt hat. Derart strikt versteht die Aussage jedoch – soweit ersichtlich – niemand. Die meisten lesen sie lediglich als eine Absage an eine *allgemeine* PKZ, nicht demgegenüber einer bPKZ (wie etwa die Steuer-ID)[158], da bei ihr die

---

[154] BVerfGE 65, 1 (48) unter Hinweis auf BVerfGE 27, 1 (6).
[155] *Hornung* (Fn. 84), S. 159 m. w. N.
[156] *Hornung* (Fn. 84), S. 160.
[157] BVerfGE 65, 1 (53).
[158] Wenngleich in Deutschland bislang keine allgemeine PKZ Verwendung findet, so nutzt die Verwaltung bereits heute Ordnungsnummern zur eindeutigen Identifizierung der Bürger, vgl. Fn. 16. Ihre Verwendung ist nicht unumstritten. Insbesondere die Einführung der Steuer-ID hat in der jüngsten Vergangenheit hohe Wellen geschlagen. Das Bundeszentralamt für Steuern teilt jedem Steuerpflichtigen eine einheitliche und dauerhafte Steuer-ID zu (§ 139a Abs. 1 S. 1 Hs. 1 AO), siehe FG Köln, Urt. v. 7.7.2010 - 2 K 2999/08 –, juris, Rn. 136. Sie dient seiner eindeutigen Identifizierung in Besteuerungsverfahren und ist gegenüber den Finanzbehörden bei Anträgen, Erklärungen oder Mitteilungen anzugeben (§ 139a Abs. 1 S. 3 AO). Die Finanzbehörden dürfen die Steuer-ID grundsätzlich nur verwenden, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben notwendig ist (§ 139b Abs. 2 AO), während Dritte die Steuer-ID nur zur Erfüllung ihrer Meldepflichten gegenüber den Finanzbehörden nutzen dürfen (§ 139b Abs. 2 AO). Seinerzeit hegten das FG Köln und der Bundesdatenschutzbeauftragte *Peter Schaar* Bedenken gegen die verfassungsrechtliche Zulässigkeit dieser Ordnungsnummer FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 –, juris, Rn. 58, 82, 90; *Schaar* (Fn. 14), 49 f. Der Bundesfinanzhof teilte die Zweifel aber nicht und urteilte, dass die Steuer-ID – jedenfalls zum damaligen Zeitpunkt – den verfassungsrechtlichen Anforderungen gänzlich entspreche, BFH, Urt. v. 18.1.2012 – II R 49/10 –, juris, Rn. 46.

Gefahr einer umfassenden Profilbildung im Vergleich zu einer einheitlichen PKZ deutlich sinkt.[159]

So ließ etwa das FG Köln in seiner Entscheidung zur rechtlichen Zulässigkeit der Steuer-ID – unter Verweis auf die Judikatur des BVerfG im Volkszählungsurteil[160] – verlauten, dass es die Einführung einer allgemeinen (also nicht lediglich bereichsspezifischen) PKZ für verfassungswidrig hält („von vornherein unverhältnismäßig im engeren Sinne und damit verfassungswidrig“).[161] Die Steuer-ID ordnete das FG Köln in seinem Urteil demgegenüber nicht als (allgemeine) PKZ ein.[162] Zwar meldete es an ihrer Verfassungskonformität Bedenken an. Schlussendlich war es aber von der Verfassungswidrigkeit nicht restlos überzeugt:[163] „Mit der Einführung der Steueridentifikationsnummer“ sei zwar „der erste, möglicherweise entscheidende, Schritt in eine solche vermeintliche Richtung“ getan.[164] Es sei aber nicht erwiesen, „dass §§ 139a, 139b AO im Zusammenwirken mit anderen Vorschriften darauf zielen oder hinauslaufen, eine allgemein umfassende Datensammlung zur weitestmöglichen Rekonstruierbarkeit jedweder Aktivitäten der Bürger zu schaffen“.[165] Der BFH bestätigte die Ausgangsentscheidung des Finanzgerichts in diesem Punkt: Er erkannte in der Steuer-ID keinen Verstoß gegen das Recht auf informationelle Selbstbestimmung.[166] Zur Verfassungsmäßigkeit einer darüber hinausgehenden, allgemeinen PKZ äußerte sich der BFH – anders als das FG Köln – aber nicht.[167]

(b) Weite Deutung: Ergebnisorientiertes Verbot, „eine umfassende Registrierung und Katalogisierung der Persönlichkeit“ zu ermöglichen (statt eines instrumentellen Verbots)

Indem das BVerfG in seinem Volkszählungsurteil nicht nur auf das „einheitliche Personenkennzeichen“, sondern auch auf ein „sonstiges Ordnungsmerkmal“ abgestellt hat, eröffnet es eine weitere Deutungsmöglichkeit: Nicht die Kennzeichnung einer Person mittels einer Zahl als solche ist verfassungsrechtlich untragbar, sondern vielmehr vorrangig die sich aus dieser Kennzeichnung ergebenden Verknüpfungsmöglichkeiten personenbezogener Daten zu einem „persönlichkeitsfeindlichen“ Datenbestand in staatlicher Hand. Im Vordergrund der verfassungsrechtlichen Analyse einer PKZ steht dann die mit ihr

---

[159] So etwa *Steinmüller*, DuD 1984, 91 (95).
[160] Siehe FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 – juris, Rn. 135.
[161] FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 – juris, Rn. 134.
[162] Vgl. FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 – juris, Rn. 135 f.
[163] FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 – juris, Rn. 90.
[164] FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 – juris, Rn. 144. Vgl. zu der Befürchtung, dass die initiale Einführung einer PKZ sich später als Trojanisches Pferd entpuppt, unten S. 43.
[165] FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 – juris, Rn. 144.
[166] BFH, Urt. v. 18.1.2012 – II R 49/10 –, juris, Ls.
[167] Das könnte dafür sprechen, dass das FG Köln die Referenz zu einer allgemeinen PKZ mehr als Argumentationsstütze einer Abgrenzung des Gefahrpotenzials „nach oben“ – und weniger als Feststellung im Sinne eines *obiter dictum* – genutzt hat.

einhergehende Gefahr für das Recht auf informationelle Selbstbestimmung durch eine umfassende Profilbildung.

Für diese Lesart streitet ein wichtiger Aspekt: Eine Fixierung auf das regulatorische Mittel „PKZ" droht den zeitlichen Kontext der Entscheidung und den Kern der Botschaft, welche das BVerfG 1983 ausgesandt hat, aus den Augen zu verlieren. Denn zur damaligen Zeit waren die Möglichkeiten automatisierter Datenverarbeitungen im heutigen Stil – und die damit verbundenen Vor- und Nachteile – in ihrem Ausmaß noch nicht im Ansatz absehbar. Unterdessen ermöglichen es Big-Data-Technologien, insbesondere Verfahren des Data Mining, unterschiedliche Daten, die für sich genommen nur einen schwachen Personenbezug aufzuweisen brauchen, zu einem einheitlichen Persönlichkeitsprofil zusammenzuführen.[168] Bereits ohne die Existenz einer verbindenden PKZ macht die Kombination weniger (personenbezogener) Daten den Einzelnen im Datenmeer des Word Wide Web identifizierbar. Wenige Daten reichen typischerweise aus, um den Einzelnen konkret zu erfassen und von Namensvettern oder Nachbarn abzugrenzen; sie eignen sich potenziell als Grundlage, um durch Zuspeicherung weiterer Informationen ein Persönlichkeits- oder Bewegungsprofil zu erstellen.[169] Vor dem Angesicht moderner Datenverarbeitungsmittel präsentiert sich eine PKZ als nur *eines von vielen anderen Mitteln*, um eine Person fehlerfrei zu identifizieren und personenbezogene Informationen zu einem Profil zusammenzufügen.[170] Gegen diese strukturierte, in Summe persönlichkeitsfeindliche Zusammenführung als verfassungswidrigen Ergebniszustand richtet sich das Diktum des BVerfG, nicht gegen das *Mittel*, das die Zusammenführung herbeiführt.[171]

Im 21. Jahrhundert ist die PKZ also nicht länger die *einzige* Büchse der Pandora, in der die Gefahr einer umfassenden Profilbildung schlummert – sondern im Grundsatz lediglich eines unter mehreren Vehikeln, das den Einzelnen verlässlicher und weniger fehleranfällig individualisiert als andere personenbezogene Daten in Kombination.[172] Einer PKZ wohnt daher mit Blick auf die Möglichkeit zur Profilbildung keine diese erst ermöglichende, sondern lediglich eine die persönlichkeitssensible Datenverquickung *erleichternde* Funktion inne.[173]

---

[168] *Gola* (Fn. 5), Art. 87, Rn. 3; *Hornung* (Fn. 84), S. 161; *Weichert* (Fn. 6), Art. 87, Rn. 20; *Martini*, Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz, in: Hill/Martini/Wagner (Hrsg.), Die digitale Lebenswelt gestalten, 2015, S. 97 (105, 121 ff.).
[169] Dazu bspw. BVerfGE 125, 260 (319); *Montjoye/Laura Radaelli et al.*, science 347 (2015), 536 ff.
[170] Ihr kommt allerdings wohl das größtmögliche Maß an Eindeutigkeit zu.
[171] Deshalb kommt es letztlich auch nicht darauf an, ob man von Personenkennziffer, Identifikationsnummer oder Ordnungsnummer spricht. Entscheidend ist das normative Konzept, das sich hinter der Terminologie verbirgt.
[172] In diesem Sinne auch *Hornung* (Fn. 84) S. 161.
[173] Ähnlich in der Sache auch *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein* (Fn. 50), S. 73 f., das hiermit aber die Verfassungswidrigkeit einer einheitliche PKZ begründet.

Mit Blick auf die veränderten technischen Möglichkeiten[174] entspricht es einer zeitgemäßen und am geschützten Rechtsgut der informationellen Selbstbestimmung orientierten Deutung, die Aussagen des Volkszählungsurteils nicht als an das Instrument „PKZ" anknüpfendes pauschales Verbot zu begreifen.[175] Vielmehr verstößt eine PKZ nur insoweit gegen die Verfassung, als von ihr die nicht hinnehmbare Gefahr ausgeht, dass der Staat sie zur umfassenden Verknüpfung vorhandener Datenbestände nutzt und so einer persönlichkeitsfeindlichen Katalogisierung des Einzelnen den Weg ebnet.

Lassen sich die Gefahren für das informationelle Selbstbestimmungsrecht hingegen durch wirksame technische, organisatorische und rechtliche Maßnahmen effektiv bannen, so bewegt sich ihre Nutzung innerhalb der Zulässigkeitsgrenzen des Grundgesetzes.[176] Insofern deckt sich die Wertung des deutschen Verfassungsrechts im Grundsatz weitgehend dem normativen Wertungsprogramm des Art. 87 DSGVO.[177]

Welche organisatorischen, technischen und rechtlichen Maßnahmen der Gesetzgeber in concreto vorsehen muss, sagt die Verfassung nicht. Insoweit verfügt der Gesetzgeber über einen Handlungsspielraum. Er findet seine Grenze allerdings in dem Gebot hinreichend effektiven Grundrechtsschutzes vor einer umfassenden Katalogisierung der Persönlichkeit.

(2) Schlussfolgerungen und Zwischenfazit: keine umfassende Datenzusammenführung mittels Personenkennziffer

In der Sache hat das BVerfG in seinem Volkszählungsurteil eine spezifische Verwendung der PKZ, die namentlich eine umfassende Katalogisierung der Persönlichkeit ermöglicht, als unzulässig deklariert: Eine solche Nummer darf zur Zusammenführung „sämtlicher Daten aus bereits vorhandenen Dateien der Verwaltung" keine Verwendung finden.[178] Eine Datensammlung unter dem Dach einer PKZ, die den Versuch unternimmt, die Persönlichkeit einer bestimmten Person digital abzubilden und sämtliche über sie vorhandenen Informationen zusammenzutragen, ist mithin verfassungswidrig. Denn dann wäre eine Katalogisierung des Einzelnen in einer staatlichen Datenbank nicht nur zu befürchten, sondern die logische Folge. Die Errichtung eines „Super-Registers", in dem sich mit Hilfe der

[174] Das gilt nicht nur für neue Big-Data-Verfahren zur Identifizierung einzelner Personen aus unstrukturierten digitalen Datenmassen, sondern auch für neue Möglichkeiten des technischen Datenschutzes, insbesondere der Pseudonymisierung und Verschlüsselung. So war es zur Zeit des Volkszählungsurteils etwa noch nicht vorstellbar, dass es – wie in Österreich – zwar eine Stammzahl gibt, dass diese aber keine – außer der sie verwaltenden – Behörde zu Gesicht bekommt; dazu im Einzelnen unten S. 36 ff. Das BVerfG hatte wohl eher eine Kennziffer vor Augen, die auf Papierdokumenten, in Akten und in statistischen Erhebungen offen und untrennbar zu den Stammdaten der Bürger hinzutritt und deshalb einen weiten, für den Bürger kaum überblickbaren Anwendungsradius eröffnet.
[175] Im Ergebnis wohl auch *Podlech*, in: Denninger/Hoffmann-Riem/Schneider et al. (Hrsg.), AK-GG, 3. Aufl., 2001, Art. 2 Abs. 1, Rn. 79 Fn. 115.
[176] So auch schon *Martini* (Fn. 84), S. 25 f. zur Einführung einer Ordnungsnummer durch § 13 ZensG 2011.
[177] Dazu ausführlich oben S. 6.
[178] BVerfGE 65, 1 (56).

PKZ alle Informationen über die Bürger aus sämtlichen Einzelregistern zusammentragen lassen, bräche mit der Wertordnung der Verfassung.

Ein generelles Verbot, ein Konzept mit dem Namen „Personenkennziffer" einzuführen, ergibt sich daraus jedoch nicht. Die tatsächlichen Rahmenbedingungen der Verarbeitung personenbezogener haben sich seit dem Jahre 1983 drastisch verändert. Zugleich kann der Verweis auf neue technologische Entwicklungen aber nicht darüber hinwegtäuschen, dass ein zusätzliches Identifikationsmerkmal in staatlichen Registern neue Gefahrenpotenziale heraufbeschwört. Selbst wenn der Gesetzgeber die Verwendung einer PKZ auf den Abgleich oder die Zusammenführung der Daten aus öffentlichen Registern beschränkt, erleichtert er der Verwaltung damit die Profilbildung. Es besteht dann die *Gefahr*, dass der Staat beginnt, mit Hilfe der Personenkennzeichen Daten seiner Bürger zusammenzuführen und Persönlichkeitsprofile zu erstellen. Diese Gefahr muss der Gesetzgeber durch geeignete und wirksame technische organisatorische sowie rechtliche Anforderungen einhegen.[179]

Vor allem im Rahmen der Durchführung eines registergestützten Zensus ist der Einsatz einer allgemeinen PKZ verfassungsrechtlich besonders heikel, kommt ihr doch dort die Funktion zu, die Daten der unterschiedlichen Register zum Zwecke der statistischen Erhebung zusammenzuführen.[180] Je nachdem, wie viele und welche Register ein Zensus auf diese Weise miteinander verschneidet, kann daraus unmittelbar ein Profil des einzelnen Bundesbürgers entstehen. Auch der Umstand, dass diese Profilbildung „in der Anonymität einer statistischen Erhebung" geschieht, mindert die Belastungswirkung nicht signifikant.[181] Aus verfassungsrechtlicher Sicht muss es deshalb auch weiterhin bei dem sogenannten Rückspielverbot bleiben: Daten, die der Staat zu statistischen Zwecken erhebt, darf er anschließend nicht zum Verwaltungsvollzug verwenden.[182]

bb) Verfassungskonforme Ausgestaltung der Personenkennziffer: technische, organisatorische und rechtliche Maßnahmen, die eine Profilbildung durch die Personenkennziffer verhindern

Welche Maßnahmen technisch, organisatorisch und rechtlich hinreichend geeignet sind, um der Gefahr einer umfassenden Profilbildung wirksam entgegenzutreten, lässt sich nicht pauschal beantworten, sondern nur abstrakt beschreiben: Das Maß der Schutzmaßnahmen muss mit dem Gefahrengrad korrespondieren, den die jeweilige Konzeption der PKZ in ihrem individuellen Zuschnitt birgt. Sie müssen insbesondere dem Gebot der Zweckbindung (a) sowie dem Gebot der Transparenz und effektiven Rechtsschutzes (b) genügen.

---

[179] So bereits *Martini* (Fn. 84), S. 25. Dazu im Einzelnen sogleich S. 34 ff. Insbesondere Fragen nach geeigneten Maßnahmen der IT-Sicherheit und des technischen Datenschutzes sollte der Gesetzgeber frühzeitig in seine Überlegungen miteinbeziehen.
[180] Zu der Funktion der PKZ siehe S. 1 f.
[181] BVerfGE 27, 1 (6); BVerfGE 65, 1 (53). Heute, in Zeiten von Big Data, wiegen die Risiken wegen der Möglichkeit, eine De-Anonymisierung vorzunehmen, tendenziell noch schwerer.
[182] *Martini* (Fn. 84), S. 26.

(1) Anforderungsprofil an rechtliche Maßnahmen zur Verhinderung einer Profilbildung mittels Personenkennziffer

(a) Zweckbindung

Maßnahmen, die einer Profilbildung entgegenwirken, finden ihre normative Fundierung und Absicherung insbesondere im datenschutzrechtlichen Zweckbindungsgrundsatz.[183] Er ist kein bloßes Konstrukt des einfachgesetzlichen Datenschutzrechts, sondern – ebenso wie im unionalen Recht[184] – ein „Kernelement des verfassungsrechtlichen Datenschutzes".[185] Gleichwohl sind Zweckänderungen auch nach den Wertungen des nationalen Verfassungsrechts nicht schlechthin unzulässig[186] – sie bedürfen jedoch einer eigenen gesetzlichen Grundlage.[187]

Dem Staat steht es zudem offen, Daten von Beginn an zu mehreren Zwecken zu erheben. Dann wächst dem Gebot der Normenklarheit[188] eine besondere Bedeutung zu: Der Bürger muss zweifelsfrei erkennen können, für welche Zwecke seine Daten Verwendung finden.[189]

(b) Transparenz und Rechtsschutz

Neben einer hinreichend engen Zweckbindung entlang der Kette der Datenverarbeitungsprozesse muss der Gesetzgeber seinen Umgang mit personenbezogenen Daten auch transparent gestalten: Transparenz ist eine *condicio sine qua non* des grundrechtlichen Datenschutzes.[190] Denn erst die Kenntnis der Datenverarbeitung ermöglicht es dem Betroffenen, seine Rechte (etwa das Recht auf Löschung personenbezogener Daten) geltend zu machen.[191]

---

[183] Siehe auch FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 –, juris, Rn 130.
[184] Siehe dazu bereits S. 11 ff.
[185] BVerfG, NJW 2016, 1781 (1802) mit Verweis auf BVerfGE 65, 1 (45 f., 61 f.). Im Volkszählungsurteil judizierte das BVerfG: „Die Verwendung der Daten ist auf den gesetzlich bestimmten Zweck begrenzt. Schon angesichts der Gefahren der automatischen Datenverarbeitung ist ein – amtshilfefester – Schutz gegen Zweckentfremdung durch Weitergabeverbote und Verwertungsverbote erforderlich." BVerfGE 65, 1 (46).
[186] BVerfGE 125, 260 (333).
[187] BVerfGE 125, 260 (333) mit Verweis auf die vorangegangene eigene Judikatur.
[188] Ausführlich mit Verweisen auf die Judikatur des BVerfG *Gersdorf*, in: Gersdorf/Paal (Hrsg.), BeckOK InfoMedR, 16. Ed., 2017, Art. 2 GG, Rn. 72 ff.
[189] Anders als in der Zeit des Volkszählungsurteils ist es in modernen IT-Umgebungen tendenziell leichter, die Zielsetzung der Zweckbindung durch technische Maßnahmen abzusichern. Ging es bei der Zweckbindung in Zeiten der Aktenbearbeitung durch Sachbearbeiter aus Fleisch und Blut insbesondere darum, durch normative Vorgaben tatsächlichen Möglichkeiten unzulässiger Weiterverwendung bestimmter Datengrenzen zu setzen, lässt sich die Zugriffsmöglichkeit heute bereits in der Programmierphase (insbesondere in der Konfiguration der Schnittstellen) berücksichtigen – nicht erst auf Ebene der Handlungskontrolle.
[190] BVerfGE 125, 260 (335). Siehe auch BVerfGE 65, 1 (46): „Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungspflichten, Auskunftspflichten und Löschungspflichten wesentlich."
[191] BVerfGE 100, 313 (361).

Wie die verfassungsrechtlich geforderte Transparenz im Einzelnen herzustellen ist, gibt das Grundgesetz nicht detailliert vor.[192] Ein Weg kann darin bestehen, dem Verantwortlichen Informationspflichten aufzuerlegen und/oder dem Betroffenen Auskunftsrechte zuzugestehen.[193] Auf diese Weise kann sich der Betroffene bspw. darüber vergewissern, welche eigenen personenbezogenen Daten die Behörde tatsächlich mit der PKZ verknüpft hat. Art. 15 DSGVO etabliert ein solches Auskunftsrecht bereits – ebenso Informationspflichten (Art. 13 ff. DSGVO).

Zu den zwingenden Schutzmechanismen gehört auch die Verbürgung des Rechts, die persönlichkeitsrechtlichen Gewährleistungen gerichtlich durchsetzen zu können (Art. 79 DSGVO; Art. 19 Abs. 4 GG).

Darüber hinaus kommt der Kontrollinstanz „unabhängige Datenschutzbeauftragte“ eine wichtige grundrechtssichernde Funktion zu.[194] Als Scharnier des Datenschutzes zwischen Verantwortlichem und Betroffenem können sie Verstöße gegen das informationelle Selbstbestimmungsrecht frühzeitig erkennen, unterbinden und anprangern. Geht aus der Rechtsprechung des BVerfG auch nicht eindeutig hervor, ob und inwiefern die Einbindung von Datenschutzbeauftragten als Bestandteil des verfahrensrechtlichen Grundrechtsschutzes zwingend vorzusehen ist,[195] hat sich diese Institution als Baustein verfahrensbezogenen Grundrechtsschutzes jedenfalls bewährt.[196]

(2) Ausgestaltungsmöglichkeiten – best-practice-Beispiel für technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes (Datenschutz by Design): die österreichische Stammzahl

Einen instruktiven Versuch, durch technische Maßnahmen die Persönlichkeitsrechte Betroffener mit den staatlichen Verarbeitungsbedürfnissen zu versöhnen, hat Österreich unternommen:[197] Die Alpenrepublik nutzt ein komplexes System, bestehend aus Bürgerkarte, allgemeiner PKZ (sog. „Stammzahl“ [198]) und verschiedenen bereichsspezifischen Personenkennziffern, um natürliche Personen eindeutig zu identifizieren und Registeroptimierungen durchführen zu können. Das Konzept ist von dem Leitgedanken eines

---

[192] BVerfGE 100, 313 (361).
[193] So handhaben es sowohl das BDSG a. F. als auch die DSGVO (Art. 13 ff.).
[194] BVerfGE 65, 1 (46, 59).
[195] Vgl. *Brink*, in: Wolff/Brink (Hrsg.), BeckOK DatenschutzR, 20. Ed., Stand: 1.5.2017, Grundrechtsschutz durch Verfahrensgestaltung, Rn. 124; *Simitis*, in: ders. (Hrsg.), BDSG, 8. Aufl., 2014, Einleitung: Geschichte - Ziele - Prinzipien, Rn. 37; *Busch*, DVBl 1984, 385 (388). Gegen eine verbindliche Vorgabe durch die Verfassung aber etwa *Scholz/Pitschas*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, 1984, S. 45 ff.; *Di Fabio*, in: Maunz/Dürig (Hrsg.), GG, 39. Erg.-Lfg. , Art. 2, Rn. 186.
[196] Siehe etwa *Gürtler-Bayer*, Der behördliche Datenschutzbeauftragte, 2014, S. 39 f.
[197] Zur detaillierten Darstellung des österreichischen Modells siehe *McKinsey & Company Inc.* (Fn. 4), S. 15 ff.; *Statistisches Bundesamt* (Fn. 7), S. 15 ff.
[198] Nach der Legaldefinition des § 2 Nr. 8 EGovG Österreich handelt es sich bei der Stammzahl um „eine einem Betroffenen zu dessen eindeutiger Identifikation zugeordnete Zahl, die auch für die Ableitung von bereichsspezifischen Personenkennzeichen (bPK) gemäß §§ 9 und 14 bestimmt ist“.

Datenschutzes durch sachadäquate technische Gestaltung (Datenschutz by Design – vgl. auch Art. 25 Abs. 2 DSGVO) durchdrungen.

(a) Gesetzliche Konzeption

Österreichische Bürger können sich gegenüber ihrer Verwaltung mit Hilfe einer Bürgerkarte[199] identifizieren (§ 4 EGovG Österreich). Darauf ist eine Stammzahl gespeichert (§§ 4 Abs. 2; § 6 Abs. 1 EGovG Österreich). Die Stammzahlenregisterbehörde[200] leitet die (nur ihr bekannte) Zahl durch ein mathematisches Verfahren aus der Nummer ab, unter der ein Betroffener im Melderegister erfasst ist (§ 6 Abs. 2 EGovG Österreich).[201]

Nutzt der Betroffene seine Bürgerkarte zur Identifikation, so überprüft die Stammzahlenregisterbehörde seine Identität anhand der Stammzahl (§ 6 Abs. 1 EGovG Österreich). Nach der Bestätigung der Identität generiert ein automatisches Verfahren anhand einer nicht umkehrbaren Ableitung für bestimmte Anwendungsfälle eine bPKZ (§§ 10 Abs. 1; 13 Abs. 1 S. 1 EGovG Österreich).[202]

i. Reichweitenbegrenzung durch bereichsspezifische Personenkennziffern

Jede bPKZ kommt jeweils ausschließlich für *einen* staatlichen Tätigkeitsbereich zum Einsatz (§ 9 Abs. 1 S. 2 EGovG Österreich).[203] Kraft normativer Konzeption ist die bPKZ so gestaltet, „dass zusammengehörige Lebenssachverhalte in ein- und demselben Bereich zusammengefasst werden und miteinander unvereinbare Datenverwendungen (§ 6 Abs. 1 Z 2 DSG 2000) innerhalb desselben Bereichs nicht vorgesehen sind“ (§ 9 Abs. 2 S. 1 EGovG Österreich).

Im Gegensatz zur Stammzahl verlässt die bPKZ die Sphäre der Stammzahlenregisterbehörde; die jeweilige Fachbehörde kann sie zur Ausgestaltung ihrer Datenanwendungen umfänglich nutzen. Dabei ist eine bPKZ aber – neben der Stammzahlenregisterbehörde – immer nur denjenigen Behörden bekannt, die für das jeweilige staatliche Tätigkeitsfeld zuständig sind, in dem sie konkret Anwendung findet.

Weil ein Tätigkeitsfeld immer nur „zusammengehörige Lebenssachverhalte“ umfasst (etwa den Bereich „Sozialhilfe“, „Rente“ oder „Grundstücksangelegenheiten“), lassen sich unter einer bPKZ aber nicht so viele Daten sammeln, dass sich auf ihrer Grundlage ein umfassendes

---

[199] Ausführliche Informationen hierzu unter https://www.buergerkarte.at/.
[200] Sie ist organisatorisch bei der datenschutzrechtlichen Aufsichtsbehörde verankert – zu ihrer institutionellen Stellung näher auf der folgenden Seite.
[201] Die Stammzahlenregisterbehörde führt für natürliche Personen, die nicht im zentralen Melderegister eingetragen sind; ein Ergänzungsregister. Auf dieser Grundlage kann sie sog. Ersatzstammzahlen bilden.
[202] Behörden können die bPKZ in ihren Datenanwendungen auch zur Identifikation Betroffener nutzen, wenn diese sich nicht zuvor per Bürgerkarte selbst identifiziert haben. Den rechtlichen Rahmen hierfür setzt § 10 Abs. 2 EGovG Österreich.
[203] Die Bereiche legt die E-Government-Bereichsabgrenzungsverordnung fest. Sie unterscheidet bspw. zwischen „Bauen und Wohnen“, „Gesundheit“, „Kunst und Kultur“, „Umwelt“ sowie „Wirtschaft“.

Persönlichkeitsprofil erstellen ließe. Die bereichsspezifische Begrenzung schützt die Daten vor einem Durchgriff in andere Bereiche. Auf diese Weise will der österreichische Gesetzgeber verhindern, dass die Verwaltung Daten, die in keinem sachlichen Kontext zueinander stehen, unter einer bPKZ sammelt. Das soll die Entstehung umfangreicher Persönlichkeitsprofile und damit unvertretbare Gefahren für das Persönlichkeitsrecht Betroffener bereits a priori wirksam verhindern.

In dem Grundkonzept dezentraler Verwaltung unterscheidet sich das österreichische Konzept auch von dem (gescheiterten) deutschen ELENA-Verfahren: Es hat den Versuch unternommen, Daten, die für Bezug von Sozialleistungen relevant sind, digital zu verwalten. Das Modell zielte darauf ab, Daten von Arbeitnehmern, darunter vor allem Einkommensnachweise, zentral und in verschlüsselter Form zu speichern. Nach kontroversen Debatten mit Blick auf Missbrauchsmöglichkeiten, die von einer zentralen Speicherung potenziell ausgehen können, begrub die Bundesregierung das Konzept aber wieder.[204]

ii. Unabhängige Datenschutzaufsicht als Wächterin über die Stammzahlen

Auch das österreichische Modell mehrerer bereichsspezifischer Personenkennziffern ist nicht gänzlich frei von Risiken für den Persönlichkeitsschutz. So lassen sich alle bereichsspezifischen Personenkennziffern von den Stammzahlen ableiten und sind über diese miteinander verbunden. Vor diesem Hintergrund wird deutlich, dass es sich bei der Stammzahl in der Sache um eine allgemeine PKZ handelt. Im Gegensatz zu dem klassischen Modell einer PKZ[205] findet die Stammzahl aber nicht unmittelbar zum Zwecke eines Datenaustauschs Verwendung – insbesondere nicht im interbehördlichen Verkehr. Sie ist nur der Stammzahlenregisterbehörde bekannt. Dadurch minimiert die Republik Österreich den Verbreitungsgrad der Stammzahl als allgemeiner PKZ.

Eine institutionelle Sicherung zieht die Alpenrepublik dadurch ein, dass sie die Stammzahl in vertrauenswürdige Hände legt: Die Datenschutzaufsichtsbehörde ist zugleich die Stammzahlenregisterbehörde (§ 7 Abs. 1 EGovG Österreich). Ihr Kernauftrag ist es, die Daten der Bürger zu schützen, und sie ist aufgrund der unionalen Vorgabe des Art. 52 Abs. 2 DSGVO (und ehemals Art. 28 Abs. 1 RL 95/46/EG) in der Wahrnehmung dieses Auftrags „völlig unabhängig“.[206] Infolge dieser organisationsrechtlichen Absicherung, die sie aus der allgemeinen Behördenhierarchie herauslöst, ist die Datenschutzaufsichtsbehörde

---

[204] *Anonymous*, NJW-Spezial 2011, 596 (596).
[205] Dieses klassische Modell hatte auch das BVerfG beim Volkszählungsurteil vor Augen, da es im Jahre 1983 noch keine für den Massenverkehr praxistauglichen kryptographischen Methoden (geschweige denn die Infrastruktur des Internets) gab.
[206] Zur Bestimmung der Reichweise des Unabhängigkeitsmerkmals durch den EuGH unter Geltung der Datenschutzrichtlinie siehe insbesondere EuGH, Urt. v. 9.3.2010 – C-518/07 und EuGH, Urt. v. 16.10.2012 – C-614/10. Die Aussagen dürften auch für die DSGVO maßgeblich sein, *Kühling/Martini et al.* (Fn. 30), S. 160 m. w. N.

prädestiniert, die Verwaltung äußerst sensibler Daten der Bevölkerung rechtskonform und sachgerecht wahrzunehmen.[207]

Kraft ihrer Funktion und organisatorischen Unabhängigkeit bürgt die Stammzahlenregisterbehörde hinreichend dafür, dass *sie selbst* keine Datensammlung unter der Stammzahl vornimmt und ein rechtswidriges Zugriffsersuchen anderer Behörden abschlägig bescheiden wird.[208] Der österreichischen Konstruktion gelingt es dadurch, das Missbrauchsrisiko und die Gefahr eines Datenlecks signifikant zu senken. Denn keine andere Stelle als die unabhängige Datenschutzaufsichtsbehörde kann die Stammzahl (bzw. allgemeine PKZ) einsehen und verarbeiten.

iii. Geheimhaltung der Stammzahl

Die PKZ nach österreichischem Vorbild begrenzt das Risiko einer unzulässigen Profilbildung auch dadurch, dass die Stammzahl verschlüsselt abzulegen ist, nicht außerhalb des Errechnungsvorgangs für eine bPKZ gespeichert werden darf, insbesondere umgehend wieder zu löschen ist, und bPKZ in Mitteilungen an den Bürger keine Erwähnung finden (§ 12 Abs. 1 Nr. 1 u. 2, § 11 EGovG Österreich). Das wirkt der Gefahr unregulierter behördenübergreifender Datenzusammenführungen entgegen.

Übermittelt Behörde A eine bPKZ (samt der verbundenen Daten) aus ihrem Zuständigkeitsbereich an Behörde B, die in einem anderen Lebensbereich zuständig ist, so kann B die pseudonymisierte bPKZ unmittelbar keinem der bei ihr hinterlegten Betroffenen zuordnen. Eine Zuordnung wäre nur dann möglich, wenn auch die Stammdaten übermittelt würden. In diesem Fall verwirklicht sich aber weniger das spezifisch in der bPKZ angelegte Risiko, sondern eher das bereits bestehende generelle Risiko der behördlichen Datenvorhaltung.

iv. Behördenübergreifende Datenabfragen und Datenaustausch

Österreichische Behörden können die bPKZ auch tätigkeitsfeldübergreifend zum Austausch von Daten einsetzen. Behördenübergreifende Datenabfragen auf der Grundlage einer bPKZ sind aber ausschließlich unter Einschaltung der Stammzahlenregisterbehörde zulässig: Sie gibt eine Abfrage nur frei, wenn der Datenaustausch der Behörden nicht gegen das DSG 2000 verstößt (§ 10 Abs. 2 S. 1 EGovG Österreich). Will die Behörde A von der Behörde B also Daten eines Betroffenen – etwa Informationen über ein auf ihn zugelassenes KfZ – erfragen, so kann sie also bei der Stammzahlenregisterbehörde eine bPKZ beantragen, anhand derer sie im

---

[207] Eine Ansiedlung der PKZ-Verwaltung und des Datenaustauschs bei datenschutzrechtlichen Aufsichtsbehörden führt jedoch dazu, dass deren Aufgabe der Kontrolle sich mit eigenen verwaltungsrechtlichen Aufgaben verwebt. Je mehr Aufgaben nicht-aufsichtsrechtlicher Natur die Behörde übernimmt, desto eher kann sich die Frage nach ihrer Aufsichtsneutralität stellen. Vor diesem Hintergrund spricht einiges dafür, die Aufgaben der Aufsicht und der Datenverwaltung auch innerbehördlich klar voneinander zu trennen.

[208] Einen konzeptionell ähnlichen Ansatz verfolgt Estland: Dort gibt es eine zentrale Informationsbehörde, die nur verbindet, aber nichts selbst speichert, vgl. *McKinsey & Company Inc.* (Fn. 4), S. 27.

Anschluss den gewünschten Datenaustausch mit der jeweiligen Fachbehörde vornehmen kann. Die Stammzahlenregisterbehörde bildet daraufhin (unter den Voraussetzungen des § 10 Abs. 2 S. 1 EGovG Österreich) die erforderliche bPKZ und übermittelt sie in verschlüsselter Form an die ersuchende Behörde A (§ 10 Abs. 1 S. 2 EGovG Österreich). Auf diese Weise lässt sich eine bPKZ auch zum tätigkeitsfeldübergreifenden Datenaustausch einsetzen, ohne dass eine Behörde direkten Zugriff auf die bPKZ erhält, die nicht auch selbst für das entsprechende Tätigkeitsfeld zuständig ist. Behörde A übermittelt ihre Datenanfrage mitsamt der verschlüsselten bPKZ an die Behörde B, welche die bPKZ entschlüsseln und die Datenanfrage bearbeiten kann (§ 13 Abs. 2 EGovG Österreich).

Anders als ein System, das mit einer offenen Stammzahl operiert, erweitert der österreichische Ansatz die Möglichkeiten von Datenabfragen und Zusammenführungen gegenüber einem konventionellen, auf Stammdaten basierenden System also nicht. Vielmehr trägt es durch seine instrumentellen Sicherungen dem Gedanken „privacy by design" Rechnung und wählt mit der Einführung der Kombination aus Stammzahl und bPKZ eine im Grundsatz grundrechtsschonende Lösung. Zugleich stellt es Datenabgleich und Datenaustausch gleich effektiv sicher wie ein System mit offener PKZ. Ein weiterer datenschutzrechtlicher Vorteil liegt darin, dass die bPKZ – anders als etwa die deutsche Steuer-ID – nicht nach außen gelangt: Weder Dritte noch der Betroffene selbst erfahren die bPKZ (§ 11 EGovG Österreich).

v. Bereichsspezifische Personenkennziffer „amtliche Statistik" für Zensuszwecke

Für den Zensus nutzt *Statistik Austria* (vgl. § 22 BStatG Österreich), das österreichische Pendant zum deutschen Statistischen Bundesamt, die bPKZ „amtliche Statistik": Sie ist mit den Daten aus den jeweils für den Zensus maßgeblichen Registern verbunden.

Anhand dieser bPKZ kann *Statistik Austria* Informationen von den registerführenden Behörden abrufen, ohne dabei Daten zu übermitteln, die einen unmittelbaren Personenbezug aufweisen. So lassen sich Daten aus unterschiedlichen Verwaltungsbereichen für den Zensus fruchtbar machen, ohne dass *Statistik Austria* oder eine andere öffentliche Stelle damit einhergehend Zugriff auf vollständige Bürgerprofile erhält. Österreich setzt sein bPKZ-Modell also auch gezielt zum Zwecke der Pseudonymisierung der übermittelten Daten ein. Eine solche Pseudonymisierung ist nach der Wertung des DSGVO geeignet, die Gefahren für das Persönlichkeitsrecht zu minimieren.[209]

Vollständig ausschließen können diese Maßnahmen eine Identifizierung natürlicher Personen in einer Big-Data-Umwelt aber im Grundsatz nicht.[210] Ob es den verfassungsrechtlichen Anforderungen genügt, die das BVerfG im Anschluss an das Volkszählungsurteil heute stellen

[209] Eine Pseudonymisierung ist nach der Wertung des DSGVO geeignet, die Gefahren für das Persönlichkeitsrecht zu minimieren. Vgl. zur Pseudonymisierung *Schild* (Fn. 70), Art. 4 DSGVO, Rn. 69.
[210] Vgl. nur *Härting*, NJW 2013, 2065 (2065). Weniger pessimistisch *Kühling/Klar*, NJW 2013, 3611 (3613).

würde, ist ungewiss. Denn das Gericht legt insoweit die Messlatte der Anforderungen hoch: Eine vollständige Katalogisierung des Einzelnen ist selbst dann unzulässig, wenn sie „in der Anonymität statistischer Erhebungen" erfolgt.[211]

Auch wenn eine Re-Identifizierung der Person, die hinter einer bPKZ steht, denkbar ist, so wird sie in der Vielzahl der Fälle immerhin mit einem hohen Aufwand verbunden sein. Schließt die Pseudonymisierung die Profilbildung auch nicht gänzlich aus, kann sie den Weg dorthin doch zumindest deutlich erschweren. Es bedarf dann einer nicht unerheblichen Bereitschaft zum offenen Rechtsbruch, um das Schutzsystem der Datenschutzaufsichtsbehörde zu durchbrechen oder mithilfe eines Data-Mining-Verfahrens die Angaben ohne unmittelbaren Personenbezug zu einem Persönlichkeitsprofil zu verdichten.

Die Wahrscheinlichkeit, den Einzelnen zu identifizieren, nimmt in Abhängigkeit von der Größe der Datensammlung zu.[212] Wenn einmal bspw. Meldeadresse, Alter oder Behinderungsgrad bekannt sind, kann aus einem pseudonymisierten Datensatz schon mit wenigen Klicks eine Identifizierung gelingen. Die datenhaltende Stelle steht daher umso mehr vor der Herausforderung, zu prüfen, inwiefern ein ausreichendes Maß an Pseudo- bzw. Anonymität noch gewahrt ist und ob sie nicht ggf. zusätzliche Maßnahmen ergreifen muss, um den gebotenen Schutzstandard aufrechtzuerhalten, damit es nicht zu einer Re-Identifizierung des Einzelnen kommt.[213] Kryptographische Methoden, wie Hash-Verfahren[214], können dabei eine wichtige Hilfe sein.

(b) Zwischenergebnis

Der Blick nach Österreich zeigt: Technische Maßnahmen der Pseudonymisierung und eine organisatorische Aufspaltung der Zugriffsrechte auf Personenkennziffern unter der schützenden Hand der Datenschutzaufsichtsbehörde wirken dem Risiko rechtswidriger Profilbildungen entgegen. Verknüpfungsmöglichkeiten zwischen den verschiedenen Registern, die für einen Registerabgleich und Datenaustausch sachlich notwendig sind, schöpft die Alpenrepublik dennoch voll aus. Die kryptographische Erzeugung und verschlüsselte Übertragung der bPKZ sowie ihr begrenzter Anwendungsbereich tragen zu dem Schutzmechanismus bei. Sie bilden wichtige Faktoren, um das Recht auf informationelle Selbstbestimmung des Bürgers gegen das Risiko einer Profilbildung zu verteidigen. Einen unüberwindlichen Schutzwall gegen verfassungswidrige Datensammlungen durch den Staat oder Private errichten sie jedoch nicht.

---

[211] Siehe BVerfGE 65, 1 (53). Ob diese Aussage konsistent ist, lässt sich hinterfragen. Denn Anonymisierung schließt ihrem Wesen nach die Möglichkeit aus, mit vertretbaren Mitteln auf einzelne Personen rückzuschließen.
[212] *Weichert*, ZD 2013, 251 (259).
[213] *Marnau*, DuD 2016, 428 (429).
[214] Vgl. zur nicht umkehrbaren Ableitung der bPKZ aus der Stammzahl und dem Bereichskürzel in Österreich *McKinsey & Company Inc.* (Fn. 4), S. 28, Abb. 8.

cc) Gesamtabwägung: Ist die Einführung einer Personenkennziffer mit Blick auf den ihr zugedachten Zweck und die mit ihr verbundenen Belastungen angemessen?

Der Eingriff in das Recht auf informationelle Selbstbestimmung, den die Einführung und Verwendung einer PKZ nach sich zieht, ist nur dann angemessen, wenn das Gemeinwohlinteresse an effizienteren und qualitativ besseren Registern das Grundrecht des Einzelnen aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG überwiegt.

(1) Nutzen

Eine PKZ als Baustein der Modernisierung der Registerlandschaft in Deutschland einzuführen, befriedigt ein wichtiges Interesse des Gemeinwohls: Ihr Einsatz erlaubt die fehlerfreie Zuordnung von Registerdaten zu Einzelpersonen und somit die Verknüpfung der in den verschiedenen Registern vorrätigen Daten. Dies markiert eine Grundvoraussetzung, um Daten aus verschiedenen Registern durch automatisierte Datenverarbeitungsvorgänge sinnvoll miteinander abzugleichen und zu synchronisieren sowie Erfassungsfehler zu vermeiden und zu bereinigen. Im Vergleich zu einem manuellen Registerabgleich ist eine automatisierte Lösung weniger fehleranfällig und kostengünstiger. Zugleich gewährleistet sie eine höhere Registeraktualität und damit zugleich eine bessere Qualität der Registerdaten. Diese Potenziale einer Registermodernisierung lassen sich durch den Einsatz einer PKZ ausschöpfen.

Ein besseres Registerwesen ist kein Selbstzweck: In Ländern, die in der Digitalisierung der Verwaltung eine Vorreiterrolle einnehmen, war ein modernes Registerwesen ein zentraler Baustein ihres Digitalisierungserfolgs.[215] Digitale und miteinander verknüpfte Register erlauben es der Verwaltung, vollständig digitale und zunehmend automatisierte Bürgerangebote zu etablieren.

Der Anwendungsfall eines registerbasierten Zensus macht dies paradigmatisch deutlich: Gestützt auf moderne Register können statistische Erhebungen künftig aktuellere Daten mit höherer Periodizität und Genauigkeit liefern. Diese Daten bilden eine zentrale Grundlage gesamtstaatlicher legislativer sowie exekutiver Planungs- und Strukturentscheidungen und tragen damit entscheidend zum effizienten Einsatz der Ressourcen des Gemeinwesens bei.[216]

(2) Risiken

(a) Grundrechtsgefährdung durch die abstrakte Möglichkeit der Profilbildung

Dem hohen Nutzen, welchen die Einführung einer PKZ für das Gemeinwesen generieren kann, stehen auf der anderen Seite auch neue, tiefgreifende Gefahren für das Recht auf informationelle Selbstbestimmung der Bürger gegenüber. Denn Daten aus verschiedenen

[215] *Nationaler Normenkontrollrat* (Fn. 3), S. 1.
[216] Dazu auch bereits *Martini* (Fn. 84), S. 13 ff.

Registern lassen sich nicht nur zu legitimen Zwecken, wie anonymen statistischen Erhebungen, die dem Gemeinwesen eine valide Planungsgrundlage liefern sollen, zusammenführen, sondern – jedenfalls theoretisch – auch zu verfassungswidrigen Zwecken, insbesondere zur Erstellung umfassender Persönlichkeitsprofile.

Selbst wenn der Staat für eine persönlichkeitsfeindliche Katalogisierung erst weitere Folgemaßnahmen einleiten müsste, die sich an die Einführung der PKZ anschlössen und die ihrerseits Gegenstand einer verfassungsrechtlichen Prüfung wären, kann sich eine PKZ in den Augen der Bürger als erster Schritt zu ihrer vollständigen informatorischen Ausleuchtung darstellen. Befürchtungen informationeller Katalogisierung und das Gefühl panoptischer Überwachung können den Einzelnen in seiner informationellen Selbstbestimmung qualitativ in ähnlicher Weise beeinträchtigen wie eine umfassende reale Profilbildung selbst.[217] Eine vergleichbare „Beunruhigung" der Bürger trieb das BVerfG bereits im Volkszählungsurteil als einem seiner wesentlichen Entscheidungsgesichtspunkte um.[218]

In Zeiten sich überschlagender Entwicklungen der Digitalisierung erleichtern es die technischen Möglichkeiten, die bspw. neue Big-Data-Anwendungen vermitteln, zusätzlich, isoliert vorliegende Daten binnen eines Wimpernschlags miteinander zu verquicken und gebündelt auszuwerten, deren Zusammenführung noch vor wenigen Jahren einen unverhältnismäßigen Aufwand erzeugt hätte. Die abstrakte Gefahr der (staatlichen) Profilbildung hat sich dadurch zwar einerseits ohnedies erhöht. Das rechtfertigt andererseits aber nicht, das Anforderungsprofil an den Schutz des Einzelnen vor solchen Gefahren abzusenken, die mit einer Zusammenführung sensibler persönlicher Daten einhergehen. Es wäre problematisch, wenn in Zeiten wachsender Gefährdung der grundrechtlichen Entfaltung durch digitale Anwendungen gerade der Staat die Gefahr der Datenmacht, die in seinen Hand liegt, in einer für die Bürger nicht erfassbaren Weise erhöht, statt sie vor den Gefahren zu schützen, welche die technischen Möglichkeiten der Big-Data-Welt vorhält.

Aus verfassungsrechtlicher Sicht ist es deshalb aber noch nicht prima facie geboten, das Instrument „PKZ" mit einem legislativen Bann zu belegen: Der Staat muss vielmehr in Abwägung mit den Gemeinwohlzielen, die eine PKZ verfolgt, durch geeignete Maßnahmen sicherstellen, dass das verfassungsrechtlich gebotene Maß des Persönlichkeitsschutzes auch unter den modernen Bedingungen der Datenverarbeitung erhalten bleibt. Erst wenn sich eine persönlichkeitsfeindliche Katalogisierung des Individuums auch dadurch nicht vermeiden lässt, überschreitet die PKZ eine rote Linie.

(b) Profilbildungsmöglichkeit durch spätere gesetzliche Maßnahmen

Selbst wenn eine durch Schutzmaßnahmen flankierte PKZ eine umfassenden Profilbildung (und damit einen verfassungswidrigen Zustand) noch nicht unmittelbar ermöglichen sollte, so

---

[217] *Schlink*, Der Staat 25 (1986), 233 (247).
[218] BVerfGE 65, 1 (3 f.).

ist dennoch denkbar, dass sie durch spätere gesetzgeberische Schritte das Grundrecht auf informationelle Selbstbestimmung verletzt: Immerhin besteht die Möglichkeit und die daran anknüpfende Sorge, der Gesetzgeber könne im Laufe der Zeit die Speicherung immer weiterer personenbezogener Daten zur PKZ gestatten.[219] Das Risiko, dass sich die PKZ mit der Zeit als trojanisches Pferd entpuppt, eröffnet der Gesetzgeber zwangsläufig bereits mit Einführung der PKZ.

Der Losung „Wehret den Anfängen" folgend, lässt sich eine allgemeine PKZ für alle Deutschen als der Universalschlüssel verstehen, welcher der Verwaltung die Bildung von Persönlichkeitsprofilen der Bürger grundsätzlich eröffnet – oder dieses Vorhaben pro futuro jedenfalls erheblich vereinfacht.[220] Aus dieser Perspektive tritt die Verwaltung hinsichtlich der Katalogisierung des einzelnen Bürgers gewissermaßen bereits in das „Vorbereitungsstadium" einer freiheitsraubenden digitalen Vermessung ein. Der gläserne Bürger und staatliche Datendepots, die mit sensiblen privaten Informationen gefüllt sind, stehen den Deutschen insofern als Warnbildern der Geschichte insoweit noch unmittelbar vor Augen.[221]

Dieser gesellschaftspolitisch brisante Hintergrund wird die Öffentlichkeit mit besonders wachsamem Auge auf eine Einführung einer (institutionell geschützten= Stammzahl in Kombination mit dem Einsatz einer bPKZ nach österreichischem Muster blicken lassen. Denn der Gesetzgeber könnte die technischen und organisatorischen Maßnahmen, die gerade den typischen Gefahren einer allgemeinen PKZ entgegenwirken sollen, künftig wieder lockern oder gar aufgeben. Durch spätere gesetzliche Modifikationen könnte er das nun bereits aufgestoßene Tor zu einer verfassungswidrigen Profilbildung problemlos durchschreiten.

Genau darin, also in einer Unterschreitung des grundrechtlich gebotenen Maßes hinreichender technischer, organisatorischer und rechtlicher Sicherungsmaßnahmen aufgrund späterer Änderung liegt dann der Verfassungsbruch – nicht aber schon in der Zulassung einer bPKZ selbst bzw. in der *gesetzlichen Ausgestaltung der Registerführung mittels PKZ als solcher*. Erst dann überschreitet der Staat die grundrechtlich kritische Schwelle und wäre das BVerfG als Wächter über die verfassungsrechtliche Ordnung aufgerufen, dem (bspw. auf eine Verfassungsbeschwerde hin) Einhalt zu gebieten.

(c) Faktische Risiken: Missachtung der gesetzlichen Vorgaben und Gefahr einer Datenpanne

Allen Bemühungen zum Trotz, die Gefahr einer staatlichen Profilbildung durch geeignete Maßnahmen zu verhindern, besteht das Risiko, dass sich Behörden oder Private über die

---

[219] Vgl. zur Steuer-ID FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 –, juris, Rn 144.
[220] So vertrat das FG Köln die Auffassung, die Steuer-ID sei „eine erste Voraussetzung für die Möglichkeit der Erstellung von Persönlichkeitsprofilen", FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 –, juris, Rn. 76 sowie a. a. O., Rn. 144. Dazu bereits oben S. 31.
[221] Näher dazu oben S. 3.

gesetzlichen Vorgaben hinwegsetzen und (bereichsbezogene) Personenkennziffern entgegen ihrer eigentlichen Konzeption zur verfassungswidrigen Profilbildung missbrauchen.

Die Verwaltung ist zwar an Recht und Gesetz gebunden (Art. 20 Abs. 3 GG). Der Gesetzgeber darf ihr grundsätzlich unterstellen, dass sie die geltenden Vorschriften befolgt. Sich auf die Gesetzesbindung alleine zu verlassen, reicht als Schutzmechanismus aber nicht aus. Flankierende Sicherungen, die einen Missbrauch – insbesondere gegen rechtswidrige Nutzung – auch in tatsächlicher Hinsicht sicherstellen, sind nicht nur sinnvoll, sondern auch notwendig.

i. Sanktionsmaßnahmen

Eine wichtige Mission geeigneter Sicherungsmaßnahmen ist es, Akteuren den Anreiz zu nehmen, einen Gesetzesverstoß in Kauf zu nehmen, der in Persönlichkeitsverletzungen mündet. Zu den normativen Maßnahmen, die einem rechtswidrigen Zugriff entgegenwirken, können insbesondere Sanktionstatbestände gehören. Mit ihrer Hilfe lässt sich ein gesetzeswidriges Verhalten grundsätzlich in einer für den Adressaten spürbaren Weise ahnden. Die rational kalkulierende Bilanz, die einen Gesetzesverstoß einpreist, fällt mit zunehmender Sanktionshärte in der Mehrzahl negativ aus, sodass der jeweilige Akteur im Zweifel von einer Missachtung des Gesetzes Abstand nehmen wird. Taugliche Sanktionsformen mit hinreichender Belastungswirkung und Drohkulisse sind insoweit vornehmlich die Geldbuße und die Kriminalstrafe.[222]

Sanktionsmaßnahmen wirken zwar auch generalpräventiv. Sie werden ihrem Wesen nach aber nur in solchen Fällen verhängt, in denen das Kind gleichsam in den Brunnen gefallen ist, eine Persönlichkeitsverletzung also bereits (im Zweifel unwiderruflich) eingetreten ist. Die Strafdrohung allein ist mithin bereits sachlogisch nicht geeignet, den Gesetzesverstoß mit Gewissheit zu verhindern. Sie kann nur *ein Bestandteil* eines umfassenderen Maßnahmenbündels sein.

ii. Maßnahmen der Datensicherheit gegen den unberechtigten Zugriff Dritter

Wenn der Staat sehr sensible personenbezogene Daten verarbeitet oder ein Instrument zu ihrer Verknüpfung vorhält, obliegt es ihm, in besonderer Weise für die Sicherheit der Daten vor einem Missbrauch Sorge zu tragen; er muss einen wirksamen Schutz vor Datenpannen sicherstellen. [223] Für das Maß des einzuhaltenden Sicherheitsschutzes gibt das

---

[222] Die DSGVO sanktioniert die Verarbeitung ohne entsprechende Grundlage in Art. 83 Abs. 5 lit. a mit „Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs […], je nachdem, welcher der Beträge höher ist“. Ob Geldbußen auch gegenüber Behörden und ihren Mitarbeitern ausgesprochen werden können, entscheiden die Mitgliedstaaten in eigener Verantwortung (Art. 83 Abs. 7 DSGVO). Der Bundesgesetzgeber hat sich dazu entschieden, von dieser Ermächtigung keinen Gebrauch zu machen (vgl. § 43 Abs. 3 BDSG-neu).
[223] Vgl. auch *Zelyk* (Fn. 20), S. 110. Zur Gefahr eines Datenlecks bei den Zensusdaten *Stepputat*, DÖV 2011, 111, 115.

Verfassungsrecht keine konkreten Maßgaben vor;[224] sie verlangt ihm aber – gerade mit Blick auf die Unumkehrbarkeit eintretender Persönlichkeitsverletzungen[225] – ein hinreichendes Maß an Ergebnissicherheit ab.

Wichtigste Determinante der IT-Sicherheit ist der zu schützende Datenbestand selbst.[226] Ist er besonders sensibel – wie etwa bei der Speicherung von Telekommunikationsverkehrsdaten auf Vorrat – muss er „ein besonders hohes Maß an Sicherheit" verbürgen.[227] Dieser Maßstab ist auch an die Einführung einer PKZ anzulegen.

Die geheime Stammzahl verknüpft alle unter den bereichsspezifischen Personenkennziffern verbundenen Daten. Gelänge einem Unbefugten, z. B. durch einen Hackerangriff, der widerrechtliche Zugriff auf die Stammzahl (und den Algorithmus, der aus ihr eine bPKZ generiert), so vermittelte ihm dies (wenn auch mittelbar) die Möglichkeit, auf die mit den bereichsspezifischen Kennzeichen verbundenen Daten zuzugreifen. Er könnte nicht nur umfassende Persönlichkeitsprofile erstellen, sondern im schlimmsten Fall auch weitere Datenverarbeitungen vornehmen, die Bürgern massive Schäden, wie etwa Identitätsdiebstahl, finanzielle Verluste, oder Rufschädigungen zufügen. Um einen flächendeckenden Schaden anrichten zu können, müsste ein Angriff auf das PKZ-System aber zusätzlich wohl auch in die Schnittstellen der Register und das Zugriffsrechtemanagement für die jeweiligen Behörden für einen Datenaustausch eindringen. Auch das lässt sich – mit Blick auf die Werthaltigkeit der Daten – keinesfalls ausschließen.

Zugleich geht bereits von dem Bekanntwerden etwaiger Sicherheitslücken in sensiblen Datenverarbeitungssystemen wegen der damit einhergehenden Verunsicherung der Bürger[228] ein erheblicher Eingriff in deren Recht auf informationelle Selbstbestimmung aus.[229]

Neben hinreichend bestimmten und verbindlichen Vorgaben muss der Gesetzgeber sicherstellen, dass sich die Schutzmaßnahmen an dem „Entwicklungsstand der Fachdiskussion" orientieren, und ihn fortlaufend an neue Erkenntnisse und Einsichten anpassen.[230]

Die Gefahr, dass sich Dritte trotz solcher Maßnahmen widerrechtlich Zugriff auf die PKZ-Infrastruktur verschaffen, ist als technisch, organisatorisch und rechtlich nicht auszuschließendes Restrisiko nur dann hinnehmbar, wenn sich die Wahrscheinlichkeit des

---

[224] Siehe BVerfGE 125, 260 (326).
[225] Insbesondere Stammdaten ändern sich typischerweise nicht, sodass ihre einmalige rechtswidrige Offenlegung eine Vielzahl weiterer Missbrauchsmöglichkeiten nach sich zieht.
[226] Vgl. das BVerfG zur Vorratsdatenspeicherung, BVerfGE 125, 260 (326).
[227] BVerfGE 125, 260 (326).
[228] So schlug das Bekanntwerden noch nicht näher benannter Sicherheitslücken bei der estnischen ID-Karte hohe Wellen, vgl. etwa *Hanfeld*, Tallinn, wir haben ein Problem, FAZ online vom 7.9.2017; *Reinvere*, Das Risiko für Estland ist essenziell, FAZ online vom 8.9.2017.
[229] Vgl. S. 20 f.
[230] BVerfGE 125, 260 (326 f.).

Schadensrisikos und die Schadenshöhe in einem vertretbaren Ausmaß bewegen, also selbst im Falle ihres Eintretens keine nachhaltigen Persönlichkeitsverletzungen zu befürchten sind.[231] Dem Gesetzgeber stellt das auf dem Weg zur Einführung einer PKZ hohe Hürden auf den Weg.

(3) Güterabwägung

Bei einer Gesamtabwägung erweist sich die Einführung einer PKZ vor dem Hintergrund der mit ihr verbundenen Risiken nur dann als verfassungsgemäß, wenn hinreichende rechtliche, technische und organisatorische Maßnahmen sicherstellen, dass ihre Einführung die abstrakte Gefahr der Bildung umfassender Persönlichkeitsprofile nicht in verfassungsrechtlich unvertretbarer Weise ansteigen lässt. Die Risiken, die sich mit einer PKZ verbinden, darf der deutsche Gesetzgeber grundsätzlich ausschließlich dann eingehen, wenn er der Fachverwaltung – dem österreichischen Vorbild[232] folgend – nur Zugriff auf solche bereichsspezifischen Personenkennziffern gestatten, die bereits konzeptionell nicht die Erstellung umfassender Persönlichkeitsprofile erlauben, weil sie sich nicht mit der notwendigen Datenmenge verknüpfen lassen. Jede bPKZ ist dann auf einen scharf umrissenen Lebensbereich limitiert, der keinen umfassenden Blick auf die Gesamtpersönlichkeit eines Menschen freilegt. In einem solchen Modell erscheint auch die Nutzung einer allgemeinen PKZ, welche die bPKZ auf Metaebene miteinander verbindet, verfassungsrechtlich vertretbar, wenn nur die Datenschutzbehörden Zugriff auf dieses verschlüsselt abgespeicherte Bindeglied haben. Kraft ihrer organisatorischen Ausgliederung und verbürgten Unabhängigkeit bieten sie eine hinreichende Gewähr dafür, dass eine allgemeine PKZ nicht das Schicksal eines Missbrauchs erleidet. Sofern die Datenschutzbehörde die PKZ nur verwaltet, aber selbst keinen Zugriff auf Registerdaten hat oder über Befugnisse der Datensammlung verfügt, hegt dies Risiken in grundsätzlich vertretbarer Weise ein.

Dennoch verbleiben erhebliche Gefahrpotenziale, die sich auch durch hohe Anforderungen an die Ausgestaltung der IT-Systeme[233] oder durch entsprechend scharfe Sanktionen[234] nicht restlos beseitigen lassen. Diese entsprechen zwar im Grundsatz denjenigen Risiken, die mit jedem Einsatz informationstechnischer Systeme einhergehen. Das rechtfertigt aber – gerade mit Blick auf die Sensibilität der Daten – noch nicht, sie hinzunehmen. Vielmehr bemisst sich ihre verfassungsrechtliche Vertretbarkeit nach der Wahrscheinlichkeit und Höhe eintretender Schäden. Die Missbrauchsgefahr für die Rechte Betroffener liegt (stärker als in der Existenz eine PKZ als solcher) insbesondere darin, dass sie sich als Hilfsmittel möglicher späterer Zusammenführungsverstöße entpuppt. Zwar könnten unbefugte Personen sich auch auf andere Weise Zugriff auf die bei der gesamten Verwaltung hinterlegten Daten verschaffen und auf dieser Grundlage Persönlichkeitsprofile (etwa durch Anknüpfung an Stammdaten)

[231] So für die Steuer-ID BFH, Urt. v. 18.1.2012 – II R 49/10 –, juris, Rn. 102
[232] Vgl. S. 34 ff.
[233] Vgl. S. 37.
[234] Vgl. S. 45.

erstellen oder anderweitig das Recht auf informationelle Selbstbestimmung der Betroffenen oder auch andere Rechtsgüter beeinträchtigen.

Eine allgemeine PKZ schafft dafür jedoch einen Zentralschlüssel. Auch eine bPKZ vereinfacht die missbräuchliche Zusammenführung von Daten über eine individuelle Kennziffer jedes Bürgers. Ihre Pseudonymisierung grenzt das Risiko jedoch ein, da eine solche Zusammenführung dann erst demjenigen möglich ist, der die Verbindung zwischen den Daten und der sich dahinter verbergenden Person herstellen kann. Für sich genommen ermöglicht zumindest eine bPKZ dem Staat nicht, ein Gesamtpersönlichkeitsbild zu entwerfen, das gleichsam das Innerste des Bürgers ausleuchtet und damit die Persönlichkeit spiegelt. Hierzu müsste er auch die individuelle Stammzahl des Bürgers kennen, da nur sie die Querverbindung der unterschiedlichen bPKZ erlaubt. Im österreichischen Modell müsste die Person dafür zumindest die Sicherungsmechanismen der Datenschutzaufsichtsbehörde überwinden.

Wichtige Voraussetzung verfassungsrechtlicher Verantwortbarkeit ist jedoch, dass der Staat sich ausreichender technischer Sicherungsmaßnahmen bedient. Durch flankierende Maßnahmen – etwa den Einsatz einer Ende-zu-Ende-Verschlüsselung und sonstiger kryptographischer Methoden innerhalb der digitalen Register – lässt sich ein spürbarer Zuwachs an Sicherheit für die Persönlichkeitsrechte der Betroffenen erzielen. Solange technische Maßnahmen die Daten wirksam schützen und damit die Identifizierung einer Person unverhältnismäßig erschweren, bildet die bPKZ eine grundsätzlich funktionale, verantwortbare Synthese aus Sicherheit und Effizienz.

Der Einsatz einer PKZ als Metaebene für nationale Register erweist sich dann als verantwortbar, wenn ihr Missbrauch zu Zwecken rechtswidriger Zusammenführung sowohl rechtlich als auch faktisch durch geeignete Sicherungsmaßnahmen, insbesondere durch eine organisatorische und technische Sicherung der PKZ-Verwaltung bei der Datenschutzaufsichtsbehörde wirksam verhindert wird. Zu den erforderlichen Sicherungsmaßnahmen gehören dann auch Zusammenführungsverbote sowie daran anknüpfende wirksame Sanktionen sowie das Rückspielverbot – sowohl bei der Durchführung eines Zensus als auch bei der Pflege der Register: Daten, die zu statistischen Zwecken erhoben werden, dürfen nicht zurück an die Exekutive fließen.[235]

Legt man an die verfassungsrechtliche Zulässigkeit einer allgemeinen PKZ den Maßstab an, dass sie mit einer absoluten Gewähr gegen *jeden denkbaren* Missbrauch immunisiert sein muss, der eine Persönlichkeitsverletzung nach sich ziehen kann, lässt sie sich nicht in einer rechtlich tragfähigen Weise rechtfertigen. Lässt man demgegenüber ausreichen, dass technische, organisatorische und rechtliche Maßnahmen das erdenklich Mögliche tun, um eine Persönlichkeitsverletzung mit einer nach menschlichem Ermessen hinreichenden

[235] BVerfGE 65, 1 (49 ff.).

Sicherheit auszuschließen, kann das einer allgemeinen PKZ den Weg bahnen. Mit dieser Elle gemessen, kann sich die Einführung einer allgemeinen PKZ und verschiedener bereichsspezifischer Personenkennziffern nach österreichischem Vorbild bei restriktiver Ausgestaltung als *im Grundsatz* rechtlich tragfähiger Kompromiss zwischen den Bedürfnissen der Registermodernisierung und des informationellen Selbstbestimmungsrechts erweisen.[236]

[236] Damit ist freilich nicht gesagt, dass sich das österreichische Modell auch tatsächlich eins zu eins in verfassungsrechtlich zulässiger Weise auf Deutschland übertragen lässt.

B. Zulässigkeit einer Unternehmenskennziffer

Die Qualität staatlicher Register verbessert sich nicht nur, wenn sie Verwechslungen zwischen natürlichen Personen ausschließen. Auch die Einführung einer Kennziffer für Unternehmen geltenden (UKZ) kann mit Hilfe ihrer Identifizierungs-, Repräsentations- und Ordnungsfunktion[237] zahlreiche Kosteneinsparungen erzielen und Fehlerrisiken minimieren. Bereits heute existieren diverse öffentlich zugängliche Register mit unternehmensbezogenen Daten, etwa das Gewerbezentralregister (§ 149 GewO), das Handelsregister (z. B. § 8 HGB, § 36 AktG, § 7 GmbHG) oder die Handwerksrolle (§ 6 HwO). Denkbar ist daneben bspw. ein auch Auftragnehmerregister, welches die Auftragnehmer öffentlicher Aufträge erfasst und katalogisiert.

An einem einheitlichen Unternehmensregister bzw. einer übergreifenden UKZ fehlt es bislang im deutschen Rechtsverkehr. Sie könnte die Grundlage dafür bilden, unternehmensbezogene Registerdaten abgleichen und austauschen zu können. So ließe sich verhindern, dass – wie bislang – selbst zentrale unternehmensbezogene Daten (beispielsweise Adressen) in verschiedenen Registern unabhängig voneinander und mit teils divergierendem Inhalt liegen.[238]

Die Einführung einer UKZ erfolgt indes nicht im rechtsfreien Raum. Sie ist zugleich nicht in gleichem Maße persönlichkeitsrechtlich sensibel wie eine PKZ. Besonderer Rechtfertigungsbedarf entsteht aber, sofern der Staat durch die Nutzung der UKZ in den Schutzbereich der unionsrechtlichen (II.) oder nationalen (III.) Grundrechte eines Unternehmens (I.) eingreift.

I. Unternehmensbegriff und unternehmensbezogene Daten

Das Recht gebraucht den Begriff „Unternehmen“ nicht einheitlich.[239] Über seinen Inhalt bestimmt jeweils der Regelungszweck der Gesetze, die ihn verwenden.[240] Einige davon stellen auch nicht auf das „Unternehmen“, sondern auf andere Begrifflichkeiten, etwa den „Gewerbebetrieb“ (vgl. § 1 Abs. 1 GewO) ab. Dementsprechend ist der Unternehmensbegriff auch innerhalb der deutschen Registerlandschaft heterogen.

---

[237] Dazu oben S. 1.
[238] *McKinsey & Company Inc.* (Fn. 4), S. 18.
[239] BGHZ 31, 105 (108 f.); BGHZ 36, 91 (102 f.); BGHZ 69, 334 (335 f.).
[240] Vgl. BGHZ 36, 91 (103); BGHZ 69, 334 (335 f.). Siehe beispielsweise *Zipperer*, in: Uhlenbruck/Hirte/Vallender (Hrsg.), InsO, 14. Aufl., 2015, § 158, Rn. 3 m. w. N. zu § 158 InsO: „jedes organisatorisches Gebilde, das die vermögenswerten Rechte des Schuldners als Unternehmer zusammenfasst“. Die Legaldefinition des § 265b Abs. 3 Nr. 1 StGB sieht vor: „Betriebe und Unternehmen [sind] unabhängig von ihrem Gegenstand solche, die nach Art und Umfang einen in kaufmännischer Weise eingerichteten Geschäftsbetrieb erfordern“; vgl. auch *Hopt*, in: Baumbach/Hopt (Hrsg.), HGB, 37. Aufl., 2016, § 1, Rn. 22-29, *Hirschmann*, in: Hölters (Hrsg.), AktG, 3. Aufl., 2017, § 15, Rn. 4.

Soll eine UKZ bereichsübergreifend sein, muss sie ihren Bezugspunkt daher notwendig unter Zugrundelegung eines weiten Unternehmensverständnisses wählen: Sie sollte möglichst alle Einheiten erfassen, die Wirtschaftsleistungen erbringen. Andernfalls kann sie die ihr zugedachte Funktion – die eindeutige Identifizierung sämtlicher unternehmerisch am Wirtschaftsleben teilnehmender Akteure – nicht erfüllen. Eine UKZ sollte daher sinnvollerweise – entsprechend dem funktionellen Unternehmensbegriff des Unionsrechts – jede Einheit erfassen, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform und der Art ihrer Finanzierung[241].[242] Unternehmensbezogene Daten sind in diesem Sinne dann analog zum Begriff „personenbezogene Daten" (vgl. § 3 Abs. 1 BDSG; Art. 4 Nr. 1 DSGVO) sämtliche Einzelangaben über ein bestimmtes oder bestimmbares Unternehmen („unternehmensbezogene Daten").

II. Unionsrechtlicher und einfachgesetzlicher Rahmen

1. Überlappungen zwischen Persönlichkeitsschutz und Unternehmensschutz

Das deutsche und unionale Datenschutzrecht ziehen der Einführung einer UKZ keine klaren Grenzen. Da sich sowohl der Anwendungsbereich der DSGVO (Art. 1 Abs. 1, Art. 2 Abs. 1 DSGVO) als auch der des BDSG (§ 1 Abs. 1 und Abs. 2 BDSG) auf personenbezogene Daten natürlicher Personen beschränkt, sind unternehmensbezogene Daten schon a priori nicht ihr Gegenstand. Das Datenschutzrecht findet allerdings dann ausnahmsweise Anwendung, wenn Unternehmensdaten, z. B. bei Kleinunternehmern, zugleich Informationen über natürliche Personen offenlegen[243]. Unternehmensbezogene und personenbezogene Daten stehen zueinander nicht im Verhältnis der Exklusivität. Unternehmensbezogene Daten können ihrerseits zugleich auch einen Personenbezug aufweisen. Vor allem dann, wenn sich natürliche Personen als Unternehmen betätigen, wie z. B. der klassische Einzelkaufmann, wird das Bedürfnis nach einem sachgerechten Persönlichkeitsschutz virulent. Insbesondere ist der Unternehmensbegriff nicht mit demjenigen der juristischen Person deckungsgleich. Unternehmensbezogene Daten weisen daher eine nicht unbeträchtliche Schnittmenge mit personenbezogenen Daten auf. Für solche Unternehmensdaten mit Personenbezug gelten die Vorbehalte, denen eine PKZ unterworfen ist, im Grundsatz in gleichem Maße.[244] Zulässig sind solche Kennziffern insoweit also nur, soweit der Staat hinreichende Schutzmechanismen zum Schutz des informationellen Selbstbestimmungsrechts gegen umfassende

---

[241] EuGH, Urt. v. 23.4.1991 – Rs. C-41/90 –, ECLI:EU:C:1991:161, Rn. 21, st. Rspr.

[242] Der Begriff „Einheit" lässt sich seinerseits unter Zugrundelegung normativer (Anknüpfung an eine eigene Rechtsform; juristische Eigenständigkeit) oder faktischer Kriterien (insbesondere eine wirtschaftliche Verbindung) bestimmen. Der Gesetzgeber ist aufgerufen, festzulegen, ob er rechtliche oder wirtschaftliche Einheiten mit eine UKZ adressieren will; vgl. auch *McKinsey & Company Inc.* (Fn. 4), S. 24.

[243] *Stancke*, BB 2013, 1418 (1419 f.).

[244] Siehe dazu S. 1 ff. Das gilt auch für die Vorschrift des Art. 87 DSGVO. Da sich der Regelungsanspruch der DSGVO auf die Verarbeitung personenbezogener Daten beschränkt (Art. 1 Abs. 1 DSGVO), erstreckt sich der Regelungsanspruch des Art. 87 nicht auf jegliche nationale Kennziffer, sondern nur auf solche, welche personenbezogene Daten verarbeiten.

Persönlichkeitsprofile vorsieht. Wirtschaftsbezogene Sachverhalte, die Gegenstand von Wirtschaftsregistern sind, leuchten allerdings grundsätzlich nicht die Persönlichkeit eines Menschen als solchen aus, sondern nehmen einen spezifischen Aspekt wirtschaftsbezogener Persönlichkeitsentfaltung in den Blick. Ein Unternehmen als verkörpertes Eigentum[245] schuldet dem Staat aufgrund der Sozialgebundenheit des Eigentums[246] darüber hinaus um ein Vielfaches mehr Rechenschaft über seine Betätigung als eine Privatperson.[247] Der Schutz wirtschaftsbezogener Sachverhalte steht in einer stärkeren Beziehung zur (weniger stark geschützten) Sozialsphäre der Persönlichkeit und genießt insofern einen weniger starken Schutz vor Offenbarung von Sachverhalten. Mögliche Überschneidungen zwischen privater und gewerblicher Sphäre (z. B. identische Adressen aufgrund gewerblicher Tätigkeit in den privaten Wohnräumen) darf der Staat umgekehrt aber nicht dazu nutzen, um gleichsam durch die Hintertür unternehmerischer Rechenschaftspflicht missbräuchlich die Privatsphäre auszuhöhlen.

2. Ausgestaltung bereichsspezifischer Unternehmenskennziffern de lege lata

Das bereichsspezifische (Datenschutz-)Recht hält einige Regelungen zur Verarbeitung unternehmensbezogener Daten bereit. So regeln etwa § 139a Abs. 1 S. 3 Hs. 2 und § 139c AO die Vergabe einer Wirtschafts-Identifikationsnummer.[248] Für Wirtschaftsteilnehmer bildet sie das Äquivalent zur Steuer-ID.[249] Ihre Funktion besteht darin, jedem Steuerpflichtigen ein einheitliches und dauerhaftes Merkmal zu verleihen, das ihn in Besteuerungsverfahren eindeutig identifizierbar macht (§ 139a Abs. 1 S. 1 AO). Die Wirtschafts-Identifikationsnummer besteht aus den Buchstaben ‚DE' und 9 Ziffern. Ihr Format entspricht damit dem der Umsatzsteuer-Identifikationsnummer. Bislang hat sie im Rechtsverkehr allerdings noch keine praktische Bedeutung erlangt: Sie harrt noch einer praktischen Implementierung.

Das Unternehmensregister i. S. d. § 8b HGB verfolgt wiederum eine andere Zielsetzung. Es führt relevante Daten aus verschiedenen Registern zusammen und erlaubt damit den einheitlichen Datenzugriff über ein zentrales Portal. Im Unterschied zur Steuer-ID soll das Unternehmensregister die Publizitätspflichten von Unternehmen unterstützen. Die dort abrufbaren Informationen beschränken sich also auf solche Daten, die Unternehmen verpflichtend veröffentlichen müssen (etwa Jahresbilanzen). Die potenziellen Bedenken

---

[245] *Axer*, in: Epping/Hillgruber (Hrsg.), BeckOK GG, 32. Ed., Stand: 1.3.2017, Art. 14, Rn. 51 ff.
[246] *Axer* (Fn. 245), Art. 14, Rn. 14.
[247] Vgl. dazu auch BVerfGE 65, 1 (44); *Wiebe/Schur*, ZUM 2017, 461 (465).
[248] Auch andere Rechtsbereiche regeln die Verarbeitung von Unternehmensdaten. So regelt etwa das Sozialrecht die Verarbeitung der Betriebsnummern in §§ 18i–18n SGB IV. Auch das Onlinezugangsgesetz (OZG) regelt, welche Daten bei einer juristischen Person oder einer Personengesellschaft „zur Feststellung der Identität des Nutzers eines Nutzerkontos" verarbeitet werden dürfen (§ 8 Abs. 1 S. 2 Nr. 2 OZG).
[249] Zugleich sah sich die Bundesregierung trotz der gesetzlich vorgesehenen Ermächtigung (§ 139d AO) auch nicht dazu veranlasst, technische und organisatorische Maßnahmen zur Verhinderung eines unbefugten Zugangs zu den mit der Wirtschafts-ID verbundenen Daten in einer Rechtsverordnung festzuschreiben. *Cöster*, in: Koenig (Hrsg.), AO, 3. Aufl., 2014, § 139d AO, Rn. 1.

gegen eine zentrale Zusammenführung von Registerdaten sind in diesem Bereich demnach bereits dadurch gemildert, dass es sich nicht um hochsensible Interna, sondern um ohnedies bereits andernorts öffentlich einsehbare Daten handelt.

Mit einer UKZ, über die sich auch nicht-öffentliche Daten aus staatlichen Registern miteinander verknüpfen lassen, ist das Unternehmensregister also nur in seiner grundsätzlichen Funktionsweise vergleichbar. Allerdings zeigt das Beispiel des Unternehmensregisters, dass in Bezug auf juristische Personen eine zentrale Datenzusammenführung wesentlich unproblematischer umsetzbar ist, als dies bei natürlichen Personen der Fall ist.

III. Verfassungsrechtlicher Rahmen

Wenngleich das BDSG und die DSGVO die Verarbeitung unternehmensbezogener Daten sowie die Einführung einer UKZ nicht explizit regulieren, hält zumindest das Grundgesetz rechtliche Direktiven bereit.

1. Unternehmenspersönlichkeitsrecht?

Ein besonderer verfassungsrechtlicher Rechtfertigungsbedarf für die Einführung einer UKZ entsteht (außer in Fällen eine Überlappung personenbezogener und unternehmensbezogener Daten)[250], soweit privatrechtliche Unternehmen in gleicher Weise wie Einzelpersonen ebenfalls ein Recht auf informationelle Selbstbestimmung besitzen (sog. Unternehmenspersönlichkeitsrecht).

a) Schutzbereich

Das verfassungsrechtlich geschützte allgemeine Persönlichkeitsrecht zeichnet sich durch einen hohen Menschenwürdebezug aus.[251] Da Unternehmen als solchen ihrem Wesen nach keine *Menschen*würde eigen ist,[252] liegt die wesensmäßige Anwendbarkeit (Art. 19 Abs. 3 GG) des informationellen Selbstbestimmungsrechts (Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG) auf Unternehmen zumindest *a prima vista* nicht nahe.

Zugleich sind einzelne Ausprägungen des Schutzes bestimmter Teilaspekte des allgemeinen Persönlichkeitsrechts, etwa des Rechts am eigenen Namen, durchaus auf Unternehmen übertragbar. Der BGH erkennt dies an. Zur Anwendbarkeit des allgemeinen Persönlichkeitsrechts auf Unternehmen judiziert er daher: „Eine Ausdehnung der Schutzwirkung [des allgemeinen Persönlichkeitsrechts] über natürliche Personen hinaus auf juristische Personen erscheint – auch mit Blick auf Art. 19 Abs. 3 GG – […] insoweit gerechtfertigt, als sie aus ihrem Wesen als Zweckschöpfung des Rechts und ihren Funktionen

[250] Dazu S. 51.
[251] BVerfGE 35, 202 (219 f.), st. Rspr.
[252] BVerfGE 35, 202 (219 f.), st. Rspr., vgl. *Kingreen/Poscher*, Grundrechte, 32. Aufl., 2016, Rn. 173.

dieses Rechtsschutzes bedürfen. Dies ist der Fall, wenn sie in ihrem sozialen Geltungsanspruch als Arbeitgeber oder als Wirtschaftsunternehmen betroffen werden."[253]

Das BVerfG erkennt die Anwendbarkeit des Rechts auf informationelle Selbstbestimmung auf Unternehmen im Grundsatz an:[254] Der sachliche Schutzbereich des Rechts auf informationelle Selbstbestimmung bei Unternehmen erfasst den Schutz „vor Gefährdungen, die von staatlichen informationellen Maßnahmen ausgehen können".[255] Anders als der Schutz personenbezogener Daten sind Unternehmensdaten aber primär im wirtschaftsbezogenen Kontext sensibel und schützenswert.[256] Der Schutzbereich erstreckt sich somit stets nur auf das konkrete Tätigkeitsfeld des Unternehmens im Einzelfall („ihrer spezifischen Freiheitsausübung").[257]

Erlangt der Staat also Kenntnis von unternehmensbezogenen Daten, ist das – anders als bei personenbezogenen Daten – für sich genommen grundrechtlich unsensibel.[258] Der Schutzbereich der unternehmensbezogenen Grundrechte ist erst dann eröffnet, wenn sich die staatliche Informationsmaßnahme auf das unternehmerische Tätigkeitsfeld des Unternehmens auswirkt.[259]

Verknüpft der Staat verschiedene Unternehmensdaten, kann dadurch jedoch im Grundsatz ein Unternehmensprofil entstehen. Eine UKZ kann die Möglichkeit zur Profilbildung eröffnen, namentlich übergreifende Informationseinblicke erschließen, die über das zur staatlichen Aufgabenerfüllung erforderliche Maß hinausgehen und negative Ausstrahlungen auf die unternehmerische Tätigkeit auslösen. Das Recht der Unternehmen auf informationelle Selbstbestimmung ist dann tatbestandlich betroffen.

---

[253] BGH, NJW 1975, 1882 (1884).
[254] Siehe BVerfGE 118, 168 (203 f.). Zu der wesensmäßigen Anwendbarkeit des informationellen Selbstbestimmungsrechts auf Unternehmen urteilt das Gericht: „Staatliche informationelle Maßnahmen können Gefährdungen oder Verletzungen der grundrechtlich geschützten Freiheit juristischer Personen herbeiführen und einschüchternd auf die Ausübung von Grundrechten wirken (vgl. BVerfGE 113, 29 [46]). In dieser Hinsicht besteht ein Schutzbedürfnis, das dem natürlicher Personen im Ansatz entspricht. Allerdings ergibt sich insoweit ein Unterschied, als der Tätigkeitskreis juristischer Personen anders als der natürlicher Personen in der Regel durch eine bestimmte Zwecksetzung begrenzt wird. Die Unterschiede, die zwischen den Schutzbedürfnissen natürlicher und juristischer Personen im Hinblick auf das Recht auf informationelle Selbstbestimmung bestehen, sind bei der Bestimmung der grundrechtlichen Gewährleistung zu beachten." In einer vorherigen Entscheidung hatte das BVerfG noch offengelassen, ob Unternehmen dem persönlichen Schutzbereich des allgemeinen Persönlichkeitsrechts unterfallen, BVerfG, Kammerbeschl. v. 3.5.1994 – 1 BvR 737/94 –, juris, Rn. 7.
[255] BVerfGE 118, 168 (204).
[256] Vgl. BVerfGE 118, 168 (204); *Stancke* (Fn. 243), 1419.
[257] BVerfGE 118, 168 (204).
[258] BVerfGE 118, 168 (204).
[259] BVerfGE 118, 168 (204): „Die informationelle Maßnahme muss vielmehr die betroffene juristische Person einer Gefährdung hinsichtlich ihrer spezifischen Freiheitsausübung aussetzen. Maßgeblich kommt es insoweit insbesondere auf die Bedeutung der betroffenen Informationen für den grundrechtlich geschützten Tätigkeitskreis der juristischen Person […] sowie auf den Zweck und die möglichen Folgen der Maßnahme an."

Ein solche staatliche Tätigkeit kann zudem den Schutzgegenstand der wirtschaftlichen Handlungs- (Art. 2 Abs. 1 GG)[260], der Berufs- (Art. 12 Abs. 1 GG) und der Eigentumsfreiheit (Art. 14 Abs. 1 GG) berühren. Das BVerfG scheint dann von einer Idealkonkurrenz dieser Grundrechte (zumindest des Art. 12 Abs. 1 GG) zum Recht auf informationelle Selbstbestimmung auszugehen.[261] Einen im Vergleich zur informationellen Selbstbestimmung größeren Schutzumfang für die Informationserhebung bei Unternehmen bieten die wirtschaftsbezogenen Grundrechte jedenfalls nicht.[262]

b) Eingriff

Sowohl die Einführung einer UKZ als auch jede weitere Verwendung unter Verarbeitung von Daten, die dem Schutzbereich des Unternehmenspersönlichkeitsrechts unterfallen, greifen in dieses Grundrecht ein und sind daher rechtfertigungsbedürftig.

c) Rechtfertigung

Ebenso wie beim Abgleich der Daten natürlicher Personen verfolgt die Steigerung der Registerqualität, die eine UKZ ermöglicht, ein verfassungsrechtlich legitimes Ziel. Denn nicht nur dann, wenn sich die Verwechslungsgefahr zwischen den Adressaten von Rechtsnormen auf ein Minimum reduziert, verbessert sich die Qualität staatlicher Register. Auch die Unternehmen selbst können von einer UKZ durch ihre Identifizierungs-, Repräsentations- und Ordnungsfunktion profitieren. Insbesondere kann sie dazu beitragen, Bürokratiekosten zu senken, indem sie die Kommunikation mit Behörden, etwa bei der Erfüllung von Meldepflichten oder der Erfüllung staatlicher Lasten, aufgrund ihrer eindeutigen Zuordnung vereinfachen und Fehlerrisiken minimieren. Meldepflichtige Daten muss das Unternehmen dann nicht wiederholt an den Staat übermitteln, weil diese ohnedies bereits mit der UKZ verknüpft sind. Dafür müssen Unternehmen im Rahmen der automatisierten Datenverarbeitung aber eindeutig gekennzeichnet und fehlerfrei identifizierbar sein. Ohne UKZ wären vielfach manuelle Kontrollen der automatisierten Datenverarbeitung notwendig, was denkbare Effizienzgewinne erheblich reduziert. Insoweit erweist sich eine UKZ als erforderlich, um die staatlichen Regulierungsziele zu erreichen.

Angemessen ist die Einführung und Verwendung einer UKZ aber nur, wenn hinreichende rechtliche, technische und organisatorische Maßnahmen sicherstellen, dass durch die Verknüpfung verschiedener Unternehmensdaten nicht ein Unternehmensprofil entsteht, das der Verwaltung einen Einblick in dessen geschäftliche Interna verschafft. Das Risiko, dass sich durch die die Verknüpfung einzelner Unternehmensdaten ein vollständiges Abbild eines

---

[260] Vgl. BVerfGE 91, 207 (221).
[261] Anders wohl *Di Fabio* (Fn. 195), Art. 2, Rn. 225.
[262] BVerfGE 118, 168 (205): „Es kann dahinstehen, ob auch die durch Art. 12 Abs. 1 in Verbindung mit Art. 19 Abs. 3 GG gewährleistete Berufsfreiheit der Beschwerdeführerin berührt ist. Jedenfalls bietet dieses Grundrecht grundsätzlich keinen über das Recht auf informationelle Selbstbestimmung hinausgehenden Schutz vor staatlichen informationellen Maßnahmen.“.

Unternehmens erzielen lässt, welches Ausstrahlungen auf die unternehmerische Tätigkeit oder hinter dem Unternehmen stehende Personen entfaltet, erweist sich bei Abgleich der Gefährdungsindikatoren als gering. Denn die Einführung einer UKZ schafft für sich genommen kein Mittel, welches durch seine Funktionsweise ein vollständiges Unternehmensbild erzeugt, sondern erst die Zusammenführung von Daten. Für diese hat der Gesetzgeber Schutzregeln zu erlassen sowie geeignete technische und organisatorische Maßnahmen vorzusehen, die möglichen Verletzungen entgegenwirken. Die Sensibilität der Zusammenführung ist mit derjenigen personenbezogener Daten in ihrer Beeinträchtigungswirkung nicht vergleichbar.

Führt der Staat über eine UKZ (außer unternehmensbezogenen) zugleich personenbezogene Daten zusammen, zieht ihm aber das informationelle Selbstbestimmungsrecht der dadurch betroffenen Einzelperson zusätzliche Grenzen: Umfassende Persönlichkeitsprofile natürlicher Personen darf er durch die Zusammenführung unterschiedlicher personenbezogener Daten weder unter einer PKZ noch einer UKZ erstellen.[263] Verknüpft der Staat verschiedene Unternehmensdaten aus dem jeweiligen Tätigkeitsfeld, so muss er sicherstellen, dass diese die Datenzusammenführung im Ergebnis nicht in ein Persönlichkeitsprofil natürlicher Personen mündet.[264]

2. Eigentumsrecht und Berufsfreiheit (Betriebs- und Geschäftsgeheimnisse)

Unternehmensdaten stehen nicht nur unter dem Schutz des Rechts auf informationelle Selbstbestimmung, sondern auch der Eigentums- und die Berufsfreiheit. Der Schutz von Betriebs- und Geschäftsgeheimnissen[265], die einen besonderen Teilausschnitt der vom Recht auf informationelle Selbstbestimmung geschützten Unternehmensdaten repräsentieren, steht einer unbegrenzten staatlichen Datensammlung im Wege.

a) Schutzbereich

Der Schutz geistigen Eigentums unterfällt dem verfassungsrechtlichen Eigentumsbegriff im Sinne des Art. 14 Abs. 1 S. 1 GG.[266] Der wohl wichtigste Unterfall für die Beeinträchtigung unternehmerischer Tätigkeitsfelder ist die Offenlegung von Betriebs- und Geschäftsgeheimnissen. Ihr Schutz ist die schillerndste und wohl bekannteste Ausprägung eines Unternehmensdatenschutzes.[267] Auf sie nimmt das einfache Recht bisweilen ausdrücklich Bezug und sorgt für einen normativen Schutz, so etwa im Informationsrecht (vgl.

---

[263] BVerfGE 65, 1 (48) unter Hinweis auf BVerfGE 27, 1 (6). Siehe hierzu auch bereits die Ausführungen auf S. 29.
[264] Siehe zu den Anforderungen im Einzelnen S. 34 ff.
[265] *Kloepfer/Greve*, NVwZ 2011, 577 (578 f.).
[266] *Papier*, in: Maunz/Dürig (Hrsg.), GG, 59. Erg.-Lfg. , Art. 14, Rn. 197 m. w. N.
[267] Zum Inhalt des Begriffs führt das BVerfG in BVerfGE 115, 205 (230 f.) aus: „Als Betriebs- und Geschäftsgeheimnisse werden alle auf ein Unternehmen bezogene Tatsachen, Umstände und Vorgänge verstanden, die nicht offenkundig, sondern nur einem begrenzten Personenkreis zugänglich sind und an deren Nichtverbreitung der Rechtsträger ein berechtigtes Interesse hat. Betriebsgeheimnisse umfassen im Wesentlichen technisches Wissen im weitesten Sinne; Geschäftsgeheimnisse betreffen vornehmlich kaufmännisches Wissen."

§ 6 S. 2 IFG).[268] Offenbaren unternehmensbezogene Daten solche Betriebs- oder Geschäftsgeheimnisse, darf der Staat sie nicht ohne Weiteres verarbeiten.

Neben Art. 14 Abs. 1 GG schützt auch Art. 12 Abs. 1 GG die Betriebs- und Geschäftsgeheimnisse eines Unternehmens.[269]

b) Eingriff

Die Einführung und Verarbeitung einer UKZ greift dann in den Schutzbereich der Eigentums- und Berufsfreiheit ein, wenn Betriebs- und Geschäftsgeheimnisse öffentlich werden (können).[270] Denn sofern „exklusives wettbewerbserhebliches Wissen den Konkurrenten zugänglich [wird], mindert dies die Möglichkeit, die Berufsausübung unter Rückgriff auf dieses Wissen erfolgreich zu gestalten."[271]

aa) Grundrechtseingriff durch die Registerführung?

Sofern der Staat Daten in Registern sammelt, bei denen es sich zumindest potenziell um Unternehmens- und Betriebsgeheimnisse handelt, können Dritte diese Register derzeit nur bei Vorliegen eines überwiegenden Interesses einsehen.[272] Behörden dürfen solche sensiblen Unternehmensdaten allenfalls nach einer Abwägung der grundrechtlich geschützten Rechtspositionen an Dritte weitergeben.

Auch innerhalb der Verwaltung dürfen Betriebs- und Geschäftsgeheimnisse nicht frei von normativen Vorgaben unbegrenzt zirkulieren. Denn ihre Wahrung ist für die wirtschaftliche Tätigkeit eines Unternehmens essenziell. Schon die Befürchtung, dass Betriebs- und Geschäftsgeheimnisse in den Händen der Verwaltung nicht hinreichend sicher sind, kann die wirtschaftliche Entfaltung eines Unternehmens beeinträchtigen. Staatliche Datenverarbeitungen, die diesen sensiblen Bereich berühren, wirken sich also auf das

---

[268] Das Vorliegen von Betriebs- oder Geschäftsgeheimnissen schließt den Informationsanspruch bei fehlender Einwilligung seitens des Betroffenen aus („absoluter Ausschlusstatbestand"), vgl. *Schoch*, IFG, 2. Aufl., 2016, § 6 Rn. 69, 116; ein anderes Beispiel ist § 17 Abs. 1 UWG: er statuiert einen Straftatbestand für die Weitergabe von Betriebs- bzw. Geschäftsgeheimnissen.

[269] Sie stehen in Idealkonkurrenz zueinander. Vgl. dazu ausführlich *Kloepfer/Greve* (Fn. 265), 579 m. w. N. So wohl auch BVerfGE 115, 205 (213) und Fn. 261.

[270] Zum Schutzbereich von Art. 12 Abs. 1 GG, vgl. BVerfGE 115, 205 (230): „Werden […] Betriebs- und Geschäftsgeheimnisse durch den Staat offen gelegt oder verlangt er deren Offenlegung, ist Art. 12 Abs. 1 GG in seinem Schutzbereich berührt. Denn dadurch kann die Ausschließlichkeit der Nutzung des betroffenen Wissens für den eigenen Erwerb […] beeinträchtigt werden. […] (BVerfG, Beschluss vom 14. März 2006 – 1 BvR 2087/03 –, Rn. 85, juris)".

[271] Das BVerfG sieht die Gefahr, dass Dritte auf der Grundlage gewonnener Informationen unternehmerische Strategien durchkreuzen: „Auch kann ein Anreiz zu innovativem unternehmerischen Handeln entfallen, weil die Investitionskosten nicht eingebracht werden können, während gleichzeitig Dritte unter Einsparung solcher Kosten das innovativ erzeugte Wissen zur Grundlage ihres eigenen beruflichen Erfolgs in Konkurrenz mit dem Geheimnisträger nutzen." BVerfGE 115, 205 (230).

[272] Etwa das Deckungsregister (§ 5 PfandBG).

unternehmerische Tätigkeitsfeld des Unternehmens aus. Daher unterliegt auch deren Weitergabe innerhalb der Verwaltung einem Gesetzesvorbehalt.

bb) Offenbarung von Betriebs- und Geschäftsgeheimnissen durch eine Datenzusammenführung mittels UKZ als Eingriff

Die UKZ lässt sich nicht nur zum behördlichen Datenaustausch nutzen. Sie bietet – zumindest theoretisch – auch die Möglichkeit, Daten, die isoliert betrachtet keine Betriebs- und Geschäftsgeheimnisse enthalten, mittels UKZ zusammenzuführen und so weitergehende Einblicke in Geschäfts- und Betriebsgeheimnisse zu erlangen.

Allerdings sind kaum Fälle denkbar, in denen *allein* die Datenzusammenführung mittels UKZ Betriebs- und Geschäftsgeheimnisse offenbart. Die Zusammenführung von Unternehmensdaten, die in verschiedenen Registern oder mit einer PKZ verknüpften Unterlagen verstreut sind, ohne für sich genommen Betriebs- und Geschäftsgeheimnisse zu enthalten, wird regelmäßig keine neue Qualität dergestalt zukommen, welche die kritische Schwelle zu Betriebs- oder Geschäftsgeheimnis überschreitet. Der Staat deckt Betriebs- und Geschäftsgeheimnisse vielmehr primär regelmäßig dadurch auf, dass er bestimmte sensible Daten (für ein bestimmtes Register) unzulässig erhebt. Vorstellbar ist eine Überschreitung der Zulässigkeitsschwelle durch Zusammenführung dann, wenn Behörden oder Private Unternehmensdaten zusammenführen, ohne dafür eine Verarbeitungsbefugnis zu besitzen. Unzulässig ist dann aber nicht schon selbstredend die UKZ, sondern die unzulässige Zusammenführung der Daten, d. h. das Fehlen einer Verarbeitungsbefugnis. Von der UKZ selbst geht insoweit grundsätzlich lediglich eine Grundrechtsgefährdung aus.

c) Rechtfertigung

Im Rahmen der verfassungsrechtlichen Rechtfertigung bedarf es einer Abwägung des Interesses des Staates an qualitativ hochwertigen Registern mit dem durch die Berufs- und Eigentumsfreiheit geschützten Geheimhaltungsinteresse des Unternehmens. Eine verfassungsrechtlich kritische Grenze ist dann erreicht, wenn die Möglichkeit, Daten im Gefolge einer Modernisierung des Registerwesens zusammenzuführen, Gesamteinblicke in schutzwürdige Geschäftsprozesse ermöglicht, welche die legitimen unternehmerischen Schutzinteressen nachhaltig gefährden.

Die Hürden dafür liegen aber hoch. Die Möglichkeit, Stammdaten eines Unternehmens zu verknüpfen, reicht dafür jedenfalls nicht aus. Ermöglicht eine UKZ tiefer gehende Einblicke in Betriebs- und Geschäftsgeheimnisse, muss der Staat dieses Risiko durch technische und organisatorische Maßnahmen einfangen. Hierzu kann er sich an den Maßnahmen orientieren, die Teil der Schutzmaßnahmen einer PKZ sind.34[273]

[273] Vgl. S. 34.

IV. Das Rückspielverbot im Kontext des Unternehmensdatenschutzes

Nicht nur im Hinblick auf natürliche Personen, sondern auch in Bezug auf Unternehmen muss der Staat – unter den besonderen Vorzeichen der Schutzbedürftigkeit von Unternehmensdaten – das Rückspielverbot beachten:[274] Es bietet auch hier die Gewähr für die Zuverlässigkeit der erfragten Unternehmensangaben, indem es den Befragten ein berechtigtes Vertrauen auf die Geheimhaltung ihrer Angaben vermittelt.[275]

[274] Schließlich haben auch Unternehmensdaten an dem Schutz der informationellen Selbstbestimmung Teil (vgl. S. 53), welchen das Rückspielverbot zu schützen gedenkt (vgl. A.II.2.b) bb) (2) (c) S. 15).
[275] Vgl. BT-Drs. 10/5345, S. 20 sowie VGH Kassel, Urt. v. 30.7.2015 – 6 A 1998/13 –, juris Rn. 44.

C. Zusammenfassung

Den rechtlichen Rahmen für die Einführung und Nutzung einer allgemeinen PKZ in der Bundesrepublik Deutschland stecken die DSGVO und das deutsche Verfassungsrecht ab.

I. Unionsrecht, insbesondere DSGVO

Art. 16 AEUV und Art. 8 GrCh sichern den Schutz personenbezogener Daten grundrechtlich ab. Der europäische Gesetzgeber hat ihren Schutzradius nunmehr durch die DSGVO sekundärrechtlich mit Inhalt gefüllt. Die Verordnung steht einer nationalen PKZ grundsätzlich offen gegenüber: Art. 87 S. 1 DSGVO erlaubt den Mitgliedstaaten die Nutzung einer PKZ und ermächtigt sie, die normativen Anforderungen an ihre Verarbeitung im nationalen Recht näher zu konkretisieren. Der Mitgliedstaat muss den Betroffenen aber ein Schutzniveau verbürgen, das mit demjenigen der DSGVO vergleichbar ist (Art. 87 S. 2 DSGVO).

Während die DSGVO den Mitgliedstaaten für die Verarbeitung der PKZ (und der Daten, die mit ihr verknüpft sind, soweit sie ein notwendiger Zwischenschritt zur Erteilung der PKZ sind) als solcher eine Öffnungsklausel zur Verfügung stellt, die sie selbst normativ bespielen dürfen, gelten für die Verarbeitung der Daten, die mit dem Kennzeichen verbunden sind, die allgemeinen Vorgaben der DSGVO unmittelbar. Art. 87 DSGVO erfasst diese Daten nicht.

Sofern der Staat im Rahmen der Registermodernisierung aber neue Daten unter einer PKZ erheben will, bedarf er hierfür einer gesetzlichen Grundlage. Eine solche darf der deutsche Gesetzgeber aufgrund der Öffnungsklausel des Art. 6 Abs. 1 UAbs. 1 lit. e i. V. m. Abs. 3 S. 1 lit. b DSGVO jedoch kraft eigenen Rechts etablieren.

Gleicht der Staat bereits erhobene Daten mit Daten aus staatlichen Registern ab, verknüpft er sie mit ihnen oder will er sie in andere Register übertragen, ändert er hiermit den ursprünglichen Verarbeitungszweck. Für eine solche Zweckänderung kann und muss der deutsche Gesetzgeber eine Rechtsgrundlage schaffen (Art. 6 Abs. 4 DSGVO i. V. m. Art. 23 Abs. 1 lit. e DSGVO). Da es sich bei der öffentlichen Registerführung um ein schützenswertes öffentliches Interesse i. S. v. Art. 23 Abs. 1 lit. e DSGVO handelt,[276] darf der deutsche Gesetzgeber auch Ausnahmen von den Betroffenenrechten der Art. 12–22 und 34 DSGVO etablieren – dies jedoch nicht vorbehaltlos, sondern nur soweit dies zur Zielerreichung erforderlich ist und sich insbesondere nicht als unverhältnismäßige Einschränkung des Rechts auf informationelle Selbstbestimmung entpuppt.

[276] Dies bezeugt die DSGVO explizit in ErwGr. 73 S. 1 DSGVO („das Führen öffentlicher Register aus Gründen des allgemeinen öffentlichen Interesses“).

II. Nationales Verfassungsrecht

Problematischer als aus der Perspektive des Unionsrechts stellt sich die anvisierte Registermodernisierung mithilfe allgemeiner Personenkennzeichen aus der Perspektive des nationalen Verfassungsrechts dar. Ein dauerhaftes Kennzeichen für jeden Deutschen gilt – vor dem Hintergrund der deutschen Erfahrungen mit totalitären Herrschaftssystemen – als „rotes Tuch" der Staat-Bürger-Beziehung.[277] Denn in dem Kennzeichen schlummert die Möglichkeit, dass der Staat umfassende Persönlichkeitsprofile erstellt und damit das informationelle Selbstbestimmungsrecht der Grundrechtsträger durch eine Katalogisierung der Persönlichkeit systematisch aushöhlt.[278]

1. Allgemeine PKZ als verhältnismäßiger Eingriff in Art. 2 I i. V. m. Art. 1 I GG?

Eine PKZ schafft für jeden Betroffenen ein neues personenbezogenes Datum, über dessen weitere Verwendung er fortan nicht mehr ausschließlich selbst entscheiden kann. Bereits mit Blick auf das durch sie hervorgerufene Gefahrenszenario kommt allgemeinen Personenkennziffern Eingriffsqualität zu.[279]

Nicht nur die Einführung einer PKZ, sondern auch jede (weitere) Verarbeitung personenbezogener Daten im Zuge der Registermodernisierung ist vor dem Recht auf informationelle Selbstbestimmung rechtfertigungsbedürftig. Gerechtfertigt sind diese Eingriffe, wenn sie sich auf eine hinreichend konkrete gesetzliche Grundlage stützen können (Wesentlichkeitstheorie, Gebot der Normenklarheit). Darüber hinaus muss der Eingriff im überwiegenden Allgemeininteresse erfolgen und darf nicht unverhältnismäßig sein.

Die Registermodernisierung und die Einführung einer PKZ sind wichtigen Gemeinwohlzielen verschrieben. Sie verhindern Doppelzuordnungen und dadurch bedingte Fehler bei der Zuweisung staatlicher Leistungen oder der Besteuerung bestimmter Lebenssachverhalte. Darüber hinaus bilden sie eine zentrale Voraussetzung, um einen Zensus mit hinreichender Treffsicherheit registerbasiert durchführen zu können. Für das Gemeinwesen verbinden sich damit ein erhebliches Einsparpotenzial und Effizienzgewinne.

Aller Gemeinwohlbelange, die eine PKZ fördern soll, zum Trotz, ist es dem Staat verfassungsrechtlich verwehrt, Daten in einer Weise zu sammeln, die in eine „persönlichkeitsfeindliche Registrierung und Katalogisierung des Einzelnen" mündet.[280] Ein umfassendes Persönlichkeitsprofil tangiert die Menschenwürde und ist daher mit dem

---

[277] Wegen datenschutzrechtlicher Bedenken hat der Gesetzgeber in den 70er Jahren von einem entsprechenden Gesetzgebungsprojekt Abstand genommen, vgl. dazu *Zelyk* (Fn. 20), S. 7 f. und oben S. 3 ff. Anschließend verschwand die Thematik aus dem Fokus der Öffentlichkeit. Erst die Einführung der Steuer-ID als bPKZ hat die Diskussion um die Einführung von PKZ wieder befeuert.
[278] So zur Steuer-ID FG Köln, Urt. v. 7.7.2010 – 2 K 2999/08 –, juris, Rn. 76.
[279] Vgl. BVerfGE 120, 378 (397).
[280] BVerfGE 65, 1 (48) unter Hinweis auf BVerfGE 27, 1 (6).

Persönlichkeitsrecht der Betroffenen nicht vereinbar. Diese rote Linie sieht das BVerfG überschritten, „soweit eine unbeschränkte Verknüpfung [erhobener] Daten mit den bei den Verwaltungsbehörden vorhandenen, zum Teil sehr sensitiven Datenbeständen oder gar die Erschließung eines derartigen Datenverbundes durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal möglich wäre".[281] Denn ein solches Kennzeichen ermöglicht die Verknüpfung aller Daten, die mit der PKZ verbunden sind. Diese Verknüpfung kann in eine persönlichkeitsfeindliche Katalogisierung des Einzelnen münden.

Eine generelle, vorbehaltlose Absage hat das BVerfG der Einführung und Verwendung einer PKZ im Volkszählungsurteil aber nicht erteilt.[282] Ihre Einführung ruft solange keine untragbaren Konflikte mit dem Recht auf informationelle Selbstbestimmung hervor, wie der Staat eine Verknüpfung der Daten, die mit dem Kennzeichen verbunden sind, durch organisatorische, technische und rechtliche Maßnahmen wirksam verhindert. Bezieht man die Möglichkeiten moderner Big-Data-Anwendungen in die Risikoanalyse ein, zeigt sich, dass eine gleichwertige Verknüpfung von Daten im 21. Jahrhundert auch ohne die Zuhilfenahme der PKZ möglich ist.[283] Eine PKZ präsentiert sich dann als nur *eines von vielen anderen Mitteln*, um eine Person fehlerfrei zu identifizieren und personenbezogene Informationen zu einem Profil zusammenzufügen. Auch deshalb ist es sachgerecht, den verfassungsrechtlichen Fokus vom Instrument „Personenkennziffer" auf die Vereinbarkeit der konkreten Ausgestaltung mit den Grundwerten der Rechtsordnung zu lenken.

2. Ansatzpunkte für angemessene organisatorische, technische und rechtliche Rahmenbedingungen der Registermodernisierung mittels PKZ

Welche organisatorischen, technischen und rechtlichen Maßnahmen der Gesetzgeber in concreto vorsehen muss, sagt die Verfassung nicht. Die Legislative verfügt über einen Handlungsspielraum, der aber einem hinreichenden Maß an Ergebnissicherheit genügen muss.

Mechanismen, mit deren Hilfe der Gesetzgeber die Eingriffsintensität abschwächen und die Gefahr einer umfassenden Profilbildung eindämmen kann, sind insbesondere strenge Anforderungen an die Zweckbindung der Datenverarbeitung und Sanktionstatbestände, die ein Fehlverhalten in hinreichend abschreckender Weise ahnden.

Eine taugliche Blaupause für technische und organisatorische Vorkehrungen, die eine umfassende Profilbildung effektiv erschweren oder gar unmöglich machen, liefert die Republik Österreich.[284] Die Struktur mehrerer bereichsspezifischer Personenkennziffern für eng konturierte Lebensbereiche stellt auf einer ersten Stufe sicher, dass kein allumfassendes

---

[281] BVerfGE 65, 1 (53).
[282] Zur Auslegung näher oben S. 29 ff.
[283] *Weichert* (Fn. 6), Art. 87, Rn. 20.
[284] Zu dem österreichischen Modell siehe *McKinsey & Company Inc.* (Fn. 4), S. 15 ff.; *Statistisches Bundesamt* (Fn. 7), S. 15 ff.

„Superregister“ entsteht. Kristallisationspunkt der Datensynchronisation innerhalb der österreichischen Verwaltung ist – auf einer zweiten Stufe – die bei der Datenschutzaufsichtsbehörde angesiedelte Stammzahlenregisterbehörde: Nur sie verfügt über die PKZ und kann sie einer bestimmten Person zuordnen. Sie vermittelt letztlich nur zwischen den jeweiligen Fachbehörden, die ihrerseits nach wie vor Hüter der bei ihnen separat gespeicherten Fachdatensätze bleiben.

Das Modell einer PKZ, die auf der Grundlage lebensbereichsspezifischer Kennziffern aufbaut und eine Zusammenführung der Daten durch organisatorische Trennung und technische Maßnahmen wirksam verhindert, kann – unter erheblichen verfassungsrechtlichen Kautelen – auch in Deutschland rechtlich zulässig sein.

Der Gesetzgeber muss dann aber auch ausreichende flankierende Sicherungsmechanismen im Recht der behördlichen Datenverarbeitung einziehen. Dies gilt insbesondere für die Ermächtigungsgrundlagen zur Einführung einer PKZ als auch für die Reglementierung ihrer Nutzung im interbehördlichen Datenverkehr.

Je nachdem, welche konkrete Verwendungen der Gesetzgeber für die bPKZ vorsehen will, muss er die Behörden zumindest partiell von dem unionsrechtlichen Zweckbindungsgrundsatz dispensieren. Dafür lässt ihm die DSGVO aber den notwendigen Freiraum.

III. Unternehmenskennziffer

Eine UKZ ist verfassungsrechtlich weit weniger sensibel als eine PKZ. Eine Kennziffer für deutsche Unternehmen berührt grundsätzlich keine Persönlichkeitsrechte, soweit Unternehmensdaten nicht zugleich Rückschlüsse auf personenbezogene Daten natürlicher Personen (z. B. eines Einzelunternehmers) zulassen. Der Staat muss aber sicherstellen, dass die Verarbeitung der Unternehmensdaten nicht in verfassungswidriger Weise in die Grundrechte des Unternehmens eingreift.

D. Literaturverzeichnis

Anonymous, ELENA-Verfahren wird eingestellt, NJW-Spezial 2011, S. 596.

Augsberg, Steffen, Von der Solange- zur Soweit-Rechtsprechung: Zum Prüfungsumfang des Bundesverfassungsgerichts bei richtlinienumsetzenden Gesetzen, DÖV 2010, S. 153–160.

Baumbach, Adolf/*Hopt*, Klaus J. (Hrsg.), Handelsgesetzbuch, mit GmbH & Co., Handelsklauseln, Bank- und Börsenrecht, Transportrecht (ohne Seerecht), 37. Aufl. Bd. 9, München, 2016.

Beck, Roman/*Hilgers*, Dennis/*Krcmar*, Helmut/*Krimmer*, Robert, et al., Digitale Transformation der Verwaltung, Empfehlungen für eine gesamtstaatliche Strategie, 2017.

Bundesministerium des Innern, Personenkennzeichen, Bonn, 1971.

Busch, Jost-Diedrich, Anmerkung zu BVerfG, Urt. v. 15.12.1983 – BvR 209/83 –, DVBl 1984, S. 385–389.

Denninger, Erhard/*Hoffmann-Riem*, Wolfgang/*Schneider*, Hans-Peter/*Stein*, Ekkehart (Hrsg.), Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, Reihe Alternativkommentare, 3. Aufl., Neuwied, 2001.

Ehmann, Eugen/*Selmayr*, Martin (Hrsg.), Datenschutz-Grundverordnung, Kommentar, München, 2017.

Epping, Volker/*Hillgruber*, Christian (Hrsg.), Beck'scher Online-Kommentar GG, 32. Ed., Stand: 1.3.2017.

Gersdorf, Hubertus/*Paal*, Boris P. (Hrsg.), Beck'scher Online-Kommentar Informations- und Medienrecht, 16. Ed., München, 2017.

Gola, Peter (Hrsg.), Datenschutz-Grundverordnung, Kommentar, München, 2017.

Gola, Peter/*Schomerus*, Rudolf (Hrsg.), BDSG, 12. Aufl., München, 2015.

Greis, Friedhelm, EU-Kommission lehnt deutschen Sonderweg ab, golem.de vom 21.4.2017, https://www.golem.de/news/datenschutzreform-eu-kommission-lehnt-deutschen-sonderweg-ab-1704-127430.html (18.9.2017).

Gürtler-Bayer, Manuela, Der behördliche Datenschutzbeauftragte, Eine Analyse rechtlicher Probleme in der Konzeption des behördlichen Datenschutzbeauftragten unter Berücksichtigung der EU-Datenschutz-Grundverordnung, Hamburg, 2014.

Hanfeld, Michael, Punkte für gefälliges Verhalten, faz.net vom 10.10.2015, http://www.faz.net/video/medien/punktrichter-citizen-score-ueberwachung-in-china-13848403.html (21.8.2017).

– Tallinn, wir haben ein Problem, FAZ online vom 7.9.2017, http://www.faz.net/aktuell/feuilleton/debatten/estland-sicherheitsluecke-bei-elektronischen-personalausweisen-15186516.html (20.9.2017).

Härting, Niko, Anonymität und Pseudonymität im Datenschutzrecht, NJW 2013, S. 2065–2072.

Hill, Hermann/*Martini*, Mario/*Wagner*, Edgar (Hrsg.), Die digitale Lebenswelt gestalten, Baden-Baden, 2015.

Hölters, Wolfgang (Hrsg.), Aktiengesetz, 3. Aufl., München, 2017.

Hornung, Gerrit, Die digitale Identität, Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden, 2005.

Kingreen, Thorsten/*Poscher*, Ralf, Grundrechte, 32. Aufl., Heidelberg, 2016.

Kloepfer, Michael/*Greve*, Holger, Das Informationsfreiheitsgesetz und der Schutz von Betriebs- und Geschäftsgeheimnissen, NVwZ 2011, S. 577–584.

Koenig, Ulrich (Hrsg.), Abgabenordnung, 3. Aufl., München, 2014.

Körner, Anne/*Leitherer*, Stephan/*Mutschler*, Bernd/*Brandts*, Ricarda (Hrsg.), Kasseler Kommentar Sozialversicherungsrecht, Losebl. (Stand 59. ERf-Lfg.), München, 2017.

Kühling, Jürgen/*Buchner*, Benedikt (Hrsg.), Datenschutz-Grundverordnung, Kommentar, München, 2017.

Kühling, Jürgen/*Klar*, Manuel, Unsicherheitsfaktor Datenschutzrecht – Das Beispiel des Personenbezugs und der Anonymität, NJW 2013, S. 3611–3617.

Kühling, Jürgen/*Martini*, Mario, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, S. 448–454.

Kühling, Jürgen/*Martini*, Mario/*Heberlein*, Johanna/*Kühl*, Benjamin, et al., Die DSGVO und das nationale Recht, Erste Überlegungen zum nationalen Regelungsbedarf, Münster, 2016.

Marnau, Ninja, Anonymisierung, Pseudonymisierung und Transparenz für Big Data, Technische Herausforderungen und Regelungen in der Datenschutz-Grundverordnung, DuD 2016, S. 428–433.

Martini, Mario, Der Zensus 2011 als Problem interkommunaler Gleichbehandlung, Berlin, 2011.

– Big Data als Herausforderung für das Datenschutzrecht und den Persönlichkeitsschutz, in: Hill, Hermann/Martini, Mario/Wagner, Edgar (Hrsg.), Die digitale Lebenswelt gestalten, Baden-Baden, 2015, S. 97–162.

– Wie neugierig darf der Staat im Cyberspace sein?, Social Media Monitoring öffentlicher Stellen – Chancen und Grenzen, VerwArch. 2016, S. 307–358.

– Transformation der Verwaltung durch Digitalisierung, DÖV 2017, S. 443–455.

Martini, Mario/*Wenzel*, Michael, „Once only“ versus „only once“: Das Once-only-Prinzip zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit, DVBl 2017, S. 749–758.

Maunz, Theodor/*Dürig*, Günter (Hrsg.), Grundgesetz, Kommentar, Losebl. (Stand: 79. Erg.-Lfg.), München, 2016.

McKinsey & Company Inc., Mehr Leistung für Bürger und Unternehmen: Verwaltung digitalisieren. Register modernisieren, Berlin, Okt. 2017.

Montjoye, Yves-Alexandre de/*Laura Radaelli/Singh*, Vivek Kumar/*Pentland*, Alex “Sandy”, Unique in the shopping mall: On the reidentifiability of credit card metadata, science 347 (2015), S. 536–539.

Nationaler Normenkontrollrat, Leistungsbeschreibung NKR Gutachten 2017, Berlin, 2017.

Paal, Boris P./*Pauly*, Daniel A. (Hrsg.), Datenschutz-Grundverordnung, Kommentar, München, 2017.

Plath, Kai-Uwe (Hrsg.), BDSG/DSGVO, Kommentar zum BDSG und zur DSGVO sowie den Datenschutzbestimmungen des TMG und TKG, 2. Aufl., Köln, 2016.

Reinvere, Jüri, Das Risiko für Estland ist essenziell, FAZ online vom 8.9.2017, http://www.faz.net/aktuell/feuilleton/debatten/estlands-praesidentin-glaubt-an-den-digitalen-staat-15188049.html.

Schaar, Peter, Steuer-ID darf kein allgemeines Personenkennzeichen werden!, ZD 2011, S. 49–50.

Schlink, Bernhard, Das Recht der informationellen Selbstbestimmung, Der Staat 25 (1986), S. 233–250.

Schmidt-Bleibtreu, Bruno/*Hofmann*, Hans/*Henneke*, Hans-Günter (Hrsg.), Kommentar zum Grundgesetz, 13. Aufl., Köln, 2014.

Schoch, Friedrich, IFG, Kommentar, 2. Aufl., München, 2016.

Scholz, Rupert/*Pitschas*, Rainer, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin, 1984.

Seckelmann, Margrit (Hrsg.), Digitalisierte Verwaltung – Vernetztes E-Government, 2017 (im Erscheinen).

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 8. Aufl., Baden-Baden, 2014.

Stancke, Fabian, Grundlagen des Unternehmensdatenschutzrechts - gesetzlicher und vertraglicher Schutz unternehmensbezogener Daten im privaten Wirtschaftsverkehr, BB 2013, S. 1418–1425.

Statistisches Bundesamt, Beistellung zum Gutachten “Registermodernisierung” im Auftrag des Nationalen Normenkontrollrats, 3.4 Beispiele aus anderen Ländern zur Registernutzung in Zensus und Bevölkerungsstatistik, Wiesbaden, 2017.

Steinmüller, Wilhelm, Das Volkszählungsurteil des Bundesverfassungsgerichts, DuD 1984, S. 91–96.

Stepputat, Caroline, Nach dem Volkszählungsurteil 1983: Ein verfassungsgemäßes Zensusgesetz 2011?, DÖV 2011, S. 111–116.

Uhlenbruck, Wilhelm/*Hirte*, Heribert/*Vallender*, Heinz (Hrsg.), Insolvenzordnung, Kommentar, 14. Aufl., München, 2015.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Verkettung digitaler Identitäten, Kiel, 2007.

von der Groeben, Hans/*Schwarze*, Jürgen/*Hatje*, Armin (Hrsg.), Europäisches Unionsrecht, Vertrag über die Europäische Union - Vertrag über die Arbeitsweise der Europäischen Union - Charta der Grundrechte der Europäischen Union, 7. Aufl., Baden-Baden, 2015.

von Lewinski, Kai, Datenbanken sowie Ordnungs- und Personenkennzeichen, in: Seckelmann, Margrit (Hrsg.), Digitalisierte Verwaltung – Vernetztes E-Government, 2017 (im Erscheinen).

Warislohner, Fabian, Dystopia wird Wirklichkeit: Was ist dran an Chinas „Social Credit System“?, netzpolitik.org vom 9.10.2015, https://netzpolitik.org/2015/dystopia-wird-wirklichkeit-was-ist-dran-an-chinas-social-credit-system/ (21.8.2017).

Weichert, Thilo, Big Data und Datenschutz, ZD 2013, S. 251–259.

Wiebe, Andreas/*Schur*, Nico, Ein Recht an industriellen Daten im verfassungsrechtlichen Spannungsverhältnis zwischen Eigentumsschutz, Wettbewerbs- und Informationsfreiheit, ZUM 2017, S. 461–473.

Wolff, Heinrich Amadeus/*Brink*, Stefan (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 20. Ed., München, Stand: 1.5.2017.

Zelyk, Marcus, Das einheitliche steuerliche Identifikationsmerkmal, Eine verfassungsrechtliche Analyse, Frankfurt am Main, 2012.

Zu den Autoren

Prof. Dr. Mario Martini ist Inhaber des Lehrstuhls für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht an der Deutschen Universität für Verwaltungswissenschaften, Stellvertretender Direktor des Deutschen Forschungsinstituts für öffentliche Verwaltung und Leiter des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung“ (http://www.foev-speyer.de/de/forschung/digitalisierung.php). Vor seiner Tätigkeit in Speyer hatte er eine Professur für Staats- und Verwaltungsrecht an der Ludwig-Maximilians-Universität München inne. Rufe an die Universitäten Augsburg, Passau und an die Leibniz Universität Hannover hat er abgelehnt.

Im Jahr 2006 habilitierte er sich an der Bucerius Law School mit einer Arbeit zu dem Titel »Der Markt als Instrument hoheitlicher Verteilungslenkung«. In der Zeit zwischen 2001 und 2007 war er dort als wissenschaftlicher Assistent und Habilitand am Lehrstuhl für Öffentliches Recht einschließlich Völker- und Europarecht (Prof. Dr. Jörn Axel Kämmerer) tätig. Im Anschluss an das Rechtsreferendariat in Rheinland-Pfalz (1998 – 2000) war er von 1995 bis 1998 als wissenschaftlicher Mitarbeiter an der Johannes-Gutenberg-Universität Mainz tätig. Dort wurde er im Jahre 1999 mit einer umweltrechtlichen Arbeit zu dem Thema »Integrierte Regelungsansätze im Immissionsschutzrecht« promoviert.

Prof. Dr. Mario Martini ist durch zahlreiche Veröffentlichungen im Staats-, Verwaltungs- und Europarecht sowie im öffentlichen Wirtschafts- und Digitalisierungsrecht ausgewiesen. Aktuelle Informationen (samt Stellenausschreibungen für die Mitwirkung am Lehrstuhl) finden sich unter: http://www.uni-speyer.de/de/lehrstuehle/martini//begruessung-prof-martini.php bzw. https://twitter.com/profmartini?lang=de.

Jüngste Veröffentlichungen (Auswahl):

1. Monographien

- Verwaltungsprozessrecht und Allgemeines Verwaltungsrecht - eine systematische Darstellung in Text-Bild-Kombination, 6. Aufl., München 2017.
- Die Landarztquote - verfassungsrechtliche Zulässigkeit und rechtliche Ausgestaltung, Verlag Duncker & Humblot, 235 Seiten, 2017 (mit Jan Ziekow).

- Digitalisierung als Herausforderung und Chance für Staat und Verwaltung - Forschungskonzept des Programmbereichs „Transformation des Staates in Zeiten der Digitalisierung", FÖV Discussion Papers 85, Speyer 2016.

2. Aufsätze

- Art. 91c Abs. 5 GG und das neue Zugangsregime zur digitalen Verwaltung – Quantensprung oder zu kurz gesprungen?, ZG 2017, S. 193-227 (mit Cornelius Wiesner)
- Die Blockchain und das Recht auf Vergessenwerden, NVwZ 2017, S. 1251-1259 (mit Quirin Weinzierl)
- Transformation der Verwaltung durch Digitalisierung, DÖV 2017, S. 443-455.
- Wenn Maschinen entscheiden ... – vollautomatisierte Verwaltungsverfahren und der Persönlichkeitsschutz (mit David Nink),
  - Abstract: NVwZ 2017, S. 681 f.
  - Langfassung: NVwZ-Extra 10/2017, S. 1-14.
- Die Zeitung im Sog des digitalen Wandels: Presseförderung zwischen Vielfaltssicherung und europäischem Beihilfenrecht, in: Hill/Martini/Kugelmann (Hrsg.), Perspektiven der digitalen Lebenswelt, Baden-Baden 2017, S. 203-294.
- Nationales Verfassungsrecht als Prüfungsmaßstab des EuGH? - Der Vollzug nationalen Rechts durch die EZB und seine ungelösten Folgeprobleme, NVwZ 2017, S. 177-183 (mit Quirin Weinzierl).

David Wagner ist Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung in Speyer. Er promoviert zur Bereitstellung öffentlicher Daten.

Vor seiner Tätigkeit am Forschungsinstitut war er wissenschaftlicher Mitarbeiter bei Allen & Overy.

Michael Wenzel ist Forschungsreferent am Deutschen Forschungsinstitut für öffentliche Verwaltung in Speyer. Er koordiniert dort den Programmbereich „Transformation des Staates in Zeiten der Digitalisierung“. Sein Promotionsvorhaben behandelt den Rechtspfleger aus der Perspektive des öffentlichen Rechts.

Zuvor war er am Lehrstuhl für Verwaltungswissenschaft, Staatsrecht, Verwaltungsrecht und Europarecht (Prof. Dr. Mario Martini) an der Deutschen Universität für Verwaltungswissenschaften Speyer tätig.

Jüngste Veröffentlichungen:

1. Monographien

- Die DSGVO und das nationale Recht – Erste Überlegungen zum nationalen Regelungsbedarf, 525 Seiten, Münster, 2016 (mit Kühling/Martini/Heberlein/Kühl/Nink/Weinzierl).

2. Aufsätze

- „Once only" versus „only once": Das Once-only-Prinzip zwischen Zweckbindungsgrundsatz und Bürgerfreundlichekeit, DVBl 2017, S. 749-758 (mit Prof. Dr. Mario Martini).
- „Gelbe Karte“ von der Aufsichtsbehörde: Die Verwarnung als datenschutzrechtliches Sanktionenhybrid, PinG 3/2017, S. 92-96 (mit Prof. Dr. Mario Martini).
- Bodycams zwischen Bodyguard und Big Brother - Zu den rechtlichen Grenzen filmischer Erfassung von Sicherheitseinsätzen (mit Prof. Dr. Mario Martini und David Nink), NVwZ Extra 27/2017, S. 1 ff.