Europäische Akademie für Informationsfreiheit und Datenschutz
Académie européenne pour la liberté d'information et la protection des données
European Academy for Freedom of Information and Data Protection
EAID

Berlin, den 16. Juli 2018

Stellungnahme zum Referentenentwurf zum Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetz EU – 2. DSAnpUG-EU

I. Vorbemerkung

Das Bundesministerium des Innern, für Bau und Heimat hat am 21. Juni 2018 im Rahmen der Verbändebeteiligung einen Referentenentwurf für ein Zweites Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 vorgelegt. Die Europäische Akademie für Informationsfreiheit und Datenschutz (EAID) bedankt sich für die Einbeziehung in das Abstimmungsverfahren.

Angesichts des Umfangs des Entwurfs beschränkt sich die nachfolgende Stellungnahme auf diejenigen Punkte, in denen Änderungen im Hinblick auf europa- und verfassungsrechtliche Anforderungen in besonderem Maße geboten erscheinen.

Die Anpassung des deutschen Rechts sollte der von der Datenschutzgrundverordnung (DSGVO) und der Richtlinie für Polizei und Justiz verfolgten Maxime folgen, das Grundrecht zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten gem. Art. 8 Absatz 1 der Charta der Grundrechte der Europäischen Union sowie Art. 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) zu verwirklichen (vgl. DSGVO, EG 1) und dabei ein einheitliches Datenschutzniveau in der EU zu gewährleisten. Im Hinblick darauf besteht erheblicher Änderungsbedarf an dem vorgelegten Entwurf.

Auszüge der vorliegenden Stellungnahme erscheinen auch im Newsdienst der Zeitschrift für Datenschutz (ZD) im Beck-Verlag, ZD-Aktuell 2018, 04317.

II. Änderung des Bundesdatenschutzgesetzes (Art. 10 Entwurf)

1. Vorbemerkung

Das 2. DSAnpUG-EU sollte dazu genutzt werden, das durch das 1. DSAnpUG-EU neu gefasste Bundesdatenschutzgesetz (BDSG) v. 30. Juni 2017 (BGBl. I, 2097) nachzubessern, um sicherzustellen, dass die grund- und europarechtlichen Vorgaben vollen Umfangs erfüllt werden.

Besonderer Änderungsbedarf besteht bei § 29 Abs. 3 BDSG, der die Aufsichtsbefugnisse der Datenschutzbehörden bei Berufsgeheimnisträgern in europarechtswidriger Weise

einschränkt. Ohne Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung der aufsichtsbehördlichen Aufgaben erforderlich sind, und ohne Zugang zu den Geschäftsräumen und Datenverarbeitungsanlagen (Art. 58 Abs. 1 lit. e) und f) DSGVO) bei Berufsgeheimnisträgern und deren Auftragsverarbeitern können die Datenschutzbehörden keine effektive Prüfung in besonders sensiblen Bereichen wie dem Gesundheitswesen gewährleisten.

Änderungsbedarf besteht ferner insbesondere bei den folgenden Regelungen:

- Rechte der betroffenen Person (§§ 4 Abs. 2, 29 Abs. 1, 35 Abs. 1 BDSG),
- Verarbeitung zu anderen Zwecken (§§ 23-25).

Diesbezüglich verweisen wir auf die EAID-Stellungnahme zum Entwurf der Bundesregierung für ein Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – (DSAnpUG-EU) vom 22. Februar 2017 (vgl. https://www.eaid-berlin.de/wp-content/uploads/2017/02/EAID-Stellungnahme-zum-DSAnpG-EU-v.22.2.2017.pdf).

2. Fehlende Konkretisierung der Vorgaben aus Art. 85 DSGVO (Meinungsfreiheit) und 88 DSGVO (Beschäftigtendatenschutz)

Bisher fehlen in zentralen Bereichen hinreichende, die Vorgaben der DSGVO konkretisierende, bereichsspezifische Regelungen. Regelungsbedarf besteht etwa hinsichtlich der Datenverarbeitung im Beschäftigungskontext (Art. 88 DSGVO) und des Ausgleichs zwischen der Freiheit der Meinungsäußerung und des Schutzes personenbezogener Daten (Art. 85 DSGVO). Die nun vorgesehene Gesetzesänderung sollte genutzt werden, diese Regelungslücken zu schließen.

Besonders dringend sind Regelungen im Bundesrecht, die das Recht auf den Schutz personenbezogener Daten mit dem Recht auf freie Meinungsäußerung und Informationsfreiheit in Einklang bringen. Zwar haben die Länder eine Reihe von Bestimmungen des Presse-, Rundfunk- und Medienrechts novelliert. Im Hinblick auf die von dem Landesrecht nicht erfassten Verarbeitungsvorgänge besteht allerdings weiterhin erhebliche Unsicherheit. Hinzuweisen ist hier vor allem auf den Umgang mit Fotografien und auf Beiträge mit journalistischem Inhalt, die nicht im Rahmen der Tätigkeit von Presse- und Medienunternehmen veröffentlicht werden. Davon betroffen sind vor allem Veröffentlichungen im Internet, etwa in sozialen Netzwerken und Blogs, aber auch die Tätigkeit freier Journalistinnen und Journalisten, die nicht im Auftrag eines Medienunternehmens tätig sind.

Zwar haben Vertreter des Bundesinnenministeriums und einzelne Datenschutzbeauftragte die Meinung vertreten, dass das Kunsturhebergesetz nach dem 25. Mai 2018 weiter gelte. Unklar bleibt aber, inwieweit daneben die Verpflichtungen der DSGVO, etwa im Hinblick auf Informationspflichten, Auskunfts- und Löschungsrechte der betroffenen Person bestehen. Hier besteht dringender Regelungsbedarf durch den Bundesgesetzgeber.

3. Zu Art. 10 Nr. 5 (§ 22 Abs. 1 BDSG)

Die im Referentenentwurf vorgesehenen Änderungen von § 22 Abs. 1 BDSG enthalten nicht nur - wie in der Begründung ausgeführt - zusätzliche Befugnisse nicht-öffentlicher Stellen, besondere Kategorien personenbezogener Daten nach Art. 9 Absatz 1 der DSGVO verarbeiten zu dürfen, wenn dies aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist.

Gravierender ist, dass bei öffentlichen Stellen die bisher in § 22 Abs. 1 Nr. 2 BDSG in den Fällen des § 22 Abs. 1 Nr. 2 lit. b) bis d) vorgesehene Abwägung mit den Interessen der

betroffenen Personen wegfallen soll. Damit entfällt eine zentrale, durch Art. 9 Abs. 2 lit. g) DSGVO geforderte spezifische Maßnahme zur Wahrung der Grundrechte und Interessen der betroffenen Person. Diese Einschränkung der Grundrechtspositionen ist nicht hinzunehmen, zumal der Referentenentwurf eine Begründung für den Verzicht auf die Interessenabwägung schuldig bleibt.

III. Änderung des BSI-Gesetzes (Art. 11 Entwurf)

1. Vorbemerkung

Mit den vorgeschlagenen Regelungen in Art. 11 sieht das 2. DSAnpUG-EU weitreichende Änderungen im BSIG vor, indem erstmals umfassende datenschutzrechtliche Regelungen in ein primär IT-sicherheitsbezogenes Gesetz aufgenommen werden. Hierdurch wird vor allem auch den Forderungen der vergangenen Jahre nach bereichsspezifischen Datenschutznormen im IT-Sicherheitsrecht Rechnung getragen.

2. Zu Art. 11 Nr. 3 (§ 3a BSIG)

§ 3a Abs. 2 BSIG-E enthält eine Durchbrechung des Zweckbindungsgrundsatzes. Unbeschadet der Öffnungsklausel des Art. 6 Abs. 4 der DSGVO und des § 23 BDSG bestimmt die Vorschrift, dass eine Datenverarbeitung zu anderen Zwecken als dem ursprünglichen Erhebungszweck zulässig ist, wenn sie für die Sammlung, Auswertung oder Untersuchung von Informationen über Sicherheitsrisiken oder Sicherheitsvorkehrungen für die Informationstechnik (Nr. 1 a)) oder zur Unterstützung, Beratung oder Warnung in Fragen der Sicherheit in der Informationstechnik (Nr. 1 b)) erforderlich ist und des Weiteren kein Grund zur Annahme besteht, dass das schutzwürdige Interesse einer betroffenen Person an dem Ausschluss der Verarbeitung überwiegt (Nr. 2)). Begründet wird diese weitgehende Ermächtigung damit, dass das BSI in der Lage sein muss, sämtliche ihm zur Verfügung stehenden Daten bzw. Quellen zu nutzen, um präventiv Sicherheitsrisiken vorzubeugen und um Sicherheitsvorkehrungen zu treffen. Nur so könne die Behörde ihren Aufgaben gerecht werden, die nationale und öffentliche Sicherheit sowie wichtige Ziele des öffentlichen Interesses zu schützen. Diese Zwecksetzung findet sich in ähnlicher Weise auch in den Beschränkungsgründen des Art. 23 DSGVO wieder. Die mit der Zweckdurchbrechung verbundene Interessenabwägung soll hier zwar als beschränkendes Korrektiv dienen – sinnvoll wäre es dennoch, die Hochrangigkeit betroffener Interessen ausdrücklich im Gesetz zu verankern, um eine den Datenschutz angemessen berücksichtigende Gewichtung schon im Vorfeld einer Interessenabwägung deutlich zu machen und um den Tatbestand hinreichend einzuengen – selbst wenn es um Zwecke der IT-Sicherheit geht. Fraglich ist zudem, ob jedwede und vorliegend sehr weit gefasste Art von Tätigkeit des BSI theoretisch schon geeignet sein soll, den Zweckbindungsgrundsatz zu durchbrechen.

3. Zu Art. 11 Nr. 7 (§ 6a BSIG)

§ 6a Abs. 1 BSIG-E bestimmt Ausnahmen, in denen die Informationspflichten des Art. 13 und Art. 14 DSGVO neben den in Art. 13 Abs. 4 und Art. 14 Abs. 5 DSGVO normierten Ausnahmen nicht bestehen. Die Informationspflichten entfallen tatbestandsmäßig dann, wenn die Informationserteilung die ordnungsgemäße Erfüllung der in der Zuständigkeit des Bundesamtes liegenden Aufgaben gefährden würde (Nr. 1) oder die öffentliche Sicherheit oder Ordnung oder die Gewährleistung der Netz- und Informationssicherheit auf sonstige Weise gefährden oder sonst dem Wohl des Bundes oder eines Landes Nachteile bereiten würde (Nr. 2) und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss. Die Entwurfsbegründung benennt als praktisches Szenario Incident Response-Einsätze des BSI, die nicht selten mit einer Betroffenheit von KRITIS oder Stellen des Bundes und der Länder einhergehen. Insoweit ist es auch

verständlich, dass in diesen Fällen der Schutz eines wichtigen Ziels des allgemeinen öffentlichen Interesses nach Art. 23 Abs. 1 lit. e) DSGVO vorliegt – weitere Fälle, die das „wichtige Ziel" konkretisieren würden, werden in der Entwurfsbegründung jedoch nicht aufgeführt. Da das BSI aber auch Aufgaben ausführt, die nicht immer eine besondere Eilbedürftigkeit wie in Incident Response Team-Fällen voraussetzen, greift der Tatbestand der Entbindung von der Informationspflicht gem. § 6a Abs. 1 Nr. 1 BSIG-E hier deutlich zu weit, indem er generell auf die ordnungsgemäße Aufgabenerfüllung abstellt. Selbiges muss auch für die Regelung in § 6a Abs. 1 Nr. 2 BSIG-E gelten: Diese stellt sich zurzeit noch wie ein Konvolut beliebiger Beschränkungsregelungen dar, ohne dass deutlich wird, wie die einzelnen Tatbestände voneinander abzugrenzen sind und wo deren tatsächliche Relevanz im Einzelfall liegt.

4. Zu Art. 11 Nr. 7 (§ 6b BSIG)

§ 6b BSIG-E beschränkt das Auskunftsrecht der betroffenen Personen aus Art. 15 DSGVO. Obwohl sich die Ausnahmetatbestände für das Auskunftsrecht auf gültige Beschränkungsregelungen der DSGVO aus Art. 23 beziehen, sind diese – auch gemessen an der erheblichen datenschutzrechtlichen Bedeutung des Auskunftsrechts – zu weit gefasst bzw. zu unspezifisch formuliert, auch lassen sich diese oft nicht deutlich und zweifelsfrei in ihrem jeweiligen Anwendungsbereich voneinander abgrenzen. Hier trifft die Entwurfsfassung des § 6b BSIG letztlich dieselbe Kritik wie auch schon vorangehend den § 6a BSIG-E.

5. Zu Art. 11 Nr. 7 (§ 6c BSIG)

Gem. § 6c BSIG-E besteht das Recht auf Berichtigung und Vervollständigung gem. Art. 16 DSGVO nicht, soweit die Erfüllung der Rechte der betroffenen Person zur Folge hätte, dass das BSI seine ihm obliegenden Aufgaben nicht mehr ordnungsgemäß erfüllen könnte. Für diesen Fall soll das Interesse der betroffenen Person an der Ausübung der Rechte zurücktreten. Hier stellt sich von Neuem das Problem, dass zur Beschränkung der Betroffenenrechte ganz allgemein auf die durch das BSI zu erfüllenden Aufgaben abgestellt wird. Nach § 3 BSIG sind diese vielfältig und umfassen nicht nur die Abwehr von Gefahren für IT-Systeme, sondern zum Beispiel auch die Entwicklung von Prüfkriterien, die Unterstützung und Beratung sowie den Aufbau von Kommunikationsstrukturen. Ob für jedwede solcher – auch oftmals nicht zeitkritischer Aufgaben – per se ein Zurücktreten der Betroffenenrechte angenommen werden kann, erscheint fragwürdig.

6. Zu Art. 11 Nr. 7 (§ 6d BSIG)

Auch zur Legitimierung der Beschränkung des Rechts auf Löschung gem. § 6d BSIG-E stützt sich die Entwurfsbegründung auf die Gewährleistung der Funktionsfähigkeit und Aufgabenerledigung der öffentlichen Verwaltung und somit auf den Schutz eines wichtigen Ziels des allgemeinen öffentlichen Interesses nach Art. 23 Abs. 1 lit. e) DSGVO – ohne dass ein solches öffentliches Interesse explizit im Gesetzentwurf benannt würde. Hier besteht deshalb dringender Konkretisierungsbedarf.

7. Zu Art. 11 Nr. 7 (§ 6e BSIG)

§ 6e BSIG-E bestimmt, dass die Pflicht des BSI zur Einschränkung einer Datenverarbeitung nach Art. 18 DSGVO für die Dauer der Überprüfung der Richtigkeit personenbezogener Daten nicht besteht, wenn die Verarbeitung oder Weiterverarbeitung durch das BSIG ausdrücklich geregelt wird (Nr. 1) oder eine Einschränkung der Verarbeitung die Gefahrenabwehr für die Sicherheit in der Informationstechnik gefährden würde (Nr. 2) und deshalb das Interesse der betroffenen Person an der Einschränkung zurücktreten muss. Begründet wird die Begrenzung des Rechts auf Einschränkung der Verarbeitung mit der Sicherstellung der nationalen und der öffentlichen Sicherheit und dem Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses nach Art. 23 Abs. 1 lit. a), c) und e)

DSGVO. Aber auch hier stellt sich – wie bei nahezu allen vorangegangenen Begrenzungstatbeständen auch – die Frage, an welcher Stelle das allgemeine öffentliche Interesse konkretisiert wird. Soweit ein hinreichend eng gefasster gesetzlicher Erlaubnistatbestand die Verarbeitung regelt, dürfte dies noch hinnehmbar sein, aber eine Begrenzung von Betroffenenrechten dem Wortlaut des § 6e BSIGE nach auch dann für zulässig zu halten, wenn die Einschränkung lediglich eine irgendwie geartete Abwehr von Gefahren für IT-Systeme ermöglichen soll, ist zu weit gegriffen.

IV. Änderung des Bundesmeldegesetzes (Art. 14 Entwurf)

1. Vorbemerkung

Leider verzichtet der Entwurf auf eine kritische Überprüfung der derzeitigen melderechtlichen Bestimmungen im Lichte des durch Art. 8 EUGrCH gewährleisteten Grundrechts auf Datenschutz und der DSGVO. Er beschränkt sich im Wesentlichen auf formale und sprachliche Anpassungen.

2. Umfang der Meldedaten

Leider soll nach dem Entwurf der in § 3 BMeldG vorgesehene umfangreiche Datenkatalog unverändert beibehalten werden. Damit lässt der Entwurf die Chance vergehen, die Melderegister im Sinne der durch Art. 5 lit. c) DSGVO geforderten Datenminimierung und einer effektiveren Handhabung auf Basisdaten zu beschränken.

Das Gesetzgebungsvorhaben sollte jedoch Anlass sein, den Umfang der im Meldewesen gespeicherten Daten kritisch unter die Lupe zu nehmen. Die Anreicherung der Melderegister mit zusätzlichen, über ihre eigentliche Kernaufgabe (Identifikation und Wohnungsnachweis) hinausgehenden Informationen (Waffenerlaubnis, Sprengstofferlaubnis, steuerliche Identifikationsnummer) erhöht den Aufwand, weil durch differenzierte Zugriffsregelungen der entsprechende Informationsfluss in und aus den Melderegistern reguliert werden muss. Grundsätzlich muss gelten: Jede Behörde und nicht-öffentliche Stelle darf nur die Daten erhalten, die sie für ihre Aufgaben benötigt.

3. Zu Art. 14 Nr. 3 (§ 4 BMG)

Die Vorschrift sollte generell eine datenschutzfreundliche Gestaltung des Systems der Ordnungsmerkmale gem. den Art. 24, 25 und 32 DSGVO vorgeben, auch soweit die Maßnahmen nicht für die Vermeidung von Verwechslungen erforderlich sind. Sinnvoll sind insbesondere Vorgaben, die den technologischen Datenschutz im Rahmen der notwendigen Registermodernisierung stärken, etwa zur Verwendung pseudonymisierter oder anonymisierter Daten für Zwecke der Statistik und der wissenschaftlichen Forschung.

4. Zu Art. 14 Nr. 8 (§ 9 BMG)

Das Gesetz sollte Anlass sein, die Rechte der Meldepflichtigen deutlich zu stärken.
Der vollständige Wegfall der Vorschrift, welche die Rechte der betroffenen Person regelt, ist problematisch. Damit würde auch die Bestimmung von § 9, letzter Satz BMG, entfallen, wonach Rechte, die der betroffenen Person nach anderen Vorschriften zustehen, unberührt bleiben. Zwar verweist die Begründung zutreffend darauf, dass die durch die DSGVO konstituierten Rechte der betroffenen Personen unmittelbar gelten, da das Gesetz aber hinsichtlich bestimmter Rechte (etwa des Rechts der betroffenen Person auf Auskunft) spezielle Regelungen enthält, sollte im Sinne der Rechtssicherheit klargestellt werden, dass die durch die DSGVO konstituierten Betroffenenrechte, insbesondere das Widerspruchsrecht

gem. Art. 21 DSGVO und das gerade im Bereich des Registerwesens bedeutsame Recht auf Datenübertragbarkeit gem. Art. 20 DSGVO, garantiert werden.

5. Zu Art. 14 Nr. 10 (§ 11 BMG)

Weil die Melderegister in den zurückliegenden Jahren immer mehr zu einem multifunktionalen Informationspool für Wirtschaft und Verwaltung geworden sind (vgl. etwa https://einwohnermeldeamt.com), ist es notwendig, dem Auskunftsrecht des Betroffenen im Melderecht stärker Geltung zu verschaffen. Die Betroffenen können heute kaum noch erkennen, an welche Stellen Meldedaten fließen. Der Meldepflichtige sollte deshalb insbesondere umfassend Auskunft über diejenigen öffentlichen oder privaten Stellen erhalten, die einfache Melderegisterauskünfte über ihn eingeholt haben.

Die in § 11 BMG vorgesehenen Einschränkungen des Auskunftsrechts sind vor diesem Hintergrund inakzeptabel. Sie überschreiten auch den durch die DSGVO vorgesehenen mitgliedsstaatlichen Gestaltungsspielraum.

Völlig unverhältnismäßig ist insbesondere der vorgesehene generelle Wegfall des Auskunftsanspruchs über die Kategorien der übermittelten Daten und über die Empfänger der Daten bei nicht-automatisierten Melderegisterauskünften nach den §§ 44, 46 und 50 Abs. 1 bis 3 und in Fällen der nicht-automatisierten Datenübermittlung nach § 34 an öffentliche Stellen.

Im Hinblick auf die in § 11 Abs. 2 Nr. 4 BMG vorgesehenen weiteren Einschränkungen des Auskunftsrechts sollte zudem auf den in § 11 Abs. 1 Nr. 4 BMG vorgesehenen Wegfall der Auskunftserteilung über Datenkategorien und Empfänger automatisierter Übermittlungen an die in § 34 Abs. 4 S. 1 BMG genannten Behörden (Polizeibehörden des Bundes und der Länder, Staatsanwaltschaften, Amtsanwaltschaften, Gerichte, soweit sie Aufgaben der Strafverfolgung, der Strafvollstreckung oder des Strafvollzugs wahrnehmen, Justizvollzugsbehörden, Verfassungsschutzbehörden des Bundes und der Länder, der Bundesnachrichtendienst, der Militärische Abschirmdienst, der Zollfahndungsdienst, Hauptzollämter, Finanzbehörden, soweit sie strafverfolgend tätig sind, sowie das Bundesamt für Justiz) verzichtet werden. Durch § 11 Abs. 2 Nr. 4 BMG werden berechtigte Interessen öffentlicher Stellen gegen eine Auskunftserteilung hinreichend berücksichtigt. Auf die zusätzliche Einschränkung durch § 11 Abs. 1 Nr. 4 BMG sollte deshalb verzichtet werden.

6. Zu Art. 14 Nr. 13 (§ 14 BMG)

Die vorgesehene Einschränkung der Löschungsansprüche der betroffenen Person nach Art. 17 DSGVO ist europarechtlich unzulässig, da es an einer entsprechenden Ermächtigungsgrundlage für entsprechende Abweichungen im mitgliedsstaatlichen Recht mangelt. Zudem ist es geboten, die Melderegister technisch so ausgestalten, dass sich eine rechtlich gebotene Löschung auch realisieren lässt, so dass es einer entsprechenden gesetzlichen „Erleichterung“ für die Meldebehörden nicht bedarf.

7. Zu Art. 14 Nr. 26 (§ 44 BMG)

Die Regelung des § 44 BMG zur „einfachen Melderegisterauskunft“ gehört zu den problematischsten Bestimmungen des Melderechts. Die in § 44 BMG konstituierte generelle Übermittlungsbefugnis ohne jede konkrete Interessenabwägung stellt einen unverhältnismäßigen Eingriff in das durch Art. 8 EUGrCH garantierte Grundrecht auf Schutz personenbezogener Daten dar.

Anders als durch Art. 5 Abs. 1 lit. c) DSGVO gefordert, wird die Übermittlung der auf Grund gesetzlicher Pflicht erhobenen Meldedaten nicht auf solche Fälle begrenzt, in denen die Übermittlung angemessen und erheblich sowie auf das notwendige Maß beschränkt ist

(Datenminimierung). Das vielfach zur Rechtfertigung der einfachen Melderegisterauskunft angeführte „Interesse an einem funktionierenden Meldewesen“ würde durch entsprechende Einschränkungen und Interessenabwägungen nicht gefährdet. Zumindest ist zu gewährleisten, dass das Recht auf Widerspruch gem. Art. 21 DSGVO bei der einfachen Melderegisterauskunft beachtet wird.

V. Änderung des Telekommunikationsgesetzes (Art. 134 Entwurf)

1. Vorbemerkung

Zunächst ist nicht einleuchtend, weshalb die Bundesregierung jetzt Regelungen zur Umsetzung der Richtlinie 2002/58/EG vorschlägt, über deren Ablösung durch eine ePrivacy-Verordnung gegenwärtig auf Unionsebene beraten wird. Zwar gilt die Richtlinie 2002/58/EG nach Maßgabe des Art. 95 DSGVO fort, es ist allerdings damit zu rechnen, dass die ePrivacy-Verordnung im Laufe des kommenden Jahres in Kraft treten wird. Sie würde dann unmittelbar in allen Mitgliedstaaten gelten und möglicherweise neuen, wenngleich beschränkten Anpassungsbedarf auslösen. Jedenfalls ist ein nationaler Alleingang etwa zur Nutzung von Kontaktinfomationen für Zwecke der Direktwerbung (§ 95 TKG) nicht sinnvoll. Ein Teil der Regelungen des Entwurfs ergibt sich bereits durch Auslegung des Art. 95 DSGVO und ist insoweit redundant. So wird teilweise der Verweis auf § 11 BDSG a.F. gestrichen, teilweise durch einen ausdrücklichen Verweis auf die DSGVO ersetzt (vgl. Art. 134 Nr. 13 a) einerseits und Art. 134 Nr. 17 andererseits).

2. Zu Art. 134 Nr. 7 (§ 95 TKG)

Die Regelung des Entwurfs betrifft elektronische Kontaktinformationen und will deren Nutzung für Zwecke der Direktwerbung – wie nach bisherigem Recht – zulassen, solange die Betroffenen nicht widersprechen. Das entspricht zwar der Rechtslage nach der DSGVO, die für Bestandsdaten der Telekommunikation unmittelbar gilt. Es ist allerdings ernsthaft zu überlegen, ob elektronische Kontaktinformationen nicht strenger behandelt werden sollten als Bestandsdaten, weil sie (wie z.B. die E-Mail-Adresse) bei der elektronischen Kommunikation eine weitaus größere Bedeutung etwa für die Profilbildung und das Tracking haben als die Bestandsdaten. Insoweit sollte abgewartet werden, welche Vorgaben die künftige ePrivacy-Verordnung hier machen wird.

3. Zu Art. 134 Nr. 19 (§ 115 Abs. 4 TKG) und 20 (§ 149 TKG)

Die vorgesehene Regelung würde zu einer Parallelzuständigkeit der Bundesnetzagentur und dem bzw. der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit führen. Trotz der Verpflichtung der beiden Behörden, auf eine einheitliche Anwendung des Gesetzes hinzuwirken, würde dies zu erheblicher Rechtsunsicherheit bei den verantwortlichen Unternehmen führen. So ist z.B. vorstellbar, dass die Bundesnetzagentur eine bestimmte Verarbeitungspraxis für zulässig hält, während der oder die Bundesbeauftragte deswegen ein Bußgeld verhängt (bzw. umgekehrt). Bei der gerichtlichen Überprüfung eines solchen Bußgelds könnte sich das Unternehmen auf die ihm jeweils günstigere Rechtsauffassung einer der beiden Verwaltungsbehörden berufen (mit ungewissem Ausgang). Die Zuständigkeit sollte ausschließlich bei dem bzw. der Bundesbeauftragten liegen.

Peter Schaar
Vorsitzender des Vorstandes

Dr. Alexander Dix, LL.M.
Stellvertretender Vorsitzender des Vorstandes

Dr. Dennis-Kenji Kipker
Mitglied des Vorstandes