Aus dem Inhalt des Bandes
DStJG 42 (2019)

Digitalisierung im Steuerrecht

43. Jahrestagung
der Deutschen Steuerjuristischen Gesellschaft e.V.
Köln, 17. und 18. September 2018

Herausgegeben im Auftrag der
Deutschen Steuerjuristischen Gesellschaft e.V.

von

Prof. Dr. Johanna Hey
Universität zu Köln

2019

Sonderdruck

ottoschmidt

Zitierempfehlung
Verf., DStJG 42 (2019), S. ...

Dieser Sonderdruck ist nicht im Buchhandel erhältlich.

Verlag Dr. Otto Schmidt KG
Gustav-Heinemann-Ufer 58, 50968 Köln
Tel. 0221/93738-01, Fax 0221/93738-943
info@otto-schmidt.de
www.otto-schmidt.de

Satz: WMTP, Birkenau
Druck und Verarbeitung: Kösel, Krugzell
Printed in Germany

Inhalt

Ausführliche Inhaltsübersichten jeweils zu Beginn der Beiträge.

Datenschutz und Datenaustausch

Prof. Dr. *Roman Seer*
Ruhr-Universität Bochum

I. Nationaler Datenschutz

1. Entwicklung des Rechts auf informationelle Selbstbestimmung durch das BVerfG

a) Verfassungsrechtlicher Schutzbereich

In dem grundlegenden Urteil zum Volkszählungsgesetz aus dem Jahr 1983 hat das BVerfG das *Recht auf informationelle Selbstbestimmung* aus dem allgemeinen Persönlichkeitsrecht entwickelt[1]. Das BVerfG hält dieses Recht durch die Automatisierung der Datenverarbeitung für gefährdet. Personenbezogene Daten sind technisch gesehen unbegrenzt speicherbar und ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar. Schon im Jahr 1983 erkannte das BVerfG die Möglichkeit der Vernetzung der einzelnen Datensammlungen mit der Folge, dass ein Persönlichkeitsbild erstellt werden kann. Weiß der Einzelne nicht, welche Daten über ihn erfasst werden, wird er in der Ausübung seiner Grundrechte gehemmt, um nicht aufzufallen. Die freie Entfaltung der Persönlichkeit setzt damit den *Schutz des Einzelnen gegen eine unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten* voraus. Das Recht auf informationelle Selbstbestimmung dient dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte (auch der Wirtschaftsfreiheiten in Gestalt der Berufs- und Eigentümerfreiheit, Art. 12, 14 GG) führen kann.

Der Schutzbereich umfasst alle *personenbezogenen Daten*. Dabei sind nicht nur die personenbezogenen Daten gemeint, die den Kern des Persönlichkeitsrechts ausmachen, ihrer Art nach äußerst sensibel sind und deshalb geschützt werden. Der Schutzbereich des Rechts auf informationelle Selbstbestimmung ist nicht auf diese Privatsphäre beschränkt. Vielmehr ist er weit und umfasst auch solche *individualisierbaren Besteuerungsgrundlagen*, die als wirtschaftliche Größen (Umsatz, Gewinn, Einkünfte u.a.) das Ergebnis eines „marktoffenen" Erwerbs sind[2]. Auch die Angaben, die ein Steuerpflichtiger aufgrund des geltenden Abgabenrechts zu machen hat, fallen in den Schutzbereich des Rechts auf informationelle Selbstbestimmung, da diese Daten weitreichende Einblicke in die persönlichen Verhältnisse, die persönliche Lebensführung und in die

1 BVerfG v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 (42 f.).
2 *Drüen*, Verfassungsfragen der digitalen Außenprüfung, StuW 2003, 205 (211 f.); a.A. aber noch *P. Kirchhof*, Steueranspruch und Informationseingriff, in FS Tipke, Köln 1995, S. 27 (33 ff.).

beruflichen, betrieblichen, unternehmerischen und sonstigen wirtschaftlichen Verhältnisse gewähren[3]. Selbst die Speicherung und Verwendung solcher Daten, die an sich nur einen geringen Informationsgehalt haben, können durch die technischen Verarbeitungs- und Verknüpfungsmöglichkeiten erhebliche Auswirkungen auf die Freiheit des Einzelnen haben.

b) Datenschutzspezifische Schrankenbestimmung

Das Recht auf informationelle Selbstbestimmung ist aber *nicht schrankenlos*. Vielmehr betont das BVerfG, dass das Grundgesetz das Spannungsverhältnis zwischen Individuum und Gemeinschaft im Sinne der Gemeinschaftsbezogen- und -gebundenheit der Person entschieden hat[4]. Deshalb liegt der Schwerpunkt der Rechtsprechung des BVerfG auf den sog. *Schranken-Schranken*, die den *Vorbehalt des Gesetzes*, das *Bestimmtheitsgebot* und das *Verhältnismäßigkeitsprinzip* datenschutzrechtlich fortentwickeln. Den Kern beschreibt das BVerfG im Volkszählungsurteil mit den folgenden Worten:[5]

„Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und dass die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre eine Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren. [...]

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 Weitergabe- und Verwertungsverbote erforderlich. Als weitere verfahrensrechtliche Schutzvorkehrungen sind Aufklärungs-, Auskunfts- und Löschungspflichten wesentlich."

Es liegt auf der Hand, dass der Steuerpflichtige *kein „Recht auf steuerliche Selbstbestimmung"* besitzen kann. Vielmehr nimmt der Staat im Interesse der Belastungsgleichheit an den Steuerdaten der Bürger und Unternehmen teil[6]. Dies hat das BVerfG für den Bereich des Steuerrechts in den Entscheidungen zum sog. Kontenabruf nach § 93 Abs. 7, 8 AO[7] und zur sog. IZA-Sammlung des BZSt[8] anerkannt und auf den Verfassungsrang des Gebots der Besteuerungsgleichheit sowie die eigene Rechtspre-

3 Siehe BVerfG v. 17.7.1984 – 2 BvE 11 u. 15/83, BVerfGE 67, 100 (142 f.).
4 BVerfG v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 (43 f.).
5 BVerfG v. 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1 (46).
6 *Drüen* (Fn. 2), StuW 2003, 205, (213 f.).
7 BVerfG v. 13.6.2007 – 1 BvR 1550/03 u.a., BVerfGE 118, 168 (196 ff.).
8 BVerfG v. 10.3.2008 – 1 BvR 2388/03, BVerfGE 120, 351 (366 ff.).

chung zum Verbot struktureller Vollzugsdefizite im Steuerrecht[9] hingewiesen.

In diesen Entscheidungen arbeitet das BVerfG aber zugleich *Mindestanforderungen* für den datenschutzrechtlichenen Steuereingriff heraus. Nach dem *Gebot der Normenklarheit und -bestimmtheit*[10] muss sich der betroffene Bürger auf mögliche belastende Maßnahmen einstellen können, so dass Anlass, Zweck und Grenzen des Eingriffs bereits in der Ermächtigung bereichsspezfisch, präzise und normenklar festgelegt sein müssen. Das BVerfG sieht eine spezielle Gefährdung der bürgerlichen Freiheit, wenn Informationsbestände für eine Vielzahl von Zwecken genutzt oder miteinander verknüpft werden können. Deshalb hat der Gesetzgeber den *Erhebungszweck im Gesetz festzulegen* und mindestens zu bestimmen, welche staatliche Stelle zur Erfüllung welcher Aufgaben zu der geregelten Informationserhebung berechtigt sein soll. Die Informationserhebung und -verwendung ist dabei auf das zu dem Zweck Erforderliche zu begrenzen. Eine Sammlung der dem Grundrechtsschutz unterliegenden personenbezogenen Informationen auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken ist mit dem Grundgesetz unvereinbar.

c) Informationsanspruch des Betroffenen

In der IZA-Entscheidung vom 10.3.2008 hat das BVerfG zudem herausgearbeitet, dass das Recht auf informationelle Selbstbestimmung sich nicht in einem Abwehrrecht gegen staatliche Datenerhebung und -verarbeitung erschöpft. Vielmehr schützt es auch das Interesse des Einzelnen, von staatlichen informationsbezogenen Maßnahmen, die ihn in seinen Grundrechten betreffen, auch zu erfahren[11]. Im Hinblick auf Datensammlungen, bei denen keine Pflicht der Behörde zur aktiven Benachrichtigung der Betroffenen besteht, sieht das BVerfG ein *Informationsrecht des Betroffenen* als einen zentralen Baustein einer staatlichen Informationsordnung, die den grundrechtlichen Vorgaben genügt[12]. Demgemäß hat das BVerfG den Gesetzgeber für verpflichtet gehalten, ein derartiges Informationsrecht auch im Steuerverfahren zu schaffen.

9 BVerfG v. 27.6.1991 – 2 BvR 1493/89, BVerfGE 84, 239 (268 ff.); BVerfG v. 9.3.2004 – 2 BvL 17/02, BVerfGE 110, 94 (112 ff.).
10 BVerfG v. 13.6.2007 – 1 BvR 1550/03 u.a., BVerfGE 118, 168 (186 ff.).
11 BVerfG v. 10.3.2008 – 1 BvR 2388/03, BVerfGE 120, 351 (359 ff.) mit einem ergänzenden Hinweis auf das Gebot effektiven Rechtsschutzes nach Art. 19 Abs. 4 GG.
12 So ausdrücklich BVerfG v. 10.3.2008 – 1 BvR 2388/03, BVerfGE 120, 351 (364).

Besondere Anforderungen stellt das BVerfG schließlich an *heimliche Datenerhebungen*. Sie müssen die Ausnahme bleiben und stehen unter einem *strengen Erforderlichkeitsvorbehalt*[13]. Durch heimliche Ermittlungen wird vorheriger Rechtsschutz faktisch verwehrt und nachträglicher Rechtsschutz zumindest potentiell erschwert[14]. Das Recht auf informationelle Selbstbestimmung verlangt im Grundsatz, dass der Einzelne erkennen und erfahren kann, welche Behörde was, wann und durch welche Gelegenheit über ihn weiß. Ist eine heimliche Datenermittlung zu Besteuerungszwecken notwendig, muss der Betroffene zumindest nach Durchführung der Datenerhebung – wie etwa beim Kontenabruf nach § 93 Abs. 9 Satz 2 AO – zeitnah informiert werden.

d) Schutz juristischer Personen

Das Recht auf informationelle Selbstbestimmung schützt über die Anwendung des Art. 19 Abs. 3 GG auch juristische Personen[15]. Dies mag auf den ersten Blick überraschen, weil eine juristische Person ihrem Wesen nach keine Privatsphäre besitzt. Der Begriff der Privatsphäre verdeckt aber, dass eine juristische Person – ebenso wie eine natürliche Person – Daten (z.B. *Geschäfts- und Betriebsgeheimnisse*) besitzt, die dem staatlichen Zugriff entzogen sind[16]. Nach der Rechtsprechung des BVerfG wird die juristische Person durch das Recht auf informationelle Selbstbestimmung vor Gefährdungen geschützt, denen sie sich durch die informationelle Maßnahme im Hinblick auf ihre spezifische *freiheitliche, insbesondere wirtschaftliche Betätigung* ausgesetzt sieht[17]. Maßgeblich kommt es insoweit auf die Bedeutung der betroffenen Information für den grundrechtlich geschützten Tätigkeitskreis der juristischen Person an. Handels-, Betriebs-, Berufs- und Geschäftsgeheimnisse sind für die Verwirklichung ihrer *wirtschaftlichen Freiheitsgrundrechte* (insbesondere der

13 Neben der Entscheidung zum sog. Kontenabruf (Fn. 7) s. BVerfG v. 12.4.2005 – 2 BvR 1027/02, BVerfGE 113, 29 (46 ff.) – Beschlagnahme von Datenträgern; BVerfG v. 27.2.2008 – 1 BvR 370/01 u.a., BVerfGE 120, 274 (325 f.) – Online-Durchsuchung; BVerfG v. 11.3.2008 – 1 BvR 2074/05, BVerfGE 120, 378 (402 f.) – automatische Kennzeichenerfassung; BVerfG v. 2.3.2010 – 1 BvR 256/08 u.a., BVerfGE 125, 260 (336 f.) – Vorratsdatenspeicherung.
14 So auch BFH v. 18.1.2012 – II R 49/10, BStBl. II 2012, 168 Rz. 42.
15 Siehe BVerfG v. 17.7.1984 – 2 BvE 11 u. 15/83, BVerfGE 67, 100 (142).
16 *Drüen* (Fn. 2), StuW 2003, 205 (213).
17 BVerfG v. 13.6.2007 – 1 BvR 1550/03 u.a., BVerfGE 118, 168 (204).

Berufs- und Eigentümerfreiheit) von erheblicher Bedeutung, so dass sie vom Schutz der informationellen Selbstbestimmung auch bei juristischen Personen (zu denen auch Personengesellschaften zählen) erfasst werden[18].

2. Datenschutzrechtliche Funktion des Steuergeheimnisses (§ 30 AO)

Das Steuergeheimnis war bereits in der Reichsabgabenordnung vom 13.12.1919 verankert (§ 10 Abs. 1 RAO 1919). *Enno Becker* sah in ihm nicht nur das Interesse der Steuerpflichtigen, sondern gerade auch der Verwaltung verwirklicht, der ein Steuerpflichtiger seine Einkommens- und Vermögensverhältnisse nur im Vertrauen auf Diskretion anvertrauen würde[19]. An dieser *doppelten Schutzrichtung* des Steuergeheimnisses hat sich auch unter der AO 1977 nichts geändert[20]. Jedoch hat das BVerfG bereits in seiner Entscheidung zum Flick-Untersuchungsausschuss vom 17.7.1984 die datenschutzrechtliche Funktion des Steuergeheimnisses herausgearbeitet[21]. Wenn es das Steuergeheimnis zu diesem Zeitpunkt nicht bereits gegeben hätte, hätte es der Gesetzgeber zum Schutz des Rechts auf informationelle Selbstbestimmung erfinden müssen. Denn in dessen Lichte sind die umfangreichen steuerlichen Mitwirkungs- und Offenbarungspflichten nur erträglich, wenn der offenbarende Steuerbürger gegen eine unbefugte Verwendung und Weitergabe seiner Daten geschützt ist. § 30 AO ist damit zugleich eine *bereichsspezifische Datenschutznorm*[22]. Das Steuergeheimnis schützt den Steuerbürger vor einer Weitergabe seiner Daten, die die Finanzbehörde über ihn erlangt hat. Die Weitergabe der Daten ist lediglich aufgrund der in § 30 Abs. 4 AO geregelten Ausnahmetatbeständen möglich. Die Verletzung des Steuergeheimnisses durch die Finanzbehörde ist gem. § 355 StGB strafbewehrt. Hinzu kommen für den das Steuergeheimnis verletzenden Amtsträger disziplinarrechtliche Sanktionen[23].

18 *Seer*, Informationsaustausch innerhalb der EU über sog. Advance Pricing Agreements – zum Entwurf der EU-Kommission vom 18.3.2015 in FS Gosch, 2016, 387 (399).
19 *E. Becker*, Reichsabgabenordnung, 7. Aufl. 1930, § 10 RAO Rz. 2; s.a. *Hensel*, Steuerrecht, 3. Aufl. 1933, S. 115.
20 *Drüen* in Tipke/Kruse, § 30 AO Rz. 10 (Oktober 2018).
21 BVerfG v. 17.7.1984 – 2 BvE 11, 15/83, BVerfGE 67, 100 (142 ff.).
22 *Seer*, Datenschutz im Besteuerungsverfahren, in FS Meilicke, 2010, S. 687 (688).

II. Unionsrechtlicher Datenschutz

1. Entwicklungslinien in der Rechtsprechung des EuGH

a) Primärrechtlicher Schutzbereich

Primärrechtlich ist der Datenschutz sowohl in Art. 8 EUGrCh als auch in Art. 16 AEUV verankert. Beide Artikel sind nicht als ein Recht auf „informationelle Selbstbestimmung" formuliert, sondern werden eng mit dem *Persönlichkeitsrecht*, dem *Recht auf Privatheit* (Art. 7 EUGrCh) geführt[24]. Nach Art. 8 Abs. 1 EUGrCh hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

b) Datenschutzspezifische Schrankenbestimmung

Art. 8 Abs. 2 Satz 1 EUGrCh statuiert einen *besonderen Gesetzesvorbehalt* für die Datenverarbeitung. Einschränkungen müssen nach Art. 52 Abs. 1 EUGrCh das *Verhältnismäßigkeitsprinzip* wahren. In der jüngeren Zeit hat die Große Kammer des EuGH durch mehrere Grundsatzentscheidungen dem europäischen Datenschutzgrundrecht Konturen verliehen. Sie sind zwar nicht im steuerrechtlichen Kontext ergangen, wirken aber auch auf das Steuerrechtsverhältnis auf unionaler Ebene ein. In den Fällen Schecke GbR/Eifert[25] hat der EuGH untersucht, ob die Veröffentlichung von Informationen über die Empfänger von Agrarbeihilfen auf der Website von staatlichen Stellen gegen (primäres) EU-Recht verstößt, obwohl die Veröffentlichung ausdrücklich durch Sekundärrecht vorgesehen war, um dem Grundsatz der Transparenz und dem Konzept einer „offenen Regierung" Rechnung zu tragen[26]. Der EuGH versteht – ebenso wie das BVerfG – den Begriff der „personenbezogenen Daten" nicht eng, sondern weit als jede Information, die eine bestimmte oder bestimmbare Person

23 Außerdem besitzt der Verletzte nach Art. 34 GG i.V.m. § 839 BGB einen zivilrechtlichen Amtshaftungsanspruch auf Schadensersatz gegen den Staat, s. *Drüen* in Tipke/Kruse, § 30 AO Rz. 147 ff. (Oktober 2018).
24 Zum Gewährleistungsgehalt s. *Reinhardt*, Konturen des europäischen Datenschutzgrundrechts, AöR Bd. 142 (2017), 529 (531 f.).
25 EuGH v. 9.11.2010 – C-92/09, C-93/09, ECLI:EU:C:2010:662 – Schecke GbR/Eifert.
26 VO Nr. 1290/2005 v. 12.6.2005, ABl. Nr. L 209/1; VO Nr. 1437/2007 v. 26.11.2007, ABl. Nr. L 322/1; VO Nr. 259/2008 v. 18.3.2008, ABl. Nr. L 76/28.

betrifft[27]. Darunter fallen auch Daten, die sich – wie etwa die Summe der erhaltenen Argrarbeihilfen – auf berufliche oder unternehmerische Tätigkeiten beziehen[28]. Zwar stellt der EuGH eingangs klar, dass das Grundrecht auf Schutz personenbezogener Daten kein absolutes Recht ist. Wegen des geltenden Verhältnismäßigkeitsgrundsatzes dürfen Einschränkungen dieses Rechts aber nur vorgenommen werden, wenn sie notwendig sind und Interessen der Allgemeinheit verfolgen, die auch die EU anerkennt oder Schutz der Rechte und Freiheiten anderer dienen. Die *Rechtfertigungsprüfung* nimmt der EuGH in den folgenden *drei Stufen* vor[29].

1. Gibt es ein Gesetz, das die Beeinträchtigung des Grundrechts vorsieht/erlaubt?
2. Besteht ein allgemeines Interesse, welches das EU-Recht anerkennt, und kann dieses Interesse die Beeinträchtigung des Grundrechts rechtfertigen?
3. Ist die Beeinträchtigung des Grundrechts verhältnismäßig im Hinblick auf den damit verfolgten legitimen Zweck?

Im konkreten Fall nahm der EuGH eine *unverhältnismäßige öffentliche Transparenz* an[30]. Bei seiner Prüfung hat der EuGH das Transparenzgebot einerseits und den dadurch bewirkten Eingriff in das Grundrecht auf Schutz personenbezogener Daten des Betroffenen andererseits gegenübergestellt. Dazu führte das Gericht aus, dass Ausnahmen und Beschränkungen in Bezug auf den Schutz personenbezogener Daten nur insoweit zulässig sind, als sie sich auf das *„absolut Notwendige"* beschränken[31]. Der EuGH bemängelte die fehlende Begrenzung des Eingriffs in den Schutzbereich personenbezogener Daten. So hätte etwa die Veröffentlichung von Daten unter namentlicher Nennung der Empfänger nach Maßgabe der Zeiträume, während derer diese Beihilfen erhalten haben, der Häufigkeit oder auch nach Art und Umfang dieser Beihilfen eingegrenzt werden können[32].

In zwei weiteren Entscheidungen hat die Große Kammer des EuGH die Möglichkeit wahrgenommen, Grenzen für die Speicherung oder Ver-

27 EuGH (Fn. 25) Rz. 52.
28 EuGH (Fn. 25) Rz. 59; zuvor bereits EuGH v. 20.5.2003 – C-465/00 u.a., ECLI:EU:C:2003:294 Rz. 73 f. (Österreichischer Rundfunk u.a.).
29 EuGH (Fn. 25) Rz. 66 ff.
30 EuGH (Fn. 25) Rz. 80 ff.
31 EuGH (Fn. 25) Rz. 77.
32 EuGH (Fn. 25) Rz. 81, 83.

arbeitung personenbezogener Daten gegenüber der durch EU-Richtlinien sekundärrechtlich vereinbarten *Vorratsdatenspeicherung*[33] zu setzen[34]. Zwar liegt die Bekämpfung der schweren Kriminalität und des Terrorismus unzweifelhaft im allgemeinen öffentlichen Interesse. Auch dieses öffentliche Interesse muss aber unter Berücksichtigung der Schwere der Straftaten mit dem Grundrecht auf Schutz der Privatsphäre und den Rechten aus Art. 7, 8 EUGrCh, gemessen am Grundsatz der Verhältnismäßigkeit, abgewogen werden. In der sog. Vorratsdatenspeicherung von Mobilfunkdaten erkennt der EuGH – in Übereinstimmung mit dem BVerfG – einen besonders schwerwiegenden Eingriff in das Datenschutzgrundrecht. Aus der Gesamtheit der gespeicherten Daten ließen sich sehr genaue Schlüsse auf das Privatleben der jeweiligen Personen, etwa auf Gewohnheiten des täglichen Lebens, ständige oder vorübergehende Aufenthaltsorte,ausgeübte Tätigkeiten, soziale Beziehungen und das soziale Umfeld, in dem sie verkehren, ziehen. Die staatlichen Behörden könnten damit ein *detailliertes Persönlichkeitsprofil* des jeweiligen Nutzers ziehen. Zudem sei der Umstand, dass die Vorratsspeicherung der Daten vorgenommen werde, ohne den Nutzer der elektronischen Kommunikationsdienste darüber zu informieren, geeignet, bei den Betroffenen ein Gefühl zu erzeugen, dass ihr Privatleben Gegenstand einer ständigen Überwachung sei[35].

Das Gericht vermisste klare und präzise Regeln für das Ausmaß des Eingriffs in die Grundrechte der Art. 7, 8 EUGrCh. Es beanstandete, dass die Richtlinie keine Differenzierungen, Beschränkungen oder Ausnahmen vorsehe, die im Lichte der Zielsetzung der Richtlinie (der Bekämpfung schwerer Kriminalität) geboten wären[36]. Erneut fordert der EuGH, den Eingriff in das Datenschutzrecht auf das *„absolut Notwendige"* zu beschränken[37]. Das Gericht kritisierte zudem, dass der Zugang zu den gespeicherten Daten nicht von einer vorherigen Überprüfung durch ein Gericht abhängig sei oder von einer unabhängigen Behörde durchgeführt werde, die zu überprüfen habe, ob der Zugriff auf die Daten und die an-

33 RL 2006/24/EG über Vorratsspeicherung von Daten v. 15.3.2006, ABl. EG v. 13.4.2006, L 105/54.
34 EuGH v. 8.4.2014 – C-293/12 u.a., ECLI:EU:C:2014: 238 – Digital Rights Ireland Ltd, Kärntner Landesregierung u.a.; EuGH v. 21.12.2016 – C-203/15, ECLI:EU:2016:970 – Tele2 Sverige AB: Tom Watson u.a.
35 EuGH v. 8.4.2014 (Fn. 34) Rz. 26 f., 37; EuGH v. 21.12.2016 (Fn. 34) Rz. 98 ff.
36 EuGH v. 8.4.2014 (Fn. 34) Rz. 59–63; EuGH v. 21.12.2016 (Fn. 34) Rz. 109–111, 119.
37 EuGH v. 8.4.2014 (Fn. 34) Rz. 54; EuGH v. 21.12.2016 (Fn. 34) Rz. 109.

schließende Verwendung für den damit verfolgten Zweck unbedingt erforderlich ist[38].

c) Informationsanspruch des Betroffenen

In der Entscheidung „Tele2 Sverige AB" postulierte die Große Kammer des EuGH schließlich eine *Informationspflicht* der nationalen Behörden gegenüber den Betroffenen, sobald eine Beeinträchtigung der behördlichen Ermittlungen ausgeschlossen ist[39]. Durch geeignete technische und organisatorische Maßnahmen müssten die Mitgliedstaaten ein hohes Schutz- und Sicherheitsniveau gewährleisten, um der Gefahr von Datenmissbräuchen zu begegnen. Die Daten seien nach Ablauf ihrer Speicherungsfrist unwiderruflich zu löschen.

d) Schutz juristischer Personen

In persönlicher Hinsicht unterscheidet der EuGH allerdings zwischen natürlichen und juristischen Personen. Juristische Personen können sich nach seinem Verständnis der EUGrCh nur insoweit auf den persönlichen Datenschutz berufen, als dass durch den Namen der juristischen Person eine oder mehrere natürliche Personen identifiziert werden können[40]. Selbst aber wenn die Datenerhebung und -verwendung bei einer juristischen Person Rückschlüsse auf natürliche Personen zulässt, mildert der EuGH das Datenschutzniveau für juristische Personen ab. Das Gericht argumentiert, dass juristische Personen bereits einer strengeren Verpflichtung im Zusammenhang mit der Veröffentlichung der sie betreffenden Daten unterlägen und die Verletzung des Schutzes personenbezogener Daten anders als bei natürlichen Personen zu gewichten sei[41].

Die *Ausklammerung juristischer Personen aus dem Datenschutzbereich* entspricht Art. 16 Abs. 2 AEUV, der eine spezielle datenschutzrechtliche europäische Gesetzgebung nur für natürliche Personen vorschreibt. Dementsprechend bezieht sich die DSGVO vom 27.4.2016 nur auf die Daten natürlicher Personen. Das im personellen Anwendungsbereich verengte europarechtliche Verständnis des Datenschutzes wird in der deutschen Literatur kritisiert. So macht *Kingreen* darauf aufmerksam, dass Art. 8

38 EuGH v. 8.4.2014 (Fn. 34) Rz. 62; EuGH v. 21.12.2016 (Fn. 34) Rz. 120.
39 EuGH v. 21.12.2016 (Fn. 34) Rz. 121 f.
40 So eingehend EuGH v. 9.11.2010 (Fn. 25) Rz. 53; s.a. EuGH v. 17.12.2015 – C-419/14, ECLI:EU:C:2015:832 Rz. 79 – WebMindLicenses.
41 EuGH v. 9.11.2010 (Fn. 25) Rz. 87.

Abs. 1 EUGrCh die „Person" und nicht den „Menschen" schütze. Zudem habe der Schutz von Daten nicht nur für den engen Bereich der Intim- und Privatsphäre, sondern auch für Unternehmen eine Bedeutung. Vor diesem Hintergrund überzeuge die vom EuGH gemachte Unterscheidung nicht und führe zudem bei einer Unterscheidung zwischen Personen- und Kapitalgesellschaften zu willkürlichen Ergebnissen[42].

Nun mag der EUGrCh eine dem Art. 19 Abs. 3 GG entsprechende Vorschrift fehlen und diese aus der Tradition der Mitgliedstaaten nicht als ungeschriebener Verfassungsgrundsatz ableitbar sein[43]. Dies schließt aber nicht aus, dass die Kapital- und Personengesellschaften zuzuordnenden unternehmensbezogenen Daten nicht auf der Basis anderer Normen primärrechtlichen Schutz genießen. Art. 16 EUGrCh garantiert die unternehmerische Freiheit. Art. 17 EUGrCh schützt das rechtmäßig erworbene Eigentum einschließlich des geistigen Eigentums. Auf beide Grundrechte können sich auch juristische Personen in vollem Umfang berufen[44]. Diesem *unternehmensrechtlichen Grundrechtsschutz* unterfallen insbesondere selbst geschaffene immaterielle Wirtschaftsgüter. Zwar hat die Sozialpflichtigkeit des Eigentums auch auf der Ebene des Unionsrechts in Art. 17 Abs. 1 Satz 3 EUGrCh ihren Niederschlag gefunden. Unbeschadet dessen unterliegen Eingriffe in das unternehmerische Eigentum nach Art. 52 Abs. 1 EUGrCh dem Gemeinwohlvorbehalt und dem Verhältnismäßigkeitsprinzip. Weitergehende enteignende Eingriffe unterliegen nach Art. 17 Abs. 1 Satz 2 EUGrCh dem Gesetzesvorbehalt und einer Entschädigungspflicht. In der Zusammenschau von Art. 16 und Art. 17 EUGrCh erhält der *Schutz von Handels-, Betriebs-, Berufs- und Geschäftsgeheimnissen* außerhalb des eigentlichen Datenschutzrechts eine primärrechtliche Absicherung.

e) Datenschutz bei Datentransfer in Drittstaaten

Schließlich hat die Große Kammer des EuGH zwei richtungsweisende Entscheidungen hinsichtlich des Datenschutzes in Drittstaaten-Sachverhalten getroffen. In der Rechtssache „Google Spain" hat er ein in den

42 *Kingreen* in Calliess/Ruffert (Hrsg.), EUV/AEUV, Kommentar, 6. Aufl. 2016, Art. 8 EUGrCh Rz. 11; krit. auch *Reinhardt* (Fn. 24), AöR 142 (2017), 528 (539 f.); *Knecht* in Schwarze (Hrsg.), EU-Kommentar, 4. Aufl. 2019, Art. 8 EUGrCh Rz. 3.
43 *Knecht* in Schwarze (Fn. 42), Art. 8 EUGrCh Rz. 3.
44 *Ruffert* u. *Calliess* in Calliess/Ruffert (Fn. 42), Art. 16 EUGrCh Rz. 3; Art. 17 EUGrCh Rz. 4.

USA ansässiges Unternehmen den europäischen Datenschutzstandards unterworfen, wenn dieses innerhalb der EU eine Niederlassung unterhält[45]. Materiell-rechtlich sieht der EuGH auch in der Tätigkeit von Internet-Suchmaschinen einen Akt der Datenverarbeitung, der datenschutzrechtlich relevant ist, und billigt dem Betroffenen einen Löschungsanspruch hinsichtlich seiner personenbezogenen Daten (ein „*Recht auf Vergessenwerden*") zu[46]. Für unser Thema von größerer Relevanz ist aber das nachfolgende EuGH-Urteil zur Kommissionsentscheidung[47] über die sog. „Safe harbour"-Regelung des US-Handelsministeriums[48]. Die Kommission hatte festgestellt, dass die USA als Drittland auf der Basis bestimmter vom US-Handelsministerium zur Verfügung gestellter Dokumente ein angemessenes Datenschutzniveau für von der EU in die USA transferierte Daten gewährleiste. Auf dieser Basis sind personenbezogene Daten von EU-Bürgern (so auch von Herrn *Maximilian Schrems*) auf die in den USA befindlichen Server großer amerikanischer Internetunternehmen wie z.B. der Facebook Inc. gelangt. Gegen die ungeprüfte Weitergabe seiner persönlichen Daten durch die Facebook Ireland Ltd. hatte sich Herr *Schrems* beim irischen Datenschutzbeauftragten beschwert und ein gerichtliches Verfahren initiiert. Auf Vorlage des irischen High Courts hat der EuGH nicht nur den Angemessenheitsbeschluss der EU-Kommission als von den nationalen Kontrollstellen (allerdings ohne Verwerfungskompetenz) für überprüfbar erklärt. Vielmehr hat er darüber hinaus die EU-Kommission ihrerseits zur inhaltlichen Prüfung verpflichtet, ob der jeweilige Drittstaat ein im Lichte des Datenschutzgrundrechts hinreichendes („angemessenes") Schutzniveau garantiert[49]. Dabei hat der EuGH den Maßstab des „angemessenen" Schutzniveaus leider nicht deutlich herausgearbeitet[50]. Jedoch deuten die Ausführungen des EuGH, der auf die Anforderungen seines Urteils in der Rechtssache *Digital*

45 EuGH v. 13.5.2014 – C-131/12, ECLI:EU:C:2014:317 Rz. 55 – Google Spain S.L.
46 EuGH v. 13.5.2014 (Fn. 45) Rz. 94.
47 Entscheidung der Kommission v. 26.7.2000 (2000/520/EG) gemäß der Richtlinie 95/46/EG über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „häufig gestellten Fragen (FAQ)" gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. EG v. 25.8.2000, L 215/7.
48 EuGH v. 6.10.2015 – C-362/14, ECLI:EU:C:2015:650 – Schrems.
49 EuGH v. 6.10.2015 (Fn. 48) Rz. 73.
50 Dazu etwa krit. *Kühling/Heberlein*, EuGH „reloaded": „unsafe harbor" USA vs. „Datenfestung" EU, NVwZ 2016, 7 (9).

Rights Ireland verweist[51], auf ein eher strenges Datenschutzverständnis hin. Dies gilt auch vor dem Hintergrund, dass das Schutzniveau ansonsten durch Serververlagerungen in Drittstaaten leicht umgangen werden könnte[52]. Der EuGH hat demnächst die Gelegenheit, seine Position weiter zu verdeutlichen. Nachdem sich *Maximilian Schrems* auch gegen den nachfolgenden Beschluss der EU-Kommission zum sog. „EU-US-Privacy Shield" gewandt hat, hat der irische High Court am 9.5.2018 beim EuGH ein Vorabentscheidungsersuchen mit insgesamt 11 detaillierten Fragen gestellt[53].

2. Sekundärrechtliche Harmonisierung des Datenschutzes durch die EU-Datenschutzgrundverordnung vom 27.4.2016 (EU-DSGVO)

Auf sekundärrechtlicher Ebene hat die am 25.5.2018 in Kraft getretene Europäische Datenschutzgrundverordnung vom 27.4.2016[54] die bis dahin geltende Datenschutzrichtlinie 95/46[55] abgelöst. Sie beruht auf der Ermächtigung des Art. 16 Abs. 2 Satz 1 AEUV und soll für ein „gleichmäßiges und hohes Datenschutzniveau" in sämtlichen Mitgliedstaaten sorgen[56]. Im Unterschied zur Richtlinie bedarf sie als Verordnung keiner besonderen Umsetzung in den einzelnen Mitgliedstaaten. Nach ihrer Konzeption als „Grundverordnung" hinterlässt sie aber nicht wenige „Öffnungsklauseln" für die nationale Rechtssetzung, so dass von einer „hinkenden Harmonisierung" oder einem „atypischen Hybrid aus Verordnung und Richtlinie" gesprochen wird[57]. Als „lex imperfecta" bedarf

51 EuGH v. 6.10.2015 (Fn. 48) Rz. 91 f.
52 So EuGH v. 6.10.2015 (Fn. 48) Rz. 73.
53 High Court Ireland v. 9.5.2018 (Rs. C-311/18) – Data Protection Commissioner vs. Facebook Ireland, Maximilian Schrems, ABl. EU 2018 Nr. C 249/15.
54 ABl. EU Nr. L 119/1 v. 6.5.2016; berichtigt in ABl. Nr. L 314/72 v. 22.11.2016 u. ABl. Nr. L 127/2 v. 23.5.2018.
55 RL 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr v. 24.10.1995, ABl. EG Nr. L 281/31 v. 23.11.1995.
56 Erwägungsgründe 10 ff. zur DSGVO, s. ABl. EU Nr. L119/2 f. v. 6.5.2016.
57 *Kühling/Martini*, Die Datenschutz-Grundverordnung: Revolution oder Evolution im europäischen und deutschen Datenschutzrecht?, EuZW 2016, 448 (449); *Buchholtz*, Grundrechte und Datenschutz im Dialog zwischen Karlsruhe und Luxemburg, DÖV 2017, 837 (838); *Drüen* in Tipke/Kruse, § 2a AO Rz. 1, 5 (August 2018).

die DSGVO ungeachtet ihrer unmittelbaren Geltung ergänzender mitgliedstaatlicher Rechtssetzung[58].

Entsprechend ihrer Ermächtigung in Art. 16 Abs. 2 AEUV beschränkt sich der persönliche Schutzbereich der DSGVO auf *natürliche Personen*. In sachlicher Hinsicht findet die DSGVO nach Art. 2 Abs. 2 Buchst. a keine Anwendung auf Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen. Soweit es um die *Verwaltung nationaler Steuern* (z.B. bei der Einkommen-, Erbschaft- und Schenkungsteuer) geht, sind die Vorschriften der DSGVO daher jedenfalls nicht unmittelbar anwendbar[59]. Etwas anderes gilt für den Bereich der durch *EU-Richtlinien harmonisierten besonderen Verbrauchsteuern und der Umsatzsteuer*. Jedenfalls seit der Entscheidung in der Rechtssache *Äkerberg* Fransson versteht der EuGH den Begriff der „Durchführung des Rechts der Union" i.S.d. Art. 51 EUGrCh weit und wendet die EUGrCh auf den Vollzug des Umsatzsteuerrechts einschließlich damit zusammenhängender strafrechtlicher Sanktionen an[60]. Dasselbe gilt für den Datenaustausch auf der Basis der EU-Amtshilferichtlinie 2011/16/EU vom 15.2.2011[61]. Überträgt man diese Rechtsprechung folgerichtig auf die Anwendungsbereichsbestimmung des Art. 2 Abs. 2 Bucht. a DSGVO, kann die DSGVO damit punktuell auch auf nicht harmonisierte direkte Steuern unmittelbar anwendbar sein[62].

Die DSGVO verpflichtet als „Verantwortliche" (s. Art. 4 Nr. 7 DSGVO) sowohl Privatrechtssubjekte als auch staatliche Behörden. Art. 5 DSGVO nennt als *Grundsätze der Datenverarbeitung* die Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminiminierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit. Art. 6 DSGVO statuiert dazu ein *präventives Verarbeitungsverbot mit Erlaubnisvorbehalt*[63]. Für das Steuerverfahren bedeutsam ist der Erlaubnistatbestand des Art. 6 Abs. 1 Buchst. e DSGVO. Danach ist die Verarbeitung personenbezogener Daten gestattet, wenn sie zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen worden ist. Um personenbezogene Daten steuerlich zu verarbeiten, bedürfen die Mitgliedstaaten einer speziellen gesetzlichen Grundlage, wozu Art. 6 Abs. 2–4 DSGVO gewisse Vorgaben macht. Dabei stellt Art. 9 DSGVO besondere Anforderungen an die Verarbeitung *sensibler personenbezogener Daten* (z.B. Herkunft, religiöse oder politische Weltanschauung, genetische oder biometrische Daten, sexuelle Orientierung, Gesundheitsdaten). Insoweit bedarf es grundsätzlich der Einwilligung des Betroffenen (Art. 9 Abs. 2 Buchst. a DSGVO). Unabhängig davon können die Mitgliedstaaten die Verarbeitung sensibler Daten gesetzlich vorsehen, soweit dies aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist, im angemessenen Verhältnis zum verfolgten Ziel steht, den Wesensgehalt des Datenschutzgrundrechts wahrt und die Regelung spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen des Betroffenen vorsieht (Art. 9 Abs. 2 Buchst. g DSGVO).

Art. 13, 14 DSGVO enthalten zudem *Informationspflichten* gegenüber betroffenen Personen, die ihrerseits nach Art. 15 DSGVO jeweils ein *Auskunftsrecht* besitzen. Gegenstand der Informationspflicht sind insbesondere Angaben über die Kategorie der verarbeiteten Daten und die Verarbeitungszwecke, über Empfänger bzw. Kategorien von Empfängern, an die Daten weitergeleitet werden, über die Dauer bzw. Kriterien der Speicherung und die Herkunft der Daten. Nach Art. 13 Abs. 1 DSGVO hat der Verantwortliche (d.h. hier die Finanzbehörde) den Betroffenen u.a. über den Zweck der Datenerhebung, die Rechtsgrundlage für die Datenverarbeitung, die Kontaktdaten des Datenschutzbeauftragten und eine ggf. bestehende Absicht der Datenübermittlung in ein Drittland zu informieren[64]. Art. 13 Abs. 2 DSGVO verlangt auch eine Information über die Dauer der Speicherung und eine Belehrung über die Rechte des Betroffenen. Dasselbe gilt nach Art. 13 Abs. 3 DSGVO für den Fall, dass der Verantwortliche die Daten für andere Zwecke weiterverarbeiten will. In der Gesamtschau ist die DSGVO von den Gedanken der *Transparenz* und *Ver-*

58 *Kibler/Sandhu*, Vorwirkung von EU-Verordnungen am Beispiel der Datenschutz-Grundverordnung, NVwZ 2018, 528 (531).

59 *Krumm*, Grundfragen des steuerlichen Datenverarbeitungsrechts, DB 2017, 2182 (2186); *Seer* in Tipke/Lang, Steuerrecht, 23. Aufl. 2018, § 21 Rz. 18; *Drüen* in Tipke/Kruse, § 2a AO Rz. 6 (August 2018).

60 EuGH v. 26.2.2013 – C-617/10, ECLI:EU:C:2013:105 Rz. 25–27 – Äkerberg Fransson); EuGH v. 17.12.2015 – C-419/14, ECLI:EU:C:2015:832 Rz. 67 – WebMindLicenses.

61 Siehe EuGH (Große Kammer) v. 16.5.2017 – C-682/15, ECLI:EU:C:2017:373 Rz. 33–41 – Berlioz Investment Funds SA.

62 So auch *Krumm* (Fn. 59), DB 2017, 2182 (2186) – Beispiel 3.

63 *P. Reimer* in Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 6 Rz. 1.

64 Siehe *Myßen/Kraus*, Steuerliches Datenschutzrecht: Verfahrensrechtsanpassung an die Datenschutz-Grundverordnung, DB 2017, 1860 (1868).

hältnismäßigkeit geprägt (s.a. die Anforderungen des Art. 12 DSGVO). Es gilt der *Grundsatz des offenen Visiers*. Der europäische Verordnungsgeber will mit den Informationsrechten gewährleisten, dass die betroffene Person bereits zum Zeitpunkt der Datenerhebung über deren Zweck und Ziel sowie über den weiteren Verarbeitungsvorgang unterrichtet wird[65].

Allerdings sieht Art. 23 Abs. 1 Buchst. e DSGVO für die Mitgliedstaaten die Möglichkeit vor, die vorgenannten Datenschutzrechte der Betroffenen durch Gesetzgebungsmaßnahmen zur Sicherstellung wichtiger *öffentlicher Interessen zu beschränken*. Als Beispiele nennt die Vorschrift ausdrücklich die wirtschaftlichen oder finanziellen Interessen eines Mitgliedstaates im Währungs-, *Haushalts- und Steuerbereich*. Die gesetzlichen Beschränkungen müssen dabei aber den Wesensgehalt der Grundrechte und Grundfreiheiten (insbesondere des Datenschutzgrundrechts) achten, eine notwendige und verhältnismäßige Maßnahme darstellen und dazu bestimmte, in Art. 23 Abs. 2 DSGVO detailliert aufgezählte Mindestanforderungen erfüllen.

3. Nationales Regelungsregime der §§ 2a, 29b-c, 32a-j AO an der Schnittstelle zum Unionsrecht

Das unionsrechtliche Datenverarbeitungsverbot mit Erlaubnisvorbehalt zwang den nationalen Gesetzgeber zum Handeln im Steuerrecht. Dies tat er allerdings nicht in einem speziellen steuerdatenschutzrechtlichen Gesetzgebungsverfahren, sondern ohne Beteiligung des Finanzausschusses des Deutschen Bundestages und weitgehend unter Ausschluss der steuerlichen Fachöffentlichkeit in Art. 17 des Gesetzes zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17.7.2017[66]. Das Regelungsregime erweist sich insgesamt als sehr unübersichtlich, was aber nicht nur am deutschen Gesetzgeber liegt. Der EuGH postuliert für EU-Verordnungen ein *Wiederholungsverbot*, um eine Verschleierung seines Auslegungsmonopols zu verhindern[67]. Daran anknüpfend lässt es der 8. Erwägungsgrund zu der Verordnung nur zu, dass die Mitgliedstaaten zum besseren Verständnis und zur Kohärenz ihrer nationalen Re-

65 Siehe Erwägungsgründe 60 u. 61 zur DSGVO, ABl. EU Nr. L119/12 v. 4.5.2016.

66 BGBl. I 2017, 2541. Zu den verfassungsrechtlichen Bedenken gegenüber dem Gesetzgebungsverfahren s. *Drüen* in Tipke/Kruse, § 29b AO Rz. 4 m.w.N. (August 2018).

67 EuGH v. 10.10.1973 – C-34/73, ECLI:EU:C:1973:101 Rz. 9–11.

gelungen „Teile der Verordnung" in das nationale Recht übernehmen[68]. Resultat ist, dass der Rechtsanwender mindestens zwei Quellen nebeneinanderlegen muss, um die Rechtslage zu eruieren: DSGVO und AO[69].

Vor diesem Hintergrund war eine klare Anwendungsregel wünschenswert. Das Gegenteil aber findet sich in § 2a Abs. 3 AO. Danach soll die AO insoweit keine Anwendung finden, als die DSGVO gilt. Dies ist zumindest missverständlich, weil die AO die Öffnungsklauseln der DSGVO als „spezifische mitgliedstaatliche Regelung" füllt, also nicht etwas anderes, sondern ein Element des datenschutzrechtlichen Regelungsbereichs ist[70]. Erfreulicherweise erweitert sodann § 2a Abs. 5 Nr. 2 AO den Anwendungsbereich der DSGVO auf nationaler Ebene u.a. auf Körperschaften, rechtsfähige und nicht rechtsfähige Personenvereinigungen und Vermögensmassen. Die Vorschrift lässt aber insgesamt im Unklaren, ob nun ein *gespaltenes steuerliches Datenschutzrecht* existiert, bei dem die DSGVO zusammen mit ihren AO-Ergänzungen nur auf *durch das EU-Recht determinierte Steuern* (z.B. besondere Verbrauchsteuern, Umsatzsteuer) oder auf *alle* (also auch auf die rein national determinierten) *Steuern* Anwendung findet. Der historische Gesetzgeber ging und die Finanzverwaltung geht offenbar – wie selbstverständlich – von einer umfassenden, steuerartenübergreifenden Anwendung der DSGVO aus[71]. Das ist der Sache nach zwar sinnvoll; im Gesetz fehlt dazu aber der Anhalt[72]. Die Grundfrage nach dem Regelungsregime ist nicht nur akademisch, sondern für die Ausgestaltung des Rechtsschutzes praktisch relevant. Soweit die unmittelbare Anwendung der EU-Verordnung reicht, bildet die

68 ABl. EU Nr. L119/2 v. 4.5.2016.

69 Soweit die AO auf das Bundesdatenschutzgesetz (BDSG) verweist, sind es sogar drei Rechtsquellen.

70 *Krumm* (Fn. 59), DB 2017, 2182 (2187).

71 So nennt der Bericht des Ausschusses für Arbeit und Soziales, BT-Drucks. 18/12611, 77 f., 90, Beispiele für die Einschränkung der DSGVO aus dem Bereich der Einkommensteuer (so zum Werbungskostenabzug, zu außergewöhnlichen Belastungen u. Sonderausgaben) und muss daher von der Anwendung der DSGVO auf die Einkommensteuer ausgegangen sein. Ebenso verfährt das BMF-Schreiben v. 12.1.2018 – IV A 3 - S 0030/16/10004-07, BStBl. I 2018, 185 (186, 188) Rz. 2 f., 22; für den Ausschluss nach Art. 2 Abs. 2 Buchst. a DSGVO nennt *Wargowske* in Gosch, AO/FGO, § 2a AO Rz. 20 (Juni 2018) nur die den Mitgliedstaaten selbst überlassene Tätigkeit zum Schutz der nationalen Sicherheit.

72 Krit. *Krumm* (Fn. 59), DB 2017, 2182 (2186); *Seer* in Tipke/Lang, Steuerrecht, 23. Aufl. 2018, § 21 Rz. 18; *Drüen* in Tipke/Kruse, § 2a AO Rz. 6 (August 2018).

EUGrCh und nicht das Grundgesetz den Maßstab für den Grundrechtsschutz. Insoweit ist das Auslegungsmonopol des EuGH zu achten. Soweit die Regelungskompetenz unverändert bei den Mitgliedstaaten liegt, bleiben die nationalen Grundrechte anwendbar, die dem Auslegungsmonopol des BVerfG unterfallen[73].

Im Hinblick auf die DSGVO enthält das im letzten Jahr in die AO eingeführte Regelungsregime vor allem *Beschränkungen*. § 29b Abs. 1 AO lässt die Verarbeitung personenbezogener Daten durch eine Finanzbehörde zu, wenn sie zur Erfüllung der ihr obliegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die ihr übertragen worden ist, erforderlich ist. § 29b Abs. 2 AO erhöht die Anforderung an die Verarbeitung sensibler Daten i.S.d. Art. 9 Abs. 2 DSGVO. § 29c AO unterscheidet streng zwischen der *Verarbeitung* und der *Weiterverarbeitung* personenbezogener Daten für Zwecke, die über die ursprüngliche Datenerhebung bzw. -erfassung hinausgehen. § 29c Abs. 1 AO führt insgesamt sechs Fallgruppen auf, in denen eine Weiterverarbeitung zulässig ist. Darauf wird bei der Prüfung der datenschutzrechtlichen Grenzen des Datenaustausches noch zurückzukommen sein.

§§ 32a–32c AO statuieren Einschränkungen der von Amts wegen von den Finanzbehörden zu erfüllenden *Informationspflicht* der Art. 13, 14 DSGVO sowie des damit korrelierenden *Auskunftsrechts* der betroffenen Person aus Art. 15 DSGVO. Einschränkungsgründe sind das Interesse des Staates an der ordnungsgemäßen Erfüllung der in der Zuständigkeit der Finanzbehörden und anderer öffentlicher Stellen liegenden Aufgaben i.S.d. Art. 23 Abs. 1 Buchst. d–h DSGVO sowie der Schutz überwiegender berechtigter Interessen eines Dritten (Art. 23 Abs. 1 Buchst. i DSGVO), also das Steuergeheimnis Dritter nach § 30 AO. § 32a Abs. 2 Nr. 1 AO hält die ordnungsgemäße Erfüllung der öffentlichen Aufgaben der Finanzbehörde bei bestimmten Regelungsbeispielen für gefährdet. Dazu nennt die Vorschrift Fälle, in denen die Erteilung der Information den Betroffenen oder Dritte in die Lage versetzen könnte, steuerlich bedeutsame Sachverhalte zu verschleiern oder steuerlich bedeutsame Spuren zu verwischen oder Art und Umfang der Erfüllung steuerlicher Mitwirkungspflichten auf den Kenntnisstand der Finanzbehörden einzustellen (Nr. 1). Nr. 2 ergänzt dies um Fälle, in denen die Informationserteilung Rückschlüsse auf die Ausgestaltung automationsgestützter Risikomanagementsysteme oder auf geplante Kontroll- oder Prüfungsmaßnahmen zulassen würde. Gemeinsame zusätzliche Voraussetzung für die Geheimhaltung ist, dass die Informationserteilung die Aufdeckung steuerlich bedeutsamer Sachverhalte wesentlich erschweren würde. Der Informationsausschluss setzt eine bei einer Ex-ante-Betrachtung bestehende *konkrete Gefährdungslage* voraus[74]. Es ist daher nicht (mehr) zulässig, bloß abstrakt auf die Möglichkeit einer Gefährdung hinzuweisen[75]. Daher bedarf es auch einer besonderen konkreten Begründung der Gefährdungslage, wenn die Finanzbehörden Informationsansprüche im Hinblick auf die *Kritierien sog. Risikomanagementsysteme* (Regelungsbeispiel des § 32a Abs. 2 Nr. 2 AO) abweisen wollen[76].

73 Zur Konkurrenz zwischen EU-Recht und GG s. BVerfG v. 2.3.2010 – 1 BvR 256/08 u.a., BVerfGE 125, 260 (306 f.) – Vorratsdatenspeicherung; BVerfG v. 24.4.2013 – 1 BvR 1215/07, BVerfGE 133, 277 (315) – Antiterrordatei; BVerfG v. 21.3.2018 – 1 BvF 1/13, NJW 2018, 2109 Rz. 20 m.w.N. – Transparenz im Lebensmittelrecht.

74 Eingehend *Drüen* in Tipke/Kruse, AO/FGO, § 32a AO Rz. 20 m.w.N. (Oktober 2018).

75 So aber noch FG Köln v. 15.2.2018 – 2 K 465/17, EFG 2018, 1050 m. Anm. *Hennigfeld*, was aber bereits im bisherigen Recht unzutreffend war.

76 Bereits krit. zur Intransparenz *Seer*, Modernisierung des Besteuerungsverfahrens – Gedanken zum Reformentwurf zur Modernisierung des Besteuerungsverfahrens, StuW 2015, 315 (324 f.).

III. Inländischer Datenaustausch im Lichte des Datenschutzrechts

1. Datensammlung durch Inanspruchnahme der Steuerpflichtigen

In eigenen Angelegenheiten werden Steuerpflichtige mannigfaltig zur Mitwirkung nach den §§ 90 ff. AO, also auch zur Offenbarung personenbezogener Daten, herangezogen. Im Zentrum stehen dabei die Steuererklärungspflichten der §§ 149, 150 AO, wobei personenbezogene (auch sensible) Daten vor allem im Bereich der direkten Einkommensbesteuerung zu übermitteln sind. Auch wenn man die DSGVO auf einen rein nationalen Einkommensteuerfall nicht anwendet (s. oben II.3.), ergeben sich die datenschutzrechtlichen Vorgaben aber gleichwohl aus dem vom BVerfG bereichsspezifisch entfalteten *Normenbestimmtheitsgebot* und *Übermaßverbot*. Am Beispiel der Einkommensteuer lässt sich Folgendes festhalten: Gemäß § 149 Abs. 1 AO i.V.m. § 25 Abs. 3 EStG hat die steuerpflichtige Person für den jeweiligen Veranlagungszeitraum eine eigenhändig unterschriebene Einkommensteuererklärung abzugeben. Nach § 150 Abs. 1 AO hat das auf einem amtlich vorgeschriebenen Vor-

druck zu geschehen oder – wie bei Vorliegen von Gewinneinkünften mittlerweile grundsätzlich obligatorisch – nach amtlich vorgeschriebenem Datensatz durch Datenfernübertragung. Die Parlamentsgesetze schweigen jedoch über den *Inhalt des amtlich vorgeschriebenen Vordrucks oder Datensatzes*. Stattdessen ermächtigt § 51 Abs. 4 Nr. 1 Buchst. b EStG das BMF, im Einvernehmen mit den obersten Finanzbehörden der Länder die Vordrucke für die Einkommensteuererklärungen zu bestimmen.

Diese Ausgestaltungsdelegation ist datenschutzrechtlich zweifelhaft. Jedenfalls kann diese Regelung am Maßstab des *datenschutzrechtlichen Gesetzesvorbehalts* nicht in ein freies Entscheidungsermessen der Finanzbehörden fallen. Eine gesetzlicher Hinweis zur Eingrenzung des abfragefähigen Datensatzes findet sich immerhin in § 150 Abs. 5 AO. Danach dürfen Steuererklärungsformulare auch Fragen enthalten, die zur Ergänzung der Besteuerungsgrundlagen für Zwecke einer Statistik nach dem Gesetz über Steuerstatistiken erforderlich sind. Im Umkehrschluss ergibt sich daraus, dass die in einer Steuererklärung zu offenbarenden Daten an sich *„Besteuerungsgrundlagen"* betreffen müssen. Nach § 29b Abs. 1 AO ist die Verarbeitung personenbezogener Daten durch eine Finanzbehörde (nur) zulässig, wenn sie zur Erfüllung der ihr obliegenden Aufgabe oder in Ausübung der ihr übertragenen öffentlichen Gewalt erforderlich ist. Es gilt der *zentrale Grundsatz der Zweckbindung der Datenverarbeitung* (s. auch Art. 5 Abs. 1 Buchst. b DSGVO). Vereinfacht gesagt, muss es sich um Daten handeln, die für die gesetzeskonforme Berechnung der Einkommensteuer benötigt werden. Bezogen auf die Einkommensteuererklärung gehören dazu auch sensible Daten wie z.B. der Güterstand, die Religionszugehörigkeit, der Grad einer Körperbehinderung oder der Anlass und Umfang von Krankheitskosten. Die Offenbarung all dieser Daten ist bei Anwendung des datenschutzrechtlichen Verhältnismäßigkeitsprinzips für den Betroffenen grundsätzlich nur zumutbar, wenn er sicher sein kann, dass diese Daten *nur für den steuerlichen Erhebungszweck* verwendet werden und durch das Steuergeheimnis geschützt sind. Dies entspricht der von § 29b Abs. 2 AO für sensible Steuerdaten geforderten *Rechtsgüterabwägung*, wonach die Finanzbehörde die Interessen der betroffenen Person durch angemessene und spezifische Maßnahmen wahren muss. Vor diesem Hintergrund sind die in § 30 Abs. 4 AO enthaltenenen *Durchbrechungen des Steuergeheimnisses* und vor allem dessen „Achillesferse" in § 30 Abs. 4 Nr. 5 AO („zwingendes öffentliches Interesse") *eng auszulegen*.

Aus dem datenschutzrechtlichen Verhältnismäßigkeitsprinzip folgen die in Art. 5 Abs. 1 Buchst. c, e DSGVO ebenfalls herausgestellten Grundsätze der *Datenminimierung* und *Speicherbegrenzung*. Diese verbieten, vom Erhebungszweck nicht gedeckte, für die Erfüllung der staatlichen Aufgabe überflüssige Daten zu erheben und zu speichern. In den Erwägungsgründen zur DSGVO werden für die Speicherbegrenzung in zeitlicher Hinsicht *Löschungsfristen* verlangt[77]. Im Hinblick auf vom Steuerpflichtigen selbst übermittelte Daten sucht man in der AO danach vergebens. Der Gesetzgeber scheint von einer zeitlich unbefristeten Verfügbarkeit der digitalen Daten im Besteuerungsverfahren auszugehen. Dies widerspräche aber dem datenschutzrechtlichen Verhältnismäßigkeitsprinzip und dem daraus folgenden Grundsatz der Datenminimierung.

Eine *äußere Löschungsfrist* lässt sich mittelbar aus den „Bestimmungen über das Aufbewahren und Aussondern von Unterlagen der Finanzverwaltung" (*AufbewBest-FV*) vom 1.6.2011 entnehmen. Dabei handelt es sich allerdings nur um eine bloße Verwaltungsvorschrift. Nach 4.3.1 der Anlage 1 der AufbewBest-FV beträgt die Aufbewahrungsfrist für Steuerakten eines Steuerpflichtigen grundsätzlich 10 Jahre nach Ablauf des Kalenderjahres, in dem die letzte in dem Aktenband befindliche Steuerfestsetzung unanfechtbar geworden ist[78]. Die in der Verwaltungsvorschrift enthaltene 10-Jahresfrist soll es im Einklang mit der verlängerten Festsetzungsfrist i.S.d. § 169 Abs. 2 Satz 2 AO offenbar ermöglichen, auch Steuerhinterziehungsfälle noch zu verarbeiten. Im digitalen Besteuerungsverfahren ist an die Stelle der Aktenvernichtung die Löschung der digitalen Akte zu setzen. Allerdings muss gesehen werden, dass der Eingriff in das Recht auf informationelle Selbstbestimmung bei durch algorithmische Datenverknüpfungen einsetzbaren Akten deutlich intensiver ist als bei einer manuellen Verwendung von Papier-Akteninhalten. Dies wird bei der gebotenen Anpassung der Regelungen auf die digitale Aktenführung zu berücksichtigen sein.

Seit 2012 verpflichtet § 5b Abs. 1 EStG bilanzierende Steuerpflichtige dazu, den Inhalt der Bilanz sowie der Gewinn- und Verlustrechnung nach amtlich vorgeschriebenen Datensatz durch Datenfernübertragung zu übermitteln. Der Inhalt der Bilanz und Gewinn- und Verlustrechnung folgt den handelsrechtlichen Grundsätze ordnungsgemäßer Buch-

77 39. Erwägungsgrund, Satz 12, zur DSGVO (ABl. EU Nr. L119/7 v. 6.5.2016).
78 BMF v. 1.6.2011 – Z A 1-O 1542/06/0002//2011/0449721, BStBl. I 2011, 632 (646).

führung mit den in §§ 5, 6–7 EStG normierten steuerrechtlichen Modifikationen. Auf der Ebene des Parlamentsgesetzes knüpft daran § 5b EStG, der durch das sog. Steuerbürokratieabbaugesetz vom 20.12.2008[79] eingeführt worden ist, an. Nach der Intention des historischen Gesetzgebers sollte die *E-Bilanz* Steuerverfahren beschleunigen, indem papierbasierte Verfahrensabläufe durch elektronischen Kommunikation ersetzt werden („Elektronik statt Papier")[80]. Den technischen Standard sollte nach § 51 Abs. 4 Nr. 1b EStG – vergleichbar mit der Ausgestaltung des Vordrucks der Einkommensteuererklärung – das BMF im Einvernehmen mit den obersten Finanzbehörden der Länder nur den *Mindestumfang* der elektronisch zu übermittelnden Bilanz und Gewinn- und Verlustrechnung festlegen[81]. Lediglich in den Beratungen des Finanzausschusses zu dem Gesetzesvorhaben erwähnte die Regierungskoalition beiläufig, dass eine Verkennzifferung elektronischer Bilanzen auch den Einstieg in eine risikoorientierte Betriebsprüfung eröffnen würde[82].

Auf der Grundlage des § 51 Abs. 4 Nr. 1b EStG hat das BMF dann aber nicht bloß einen sich am handelsrechtlichen Jahresabschluss orientierenden Mindestumfang an elektronisch zu übermittelnden Informationen festgelegt. Vielmehr gibt es als sog. *Taxonomie* ein Datenschema im XBRL-Format (Extensible Business Reporting Language) vor, das den Boden handelsrechtlicher Vorgaben (§§ 266, 277 HGB) verlässt und eine Gliederungstiefe bis hinunter zur Kontenebene erreicht[83]. Das BMF spricht in diesem Zusammenhang von einer *E-Taxation-Wertschöpfungskette* und feiert das E-Bilanz-Projekt als einen Erfolg und wichtigen Baustein der Digitalisierung des Besteuerungsverfahrens[84]. Im Jahr 2017 wurden bundesweit insgesamt 2,5 Millionen Datensätze von Unternehmen an die Finanzverwaltung übermittelt. Nach Meinung des BMF ist die Einführungsphase damit erfolgreich abgeschlossen und auf allgemeine Akzeptanz gestoßen.

79 BGBl. I 2008, 2850.

80 Gesetzentwurf der Bundesregierung eines Steuerbürokratieabbaugesetzes, BT-Drucks. 16/10188 v. 2.9.2008, 13.

81 Gesetzentwurf (Fn. 80), BT-Drucks. 16/10188 v. 2.9.2008, 26.

82 Bericht des Finanzausschusses zum Entwurf eines Steuerbürokratieabbaugesetzes, BT-Drucks. 16/10940, 2.

83 Siehe BMF-Schreiben v. 28.9.2011 – IV C 6 - S 2133-b/11/10009, BStBl. I 2011, 855; zuletzt aktualisiert durch BMF v. 6.6.2018 – IV C 6 - S 2133-b/18/10001, BStBl. I 2018, 714 (Taxonomie 6.2 v. 1.4.2018) mit Hinweis auf www.esteuer.de, wo die Kern-, Ergänzungs- und Spezialtaxonomien zum Abruf zur Verfügung stehen.

84 So BMF, Das Projekt E-Bilanz – ein wichtiger Baustein der Digitalisierung des Besteuerungsverfahrens, Monatsbericht August 2018, 35.

Zwar enthält das detaillierte Datenmaterial keine sensiblen personenbezogenen Daten. Jedoch fallen auch auf eine Person zurückführbare, das wirtschaftliche Ergebnis betreffende Daten in den Schutzbereich informationeller Selbstbestimmung (s. oben I.1.a, II.1.a). Die Taxonomie erhöht gegenüber dem vom Wortlaut des § 5b EStG vorgegebenen Übermittlungsniveau die grundrechtliche Eingriffsintensität und muss sich daher am datenschutzrechtlichen *Vorbehalt des Gesetzes* im Sinne einer hinreichenden gesetzlichen Normenklarheit und -bestimmtheit messen lassen[85]. Für eine spezielle Taxonomie, die nicht dem Abbau von Bürokratielasten, sondern dem Aufbau eines *finanzbehördlichen Risikomanagements* dient, geben weder § 5b EStG noch § 51 Abs. 4 Nr. 1b EStG etwas her. Es fehlt schlicht an einer gesetzlichen Grundlage. Die sog. Taxonomie ermöglicht dem staatlichen Eingriff eine unbegrenzte Nutzung und Verknüpfung der Daten, ohne dass der Betroffene einen Einblick in die weitere Verwendung seiner Daten hätte. Über die angewandten Methoden der Datenverarbeitung- und -verknüpfung informiert die Finanzverwaltung den Betroffenen nicht. Ebenso wenig werden irgendwelche Zugriffseinschränkungen oder maximale Aufbewahrungszeiten erkennbar. Damit verstößt die derzeitige E-Bilanz-Verwaltungspraxis gegen das Recht auf informationelle Selbstbestimmung der betroffenen Steuerpflichtigen und ist verfassungswidrig.

Vor dem Hintergrund des datenschutzspezifischen Übermaßverbots (s. oben I.1.b) und des unionsrechtlichen *Grundsatzes der Datenminimierung/-sparsamkeit* (s. Art. 5 Abs. 1 Buchst. c DSGVO) spricht für den „Erfolg" einer Datenerhebung nicht die beeindruckende Zahl übermittelter Datensätze. Vielmehr bedarf es einer Darlegung seitens der Finanzbehörden, was sie mit den Datensätzen konkret tun und worin der an den Steuervollzugszielen (strukturelle Sicherstellung einer gesetz- und gleichmäßigen Besteuerung) gemessene *Mehrwert der sog. E-Bilanzdaten* eigentlich besteht. Nach einer nun mehr als 5-jährigen Einführungsphase steht die Finanzverwaltung unter einem *Rechtfertigungszwang* dahingehend, ob es der E-Bilanz überhaupt bedarf und in welchem Umfang diese tatsächlich (mit welchem Erkenntnisgewinn?) zu Verifikationszwecken eingesetzt werden.

85 Eingehend *Beckmann*, E-Government im Besteuerungsverfahren am Beispiel der E-Bilanz, Diss., 2016, 159 ff.; s.a. *J. Müller* in Herrmann/Heuer/Raupach, EStG/KStG, § 5b EStG Rz. 7 m.w.N. (Mai 2017).

2. Datensammlung durch Inanspruchnahme Dritter

Das von dritter Seite den Finanzbehörden zu übermittelnde Datenvolumen hat in den vergangenen Jahren auf beachtliche Weise zugenommen. *Elektronische Mitteilungspflichten Dritter* finden sich in den Einzelsteuergesetzen, insbesondere im Einkommensteuergesetz. Beispiele dafür sind Mitteilungen über Vorsorgeaufwendungen i.S.d. § 10 Abs. 2, 2a, 4b EStG und Altersvorsorgebeiträge i.S.d. § 10a EStG (jeweils mit Einwilligung des Steuerpflichtigen), Rentenbezugsmitteilungen i.S.d. § 22a EStG, Lohnersatzleistungen i.S.d. § 32b Abs. 1 Nr. 1 EStG, Lohnsteuerbescheinigungen i.S.d. § 41b Abs. 1 EStG, Bescheinigungen i.S.d. § 43 Abs. 1 Satz 6, Abs. 2 Satz 7 EStG oder Freistellungsaufträge i.S.d. § 45d Abs. 1 EStG. Mit Einwilligung des Steuerpflichtigen können auch Zuwendungsempfänger von steuerbegünstigten Spenden i.S.d. § 10b EStG die Spendendaten nach Maßgabe des § 93c AO elektronisch übermitteln (s. § 50 Abs. 2 EStDV). Zukünftig sollen gem. § 65 Abs. 3a EStDV auch die Daten über die Feststellung einer Behinderung i.S.d. § 33b EStG von den Versorgungsämtern elektronisch übermittelt werden.

Im Unterschied zur gesetzlich nicht hinreichend determinierten E-Bilanz ergeben sich Zweck, Umfang und Verwendung der sog. *E-Daten* aber aus dem Gesetz. Die Funktionsfähigkeit des mit dem Gesetz zur Modernisierung des Besteuerungsverfahrens vom 18.7.2016[86] intendierten *vollautomatischen Steuerveranlagungsverfahrens* hängt wesentlich davon ab, dass die Finanzverwaltung über einen elektronischen Datenbestand sowohl als Grundlage der Steuerfestsetzung als auch zur Verifikation der vom Steuerpflichtigen erklärten Daten verfügt. § 93c AO liefert für die Mitteilungspflichten Dritter nunmehr eine vereinheitlichende Rahmenregelung. Während § 93c Abs. 1 Nr. 2 AO im Wesentlichen die für die Datenzuordnung erforderlichen Identifikationsmerkmale aufführt, folgen die zu übermittelnden materiellen Besteuerungsgrundlagen bezogen auf den jeweiligen Regelungsbereich aus dem Einzelsteuergesetz. Erst beide Rechtsquellen (§ 93c AO und Einzelsteuergesetze) zusammen geben ein komplettes Bild über den konkreten Gegenstand und die konkreten Mitteilungspflichten Dritter. Dies erschwert den Überblick, ist aber den unterschiedlichen Regelungsmaterien geschuldet.

§ 93c Abs. 1 AO sieht eine Frist zur elektronischen Datenübermittlung innerhalb von zwei Monaten bis zum 28.2./29.2. für den abgelaufenen Besteuerungszeitraum vor und definiert die Mindestanforderungen an

86 BGBl. I 2016, 1679.

den zu übermittelnden Datensatz. Gleichzeitig hat die mitteilungspflichtige Stelle den Steuerpflichtigen darüber zu informieren, welche für seine Besteuerung relevanten Daten sie an die Finanzbehörden übermittelt hat oder übermitteln wird (§ 93c Abs. 1 Nr. 3 AO). Die Daten sind bis zum siebten auf den Besteuerungszeitraum/-zeitpunkt folgenden Kalenderjahr von dem Dritten zu speichern und aufzubewahren. Innerhalb dieses Zeitraums sind unrichtige Daten ggf. zu korrigieren oder gar zu stornieren (§ 93c Abs. 3 AO). § 93c Abs. 4 AO berechtigt die zuständigen Finanzbehörden, die Einhaltung der Datenerfassung, -übermittlung und -aufbewahrung zu überprüfen und dazu Ermittlungen durchzuführen.

Nach § 150 Abs. 7 Satz 2 AO gelten die von Dritten nach Maßgabe des § 93c AO übermittelten Daten als Angaben des Steuerpflichtigen, soweit er nicht in dem sog. qualifizierten Freitextfeld der Steuerklärung abweichende Angaben macht. Damit werden die von dritter Seite übermittelten Daten zu Angaben des Steuerpflichtigen, soweit er ihnen nicht widerspricht. Diese Regelung ermöglicht zum einen eine automatische Steuerveranlagung. Zum anderen aber können die übermittelten Daten durch Übernahme zur *vorausgefüllten Steuererklärung* werden[87]. Auch im Hinblick auf die von dritter Seite zu übermittelnden Daten stellt sich die Frage nach der Datensparsamkeit. Immerhin hat der Gesetzgeber bei der Ausgestaltung der Übermittlungspflichten Dritter eine größere Sorgfalt als bei der Inanspruchnahme des eigentlichen Steuerpflichtigen an den Tag gelegt. Dies ist auch erforderlich, weil den Dritten nicht in eigenen, sondern in fremden Steuerangelegenheiten ein beachtlicher datentechnischer Bürokratieaufwand zugemutet wird. Schließlich stellt sich hier auch die Frage einer finanziellen Kompensation.

3. Datenaustausch zwischen den Finanzbehörden

Die von Steuerpflichtigen und Dritten in Erfüllung ihrer Mitwirkungspflichten übermittelten Daten bilden zusammen einen umfangreichen Datenbestand, den die Finanzbehörden zur Verifikation, Verprobung und Realisierung der Steueransprüche nutzen können. Hinzu kommen hoheitlich im Wege von Einzelermittlungen i.S.d. §§ 93 ff. AO, Außenprüfungen i.S.d. §§ 193 ff. AO und durch in Einzelsteuergesetzen verankerte

87 Regierungsbegründung v. 3.2.2016, BT-Drucks. 18/7457, 51.

Nachschauen[88] gewonnene Informationen. Der *ressortinterne Austausch* dieser Daten zwischen Finanzbehörden mit derselben sachlichen Zuständigkeit (s. § 16 AO i.V.m. § 17 Abs. 2 FVG: z.B. zwischen den sachlich zuständigen Finanzämtern) wurde früher datenschutzrechtlich nicht weiter problematisiert[89]. Unter dem Eindruck des von Art. 5 Nr. 1 Buchst. b DSGVO besonders herausgestellten Zweckbindungsgrundsatzes unterscheiden §§ 29b, 29c AO nunmehr scharf zwischen der *zweckgebundenen Datenerhebung* (§ 29b AO) und der *Datenweiterverarbeitung zu anderen Zwecken* (§ 29c AO). Dabei versteht das DSGVO-Anwendungsschreiben des BMF vom 12.1.2018 den Zweck der ursprünglichen Datenerhebung denkbar eng und die zweckändernde Datenweiterverarbeitung dazu komplementär weit. Das BMF hält eine Weiterverarbeitung i.S.d. § 29c Abs. 1 AO bereits dann für gegeben, wenn derselbe Amtsträger (!) die ursprünglich für die Einkommensteuer-Veranlagung erhobenen Daten auch für die Umsatzsteuer-Festsetzung verwendet[90]. Um den Anforderungen des Art. 6 Abs. 4 DSGVO zu genügen, regelt § 29c AO detailliert die Weiterverarbeitungsfälle. Der ressortinterne Datenaustausch wird dabei durch den Zulässigkeitsgrund des § 29c Abs. 1 Nr. 1 AO gedeckt, der dem Offenbarungsgrund des § 30 Abs. 4 Nr. 1 AO entspricht. Die Vorschrift sichert ferner die in § 194 Abs. 3 AO angesprochene *Kontrollmitteilungspraxis* datenschutzrechtlich ebenso ab wie einen weitergehenden *ressortübergreifenden Datenaustausch* (z.B. zwischen Landes- und Bundesfinanzbehörden, z.B. zwischen BZSt und Finanzämtern oder zwischen Finanzämtern und Hauptzollämtern) bis hin zur Weiterverarbeitung der Daten für *steuerstrafrechtliche Zwecke* durch die Strafverfolgungsbehörden.

4. Datenaustausch zwischen Finanzbehörden und anderen Behörden

Für den *ressortübergreifenden Datenaustausch* zwischen den Finanzbehörden und anderen Behörden bedurfte es schon bisher einer datenschutzspezifischen Ermächtigungsgrundlage. So finden sich in den

88 Zur Nachschau als besonderes Steueraufsichtsinstrument *Seer* in Tipke/Lang, Steuerrecht, 23. Aufl. 2018, § 21 Rz. 258 ff.

89 Dazu etwa *Vogelgesang*, Grundrecht auf informationelle Selbstbestimmung, Diss., 1987, S. 227 ff.; *Seer*, Datenschutz im Besteuerungsverfahren, FS für W. Meilicke, 2010, S. 687 (695).

90 BMF v. 12.1.2018 – IV A 3 - S 0030/16/10004-07, BStBl. I 2018, 185 (189) Rz. 26.

§§ 31–31b AO Ermächtigungen zur Weitergabe personenbezogener Daten an Verwaltungs-, Sozial- und Strafverfolgungsbehörden mit dem Ziel der Bekämpfung der Schwarzarbeit, des Leistungsmissbrauchs, der Geldwäsche und der Terrorismusbekämpfung. Der sich daraus ergebende *datenschutzrechtliche Zielkonflikt*[91] ist dadurch zu lösen, dass zwar einerseits das berechtigte öffentliche Interesse an der Sicherung der Erhebung von Sozialabgaben und der Bekämpfung des Leistungsmissbrauchs in Gestalt der Mitteilungspflicht gewahrt, andererseits aber das Steuergeheimnis auch auf die Empfängerbehörden als *sog. verlängertes Steuergeheimnis* angewendet wird[92]. Zudem dürfen die Mitteilungspflichten der §§ 31–31b AO nicht den Nemo-tenetur-Grundsatz unterlaufen, so dass die mitgeteilten Steuerdaten, die vom Steuerpflichtigen unter verfahrensrechtlichem Zwang erhoben worden sind, für strafrechtliche Zwecke unverwertbar sein dürften.

In umgekehrter Richtung ermöglicht § 93a AO i.V.m. der Mitteilungsverordnung (MV) vom 7.9.1993 einen Datenaustausch innerhalb Deutschlands anderer Behörden hin zu den Finanzbehörden. Der Kreis der dort genannten Mitteilungspflichten ist enumerativ und tatbestandlich begrenzt. Die wohl wichtigste in § 2 Abs. 1 MV aufgeführte Fallgruppe bilden die Zahlungen, die auf kein Geschäftskonto des Empfängers (also insbesondere bar) geleistet worden sind. Seine Verordnungsermächtigung hat der Verordnungsgeber aber nicht in vollem Umfang ausgeschöpft, weil er Mitteilungen über Subventionen und andere Fördermaßnahmen sowie über das Vorliegen von Anhaltspunkten der Schwarzarbeit nicht einbezogen hat. Allerdings kann insoweit eine Mitteilungspflicht nach § 116 Abs. 1 Satz 1 AO bestehen. Danach haben Gerichte und Behörden der Gebietskörperschaften dienstlich erfahrene Tatsachen, die auf eine Steuerstraftat schließen lassen, dem BZSt oder – falls bekannt – der für die Verfolgung von Steuerstraftaten zuständigen Finanzbehörde zu übermitteln.

91 *Drüen* in Tipke/Kruse, AO/FGO, Vor § 31 AO Rz. 1 (Mai 2015).

92 BFH v. 4.10.2007 – VII B 110/07, BStBl. II 2008, 42 (45); *Drüen* in Tipke/Kruse, AO/FGO, § 31a AO Rz. 8 (Mai 2015).

IV. Grenzüberschreitender Datenaustausch im Lichte des Datenschutzes

1. Zwischenstaatliche Ersuchens- und Spontanauskünfte

Die klassische Form der internationalen Amtshilfe bildet die sog. *Ersuchensauskunft*, wo ein Staat einen anderen Staat um Amtshilfe ersucht. Ihr entspricht in umgekehrter Richtung die sog. *Spontanauskunft*, wo ein Staat ohne vorheriges Ersuchen („spontan") einem anderen Staat Auskunft erteilt. Beiden Instrumenten ist gemeinsam, dass sie jeweils einen konkreten Einzelfall betreffen. Sie bilden den typischen Gegenstand der sog. Auskunftsklauseln in bilateralen Doppelbesteuerungsabkommen[93]. Sie finden sich aber ebenso in der EU-Amtshilferichtlinie 2011/16/EU vom 15.2.2011 (Art. 5, 9 DAC – Directive on Administrative Cooperation)[94] sowie in dem multilateralen Abkommen des Europarats und der OECD vom 25.1.1988/27.5.2010 (Art. 5, 7 CMAA – Convention on Mutual Administrative Assistance)[95].

Eine wichtige datenschutzrechtliche Funktion übernimmt das nach Maßgabe des Art. 26 Abs. 2 OECD-MA ausgestaltete *internationale Steuergeheimnis*. Es wirkt zweispurig. Zum einen hat der Empfängerstaat die erhaltenen Informationen ebenso geheim zu halten wie aufgrund innerstaatlichen Rechts beschaffte Informationen (Art. 26 Abs. 2 Satz 1 Halbs. 1 OECD-MA). Zum anderen dürfen die erhaltenen Informationen nur bestimmten Personen und Behörden des Empfängerstaates zu bestimmten Zwecken zugänglich gemacht werden (Art. 26 Abs. 2 Satz 1 Halbs. 2, Satz 3 OECD-MA). Zwar ist das Datenschutzniveau im internationalen Vergleich unterschiedlich ausgestaltet, so dass man in der Anknüpfung an den Empfängerstaat eine Relativierung des internationalen Steuergeheimnisses sehen kann[96]. Allerdings fängt dies Art. 26 Abs. 2 Satz 1 Alt. 2 OECD-MA durch die Zugangsbeschränkung und deutliche Zweckbindung wieder auf[97]. Letztlich wird dadurch ein *absoluter* – vom innerstaatlichen Recht losgelöster – *Geheimhaltungsstandard* begründet[98]. Die übermittelten Daten dürfen nur für steuerrechtliche (allerdings auch steuerstrafrechtliche) Zwecke verwendet werden. Der Zugang ist auf solche Personen, Behörden und Gerichte beschränkt, die mit dieser zweckgebundenen Datenverwendung betraut sind. Eine weitergehende Verwendung der Daten lässt Art. 26 Abs. 2 Satz 4 OECD-MA nur zu, wenn das Recht beider Staaten dies gestattet und die zuständige Behörde des informierenden Staates (in Deutschland: das BZSt) damit einverstanden ist.

Adressat der Geheimhaltungsverpflichtung ist ausschließlich der Empfängerstaat. Der Auskunftsstaat wird nur nach nationalem Recht (wenn die Bundesrepublik Deutschland Auskunftsstaat ist: nach § 30 AO) verpflichtet. Allerdings ist eine nach dem Vorbild des Art. 26 Abs. 2 OECD-MA abgeschlossene völkervertragliche Regelung nicht nur Bestandteil des objektiven Rechts, sondern begründet zugunsten des geschützten Geheimnisträgers auch ein *subjektives Recht*[99]. Der Betroffene kann sich auf zweierlei Wegen gegen die unbefugte Weitergabe „seiner" personenbezogenen Daten wehren. Im *Auskunftsstaat* kann er auf Einhaltung dessen nationalen Steuergeheimnisschutzes klagen. Dazu bedarf es aber der Glaubhaftmachung, dass das Steuergeheimnis im Empfängerstaat in substantieller Weise entgegen Art. 26 Abs. 2 OECD-MA gefährdet wird[100]. Dies kann den Auskunftsstaat nach Art. 26 Abs. 3 Buchst. c OECD-MA (Ordre-public-Vorbehalt) ggf. zur Auskunftsverweigerung gegenüber dem anderen Vertragsstaat berechtigen. Im *Empfängerstaat* kann sich der Betroffene nicht nur auf das dortige nationale Steuergeheimnis, sondern darüber hinaus auch auf das Schutzniveau des Art. 26 Abs. 2 OECD-MA berufen. Die deutsche Verhandlungsgrundlage sieht in dem Zusatzprotokoll in Buchst. c und d zudem eine Informationspflicht des Empfängerstaates gegenüber dem Betroffenen vor[101].

93 *Seer* in Gosch/Kroppen/Grotherr/Kraft, DBA, Kommentar, Art. 26 OECD-MA Rz. 20 ff. (30. Erg.-Lfg. 2016).
94 ABl. EU Nr. L 64/1 v. 11.3.2011.
95 SEV Nr. 127 u. 208. Die Bundesrepublik Deutschland ist dem Abkommen beigetreten und hat es mit Gesetz v. 16.7.2015, BGBl. II 2015, 966, in das innerstaatliche Recht übernommen.
96 *Engelschalk* in Vogel/Lehner, DBA, Kommentar, 6. Aufl. 2015, Art. 26 OECD-MA Rz. 78 f.
97 *Czakert* in Schönfeld/Ditz, DBA, Kommentar, 2013, Art. 26 OECD-MA Rz. 67.
98 *Hendricks* in Wassermeyer, DBA, Kommentar, Art. 26 OECD-MA Rz. 50 (Februar 2013).
99 *Herlinghaus*, Zu Möglichkeiten und Grenzen des Rechtsschutzes gegen Maßnahmen des zwischenstaatlichen Informationsaustausches nach den Doppelbesteuerungsabkommen, in FS Herzig, 2010, S. 933 (948 f.); *Engelschalk* in Vogel/Lehner, DBA, 6. Aufl. 2015, Art. 26 OECD-MA Rz. 81 f.; *Hendricks* in Wassermeyer, DBA, Kommentar, Art. 26 OECD-MA Rz. 52 (Februar 2013).
100 FG Köln v. 20.8.2008 – 2 V 1948/085, EFG 2008, 1764 m. Anm. *Herlinghaus*; *Seer/Gabert*, Der internationale Auskunftsverkehr, StuW 2010, 3 (19 f.).
101 Text bei *Schönfeld/Ditz*, DBA-Kommentar, 2013, Art. 26 DE-VG, Anh. vor Rz. 187, abgedruckt.

Eine *entsprechende Geheimhaltungsregel* enthält Art. 22 CMAA. Sie ist sogar *strenger*, weil sich das Geheimhaltungsniveau gem. Art. 22 Abs. 1 CMAA nach dem jeweils strengsten Recht der am Informationsaustausch beteiligten Vertragsstaaten richtet.

Dagegen orientiert Art. 16 Abs. 1 EU-AmtshilfeRL (DAC) das internationale Steuergeheimnis an der Ausgestaltung im Empfängerstaat. Verfügt der auskunftserteilende Mitgliedstaat über strengere Geheimhaltungsregelungen als der Empfängerstaat, besteht kein Anspruch auf Einhaltung dieser strengeren Vorschriften[102]. Allerdings begrenzt Art. 16 Abs. 1 DAC die Verwendung der Daten auf die der Amtshilfe-Richtlinie unterfallenden Steuern, einschließlich deren Beitreibung und steuerstrafrechtlichen Sanktionen. Eine weitergehende Verwendung bindet Art. 16 Abs. 2 DAC an die Zustimmung des übermittelnden Mitgliedstaates, die dieser nur dann zu erteilen hat, wenn er die Informationen nach seinem innerstaatlichen Recht in ähnlicher Weise verwenden könnte.

2. Ausbau des automatischen Austausches von Finanzkontendaten

Ein erster Einstieg in den automatischen Informationsaustausch gelang im Jahr 2003 mit der Zinsrichtlinie 2003/48/EG vom 3.6.2003[103]. Sie führte den automatischen Informationsaustausch für bestimmte Zinseinkünfte ein. Ihre Effektivität litt aber an einem engen Zinsbegriff, an der fehlenden Transparenz bei zwischengeschalteten Einheiten und an dem Umstand, dass mit Belgien, Luxemburg und Österreich drei Mitgliedstaaten zumindest zunächst einen mit einem Quellensteuerabzug bedingten Sonderstatus einnahmen.

Die EU-Zinsrichtlinie hat sich durch die weltweite Akzeptanz eines automatischen Informationsaustausches über Finanzkonten überlebt. Diese Entwicklung ist ebenso rasant wie bemerkenswert. Mit dem US-amerikanischen Foreign Account Tax Compliance Act (FATCA)[104] hat die USA erheblichen Druck zur Etablierung des automatischen Informationsaustausches als einen sog. *Common Reporting Standard (CRS)* auf ausländische Finanzinstitute ausgeübt. Vor dem Hintergrund einer unilateralen „Strafsteuer-Drohkulisse" hat die USA sog. *Intergovernmental Agreements (IGA)* entwickelt, die sie den ausländischen Staaten anbietet, um die in dem jeweiligen ausländischen Staat ansässigen Finanzinstitute der Strafsteuergefahr zu entledigen. Auf dieses Angebot der USA sind mittlerweile mehr als 100 Staaten, darunter auch alle EU-Staaten, eingegangen.

Daran anknüpfend hat die OECD den *„Global Standard for Automatic Exchange of Financial Account Information in Tax Matters"* entwickelt und inklusive Kommentar im Juli 2014 veröffentlicht[105]. Dieser besteht aus zwei Elementen:

1. der Mustervereinbarung zwischen den zuständigen Behörden über den automatischen Informationsaustausch bezüglich Finanzkonten (**„Competent Authority Agreement" – CAA**) und
2. dem gemeinsamen Melde- und Sorgfaltsstandard für Informationen über Finanzkonten (**„Common Reporting Standard" – CRS**).

Das CAA schreibt die Modalität des Informationsaustausches vor, um den angemessenen Informationsfluss zu gewährleisten[106], während der CRS die Melde- und Sorgfaltspflichten der Finanzinstitute beinhaltet, welche diesem automatischen Austausch zugrunde liegen[107]. Mit diesem globalen Schwung hat auch die EU die Melde- und Sorgfaltsvorschriften mit der Richtlinie 2014/107/EU vom 9.12.2014[108] in die EU-Amtshilferichtlinie 2011/16/EU eingearbeitet (DAC 2).

Der automatische Auskunftsverkehr ist auf ein abstraktes Risiko mit einer breiteren Streuung ausgelegt. Es werden Informationen von *abstrakt-generell definierten Fallgruppen* ohne weitergehenden konkreten Einzelfallanlass übermittelt. Dadurch unterscheidet er sich grundlegend von Spontan- und Ersuchensauskünften. Treffend beschreibt Art. 1 Nr. 1 DAC 2 den Charakter des automatischen Informationsaustausches als

„systematische Übermittlung zuvor festgelegter Informationen über in anderen Mitgliedstaaten ansässige Personen an den entsprechenden Ansässigkeitsmitgliedstaat ohne dessen vorheriges Ersuchen in regelmäßigen, im Voraus bestimmten Abständen".

102 *Glaser*, Die datenschutzrechtlichen Grenzen bei der internationalen Informationshilfe durch deutsche Steuerbehörden innerhalb der Europäischen Union, Diss., 2014, S. 111 f.
103 ABl. EG 2003 Nr. L 157/38.
104 Dazu näher *Lappas/Ruckes*, Die praktische Umsetzung von FATCA in Deutschland, ISTR 2013, 929.
105 Abrufbar unter: http://www.oecd.org/ctp/exchange-of-tax-information/standard-for-automatic-exchange-of-financial-information-in-tax-matters.htm.
106 OECD Standard, Einleitung, S. 14 Rz. 17.
107 OECD Standard, Einleitung, S. 15 Rz. 19.
108 ABl. EU 2014 Nr. L 359/1.

Die automatischen Auskünfte lassen sich damit als Teil eines *grenzüberschreitenden elektronischen Risikomanagements* verstehen[109], weil sie dem Empfängerstaat Kontrollmaterial zum automatischen Abgleich mit den Angaben der Steuererklärungen liefern. Damit die Finanzbehörden dies tun können, werden Finanzinstitute verpflichtet, ihre Kunden auf deren Ansässigkeit und eine damit zusammenhängende Steuerpflicht in einem anderen Staat zu untersuchen. Deutet eine solche *indizienbasierte Überprüfung* auf eine Steuerpflicht in einem anderen EU-Mitgliedstaat oder einem MCAA-Drittstaat hin, so hat das Finanzinstitut entsprechende Kundeninformationen jährlich dem zentralen Verbindungsbüro seines Sitzstaates (in Deutschland: dem BZSt[110]) zu melden, das die Informationen an den ausländischen Staat weiterleitet bzw. umgekehrt entsprechende Meldungen empfängt[111].

Auf der Basis der vorgenannten Rechtsgrundlagen sind für den Meldezeitraum 2016 erstmals zum 30.9.2017 Finanzkontendaten automatisch ausgetauscht worden. Nach Auskunft der Bundesregierung hat das BZSt als zentrale Finanzbehörde der Bundesrepublik Deutschland insgesamt ca. 1,5 Millionen Datensätze von insgesamt 49 Staaten erhalten[112]. Das Volumen der gemeldeten Einkünfte belief sich auf ca. 58 Mrd. €, die gemeldeten Kontenstände betrugen insgesamt ca. 85 Mrd. €. Für den Meldezeitraum 2017 werden zum 30.9.2018 insgesamt 102 Staaten am automatischen Informationsaustausch teilnehmen[113], so dass mit einer noch deutlich größeren Anzahl von Datensätzen zu rechnen ist. BZSt und Länderfinanzbehörden stehen nun vor der Aufgabe, dieses umfangreiche Datenmaterial zuzuordnen und systematisch auszuwerten. Nach Auskunft der Bundesregierung werden die technischen Voraussetzungen dafür erst

109 So bereits *Seer/Gabert* (Fn. 100), StuW 2010, 3 (14).

110 Das BZSt ist die zentrale deutsche Verbindungsbehörde, über die nach § 7 Abs. 1 i.V.m. § 3 Abs. 2 AmtshilfeRLUmsG (BGBl. I 2013, 1809) und nach § 9 Abs. 1, 2 FATCA-USA-UmsV (BGBl. I 2014, 1222) der grenzüberschreitende Informationsaustausch verläuft.

111 Zu den Details der Meldepflicht s. *Seer/Wilms*, Der automatische Informationsaustausch als neuer OECD-Standard zur steuerlichen Erfassung des Finanzkapitals im Spannungsverhältnis zu Maßnahmen der Geldwäschebekämpfung, StuW 2015, 118 (121 ff.).

112 Antwort der Bundesregierung v. 27.7.2018 auf eine Anfrage der FDP-Fraktion und einiger Abgeordneter, BT-Drucks. 19/3630, 3.

113 Liste der Signaturstaaten des Multilateral Competent Authority Agreements (MCAA) mit Stand v. 26.6.2018, s. http://www.oecd.org/tax/automatic-exchange/international-framework-for-the-crs/MCAA-Signatories.pdf. Dies deckt sich mit der Antwort der Bundesregierung (Fn. 112), 2.

im Jahr 2020 geschaffen worden sein[114]. Gleichwohl wird man den Finanzbehörden deshalb nicht den Vorwurf eines Verstoßes gegen den Grundsatz der Datenminimierung und Datensparsamkeit machen können. Um das bisher im Hinblick auf im Ausland erzielte Kapitaleinkünfte bestehende *strukturelle Vollzugsdefizit* zu beseitigen, bedarf es eines globalen Verifikationssystems. Dass dieses nicht sofort, sondern erst nach einer gewissen Implementationsphase lauffähig ist, liegt in der Natur der Sache. Allerdings müssen die Finanzbehörden unter *dauernder Beobachtung* bleiben, wie sie die umfangreichen Datensätze verwenden und welche datenschutzrechtlichen Vorkehrungen sie treffen.

Im Anwendungsbereich der DSGVO besitzt der Steuerpflichtige – wie dargelegt – nach Art. 15 DSGVO einen *Auskunftsanspruch* über die Verarbeitung personenbezogener Daten, der allerdings auf der Grundlage des Art. 23 Abs. 1 Buchst. e DSGVO durch die Mitgliedstaaten eingeschränkt werden kann. Dies ist in § 32c AO unter Verweis auf die in § 32b Abs. 1, 2 AO statuierten Informationsverweigerungsgründe geschehen. Allerdings werden die Finanzbehörden nicht pauschal auf eine irgendwie geartete Gefährdungslage verweisen können[115]. Die automatische Übermittlung von Finanzkontendaten allein begründet noch keine konkrete Gefährdungslage. Ganz im Gegenteil: Der Steuerpflichtige hat einen legitimen Anspruch darauf zu erfahren, welche Daten die Finanzbehörde über ihn und seine Vermögensverhältnisse gespeichert hat. Denn nur so wird es ihm ermöglicht, die Richtigkeit der gespeicherten Daten zu überprüfen und ggf. in seiner Steuererklärung mit einer Erläuterung zu korrigieren, um im Falle eines sog. Mismatching nicht in den Verdacht einer vorsätzlichen Steuerverkürzung zu geraten.

Etwas anderes kann dann gelten, wenn sich etwa aus einzelfallbezogenen Kontrollmitteilungen ernsthaft die Gefahr ergibt, dass der Steuerpflichtige bei deren Kenntnis den verwirklichten Sachverhalt nachträglich verschleiern und Beweismaterial verändern oder vernichten könnte. Dies könnte etwa der Fall sein, wenn die Finanzbehörde erstmalig von Auslandssachverhalten erfährt, die nicht nur bloße gewöhnliche Routine-Geldanlagen betreffen und auf noch unbekannte Steuertatbestände schließen lassen. Aber auch dann ist die Ablehnung der Auskunftserteilung gegenüber der betroffenen Person nach § 32c Abs. 4 AO zu begrün-

114 Antwort der Bundesregierung (Fn. 112), 4.

115 So aber noch VG Berlin v. 13.10.2016 – 2 K 507/15, zum Ausschlussgrund des § 3 Nr. 1 Buchst. d IFG; dagegen bereits *Seer* in Tipke/Kruse, AO/FGO, § 88 AO Rz. 82 (Januar 2017).

den. Da die Einschränkung des Datenschutzrechts unter der Schranken-Schranke des *Verhältnismäßigkeitsprinzips* steht, darf diese Begründung nicht auf einer abstrakten Ebene verbleiben, sondern muss die Gefährdungslage im Hinblick auf den *konkreten Einzelfall* des Steuerpflichtigen darlegen.

Verbreitet ist die Sorge, dass die Finanzdaten in *Drittstaaten* für nichtsteuerliche Zwecke verwendet werden. Dieser Sorge hat der EuGH in der bereits behandelten sog. Safe-Harbour-Entscheidung[116] in anderem Zusammenhang eindrucksvoll Rechnung getragen. In der Tat fordern Art. 44 ff. DSGVO für die Datenübermittlung an Drittstaaten grundsätzlich ein vergleichbares *Datenschutzniveau im Drittstaat* und eine zweistufige Legitimationsprüfung. Davon macht aber Art. 49 Abs. 1 Buchst. d DSGVO eine Ausnahme, wenn die Datenübermittlung aus *wichtigen Gründen des öffentlichen Interesses* notwendig ist. Dabei muss das öffentliche Interesse nach Art. 49 Abs. 4 DSGVO im Unionsrecht oder im Recht des Mitgliedstaates des Verantwortlichen anerkannt sein. Der Erwägungsgrund Nr. 112 zur DSGVO nennt als wichtige Gründe des öffentlichen Interesses ausdrücklich den *internationalen Datenaustausch zwischen den Steuerbehörden*[117].

Zudem ist zu beachten, dass Art. 22 CMAA mit seinem strengen Maßstab des *internationalen Steuergeheimnisses* nicht nur für Einzel- und Spontanauskünfte, sondern auch im Bereich des automatischen Informationsaustausches gilt. Das auf der Basis von Art. 6 CMAA abgeschlossene Multilateral Competent Authority Agreement (MCAA) vom 29.10.2014[118] sieht zudem in § 5 MCAA Vertraulichkeitsvorschriften und gegenseitige Datenschutzvorkehrungen vor, die als Anlage C zu dem MCAA von der Bundesrepublik Deutschland offiziell hinterlegt worden sind. Diese dürfen datenschutzrechtlich allerdings nicht nur auf dem Papier stehen. Werden der Bundesrepublik Deutschland *faktische Verstöße* eines Empfängerstaats gegen das internationale Steuergeheimnis bekannt, hat es den automatischen Auskunftsverkehr vorläufig einzustellen und in Konsultationen mit dem Empfängerstaat zu treten, damit dieser seine konventionswidrige Praxis ändern kann.

116 Siehe EuGH v. 6.10.2015 (Fn. 48).

117 Erwägungsgrund 112 zur DSGVO, s. ABl. EU Nr. L119/21 v. 6.5.2016; darauf weist *Krumm* (Fn. 59), DB 2017, 2182 (2190) mit Recht hin.

118 In das nationale Recht übernommen durch Gesetz v. 21.12.2015, BGBl. I 2015, 2531.

3. Ausbau des automatischen Austausches von Unternehmensdaten

Anknüpfend an die Anti-BEPS (Base Erosion and Profit Shifting)-Aktionspläne Nr. 5, 13 der OECD/G20 hat die EU zur *Transparenzsteigerung* das Instumentarium des automatischen Datenaustausches jüngst auch auf bestimmte Unternehmensdaten erstreckt. Dazu ist die EU-Amtshilfe-Richtlinie 2011/16/EU (DAC) gleich mehrfach geändert worden. Vor dem Hintergrund der von der EU-Kommission gegen mehrere Mitgliedstaaten eröffneten EU-Beihilfeprüfverfahren[119] verpflichtet die Richtlinie (EU) 2015/2376 vom 8.12.2015 (DAC 3) die Mitgliedstaaten nunmehr, Informationen über „grenzüberschreitende Vorbescheide" (sog. Advance Tax Rulings – ATR) und Verrechnungspreis-Vorabverständigungsvereinbarungen (sog. *Advance Pricing Agreements – APA*)[120] miteinander automatisch auszutauschen[121].

Die mit DAC 3 verankerte neue Idee ist es, den *automatischen Auskunftsverkehr* mit einem daran anschließenden *Einzelauskunftsersuchen zu verknüpfen*. Deshalb sollen die automatisch weiterzugebenden Informationen zum einen so knapp wie möglich gehalten, zum anderen aber so hinreichend sein, dass die Informationen empfangenden Mitgliedstaaten beurteilen können, ob sie vom Auskunftsstaat weitere Informationen anfordern. Auf der zweiten Stufe haben diejenigen Mitgliedstaaten, die nachweisen können, dass die Informationen für sie voraussichtlich relevant sind, dann die Möglichkeit, im Wege eines konkreten Einzelauskunftsersuchens vom Auskunftsstaat detailliertere Informationen zu erlangen. Das Auskunftsersuchen kann in dieser Verfah-

119 Die EU-Kommission hatte in 2014 gegen Irland, Luxemburg und die Niederlande Beihilfeverfahren zur Prüfung von Verrechnungspreisvereinbarungen eingeleitet (s. IWB 2014, 435 und *Rasch*, IWB 2015, 163; *Linn*, IStR 2015, 114). Laut Pressemitteilung v. 17.12.2014 (IP/14/2742) hat sie ihre Untersuchungen zwischenzeitlich sogar auf alle Mitgliedstaaten ausgeweitet. Laut Pressemitteilung v. 21.10.2015 (IP/15/5880) hat die EU-Kommission die beihilferechtliche Unzulässigkeit von Vereinbarungen zwischen Luxemburg und der Fa. Fiat Finance sowie zwischen der Niederlande und der Fa. Starbucks festgestellt und beide Staaten verpflichtet, die gewährten Vorteile zurückzufordern, d.h. Steuern nachträglich festzusetzen.

120 Zu den Begrifflichkeiten s. *Seer* (Fn. 18) in FS Gosch, 2016, S. 387 (388 ff.).

121 RL 2015/2376/EU v. 8.12.2015, ABl. EU Nr. L 332/1, umgesetzt in das nationale Recht in § 7 Abs. 3–9 EUAHiG durch Gesetz v. 20.12.2016, BGBl. I 2016, 3000 (3005 ff.).

rensphase auch auf die Anfrage nach dem vollständigen Inhalt des ATR bzw. des APA gerichtet sein.

Die Richtlinie 2016/881/EU vom 25.5.2016 (= DAC 4) erweitert den automatischen Informationsaustausch außerdem auf länderbezogene Berichte multinationaler Konzerne (sog. *Country-by-Country-Reporting [CbCR]*)[122]. DAC 4 folgt der am 27.1.2016 durch 31 Staaten abgeschlossenen zweiten mehrseitigen Vereinbarung (MCAA 2)[123]. Danach haben multinationale Konzerne mit einem konsolidierten Jahresumsatz von mindestens 750 Mio. € länderbezogene Berichte nach einem bestimmten elektronischen Datenschema zu erstellen und den jeweiligen nationalen zentralen Finanzbehörden (in Deutschland: dem BZSt) zu übermitteln, die dann zwischen den Mitglieds- bzw. Vertragsstaaten automatisch ausgetauscht werden. Die automatisch ausgetauschten Länder-Basisdaten sollen den Finanzbehörden die steuerliche Prüfung von Konzernstrukturen und Wertschöpfungsketten erleichtern und ihnen Anhaltspunkte für weitere konkrete Einzelauskunftsersuchen bieten. Das Konzept entspricht damit dem mit DAC 3 in die EU-AmtshilfeRL implementierten *zweistufigen Informationsaustauschsystem*.

Zuletzt hat die EU schließlich am 25.5.2018 den Informationsaustausch für *grenzüberschreitende Steuergestaltung*, die sog. Intermediäre den nationalen Finanzbehörden zukünftig anzuzeigen haben, durch eine erneute Änderung der Amtshilfe-Richtlinie eingeführt (Richtlinie (EU) 2018/822 = DAC 6[124]). Nach der auf den Anti-BEPS-Aktionsplan Nr. 12 der OECD/G20 zurückgehenden Regelung sind sog. Intermediäre zur Vorlage der ihnen bekannten, in ihrem Besitz oder unter ihrer Kontrolle befindlichen Informationen über meldepflichtige grenzüberschreitende Gestaltungen innerhalb von 30 Tagen, nachdem die Gestaltung zur Nutzung bereit gestellt ist, zu verpflichten. Die von den sog. Intermediären zu liefernden Informationen ergeben sich mittelbar aus dem zwischen den Mitgliedstaaten auszutauschenden Informationskatalog i.S.d. Art. 8ab Abs. 14 DAC 6. Dieser Katalog umfasst konkrete Angaben über

122 RL 2016/881/EU v. 25.5.2016, ABl. EU Nr. L 146/8: Die länderbezogene Berichtspflicht statuiert auf nationaler Ebene § 138a AO, der automatische Informationsaustausch ist in § 7 Abs. 9–13 EUAHiG verankert.

123 Mittlerweile haben 72 Staaten das MCAA 2 unterzeichnet und sich zum Datenaustausch verpflichtet, s. http://www.oecd.org/ctp/beps/CbC-MCAA-Signatories.pdf (letztes Update 18.11.2018). In Deutschland ist das Abkommen durch Gesetz v. 19.10.2016, BGBl. II 2016, 1178 in das nationale Recht übernommen worden.

124 Richtlinie (EU) 2018/822 v. 25.5.2018, ABl. EU v. 5.6.2018, L 139/1.

die Steuerintermediäre und Steuerpflichtigen sowie zu den eine Meldepflicht auslösenden Kennzeichen, eine Zusammenfassung des Inhalts der meldepflichtigen grenzüberschreitenden Gestaltung und über dessen Wert. Diese und weitere mitteilungspflichtige Daten sollen sodann durch die Mitgliedstaaten der EU-Kommission mittels eines elektronischen Datenblatts gemeldet und dort in ein Zentralverzeichnis eingestellt werden, auf das die einzelnen Mitgliedstaaten zugreifen können (s. Art. 21 Abs. 5 DAC 6). Art. 25a DAC verpflichtet die Mitgliedstaaten, Sanktionen einzuführen, die „wirksam, verhältnismäßig und abschreckend" sein sollen. DAC 6 ist bis zum 31.12.2019 in das nationale Recht umzusetzen. Ein erster Informationsaustausch über die anzeigepflichtigen Steuergestaltungen soll im Herbst 2020 erfolgen.

Das *Konzept digitaler Zentralregister* der EU-Kommission, auf das die Mitgliedstaaten zugreifen können, findet sich bereits in DAC 3 für die automatisch zu übermittelnden Daten grenzüberschreitender ATR und APA. Die zentrale Erfassung der Daten soll einen effizienten Ressourceneinsatz gewährleisten und vermeiden, dass alle EU-Mitgliedstaaten einzeln ähnliche Änderungen an ihren nationalen Systemen zur Speicherung von Daten vornehmen müssen. Der auf die Information der Finanzbehörden der Mitgliedstaaten beschränkte Datenerhebungszweck verbietet es aber, das Register öffentlich zu machen[125].

Der automatische Auskunftsverkehr passt zu *Massenverfahren* und zur Übermittlung leicht abgreifbarer, elektronisch vorrätiger Daten wie z.B. Kapitalerträge, Kontenstände, Gehalts-, Renten- oder Beitragszahlungen. Dem entspricht der bereits behandelte Standard für den automatischen Informationsaustausch über Finanzkontendaten. In diesem Bereich besteht das dringende Bedürfnis vor allem nach der *wirksamen Ausgestaltung des internationalen Steuergeheimnisses*, damit die Steuerpflichtigen sicher sein können, dass ihre Finanzdaten auch im ausländischen Staat nur für Besteuerungszwecke verwendet werden. Das vorgelagerte Problem möglicher Verletzung von Unternehmensgeheimnissen stellt sich hier typischerweise nicht.

Das internationale Informationshilferecht verlässt sich aber nicht auf die Einhaltung des internationalen Steuergeheimnisses, soweit es um *Unter-*

125 So hält auch der französische Verfassungsrat in seiner Entscheidung v. 8.12.2016 (Nr. 2016-741 DC) ein öffentliches CbCR-Register (nach französischem Recht) für verfassungswidrig, s. *Lüdicke/Salewski*, Informationsaustausch: Entwurf einer EU-Richtlinie zur Veröffentlichung von Streuerdaten, Besonderheiten bei Personengesellschaften und Grundrechte, ISR 2017, 99.

nehmensgeheimnisse geht. Vor dem Hintergrund, dass die Rechtsordnungen einiger Staaten umfassende und schwer kalkulierbare Durchbrechungen des Steuergeheimnisses vorsehen, sollen sowohl die nationale Volkswirtschaft als auch die betroffenen Unternehmen vor dem *Risiko einer Wirtschaftsspionage* geschützt werden. Wenn im Zuge der verfolgten Transparenzinitiative nun generell bestimmte Unternehmensdaten automatisch übermittelt werden sollen, gerät das Instrument der automatischen Auskunft latent in Konflikt mit dem sowohl in Art. 17 Abs. 4 EU-AmtshilfeRL als auch in Art. 26 Abs. 3 Buchst. c DBA besonders pointierten Schutz von Unternehmensgeheimnissen.

Diesen Konflikt mögen ECOFIN/OECD „wegdefinieren", indem sie anordnen, dass die zum Geheimnisschutz statuierten Beschränkungen des Informationsaustausches unbeschadet bleiben. Letztlich verlagern sie damit das Problem auf die Finanzbehörden der jeweiligen Mitglieds- bzw. Vertragsstaaten[126]. Diese müssen die Relevanz der übermittelten Daten für den Unternehmensgeheimnisschutz einschätzen, um zu entscheiden, ob sie auf ermessensfehlerfreie Weise vom Recht zur Informationsverweigerung Gebrauch machen.

Jeder Mitgliedstaat hat vor der „automatischen" Weitergabe des zusammengefassten Inhalts von ATR, APA oder Country-by-Country-Reporting-Länderberichten daher zu prüfen, ob der Inhalt ein *Betriebs- oder Geschäftsgeheimnis* verletzen könnte. Bestehen hierfür nicht nur theoretische Anhaltspunkte, hat das BZSt das betroffene Unternehmen gem. § 117 Abs. 4 Satz 3 AO i.V.m. § 91 Abs. 1 AO *zuvor anzuhören*, um die Gefahr einer Preisgabe von Unternehmensgeheimnissen i.S.d. Art. 17 Abs. 4 DAC sachgerecht prüfen zu können. Dies gilt erst recht auch im Verhältnis zu Drittstaaten, die dem MCAA 2 beigetreten sind.

Im Übrigen wird mit Recht bezweifelt, ob die Sammlung der länderbezogenen Berichte nicht gegen die *Grundsätze der Datenvermeidung und -mininierung* verstoßen[127]. Der Gesetzgeber selbst sieht im länderbezogenen Bericht als solchen kein geeignetes Mittel zur Prüfung der Angemessenheit von Verrechnungspreisen. Die Berichtsgrößen (z.B. Umsatzerlöse, Eigenkapital, Beschäftigungszahl, Steuerzahlungen) haben mit dem Fremdvergleichsmaßstab nichts zu tun und können eher zu

126 *Seer*, Europäisierung des Steuerverfahrensrechts – Wege zu einem Steuerverwaltungsraum, HFSt Bd. 6, Heidelberg 2018, 191 (215).

127 *Drüen* in Tipke/Kruse, AO/FGO, § 138a AO Rz. 4 (Februar 2018).

Fehlschlüssen Anlass bieten[128]. Dementsprechend macht § 5 Abs. 2 Satz 3 und 4 MCAA 2 die folgende Verwendungseinschränkung:

„Die Informationen werden nicht als Ersatz für eine eingehende Verrechnungspreisanalyse einzelner Geschäftsvorfälle und Preise auf der Grundlage einer umfassenden Funktionsanalyse und einer umfassenden Vergleichbarkeitsanalyse verwendet werden. Es wird anerkannt, dass die Informationen im länderbezogenen Bericht für sich genommen keinen eindeutigen Nachweis für die Angemessenheit oder Nichtangemessenheit von Verrechnungspreisen darstellen und folglich Verrechnungspreiskorrekturen nicht auf dem länderbezogenen Bericht beruhen werden."

Vor diesem Hintergrund erscheint es doch sehr fraglich, ob die von § 5 Satz 2 MCAA 2 ins Feld geführten „wirtschaftlichen und statistischen Analysen" zu einer brauchbaren Risikoeinschätzung taugen, die den damit verbundenen Erfüllungsaufwand der betroffenen Unternehmen rechtfertigt. *Klaus-Dieter Drüen* macht mit Recht darauf aufmerksam, dass der fragwürdige Informationsgewinn der Finanzverwaltung mit den erheblichen Informations- und Beschaffungslasten der betroffenen Unternehmer in Relation zu setzen ist[129]. Hier drängt sich ein Missverhältnis geradezu auf.

V. Schlussbemerkungen und Ausblick

Die rasante Entwicklung der Informationstechnologie und des dadurch ermöglichten Austausches umfangreicher steuerrelevanter Daten zwischen den Finanzbehörden erhöht das Bedürfnis nach angemessenem Datenschutz. Mit der Einhegung der in der DSGVO enthaltenen Schutzrechte in einzelnen Vorschriften der AO ist es nicht getan. Vielmehr sind die Auskunfts- und Informationsrechte der betroffenen Bürger und Unternehmen zu stärken[130]. Transparenz kann nicht einseitig durch den „gläsernen Steuerbürger" geschaffen werden. Vielmehr bedarf es auch einer „gläsernen Finanzverwaltung", die offenbart, über welche Daten sie verfügt und was sie mit den vielen Daten eigentlich macht. Dies wird in nächster Zeit ein Betätigungsfeld des *Bundesbeauftragten für den Datenschutz und die Informationsfreiheit* sein, der nach § 32h AO nunmehr

128 So ausdrücklich die Reg. Begr. zum Entwurf eines Gesetzes zur Umsetzung der Änderungen der EU-Amtshilferichtlinie und von weiteren Maßnahmen gegen Gewinnkürzungen und -verlagerungen, BT-Drucks. 18/9536, 37.

129 *Drüen* in Tipke/Kruse, AO/FGO, § 138a AO Rz. 4 (Februar 2018).

130 Siehe dazu den Forderungskatalog des *Wiss. Arbeitskreises „Steuerrecht" des DWS-Instituts*, Recht auf Information und Auskunft im Besteuerungsverfahren, 2017, S. 51 ff.

die datenschutzrechtliche Aufsicht über die Finanzbehörden ausübt[131]. Zeigt sich die Finanzverwaltung auch in Zukunft weiterhin zugeknöpft, werden unweigerlich Beschwerden das BfDI erreichen. Ich denke, dass dann auch die Finanzgerichte, die für den gerichtlichen Rechtsschutz nach § 32i AO zuständig sind[132], gefragt sein werden.

131 Zu der Funktion des BfDI s. ausf. die Kommentierung von *Krumm* in Tipke/Kruse, § 32h AO (August 2018).

132 § 32i Abs. 1–3 AO enthält abdrängende Sonderzuweisungen zugunsten der FG, s. *Krumm* in Tipke/Kruse, § 32i AO Rz. 1 (August 2018).