DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins

zum Entwurf eines Gesetzes zur Neustrukturierung des Zollfahndungsdienstgesetzes (BT-Drucksache 19/12088)

Berlin, im November 2019

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Max Gröning
- Rechtsanwältin Uta Katharina Schmidt

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40, Boîte 7B
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
EU-Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit seinen über 63.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Der Entwurf eines Gesetzes zur Neustrukturierung des Zollfahndungsgesetzes[1] sieht eine umfassende Novellierung des Zollfahndungsdienstgesetzes vor. Der Schwerpunkt liegt in einer Neuausrichtung der datenschutzrechtlichen Bestimmungen sowie der Überarbeitung und Erweiterung der Ermittlungs- und Überwachungsbefugnisse.

Zu den neu eingeführten Befugnissen zählen insbesondere der Einsatz verdeckter Ermittler und Vertrauenspersonen, die sogenannte Quellen-Telekommunikationsüberwachung, die Erhebung von Nutzungsdaten i.S.v. § 15 TMG bei Diensteanbietern sowie erweiterte Auskunftspflichten im Rahmen der Befragung. Zudem wurden die Vorschriften zum (automatisierten) Datenaustausch mit anderen Behörden im In- und Ausland erweitert.

Der DAV sieht die Erweiterung grundrechtsintensiver Eingriffsbefugnisse im Gesetzesentwurf kritisch. Dies gilt insbesondere für die Einführung der Quellen-Telekommunikationsüberwachung in § 72 Abs. 3 und 4 ZFdG-E[2]. Angesichts der Rechtsprechung des EuGH zur Vorratsdatenspeicherung ist die Erhebung von Verkehrsdaten und nunmehr auch Nutzungsdaten indiskutabel. Kritisch bewertet der DAV auch die bußgeldbewährte Auskunftspflicht für die in § 55 StPO genannten Personen sowie den Einsatz von verdeckten Ermittlern und Vertrauenspersonen zur Gefahrenabwehr.

Die Vorschriften zur (automatisierten) Datenübermittlung lassen eine Ausrichtung an der Rechtsprechung des BVerfG zur Zweckbindung und Zweckänderung erkennen, sollten jedoch an einigen Stellen noch genauer bestimmte Voraussetzungen enthalten. Dies gilt auch vor dem Hintergrund des zunehmenden Gesamtumfanges von Datenerhebungsbefugnissen im Sicherheitsreicht bei gleichzeitig fortschreitender Digitalisierung aller Lebensbereiche und technischem Fortschritt in der Datenverarbeitung.

[1] Im Folgenden: Gesetzesentwurf.
[2] im Folgenden wird bei Normen aus dem Gesetzesentwurf auf die Bezeichnung ZFdG-E verzichtet.

Zu begrüßen ist die Ausgestaltung des Berufsgeheimnisträgerschutzes sowie grundsätzlich auch die Einbeziehung wichtiger Elemente zur Verbesserung des Datenschutzes und des effektiven Rechtsschutzes, welche zur Umsetzung der Vorgaben des Urteils des Bundesverfassungsgerichts zum BKAG[3] und der Richtlinie (EU) 2016/680 erfolgt. Die komplexe Struktur des Gesetzes erschwert allerdings die rechtssichere Anwendung und Rechtssicherheit bei Betroffenen.

Gesetzesstruktur

Die Gliederung des Gesetzesentwurfes erscheint insgesamt umständlich und komplex und wirft damit Fragen hinsichtlich der gebotenen Normenklarheit für Anwender und erst recht für Betroffene auf.

Das Kapitel 3 unterteilt sich zunächst in *Befugnisse des Zollkriminalamts* (Abschnitt 1), *Befugnisse der Behörden des Zollfahndungsdienstes (…)* (Abschnitt 2), *besondere Befugnisse des Zollkriminalamtes* (Abschnitt 3) und *Verfahrensregelungen* (Abschnitt 4).

In den Unterabschnitten erfolgt eine Unterteilung in *Datenverarbeitung* und *Datenübermittlung* durch die jeweiligen Behörden sowie allgemeine und besondere Maßnahmen. Diese Unterteilung wird jedoch nicht durchgehalten, sondern enthält zahlreiche inhaltliche Überschneidungen. Sodann werden allgemeine und besondere Maßnahmen in Abschnitt 2 weiter unterteilt in Unterabschnitte nach dem Zweck der Maßnahmen; etwa Gefahrenabwehr und Vorsorge für die künftige Verfolgung von Straftaten, Gefahrenabwehr, Strafverfolgung, Sicherungs- und Schutzmaßnahmen und Sicherung der Behörden des Zollfahndungsdienstes. Dadurch wird zwar eine Ausrichtung am Zweck der jeweiligen Maßnahme erreicht, allerdings kommt es insgesamt zu umfangreichen Doppelungen und Überschneidungen in den einzelnen Vorschriften. Die Bestimmungen zum Datenschutz ziehen sich entgegen der Gliederung durch alle Abschnitte des Gesetzes.

[3] Urteil des BVerfG vom 20.04.2016, Az. 1 BvR 966/09, 1 BvR 1140/09 (im Folgenden „Urteil zum BKAG“).

Der DAV empfiehlt eine stringentere Unterteilung der Befugnisse in die datenschutzrechtlichen Kategorien der Erhebung, Verarbeitung und Übermittlung. Regelungen zur Löschung könnten noch konsequenter vor die Klammer gezogen und vereinheitlicht werden.

Gesamtbetrachtung der Erweiterung der Befugnisse

Vor dem Hintergrund einer immer weiter fortschreitenden Digitalisierung aller Lebensbereiche, der stetigen Erweiterung von Datenerhebungsbefugnissen im gesamten Bereich des Sicherheitsrechts und einer zunehmenden – auch automatisierten - Verknüpfung von Datenbanken zwischen den Behörden auf Landes-, Bundes-, europäischer und internationaler Ebene steigt auch die Intensität der Grundrechtsbeeinträchtigung durch Datenerhebungen. Dies muss der Gesetzgeber nach der Rechtsprechung des Bundesverfassungsgerichts berücksichtigen, wenn er die Verhältnismäßigkeit von Überwachungsmaßnahmen abwägt:

> *„Dabei hat der Gesetzgeber in seine Abwägung auch die Entwicklung der Informationstechnik einzustellen, die die Reichweite von Überwachungsmaßnahmen zunehmend ausdehnt, ihre Durchführbarkeit erleichtert und Verknüpfungen erlaubt, die bis hin zur Erstellung von Persönlichkeitsprofilen reichen. Überwachungsmaßnahmen erhalten dadurch ein gesteigertes Eingriffsgewicht, dem in der Abwägung Rechnung zu tragen ist.“* [4]

Hinzu kommt, dass der Gesetzgeber die verfassungsrechtliche Zulässigkeit einzelner Überwachungsmaßnahmen nicht isoliert betrachten darf. Vielmehr muss er bei der Einführung neuer oder der Erweiterung bestehender Befugnisse das Wechselspiel und die Überschneidungen mit den bereits bestehenden Überwachungsbefugnissen im gesamten Recht der inneren Sicherheit beachten, worauf das Bundesverfassungsgericht ebenfalls hinweist:

> *„Beim Einsatz moderner, insbesondere dem Betroffenen verborgener Ermittlungsmethoden, müssen die Sicherheitsbehörden mit Rücksicht auf das dem ‚additiven‘ Grundrechtseingriff innewohnende Gefährdungspotenzial*

[4] Urteil des BVerfG vom 20.04.2016, Az. 1 BvR 966/09, Rn. 99.

koordinierend darauf Bedacht nehmen, dass das Ausmaß der Überwachung insgesamt beschränkt bleibt."[5]

Eine Auseinandersetzung mit dieser Problematik wäre geboten – führt man sich vor Augen, welche Befugnisse der Datenerhebung und der Datenübermittlung allein dem Zollfahndungsdienst nach dem Gesetzesentwurf in der Summe zustehen.

Ermittlungs- und Datenerhebungsbefugnisse

Unter jeweils näher eingegrenzten tatbestandlichen Voraussetzungen hat der Zollfahndungsdienst nach dem Gesetzesentwurf unter anderem folgende Ermittlungs- und Datenerhebungsbefugnisse:

- Befragung in Verbindung mit einer (bußgeldbewährten) Auskunftspflicht sowie Pflicht zur Herausgabe von geschäftlichen Unterlagen §§ 9, 29, 71
- Bestandsdatenauskunft, §§ 10, 30
- Sicherstellung, Verwahrung und Einziehung, §§ 40 ff.; 59
- Dursuchung von Personen und Sachen, §§ 44, 45, 56
- Betreten und Durchsuchen von Wohnungen, §§ 46, 60
- Längerfristige Observation, §§ 47 Abs. 2 Nr. 1, 62
- Verdeckte Bild- und Tonaufnahmen außerhalb von Wohnungen, § 47 Abs. 2 Nr. 2 lit. a) und b), § 62 Abs. 2
- Verdeckte Bild- und Tonaufnahmen innerhalb von Wohnungen, § 62 Abs. 2
- Einsatz von Vertrauenspersonen, § 47 Abs. 2 Nr. 3
- Einsatz von verdeckten Ermittlern, § 47 Abs. 2 Nr. 4 und Abs. 3
- Identitätsfeststellung, § 54
- Prüfung von mitzuführenden Dokumenten, § 55
- Erkennungsdienstliche Maßnahmen, § 57
- Überwachung der Telekommunikation sowie des Brief- oder Postverkehrs, § 72
- Sog. Quellen-Telekommunikationsüberwachung, §§ 72 Abs. 3
- Erhebung von Verkehrsdaten (§ 96 Abs. 1 TKG) und Nutzungsdaten (§ 15 Abs. 1 TMG), § 77
- Identifizierung und Lokalisierung von Mobilfunkkarten und –geräten, § 78
- Ermittlungsbefugnisse der StPO als Ermittlungspersonen der Staatsanwaltschaft, § 52

[5] aaO., Rn. 130.

Datenübermittlungen

Unter jeweils näher bestimmten Voraussetzungen können personenbezogene Daten – vielfach auch im automatisierten Verfahren – übermittelt werden unter anderem an:

- Behörden und sonstige öffentliche Stellen im Inland (§§ 21 Abs. 2, 65), darunter explizit auch das Bundeskriminalamt (§ 15 Abs. 2 Nr. 4), Strafverfolgungsbehörden (§ 76 Abs. 2), das Bundesamt für Wirtschafts- und Ausfuhrkontrolle (§ 76 Abs. 3), Verfassungsschutzbehörden des Bundes und der Länder, der Militärische Abschirmdienst (§ 76 Abs. 4) und der Bundesnachrichtendienst (§ 76 Abs. 5)
- nichtöffentliche Stellen im Inland, §§ 21 Abs. 6, 65
- öffentliche und nichtöffentliche Stellen in Mitgliedsstaaten der Europäischen Union, §§ 22 Abs. 1 Nr. 1, 66
- zwischen- und überstaatliche Stellen der Europäischen Union oder deren Mitgliedsstaaten, die mit Aufgaben der Verhütung und Verfolgung von Straftaten befasst sind, §§ 22 Abs. 1 Nr. 2, 66
- Polizeibehörden und zur Verhütung und Abwehr von Straftaten zuständige Stellen eines Schengen-assoziierten Staates, §§ 22 Abs. 2, 66
- Zoll-, Polizei- und Justizbehörden und sonstige für die Verhütung oder Verfolgung von Straftaten zuständige öffentliche Stellen in sonstigen Staaten, §§ 23 Abs. 1, 67
- entsprechende zwischen- und überstaatliche Stellen, §§ 23 Abs. 1, 67
- Hochschulen und andere Einrichtungen der wissenschaftlichen Forschung §§ 19, 37

Die Voraussetzungen an die Übermittlung sind im Gesetzesentwurf an der jeweiligen Stelle näher definiert. Die Anforderungen werden jedoch teilweise sehr allgemein gehalten. Oftmals reicht es, dass die Übermittlung „zur Erfüllung der Aufgaben erforderlich ist“, vgl. etwa §§ 21 Abs. 1; Abs. 2 S. 1 Nr. 2 a); § 23 Abs. 1 Nr. 1. Dies ist für sich genommen schon problematisch und erhöht nach dem zuvor Gesagten das Eingriffsgewicht der einzelnen Maßnahmen zur Datenerhebung. Vor diesem Hintergrund sieht der DAV die Einführung weiterer eingriffsintensiver Befugnisse im Gesetzesentwurf besonders kritisch. Im Einzelnen:

Befragungsrechte und (sanktionierte) Auskunftspflichten

In den §§ 9, 29 und 71 ist ein Befragungsrecht der Behörden des Zollfahndungsdienstes und eine damit korrespondierende Auskunftspflicht der befragten Personen vorgesehen. Für den Außenwirtschaftsverkehr wird die Auskunftspflicht in § 71 um eine Pflicht zur Herausgabe von zugehörigen geschäftlichen Unterlagen erweitert. Ähnliche Vorschriften finden sich etwa in § 52 BKAG oder in § 22 BPolG.

Gemäß § 9 Abs. 4 gilt § 136a StPO entsprechend. § 12 VwVG (unmittelbarer Zwang) findet keine Anwendung. Nach der Begründung des Gesetzesentwurfs soll aber § 11 VwVG anwendbar sein, so dass bei Nichtauskunft ein Zwangsgeld verhängt werden kann. Ferner soll die Nichterteilung gem. § 106 Abs. 1 Nr. 1 eine Ordnungswidrigkeit darstellen, die mit einem Bußgeld bis zwanzigtausend EUR sanktioniert werden kann.

Das Recht zur Auskunftsverweigerung nach §§ 52 bis 55 StPO soll gem. § 9 Abs.3, Satz 2 nicht gelten, soweit die Auskunft zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes oder Leib, Leben oder Freiheit einer Person erforderlich ist. Ausgenommen sind gem. § 9 Abs. 3 Satz 3 hiervon lediglich die in § 53 Abs. 1, Satz 1 Nr. 1 bis 3 oder Nr. 4 StPO genannten Berufsgeheimnisträger, wobei Nr. 3 nur für Rechtsanwälte und Kammerrechtsbeistände gilt. Dagegen gilt die „Rückausnahme“ des Satz 3 nicht für die Fälle der §§ 52 und 55 StPO.

Durch die sanktionierte Auskunftspflicht entsteht damit ein Wertungswiderspruch zu den Zeugnisverweigerungsrechten nach §§ 52 bis 55 StPO sowie zu §§ 138, 139 StGB[6]. Für nicht von der Rückausnahme erfasste Berufsgeheimnisträger steht die Auskunftspflicht zudem in einem schwer aufzulösenden Spannungsverhältnis zu 203 StGB. In Fällen des § 55 StPO liegt eine zwangsweise herbeigeführte Selbstbezichtigung vor, die verfassungsrechtlich nur zulässig ist, wenn sie mit einem strafrechtlichen Verwertungsverbot einhergeht.[7]

[6] So bereits DAV-Stellungnahem Nr. 49/2008 zur Einführung einer entsprechenden Vorschrift im BKAG.
[7] BVerfGE 56, 37 <50 f.

Quellen-Telekommunikationsüberwachung

In § 72 Abs. 3 wird dem Zollkriminalamt die Befugnis für die sogenannte Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) eingeräumt. Bislang enthält das ZFdG lediglich Befugnisse für die Überwachung und Aufzeichnung der Telekommunikation. Der Wortlaut des nunmehr vorgesehenen § 72 Abs. 3 ist identisch mit der Regelung zur Quellen-TKÜ in § 100a Abs. 1 StPO. § 75 Abs. 2 entspricht mit ebenfalls identischem Wortlaut der Regelung des 100a Abs. 5 StPO.

Der Deutsche Anwaltverein stand bereits der Einführung der Quellen-TKÜ in § 100a StPO sehr kritisch gegenüber[8]. Bedenken bestehen insoweit insbesondere hinsichtlich des weit gefassten Straftatenkataloges des 100a StPO, der eingesetzten Schadsoftware und der fehlenden Bestimmtheit der Norm. Problematisch sieht der DAV weiterhin die Abgrenzbarkeit der Quellen-TKÜ von der Onlinedurchsuchung, die wesentlich höheren verfassungsrechtlichen Anforderungen unterliegt. Schließlich hat der DAV auch Bedenken hinsichtlich der technischen Umsetzbarkeit und des Umgangs mit Sicherheitslücken.

Das Bundesverfassungsgericht hat auf die besonderen Risiken hingewiesen, die mit einer Quellen-TKÜ verbunden sind.[9] Mit der Infiltration des Systems sei die entscheidende Hürde gefallen, dass System insgesamt auszuspähen.[10] Diese Gefahren entstehen nicht nur durch das gezielte Auslesen des Systems durch Ermittlungsbehörden, sondern auch durch abstrakte Gefährdungen wie etwa der Nutzung von Sicherheitslücken im System durch die Behörden oder auch die Nutzung der Infiltration durch Dritte. Aufgrund des aus dieser Infiltration des informationstechnischen Systems folgenden intensiveren Eingriffs der Ermittlungsmaßnahme ist die Eingriffsschwelle für eine entsprechende Maßnahme deutlich höher anzusetzen als bei herkömmlichen TKÜ-Maßnahmen.[11] Dies folgt ohne weiteres schon aus der für den Gefahrenabwehrbereich getroffenen Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2008, nach der entsprechende Eingriffe nur zulässig sein sollen, wenn ein „überragend wichtiges Rechtsgut“ betroffen ist[12], wobei

[8] Vergleiche DAV-Stellungnahme Nr. 44/2017.
[9] vgl. BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07, Rn. 187/188.
[10] vgl. BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07, Rn. 188.
[11] vgl. Stellungnahme der Bundesdatenschutzbeauftragten Voßhoff v. 29.05.17, S. 3.
[12] vgl. BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07, Rn. 242.

zugleich festgestellt wurde, dass entsprechende Maßnahmen verfassungsrechtlich bedenklich sind, wenn sie zum Schutz*„sonstiger Rechtsgüter Einzelner oder der Allgemeinheit in Situationen, in denen eine existenzielle Bedrohungslage nicht besteht“* eingesetzt werden.[13]

Nach alledem bestehen Vorbehalte auch gegenüber der Einführung der Regelung im ZFdG-E. Zwar beschränkt sich der Einsatz auf die in § 72 Abs. 1,2 und 4 ausgeführten Fälle, die im Wesentlichen im Kontext der Kriegswaffenkontrolle stehen und damit dem Schutz überragend wichtige Rechtsgüter dienen.

Soweit mit dem neu eingeführten § 72 Abs. 2 Nr. 5 lit. c) jedoch auch solche Gütergruppen erfasst sind, deren Verwendung einen erheblichen Nachteil für die auswärtigen Beziehungen herbeiführen könnte, erscheint die Voraussetzungen einer existenziellen Bedrohungslage nicht erfüllt. Darüber hinaus soll die Quellen-TKÜ gem. § 72 Abs. 4 auch gegenüber Dritten zum Einsatz kommen können. Die einmal erhobenen Daten können im Anschluss gemäß § 76 Abs. 2 auch zur Verfolgung der in 100a Abs. 2 genannten Straftaten übermittelt werden.

Nach der Entscheidung des Bundesverfassungsgerichts aus dem Jahr 2008 ist beim Einsatz einer Schadsoftware zum Zwecke der Quellen-TKÜ durch „technische Vorkehrungen und rechtliche Vorgaben“ sicherzustellen, dass „sich die Überwachung ausschließlich auf Daten aus einem laufenden Telekommunikationsvorgang beschränkt“.[14] Hier sollte sich der Gesetzestext nicht lediglich darauf beschränken, die Urteilsgründe wiederzugeben, sondern zu erkennen geben, wie die technischen Vorkehrungen eingehalten und überprüft werden sollen.

Erhebung von Verkehrs- und Nutzungsdaten

Vor dem Hintergrund der Rechtsprechung des EuGH zur Vorratsdatenspeicherung ist unverständlich, dass die bisherige Regelung zur Erhebung von Verkehrsdaten in das neue Gesetz übernommen und sogar noch um die Erhebung von Nutzungsdaten ergänzt werden soll. Gemäß § 77 soll das Zollkriminalamt unter den Voraussetzungen

[13] BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07, Rn. 248.
[14] BVerfG, Beschluss v. 30.08.2007, 1 BvR 370/07 und 595/07, Rn. 190.

des § 72 Abs. 1, 2 und 4 zur Erhebung von Verkehrsdaten (§ 96 Abs. 1 TKG) und Nutzungsdaten (§ 15 Abs. 1 TMG) bei Anbietern von Telekommunikationsdiensten berechtigt sein. Sofern Verkehrs- und Nutzungsdaten für die Vergangenheit abgefragt werden, ist darin eine unzulässige Vorratsdatenspeicherung zu sehen[15].

Der EuGH hat bekanntermaßen entschieden, dass eine allgemeine und unterschiedslose Vorratsdatenspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und registrierten Nutzer in Bezug auf alle elektronischen Daten für Zwecke der Bekämpfung von Straftaten gegen Art.7, 8 und 11 sowie des Art. 52 Abs. 1 Grundrechtecharta verstößt[16].

Unabhängig davon, inwiefern Speicherpflichten für bestimmte Verkehrsdaten etwa nach § 113b TKG noch bestehen[17], widerspricht die Regelung des § 77 der klaren Wertung des EuGH. Es macht keinen Unterscheid, auf welcher rechtlichen Grundlage die Speicherung erfolgte. Sofern die Daten beim Diensteanbieter noch vorhanden sind, läuft es in beiden Fällen darauf hinaus, dass verdachtsunabhängig und flächendeckend Daten gespeichert und ggf. durch Ermittlungsbehörden abgefragt werden.

Verdeckte Ermittler und Vertrauenspersonen

Mit § 47 Abs. 2 Nr. 3 und 4 sollen der Einsatz von verdeckten Ermittlern und Vertrauenspersonen zur Verhütung von Straftaten eingesetzt werden können. Die Voraussetzungen hierfür finden sich in § 47 Abs. 1 und setzen voraus, dass „bestimmte Tatsachen die Annahme rechtfertigen, dass [die betroffene Person] innerhalb eines übersehbaren Zeitraums auf eine zumindest ihrer Art nach konkretisierte Weise eine Straftat von erheblicher Bedeutung im Zuständigkeitsbereich der Zollverwaltung gewerbs-, gewohnheits- oder bandenmäßig begehen wird“. Unter den Voraussetzungen des Abs. 1 Nr. 2 kann die Maßnahme auch gegen Dritte Personen erfolgen. Der Einsatz von Vertrauenspersonen und verdeckten Ermittlern zur Gefahrenabwehr ist ohnehin

[15] So auch schon DAV-Stellungnahme Nr. 33/2017 zur Erhebung von Telekommunikationsverkehrsdaten und Nutzungsdaten gem. § 52 BKAG.
[16] Urteil des EuGH vom 21.12.2016 (C-203/15) - Tele2 Sverige.
[17] Nach dem o.g. Urteil des EuGH und dem Beschluss des OVG NRW vom 22.06.2017, Az. 13 B 238/17 sieht die Bundesnetzagentur derzeit davon ab, die Speicherpflicht durchzusetzen. Gegen § 113b sind verschiedene Verfassungsbeschwerden anhängig; vgl. zu alledem auch DAV-Stellungnahme Nr.: 24/2018.

erheblichen Bedenken ausgesetzt [18] und ist unter den weit gefassten tatbestandlichen Voraussetzungen des § 47 unangemessen.

Datenschutz und Rechtsschutz

Zu begrüßen sind die in Umsetzung des Urteils zum BKAG und der Richtlinie (EU) 2016/680 implementierten Schutzvorkehrungen wie die Kennzeichnung von eingriffsintensiv erhobenen Daten, Kontrollen des oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, die Benennung eines Datenschutzbeauftragten Protokollierung, Dokumentation Benachrichtigungspflichten und die Erstellung eines Verzeichnisses, auf die jedoch hier im Einzelnen nicht näher eingegangen werden soll. Wünschenswert wäre im Sinne einer rechtssicheren Anwendung, die Vorschriften insbesondere zur Löschung noch weiter zu vereinheitlichen.

Schutz von Berufsgeheimnisträgern

Positiv hervorzuheben ist aus Sicht des DAV der Schutz des Berufsgeheimnisses in § 82 sowie in § 9 Abs. 3, der in konsequenter Umsetzung des BKAG-Urteils des Bundesverfassungsgerichts die Unterscheidung zwischen Strafverteidigern und sonstigen Rechtsanwälten aufhebt. Für Rechtsanwältinnen und Rechtsanwälte und weitere Berufsgeheimnisträger wird ein einheitliches und nicht abwägbares Schutzniveau etabliert und damit dem Kernbereichsbezug der jeweiligen Vertrauensverhältnisse Rechnung getragen.

[18] Vgl. Ergänzende Stellungnahme zum Entwurf eines Gesetzes zum besseren Informationsaustausch bei der Bekämpfung des internationalen Terrorismus durch den Hamburgischen Beauftragten für Datenschutz und Informationssicherheit vom 23. Juni 2016.