Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)187 G

Ass. jur. Kirsten Bock

info@kirsten-bock.de
www.kirsten-bock.de

Deutscher Bundestag
Ausschuss für Inneres und Heimat
Platz der Republik 1
11011 Berlin
Per E-Mail an: innenausschuss@bundestag.de

08. Dezember 2018

Stellungnahme zum Gesetzentwurf der Bundesregierung,
Entwurf eines Zweiten Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680
(Zweites Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU)
vom 01.10.2018

Vorgelegt zur Anhörung des Ausschusses für Inneres und Heimat des Deutschen Bundestages am 10. Dezember 2018 in Berlin

Sehr geehrte Frau Ausschussvorsitzende Lindholz,
Sehr geehrte Damen und Herren,

ich bedanke mich für die Einladung zur Anhörung und für die Gelegenheit zur Stellungnahme. In Anbetracht des Umfangs des vorgelegten Gesetzentwurfes beschränkt sich meine Stellungnahme auf einige ausgewählte Punkte und Aspekte des Entwurfs zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DSGVO) und zur Umsetzung der Richtlinie (EU) 2016/680 (JI-RL). Im Folgenden nehme ich zunächst in einer Gesamtschau zu dem umfassenden Entwurf Stellung (A), betrachte sodann ausgewählte Aspekte und Regelungsbereiche (B) und wende mich abschließend einzelnen Artikeln des vorliegenden Gesetzentwurfs zu (C).

A. Gesamtschau des Entwurfs

Die europäische Datenschutzgrundverordnung ist angetreten mit dem Ziel einer Vereinheitlichung des europäischen Rechtsrahmens im Bereich des Datenschutzes in den Mitgliedstaaten der Union. Die technische Entwicklung und deren Durchdringung des Lebensalltags sowie eine weltumspannende informationstechnische Vernetzung stellen auch das Recht und den grundrechtlich zu gewährenden Schutz natürlicher Personen vor wachsende Herausforderungen. Ziel der DSGVO ist es durch einen „soliden, kohärenteren und klar durchsetzbaren Rechtsrahmen“ mehr „Sicherheit in rechtlicher und praktischer Hinsicht“ und Vertrauen für Bürgerinnen und Bürger, die Wirtschaft und den Staat zu schaffen.[1] Ein solches Ziel ist aber nur zu erreichen, wenn bei den durch die DSGVO vorgesehenen Öffnungen, Präzisierungen oder Einschränkungen ihrer Vorschriften durch das nationale Recht, die Mitgliedstaaten die DSGVO behutsam und sorgfältig in ihr nationales Recht aufnehmen, um die „nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen.“[2]

Mit dem vorgelegten Gesetzentwurf wird sich diesem Ziel nicht genähert. Auch das 2.Umsetzungs- und Anpassungsgesetz (2. DSAnpUG-EU) verfehlt das Ziel, das Datenschutzrecht übersichtlicher und für die von ihm betroffenen Personen und Rechtsanwender verständlicher zu machen. Statt auch im bereichsspezifischen Recht auf die

[1] S. DSGVO, EWG 7.
[2] S. DSGVO, EWG 8.

DSGVO oder das BDSG zu verweisen, werden wiederum zahlreiche neue und abweichende Regelungen geschaffen, die in vielen Fällen den Anforderungen, wie sie in der DSGVO z.B.

- für Art. 6 Abs. 1 UAbs. 1 lit. c und e in Art. 6 Abs. 2 und 3 DSGVO,
- in Art. 9 Abs. 2 lit. g und Abs. 4 DSGVO sowie
- in Art. 23 DSGVO

bestimmt sind, nicht genügen. Ein Beispiel bildet etwa Art. 8 des Entwurfs, mit dem das BDBOS-Gesetz geändert wird. So erlauben die Vorgaben aus Art. 6 Abs. 2 und 3 DSGVO nur „spezifischere Bestimmungen“, die im Ergebnis die Verarbeitungsbefugnisse einschränken, aber nicht erweitern. Die Bundesregierung verpasst damit erneut eine Chance, an die Vorreiterrolle, die Deutschland im Datenschutzrecht innehatte, anzuknüpfen. Dabei bestanden schon vor Gültigkeitsbeginn der DSGVO in einigen Landesgesetzen gute Ansätze dafür, europäische Grundsätze aus der Richtlinie 95/46/EG, z.B. zu den technischen und organisatorischen Maßnahmen, die von der DSGVO übernommen wurden, weiter zu präzisieren und für den Rechtsanwender in der Praxis handhabbarer zu machen (s. dazu unter B.). Auch die vielfältigen Einschränkungen der Betroffenenrechte der Art. 12 bis 18 DSGVO dienen nicht dem angestrebten Ziel der Vertrauensbildung. Die Schaffung weiterer Rechtsgrundlagen wäre nur dann zu begrüßen, wenn die Anforderungen an gute Gesetzgebungspraxis erfüllt und alles Wesentliche in die Regelungen aufgenommen würde. Dazu gehört in allen Varianten des Art. 6 Abs. 1 DSGVO eine hinreichend konkrete Festlegung der Zwecke und eine Präzisierung der öffentlichen Interessen, um sowohl dem Anwender als auch den betroffenen Personen die Erforderlichkeit der Verarbeitung deutlich und nachvollziehbar zu machen. Gerade für den Bereich der öffentlichen Stellen erleichtern klare Rechtsgrundlagen die Verwaltungspraxis und können über geeignete Once Only-Verfahren für mehr Bürgerfreundlichkeit der Verwaltung sorgen, ohne dass dabei die Rechte der betroffenen Personen eingeschränkt werden müssen.

Über das 2. DSAnpUG-EU hinaus bestehen weiterhin Möglichkeiten und Regelungsbedarf für die Bereiche des Beschäftigtendatenschutz über Art. 88 DSGVO sowie für die Ausübung der Meinungsfreiheit über Art. 85 DSGVO (dazu s. u. C.).

B. Stellungnahme zu einzelnen Grundsatzfragen des Entwurfs

Die **Zweckbindung** folgt unmittelbar aus dem Grundrecht auf Schutz personenbezogener Daten (Art. 8 EU-Grundrechte-Charta). Sie ist ein zentraler Grundsatz für die Rechtmäßigkeit der Datenverarbeitung. Aus der Logik des Datenschutzrechts wird unmittelbar das ihm zugrunde liegenden Verbots mit Regelungsvorbehalt abgeleitet, demzufolge für einen bestimmten Zweck erhobene Daten nicht nach Belieben, sondern nur unter sehr engen, den Voraussetzungen des Art. 6 Abs. 4 DSGVO unterliegenden Bedingungen, weiterverarbeitet werden dürfen. Denn jede Verarbeitung zu einem neuen Zweck berührt den Schutzbereich und stellt damit einen (weiteren) Grundrechtseingriff dar, den es für sich zu rechtfertigen gilt. Dazu bedarf es jeweils einer eindeutigen Rechtsgrundlage. Der Kanon möglicher Rechtsgrundlagen wird in Art. 6 Abs. 1 DSGVO abschließend aufgezeigt. Die in Art. 6 Abs. 2 bis 4 DSGVO bestimmten Anforderungen entsprechen dem grundgesetzlichen Bestimmtheitsgebot. Eine pauschale Verweisung auf die Aufgaben eines Verantwortlichen genügt diesen Anforderungen nicht. Auch allgemein formulierte Zwecke, wie „öffentliches Interesse“ sind unzureichend. Zwar sei dem Bundesgesetzgeber nicht empfohlen, das Datenschutzrecht weiter durch sich wiederholende Regelungen in zahlreichen Rechtsgebieten zu zerfasern, sondern auf die DSGVO und das BDSG zu verweisen. Jedoch besteht im Bereich möglicher Zweckänderungen ein konkreter Reglungsbedarf, um den Anforderungen an die Bestimmtheit zu genügen, den der Gesetzentwurf nicht erfüllt.

An vielen Stellen erfolgt eine sprachliche Anpassung an den **Verarbeitungsbegriff** aus Art. 4 Abs. 2 DSGVO, wobei überwiegend die Begriffe „erheben, verarbeiten und nutzen“ durch den Begriff „verarbeiten“ ersetzt werden. Dabei ist zu bedenken, dass der bislang im BDSG a.F. verwendete Begriff der Verarbeitung nicht mit dem Verarbeitungsbegriff der DSGVO identisch ist. Zwar enthält Art. 4 Abs. 2 DSGVO keine echte Definition der Verarbeitung, sondern beschreibt beispielhaft Vorgänge oder Vorgangsreihen, die im Zusammenhang mit personenbezogenen Daten ausgeführt werden. Die Art der Beispiele macht aber deutlich, dass der gesamte Lebenszyklus einer personenbezogenen Information erfasst werden soll: vom Erheben über das Verändern bis zum Löschen oder Anonymisieren (Entketten von Informationsbezügen). Abweichungen ergeben sich damit in den Bereichen des Rechts, in denen der Verarbeitungsbegriff des § 3 Abs. 4 BDSG a.F. erhalten bleibt bzw. (noch) nicht geändert wurde. Dies hat besondere Auswirkungen auf Erlaubnisnormen, bei denen

nunmehr auch die Erhebung und Nutzung erfasst wird und damit der Erlaubnistatbestand erweitert wird. Regelungen mit verarbeitungsbeschränkendem Charakter trifft das gegenteilige Schicksal. Soweit nur bestimmte Formen der Verarbeitung geregelt werden sollen, ist dies kenntlich zu machen und es kann nicht auf den allgemeinen Verarbeitungsbegriff zurückgegriffen werden, wie dies beispielsweise in Art. 2 Nr. 1 des Entwurfs (Änderung des Gesetzes zur Regelung von Vermögensfragen der Sozialversicherung im Beitrittsgebiet) erfolgt. Dort werden die Wörter „verarbeiten und nutzen“ durch die Wörter „speichern, verändern, nutzen, übermitteln oder in der Verarbeitung einschränken“ gleichsam „rückübersetzt“. Erfolgt eine solche Anpassung nicht, verändert sich der erfasste Gegenstandsbereich einer Regelung.

In vielen Artikeln des Entwurfs zum 2. DSAnpUG-EU wird auf „**technische und organisatorische Maßnahmen**“ nach den „Artikeln 24, 25 und 32“ der DSGVO verwiesen, z.B. in Art. 49 Nr. 9, 18, Art. 96 Nr. 2, Art. 105 Nr. 3, Art. 107 Nr. 1, Art. 123 Nr. 19, Art 153 Nr. 6 c. Hervorzuheben ist hierbei, dass eine Zusammenführung der Art. 24, 25 und 32 DSGVO insoweit sinnvoll erscheint, als die Regelungen sich komplementär ergänzen und stets nebeneinander Anwendung finden. Während Art. 24 DSGVO primär auf organisatorische Maßnahmen Bezug nimmt (sog. Compliance Management) und Art. 32 DSGVO die eigentliche Verarbeitung regelt (Sicherheit der Verarbeitung), zielt Art. 25 Abs. 1 DSGVO auch auf das Stadium vor Anwendbarkeit der DSGVO (Vorbereitung der Verarbeitung) und bezieht dieses Stadium *ex tunc* in den Anwendungsbereich der DSGVO (Verarbeitung personenbezogener Daten) ein und konkretisiert dies für die zu treffenden Voreinstellungen in Art. 25 Abs. 2 DSGVO. Gleichwohl mangelt es in Art. 32 DSGVO an systematischer Klarheit. Hier hätte der Entwurf aufbauend auf den ehemals bestehenden Regelungen zu den Schutzzielen des Datenschutzes in den Datenschutzgesetzen der Länder[3] den Rechtsanwendern vor allem für die „Übersetzung“ der rechtlichen Regelungen der DSGVO in informationstechnische Anwendungen präzisierende Hilfestellungen leisten können.

Die **Verarbeitung besonderer Kategorien** personenbezogener Daten, wie etwa von Gesundheitsdaten (Allergiker*in, Brillenträger*in), stellt nicht in jedem Fall für die

[3] S. § 5 Schleswig-Holsteinisches Gesetz zum Schutz personenbezogener Informationen vom 9. Februar 2000, GVOBl. Schl.-H. S. 169.

betroffenen Personen einen besonders schweren Grundrechtseingriff dar. Jedoch können Verarbeitungen solcher Kategorien, wie sie z.B. in Art. 12 Nr. 8 des Entwurfs zur Änderung des Bundesdatenschutzgesetzes, in Art. 91 Nr. 4 zur Änderung des Kreditwesengesetzes oder in Art. 88 Nr. 5 lit c zur Änderung des Strahlenschutzgesetzes vorgesehen sind, typischerweise zu besonders erheblichen Folgen für die betroffenen Personen führen, die bei ihrer erstmaligen Verarbeitung nicht ohne Weiteres absehbar sind. So kann beispielsweise die Erhebung eines biometrischen Fingerabdrucks im Rahmen einer späteren Forschungsarbeit zu nachteiligen Feststellungen führen, die zum Zeitpunkt der erstmaligen Verarbeitung noch nicht denkbar waren. Die Verarbeitung der Mitgliedschaft in einer Partei oder einer Religionsgemeinschaft, kann z.B. nach einem Regierungswechsel zu Verfolgung oder zu Repressalien führen. Wesensmerkmal dieser Kategorien ist zudem, dass ein Wechsel oder eine Veränderung der Merkmale für die betroffene Person nur schwer bzw. unmöglich sind. Wird beispielsweise der Fingerabdruck gefälscht und gerät dadurch in polizeiliche Dateien, so kann die betroffene Person sich dessen nicht in zumutbarer Weise entledigen oder diesen ändern. Die Verarbeitung besonderer Kategorien der Verarbeitung soll daher nur unter besonderen Vorkehrungen erfolgen. Art. 9 Abs. 2 lit g DSGVO verlangt für gesetzliche Grundlagen insoweit, dass

- für die Regelung ein erhebliches öffentliches Interesse besteht,
- die Regelung der Verarbeitung in einem angemessenen Verhältnis zu dem verfolgten Ziel steht,
- der Wesensgehalt des Rechts auf Datenschutz gewahrt wird und
- angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Personen

vorgesehen werden. Dazu ist zunächst das erhebliche öffentliche Interesse zu konkretisieren bzw. zu begründen. Ein allgemeiner Verweis auf ein erhebliches öffentliches Interesse wie in Art. 12 Nr. 7 a des Entwurfs zur Änderung des § 22 Abs. 1 Nr. 1 lit. d BDSG, das dann bei der Anwendung zu bestimmen ist, reicht dafür nicht aus. I.d.R. wird ebenso ein bloßer Verweis auf eine gesetzliche Aufgabenerfüllung zur Begründung, wie in Art. 1 Nr. 1 des Entwurfs zur Änderung von § 31 S. 2 Staatsangehörigkeitsgesetz, nicht ausreichen. Nur durch die Konkretisierung kann dann auch beurteilt werden, ob die Regelung in einem angemessenen Verhältnis zum angestrebten Ziel steht. Das erhebliche öffentliche Interesse an der

Verarbeitung darf nicht zu Verarbeitungserlaubnissen führen, durch die der Wesensgehalt des Grundrechts auf Datenschutz berührt wird.[4] Dies ist immer dann der Fall, wenn eine Regelung eine unbegrenzte Erhebung oder Speicherung oder andere Verarbeitung zulässt oder die betroffenen Personen in einem Lebensbereich einer uneingeschränkten Beobachtung ausgeliefert[5] wird, wie es beispielsweise der Entwurf für das BSI-Gesetz vorsieht (s.u.). Die zu treffenden spezifischen Maßnahmen sind entweder direkt gesetzlich festzulegen, s. etwa in Ansätzen Art. 16 Nr. 9 c des Entwurfs, oder mit Verweis auf die Schutzziele des Datenschutzes[6] zur

- Vertraulichkeit, Integrität, Verfügbarkeit,
- Nichtverkettung (zur Umsetzung der Zweckbindung)
- Intervenierbarkeit (Kontrollfähigkeit und Rechte der Betroffenen) sowie
- Transparenz der Verarbeitung

und den umzusetzenden Schutzbedarf (z.B. normal, hoch oder sehr hoch) zur Gewährleistung der Rechte natürlicher Personen zu konkretisieren. Auch solche Festlegungen lässt der Entwurf vermissen.

Erfolgt ein **Ausschluss des Auskunftsrechts** nach Art. 15 DSGVO, müssen gem. Art. 23 DSGVO besondere Gründe dargelegt werden. Mit dem Ausschluss wird das Recht auf Kenntnis des Verarbeiters und den Umständen der Verarbeitung einschränkt. Erfolgt dies bereits „wenn die Auskunftserteilung die ordnungsgemäße Aufgabenerfüllung gefährden würde“, wie z.B. in Art. 13 zur Änderung des BSI-Gesetzes, so bleibt dies hinter den Art. 23 Abs. 1 DSGVO benannten Gründen zurück. Dieser Maßstab ist offensichtlich so niedrig, und im Hinblick auf die oft weitreichenden oder unklar beschriebenen gesetzlichen Aufgaben, dass es nicht nur für den Betroffenen, sondern auch für die Verantwortlichen und nicht zuletzt die Datenschutzaufsichtsbehörden, schwer ist, die Voraussetzungen zu prüfen.

[4] EuGH Urt. v. 06.10.2015 (Schrems), NJW 2015, 3151, 3157.
[5] S. dazu Bock/Engeler, DVBL 2016, 593.
[6] S. Bock/Meissner, DuD 2012, 425ff; Robrahn/Bock, DuD 2018, 7ff.

C. Stellungnahme zu einzelnen Änderungen

Zu Art. 1: Änderung des Staatsangehörigkeitsgesetzes

Nach Art. 1 Nr. 3 b des Entwurfs zu § 33 Abs. 4 S. 3 zur Änderung des Staatsangehörigkeitsgesetzes soll eine Übermittlung auch dann zulässig sein, „wenn das wissenschaftliche Interesse an der Durchführung des Forschungsvorhabens das Interesse der betroffenen Person an dem Ausschluss der Verarbeitung erheblich überwiegt." Diese Regelung widerspricht dem Grundsatz der Datenminimierung aus Art. 5 Abs. 1 lit. d DSGVO und erweitert die Übermittlungsbefugnisse. Art. 89 Abs. 1 DSGVO verlangt für wissenschaftliche und historische Forschungszwecke geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen durch technische und organisatorische Maßnahmen. Auch bei wissenschaftlichem Interesse sollte daher im Regelfall eine Übermittlung durch Maßnahmen der Pseudonymisierung abgesichert werden, wenn eine Anonymisierung nicht möglich ist. Insoweit könnte der Entwurf für § 33 Abs. 4 S. 3 auf § 22 Abs. 2 BDSG verweisen.

Zu Art. 5: Änderung des Rechtsextremismus-Datei-Gesetzes

Die Änderung in Nr. 7 zu § 13 enthält eine Änderung der Überschrift. Das Wort „Errichtungsanordnung" wird durch die Wörter „Festlegungen für die gemeinsame Datei" ersetzt, mit der auf das Vorliegen einer gemeinsamen Verantwortlichkeit bei dem Betrieb einer gemeinsamen Datei hingewiesen wird, ohne aber materiell rechtlich auf die für das deutsche Datenschutzrecht neue gemeinsame Verantwortlichkeit, Art. 3 Nr. 8 RL (EU) 2016/680, einzugehen. Zwar regelt § 9 RED-G die datenschutzrechtliche Verantwortlichkeit für die Erhebung und „Pflege", für die Errichtung und den Betrieb einer gemeinsamen Datei sind diese Regelungen jedoch nicht hinreichend. Ein gemeinsamer Betrieb erfordert besondere Garantien, die sicherstellen, dass technische und organisatorische Maßnahmen bestehen, die in § 13 RED-G Erwähnung finden. Ein Verweis auf § 10 RED-G allein, wird hierfür nicht genügen, es sei denn, die spezifischen Anforderungen werden in einem neuen § 10 Abs. 4 aufgenommen. Alternativ könnte ein Verweis auf die Anforderungen an die Sicherheit der Datenverarbeitung nach § 64 BDSG und das Verzeichnis von Verarbeitungstätigkeiten nach § 70 BDSG erfolgen mit einer Ergänzung der Besonderheiten einer gemeinsamen Verantwortlichkeit. Für das Verzeichnis der Verarbeitungstätigkeiten sollten über den § 70 Abs. 1 BDSG hinaus die zwingenden Angaben zur gemeinsamen

Verantwortlichkeit einschließlich eines Rollen- und Berechtigungskonzeptes sowie deren Detaillierungsgrad festgelegt werden.

Zu Art. 8: Änderung des BDBOS-Gesetzes

Der Entwurf zu § 19 Abs. 2 erlaubt Verkehrsdaten bei Vorliegen tatsächlicher Anhaltspunkte für eine rechtswidrige Inanspruchnahme von Verkehrsdaten zu verarbeiten, „soweit dies erforderlich ist, um die rechtswidrige Inanspruchnahme des Digitalfunk BOS festzustellen und zu unterbinden“. Im Hinblick auf die Nichtöffentlichkeit des Dienstes erscheint diese weitreichende Verarbeitungserlaubnis nicht in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck zu stehen. Zumindest erscheint eine Einschränkung geboten, die eine rechtwidrige Inanspruchnahme auf für den Betrieb und die Sicherstellung des Betriebs relevante Inanspruchnahmen beschränkt.

Der Entwurf zu § 19 Abs. 3 eröffnet eine Zweckänderung und damit quasi eine unbegrenzte Speicherung von Verkehrsdaten zur Weiterentwicklung des Digitalfunks BOS. Die Regelung ist selbst bei Zugrundelegung eines hohen Schutzbedarfs für ein kritische Infrastruktur unverhältnismäßig und genügt zudem nicht den Bestimmtheitsanforderungen.

Eine Speicherung über 75 Tage, wie sie der Entwurf zu § 19 Abs. 4 vorsieht, geht über die allgemein schon weitreichende Vorratsdatenspeicherung von 70 Tagen hinaus, an der ihrerseits bereits erhebliche Zweifel im Hinblick auf die Verhältnismäßigkeit bestehen.[7] Zwar ist zu begrüßen, dass die Einholung einer Einwilligung verworfen wird, die zu Recht weder als praktikabel noch im Hinblick auf die Konkretisierung der Zwecke als möglich betrachtet werden muss. Eine Speicherung von Verkehrsdaten sollte entsprechend dem Grundsatz der Datenminimierung nur soweit erfolgen, wie dies für den Betrieb einschließlich der Störungsbeseitigung erforderlich ist.

Der Entwurf wie auch die Gesetzesbegründung lassen des Weiteren eine Auseinandersetzung mit den Interessen der betroffenen Personen vermissen.

Zu Art. 11: Änderung des Bundesbeamtengesetzes

Die Auslagerung von Personalakten im öffentlichen Bereich stellt für den Staat und seine Beamten und Beamtinnen einen besonders sensiblen Bereich dar. Bei der Zulässigkeit der

[7] BVerfG 1 BvR 141/16.

Verarbeitung von Personalaktendaten im Auftrag in § 111a (Art. 11 Nr. 8 des Entwurfs) sollte daher ein Abs. 3 angefügt werden, der beim Verarbeiter besonders zu garantierende technische und organisatorische Maßnahmen zur Gewährleistung der Vertraulichkeit, Verfügbarkeit, Intervenierbarkeit zur Umsetzung der Rechte der Betroffenen und des Verantwortlichen, der Nichtverkettung (Zweckbindung, Mandantenfähigkeit) und Integrität vorsieht. Bei der Auswahl eines Verarbeiters ist dabei, wie stets im öffentlichen Bereich, sicherzustellen, dass dieser keinen Zugriffsrechten durch Geheimdienste oder anderen, in Drittstaaten belegenen, Stellen ausgesetzt ist.[8]

Zu Art. 12 Änderung des Bundesdatenschutzgesetzes

Die vorgesehenen Änderungen des Bundesdatenschutzgesetzes sind im Hinblick auf den Korrekturbedarf, der sich durch das 1. DSAnpUG-EU bspw. durch die Einschränkung der Rechte der betroffenen Personen bei der Videoüberwachung im öffentlichen Raum (§ 4 BDSG), den Rechten der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten (§ 29 Abs. 1 BDSG) sowie beim Recht auf Löschung (§ 35 Abs. 1 BDSG) ergibt, zurückhaltend geblieben. Auch die Einschnitte bei den Rechten der Betroffenen (§§ 32 ff. BDSG) bleiben bestehen. Hier sollte die Gelegenheit genutzt werden, auf die Ausnahmen zu verzichten, aber zumindest die Regelungen zu konkretisieren und damit in Übereinstimmung mit den Anforderungen aus Art. 23 Abs. 2 DSGVO zu bringen.

Zu Nr. 4: § 9 BDSG

Durch den Verweis auf § 115 Abs. 4 Telekommunikationsgesetz (TKG) bleibt es nach wie vor unklar, ob dieser Bestand haben soll. Zwar lässt auch die Gesetzesbegründung erkennen, dass „Bereiche“ des TKG, durch die DSGVO unmittelbar geregelt werden und diese aus dem TKG gestrichen würden, inwieweit davon aber der Regelungsgehalt des § 115 Abs. 4 TKG erfasst wird, bleibt durch den Verweis in dem Entwurf für § 9 Abs. 1 S. 1 BDSG unklar. Es sollte klargestellt werden, dass die Zuständigkeit bei der oder dem Bundesbeauftragten liegt, der Verweis auf § 114 Abs. 4 TKG erscheint zumindest zum gegenwärtigen Zeitpunkt überflüssig.

[8] Vgl. EuGH Urt. v. 06.10.2015 (Schrems), NJW 2015, 3151, 3157.

Zu Nr. 7. a) cc): § 22 Abs. 1 lit. d

Die Regelung genügt den Anforderungen des Art. 9 Abs. 2 lit. g DGSVO nicht. Mit dem Wechsel aus der Nr. 2 in die Nr. 1 wird die Verarbeitung aufgrund eines zwingenden erheblichen öffentlichen Interesses nunmehr auch für nichtöffentliche Stellen eröffnet. Mit der Regelung wird über den Verweis in § 24 Abs. 2 BDSG für nichtöffentliche Stellen eine Übermittlungsbefugnis von besonderen Kategorien personenbezogener Daten zu anderen Zwecken geschaffen. Dabei bleibt unklar, ob § 22 Abs. 2 BDSG Anwendung findet, da § 24 Abs. 2 lediglich auf den Ausnahmetatbestand verweist. Eine Anwendung ist auch schon deswegen notwendig, um sicherzustellen, dass die erforderlichen, angemessenen und spezifischen Maßnahmen für die Verarbeitung im Sinne des Art. 9 Abs. 2 lit g DSGVO, bei den nichtöffentlichen Stellen getroffen werden.

Zu Nr. 8: § 86 BDSG

In Satz 1 sollte klargestellt werden, dass sich der Anwendungsbereich des § 86 allein auf „staatliche“ Auszeichnungen und Ehrungen beschränkt.

Die Formulierung „als auch andere öffentliche und nicht-öffentliche Stellen“ in Abs. 1 des Entwurfs ist zu unkonkret, insbesondere da sich die Regelung auch auf besondere Kategorien personenbezogener Daten bezieht. Hier wären zumindest näher bestimmte Kategorien von Empfängern, z.B. Dienstherr*in oder Arbeitgeber*in, zu nennen.

Der Ausschluss der Betroffenenrechte, Art. 13 bis 16 DSGVO, in Abs. 2 geht über das gebotene Maß hinaus. Es kann noch nachvollzogen werden, dass eine aktive Informationspflicht bei Ehrungen entbehrlich sein kann, nicht jedoch, dass ein Recht auf Auskunft nach Art. 15 DSGVO insbesondere gegenüber „anderen Stellen“ ausgeschlossen sein soll.

Zu einer aufzunehmenden Regelung zum Schutz der allgemeinen Meinungs- und Informationsfreiheit sowie zum Schutz von künstlerischen und literarischen Zwecken

Es bedarf nach wie vor einer Regelung zum Schutz der allgemeinen Meinungs- und Informationsfreiheit sowie zum Schutz von künstlerischen und literarischen Zwecken. Die z.T.[9] vertretene Auffassung, dass Art. 85 Abs. 1 DSGVO bereits durch Art. 5 GG ausgefüllt

[9] Bmi.bund.de, FAQs zur Datenschutz-Grundverordnung.

werde und daher keine weitere Anpassung erfolgen müsse, übersieht, dass neben dem professionellen Journalismus, für den bereits durch den Bundes- und die Landesgesetzgeber[10] spezielle Vorschriften erlassen wurden, weiterer Regelungsbedarf für Datenverarbeitungen zu künstlerischen (z.B. Fotografen*, Hobbyfotografen*, Künstler*) und für die öffentliche Meinungsäußerung Privater (z.B. Blogger*, Podcaster*, Politiker*, Pressesprecher*, Twitter-Nutzer*, YouTuber*) besteht, die nicht bereits durch eine Anwendung des Art. 5 GG oder das KUG gewährleistet wird. Ein Anpassungsbedarf wird auch schon daraus deutlich, dass das 2. DSAnpUG-EU in Art. 41 für den Bereich der Deutschen Welle eine Ausnahme vorsieht. Ein Anpassungsbedarf besteht, weil auch die o.g. Gruppen sich regelmäßig öffentlich äußern und dadurch einen wichtigen Beitrag zum öffentlichen Diskurs leisten. Ein Anpassungsbedarf kann auch nicht deswegen verneint werden, weil es sich bei den o.g. Verantwortlichen nicht um professionelle Journalisten handelt. Die DSGVO führt dazu in EG 153 aus, dass Begriffe, die im Zusammenhang mit der Meinungsäußerungsfreiheit stehen, wie beispielweise der Begriff „Journalismus“ weit auszulegen seien.

Die Aufforderung, zur Schaffung von Ausnahmen oder Abweichungen, um das Recht auf freie Meinungsäußerung mit dem Recht auf Datenschutz in Einklang zu bringen, bezieht sich daher nicht nur auf den professionellen Journalismus, sondern auch auf die o.g. Aktivitäten. Nach Auffassung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[11] müssen sich Ausnahmen zur DSGVO auf konkrete und spezifische Regelungen stützen. Rechtliche Unsicherheiten im Bereich der Meinungsäußerungsfreiheit stellen schon an sich eine erhebliche Beeinträchtigung[12] des Rechts auf freie Meinungsäußerung und der Kommunikationsfreiheit dar. Anzustreben wäre in diesem Bereich eine Rechtsgrundlage, die neben den bestehenden Rechtsgrundlagen aus Art. 6 Abs. 1 lit e und f DSGVO, das Verhältnis bzw. die Bedingungen der Verarbeitung bei Datenverarbeitungen unter Art. 9 und 11 DSGVO sowie im Hinblick auf die Informationspflichten nach Art. 13 und 14 DSGVO sowie des Betroffenenrechts nach Art. 15 DSGVO für alle in Art. 85 DSGVO genannten Zwecke regelt. Dabei sollte ein besonderes Gewicht auf die grundlegende Bedeutung der Möglichkeiten zur

[10] Übersicht bei emr-sb.de, Synopse zu den geplanten Änderungen landesrechtlicher Regelungen zur Umsetzung des 21. RÄndStV und der DS-GVO.
[11] Entschließung vom 09.11.2017.
[12] S. dazu z.B. telemedicus.info/article/3307-Braucht-die-DSGVO-ein-Medienprivileg-auch-fuer-Blogger,-Fotografen-und-Pressesprecher.html.

freien Meinungsäußerung und zur Teilnahme am öffentlichen Diskurs gelegt werden, die mit dem Recht der natürlichen Personen bei der Verarbeitung personenbezogener Daten in Ausgleich zu bringen sind. Es kann dabei auf die bisherige Rechtsprechung des BVerfG und des EUGH aufgebaut werden, wobei jedoch die Besonderheiten der Verarbeitung durch informationstechnische Systeme auch vor dem Hintergrund deren technischer Weiterentwicklung sowie den Möglichkeiten der Manipulation und Dekontextualisierung mit besonderer Aufmerksamkeit bedacht werden sollten.

Zu Art. 13 Änderung des BSI-Gesetzes

Das BSI-Gesetz sieht erhebliche Verarbeitungsbefugnisse einhergehend mit umfangreichen Einschränkungen der Rechte der betroffenen Personen vor, wobei die Anforderungen an Einschränkungen aus Art. 23 Abs. 2 DSGVO nur unzureichend erfüllt werden. Selbst die Gesetzesbegründung führt aus, dass es sich bei der Einfügung des § 3a Abs. 1 und 2 um eine datenschutzrechtliche Ermächtigungsgrundlage handele, die „nur für Aufgaben und Tätigkeiten [gelte], die nicht unmittelbar durch die speziellen datenschutzrechtlichen Ermächtigungen […] erfasst“ sei. Damit handelt es sich um einen „Auffangtatbestand“.

Zu Nr. 3: § 3a Abs. 2

Die Vorschrift bedeutet eine fast konturenlose Ausweitung der Verarbeitungsbefugnisse. Insbesondere die Zwecke der „Sammlung“ in Abs. 2 Nr. 1 lit. a und „Unterstützung“ in Abs. 2 Nr. 1 lit b stellen keine hinreichend konkreten Zwecke im Sinne der Art. 5 Abs. 1 lit b und 23 Abs. 2 lit a DSGVO dar.

Zu Nr. 6 und 7: §§ 6-7

Für das BSI-Gesetz wird mit den Nr. 6 und 7 eine umfangreiche Beschränkung der Rechte der betroffenen Personen eingeleitet. Zwar ist die Verarbeitung personenbezogener Daten zum Betrieb und Schutz informationstechnischer Systeme nachvollziehbar, damit muss aber nicht ein so weitreichender Ausschluss der Betroffenenrechte verbunden sein. Die Regelungen belassen es im Belieben des BSI, wann und mit welchem Inhalt eine Auskunft erteilt wird. Es ist nachvollziehbar, dass die umfangreichen Rechte der Betroffenen im Zusammenhang mit der Sicherstellung der technischen Infrastruktur für das BSI eine zusätzliche Belastung und unter bestimmten Bedingungen auch eine Gefahr für die Erfüllung dessen Aufgaben darstellen. Gerade aber vor diesem Hintergrund, wäre eine konkrete Positivregelung

dahingehend, in welchen Fällen und unter welchen Bedingungen eine Auskunft erteilt wird, für alle Beteiligten hilfreicher und würde den Aufwand und Umfang von den - nunmehr erforderlichen - Abwägungsentscheidungen abmildern.

Zumindest die Regelung des § 6f S. 2 ist mit den Anforderungen des Art. 23 insbesondere Abs. 2 lit. f) DSGVO nicht vereinbar. Es bedarf zumindest einer Maximalfrist für die Speicherdauer. Keinesfalls kann es dem BSI anheimgestellt werden, ob zwingende Gründe für eine Verarbeitung bestehen. Eine solche Prüfung sollte unverzüglich erfolgen müssen.

Zu Art. 15 Änderung des E-Government-Gesetzes

Art. 15 zur Änderung des E-Government-Gesetzes sieht in erster Linie sprachliche Anpassungen an die DSGVO vor. Ziel des Gesetzes zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) ist es, die elektronische Kommunikation mit der Verwaltung zu erleichtern. Es soll eine gesetzliche Grundlage für die elektronische Verwaltungstätigkeit des Bundes, der Länder und Kommunen bei der Erfüllung von Bundesaufgaben schaffen. Die Anpassung an den Wortlaut der DSGVO zu § 5 in Art. 15 Nr. 1 lit. a des Entwurfs soll verdeutlichen, dass für Verarbeitungen im sog. Once Only-Verfahren[13] die Regelungen der DSGVO zur Einwilligung, Art. 4 Nr. 1 und Art. 7 DGVO, direkt gelten. Zu beachten ist in diesem Zusammenhang, dass die Einwilligung im Bereich der öffentlichen Verwaltung nur in bestimmten Zusammenhängen eingeholt werden darf. Im Verhältnis Staat – Bürger*in besteht ein Ungleichgewicht, das einer freien Entscheidung zunächst entgegensteht. Es ist daher jeweils darzulegen, dass dieses Ungleichgewicht in der konkreten Anwendungssituation ausgeglichen ist oder ausgeglichen wird. Dies ist z.B. dann der Fall, wenn die Nichterteilung der Einwilligung keine nachteiligen Folgen für die betroffene Person hat oder der Zugang zu der Verwaltungshandlung auf herkömmlichen, analogen Weg nicht künstlich, z.B. durch ein höheres Entgelt, erschwert wird.

In Art. 15 Nr. 2 d oder e des Entwurfs zu § 11 Abs. 3 oder Abs. 4 sollte klargestellt werden, dass im Rahmen der gemeinsamen Vereinbarung nach Maßgabe des Art. 26 DSGVO sichergestellt wird, dass ein höherer Schutzbedarf bei einem Verantwortlichen auf das gemeinsame Verfahren übertragen wird und, soweit erforderlich, auch bei dem

[13] Vgl. Bock „Datenschutz in der Verwaltung von Bund, Ländern und Kommunen“ in Specht/Mantz, Handbuch europäisches und deutsches Datenschutzrecht, i.E., § 20 Rn 27ff.

Verantwortlichen oder Verarbeiter Anwendung findet, für die oder den dieser Schutzbedarf nicht ermittelt wurde.

Zu Art. 16 Änderung des Bundesmeldegesetzes (BMeldG)

Das Melderecht wird gerne als informationelles Rückgrat der modernen Verwaltung bezeichnet, weil es die Rechtsgrundlagen und Regelungen für einen Grundbestand an Informationen über die Bürgerinnen und Bürger in staatlicher Hand darstellt.[14] Einerseits muss der Staat über verlässliche Informationen zur Planung und Daseinsvorsorge verfügen. Andererseits verlangt die verpflichtende Hergabe der personenbezogenen Daten an den Staat einen vertrauensvollen Umgang und Schutz. Bestand in der Vergangenheit ein gewisser faktischer Schutz in der dezentralen, mehr oder weniger analogen Verwaltung der Bürger*innendaten bei den örtlichen Meldeämtern, so sind mit der Digitalisierung der Meldedatenhaltung und des Meldeverfahrens die Zugriffsmöglichkeiten durch den Staat gestiegen. Damit einher gehen Möglichkeiten einer effizienteren Gestaltung der Verwaltungsverfahren über die Zuständigkeiten einzelner Behörden hinweg. Positiv betrachtet können damit eine Vereinfachung der Verfahren und Entbürokratisierung erfolgen. Die Kehrseite, ist die Zunahme der Zugriffs- und Verkettungsmöglichkeiten über zahlreiche Schnittstellen und eine virtuelle Zentralisierung bei wenigen Datenzentralen.[15] Dies führt zu einer virtuellen und tatsächlichen Verwundbarkeit, nicht nur individueller Bürger*innen, sondern auch der Verwaltung und damit des Staates. Die Anpassung des Bundesmeldegesetzes sollte vor diesem Hintergrund nicht nur eine formale Anpassung an die Begrifflichkeiten der DSGVO vornehmen, sondern die Erfordernisse in einer sich technisch und politisch wandelnden Welt berücksichtigen und die Voraussetzungen für ein entsprechend robustes Meldewesen zum Schutz der Rechte natürlicher Personen bei der Verarbeitung von Meldedaten schaffen. Diese Voraussetzungen sollten über technische und organisatorische Anforderungen ergänzend z.B. in Art. 16 Nr. 3 erfasst werden.[16]

[14] S. Bock, DuD 2005, 360ff.
[15] So verarbeitet beispielsweise der Informations- und Kommunikationsdienstleister Dataport mittlerweile Meldebestände aus sechs Bundesländern.
[16] Vgl. oben unter B. zu den technischen und organisatorischen Maßnahmen.

Zu Art. 16 Nr. 2 b

Es sollte in Ergänzung zu § 2 Abs. 4 S. 2 bestimmt werden, ob alle oder nur bestimmte Angaben nicht meldepflichtiger Personen erfasst werden dürfen und aus welchem Grund und zu welchen Zwecken diese verarbeitet werden dürfen. Liegen diese Informationen der betroffenen Person nicht vor, kann keine gem. Art. 7 DSGVO wirksame Einwilligung erteilt werden. Zudem gilt das oben zur Freiwilligkeit der Einwilligung im öffentlichen Bereich Ausgeführte.

Zu Art. 16 Nr. 10 a

Der Entwurf sieht für § 11 Abs. 1 Nr. 1 vor, dass das Recht auf eine Auskunft nach Art. 15 Abs. 1 lit. b und lit. c DSGVO u.a. nicht für nicht automatisierte einfache Melderegisterauskunft bestehen soll. In der Begründung des Entwurfs wird dazu ausgeführt, es handele sich bei einfachen Melderegisterauskünften um Massenauskunftsverfahren. Manuelle, d.h. nicht automatisierte Melderegisterauskünfte würden wegen des Protokollierungsaufwandes nicht erfasst, sondern „nur aufbewahrt“. Vor dem Hintergrund, dass einer einfachen Melderegisterauskunft nicht widersprochen werden kann, kann der Begründung für den Ausschluss der Auskunft aus aktueller Sicht nicht gefolgt werden. Die manuelle Melderegisterauskunft stellt schon lange nicht mehr den Regelfall der einfachen Melderegisterauskunft dar. Manuelle Auskünfte oder manuelle Nachbearbeitungen werden, schon aus Kostengründen, nur dann eingeholt, wenn eine elektronische Auskunft nicht erteilt wurde, weil z.B. ein unvollständiger oder fehlerhafter Datensatz vorlag, § 49 Abs. 4 BMG. Gerade in diesen Fällen, besteht ein begründetes Interesse der betroffenen Person auf ihr Auskunftsrecht. Gerade das Recht auf Auskunft ist für das Grundrecht auf Datenschutz wesentlich, weil nur darüber eine Transparenz für die betroffene Person hergestellt werden kann, die ihr eine Kontrolle über die über sie verarbeiteten personenbezogenen Daten ermöglicht. Der entstehende Aufwand für eine Protokollierung beim Verantwortlichen überwiegt gegenüber diesem Interesse nicht.

Zu Art. 16 Nr. 26

Der Entwurf für § 44 Abs. 3 sieht vor, dass eine einfache Melderegisterauskunft nach wie vor, unter der Bedingung erteilt wird, dass die Identität der betroffene Person aufgrund der vom Anfragende mitgeteilten Angaben nach Abs. 3 Nr. 1 lit. a bis lit. f von der Meldebehörde

eindeutig festgestellt werden kann. Der in S. 1 HS. 1 vorgesehen Fall der Einwilligung sollte nicht darüber hinwegtäuschen, dass diese nicht den Regelfall für die Auskunftserteilung darstellen wird. Bei der Vorschrift dürfte es sich in erster Linie um Makulatur handeln. Sie lädt geradezu dazu ein, sich mit Hilfe einer geschickten optischen oder textlichen Vertragsgestaltung, Verbraucher in eine „Einwilligungsfalle“ zu locken. Zwar sind die Anforderungen an die Einwilligung mit der DSGVO gestiegen. Nichtsdestotrotz ist es aber aufgrund übermäßiger Nutzung von Einwilligungen als Rechtsgrundlage nach Art. 6 Abs. 1 lit. a DSGVO bei Verbrauchern und Verbraucherinnen zu einer sog. Einwilligungsermüdung gekommen. Datenschutzrechtliche Einwilligungen, zumal wenn sie als Pop-up erscheinen, werden häufig angeklickt, weil sie als lästig empfunden werden. Der datenschutzrechtliche Wert für die Selbstbestimmung und die Schutzwirkung, die die Einwilligung eigentlich entfalten soll, geht damit verloren. Daher wird empfohlen, die Einwilligung aus § 44 Abs. 3 HS.1 zu streichen. Die Anforderungen der korrekten Identifizierbarkeit sind insbesondere im elektronischen Verfahren hoch. Die betroffenen Personen werden dadurch, auch im Verhältnis zu dem Informationsgehalt des in Frage stehenden Datensatzes, ausreichend geschützt.