

Berlin, den 1. Dezember 2016

Stellungnahme der Europäischen Akademie für Informationsfreiheit und Datenschutz (EAID) zum Referentenentwurf für ein Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) und zur Umsetzung der Richtlinie (EU) 2016/680 (JI-RL) – Datenschutz-Anpassungs- und -Umsetzungsgesetzes EU – DSAnpUG-EU – des Bundesministeriums des Innern vom 23. November 2016

I. Vorbemerkung

Das Bundesministerium des Innern (BMI) hat der Europäischen Akademie für Informationsfreiheit und Datenschutz mit E-Mail vom 23. November 2016 den Referentenentwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 (DS-GVO) und zur Umsetzung der Richtlinie (EU) 2016/680 (JI-RL) zugeleitet (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU) und die Gelegenheit zur Stellungnahme gegeben.

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. Von zentraler Bedeutung ist dabei der von der DS-GVO und der JI-RL verfolgte Zweck, 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) sicherzustellen (vgl. DS-GVO, EG 1).

Mit dem Referentenentwurf sollen das deutsche Recht sowohl an die genannten EU-Rechtsakte angepasst als auch Regelungen für die Verarbeitung auch für die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen des Bundes getroffen werden, die außerhalb des Anwendungsbereichs des Unionsrechts liegen, wie etwa die Datenverarbeitung durch das Bundesamt für Verfassungsschutz, den Bundesnachrichtendienst oder den Militärischen Abschirmdienst oder im Bereich des Sicherheitsüberprüfungsgesetzes. Die Anwendbarkeit der in unterschiedlichen Regelungskreisen vorgesehenen Bestimmungen dürfte schon deshalb erschwert sein, weil vielfach nicht erkennbar ist, auf welchen Bereich sich die jeweiligen Vorschriften des DSAnpUG-EU beziehen. Dies betrifft insbesondere die Regelungen des vorgeschlagenen neu gefassten Bundesdatenschutzgesetzes (BDSG-neu).



Europarechtlich fragwürdig sind die im BDSG-neu vorgenommenen umfangreichen Wiederholungen von Regelungen der DS-GVO. Der EuGH hat Normwiederholungen bei Verordnungen aufgrund des primärrechtlichen Vorrangs des Unionsrechts grundsätzlich abgelehnt und hält sie nur dann ausnahmsweise für zulässig, wenn eine ganze Reihe unionsrechtlicher, einzelstaatlicher und regionaler Vorschriften zusammentreffen. In diesem besonderen Fall könne es „nicht als ein Verstoß gegen das Gemeinschaftsrecht angesehen werden, dass Regionalgesetze im Interesse ihres inneren Zusammenhangs und ihrer Verständlichkeit für die Adressaten bestimmte Punkte der Gemeinschaftsverordnungen wiederholen“ (C-272/83, Rn. 27). Die im Referentenentwurf gleichwohl vorgenommenen vielfältigen — dabei teilweise sogar vom Verordnungstext abweichenden — Wiederholungen der Vorschriften der DS-GVO führen zudem zu erheblichen Anwendungs- und Auslegungsproblemen, insbesondere bei den Rechten der Betroffenen und bei den Vorgaben zur Zweckbindung (s.u.).

Schließlich lässt der Entwurf offen, inwieweit und wo zusätzliche Datenschutzregelungen getroffen werden sollen, die bisher durch bereichsspezifisches Recht geregelt sind. Damit besteht die erhebliche Gefahr, dass die sich überlappenden, teils widersprechenden Regelungen die Rechtsanwender überfordern und zu einer inkonsistenten Datenschutzpraxis führen. Dies stellt öffentliche und nicht-öffentliche Stellen, die personenbezogene Daten verarbeiten, vor kaum zu überwindende Schwierigkeiten und kann gleichzeitig auch eine Absenkung des Schutzniveaus zur Folge haben.

II. Keine Aufweichung des Datenschutzes durch nationales Recht

Die Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollen gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Das neue EU-Datenschutzrecht soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen (vgl. etwa DS-GVO, EG 2).

Dabei verfolgt die Reform das Ziel, ein gleichmäßiges und hohes Datenschutzniveau für natürliche Personen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten in der Union zu beseitigen. Deshalb sollte das Schutzniveau bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Insbesondere die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit gleichmäßig und einheitlich angewandt werden.

Hinsichtlich der Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung oder zur Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, gibt die DS-GVO den Mitgliedstaaten die Möglichkeit, nationale Bestimmungen, mit denen die Anwendung der Vorschriften dieser Verordnung genauer festgelegt wird, beizubehalten oder einzuführen. Dies gilt insbesondere für die Verarbeitung besonders sensibler personenbezogener Daten („besonderer

Kategorien von personenbezogenen Daten“), für die wegen besonderer Verarbeitungssituationen ein weiterer Regelungsspielraum besteht (vgl. DS-GVO, EG 10).

Die damit beabsichtigten nationalen Regelungsspielräume geben den Mitgliedsstaaten keineswegs die Möglichkeit, das Datenschutzniveau zu Lasten des Schutzes personenbezogener Daten abzusenken.

Während der Verhandlungen über das EU-Datenschutzpaket hatte das Bundesministerium des Innern für die Möglichkeit geworben, den Mitgliedstaaten weitgehende Regelungsmöglichkeiten zu belassen. Zur Begründung hatten die jeweiligen Ressortchefs angeführt, ihnen ginge es darum, das hohe deutsche Datenschutzniveau zu erhalten (vgl. etwa Wirtschaftswoche Online v. 5.11.2013 <http://www.wiwo.de/politik/deutschland/datenschutz-europa-tut-sich-schwer-seine-buerger-zu-schuetzen/9009564.html> und Zeit Online v. 4.12.2014, <http://www.zeit.de/news/2014-12/04/deutschland-deutsche-minister-zuversichtlich-zu-teileinigung-bei-eu-datenschutz-04101411>).

Umso erstaunlicher ist es, dass viele der im BDSG-neu vorgesehenen Vorschriften hinsichtlich ihres Schutzniveaus nicht nur hinter dem durch die DS-GVO definierten Schutzniveau zurückbleiben, sondern sogar unterhalb des bisherigen deutschen Datenschutzniveaus liegen. Dies gilt insbesondere für die in § 23 Abs. 2 BDSG-neu vorgesehenen pauschalen und nahezu uferlosen Zweckänderungsbefugnisse für nicht-öffentliche Stellen. Zwar lehnt sich die Vorschrift formal an die bisherigen, in § 28 BDSG enthaltenen Bestimmungen an, führt dabei allerdings zu einer erheblichen Ausweitung der zulässigen Zweckänderungen bei gleichzeitigem Wegfall der bisher erforderlichen Abwägung mit dem schutzwürdigen Interesse der betroffenen Person am Ausschluss der Verarbeitung.

Niemandem wäre damit gedient, wenn ab 25. Mai 2018, wenn die DS-GVO wirksam wird, – an die Stelle der 28 nationalen Datenschutzgesetze 28 neue, unterschiedliche „Ausführungsgesetze“ treten, wie es das Bundesministerium des Innern für Deutschland beabsichtigt. Das gilt insbesondere für die verschiedenen Regelungen zur Datenerhebung, Speicherung und Verwendung, mit unterschiedlichen nationalen Vorgaben zu den Rechten auf Auskunft, Löschung und Widerspruch der Betroffenen, ergänzt um Sonderregelungen, die teils deutlich hinter dem EU-Recht zurückbleiben.

Die vorgesehenen Regelungen schaden damit auch den europäischen Unternehmen, die auf Basis des EU-Rechts gleichmäßige Bedingungen für grenzüberschreitende europaweite Geschäftsmodelle brauchen, um so auf Augenhöhe mit der internationalen Konkurrenz agieren zu können. Die vom Entwurf vorgesehenen zahlreichen Abweichungen konterkarieren das vom europäischen Gesetzgeber beabsichtigte Ziel, für alle Bürgerinnen und Bürgern der EU und für die im Europäischen Wirtschaftsraum tätigen Unternehmen einen gleichmäßig wirksamen Datenschutz zu garantieren.

Große Unternehmen, die sich umfangreiche Rechtsabteilungen leisten können, werden auch in Zukunft mit einer solchen unübersichtlichen Situation umgehen können. Dies gilt aber nicht für kleinere und mittlere Unternehmen, die nicht über derartige Ressourcen verfügen. Neben den Bürgerinnen und Bürgern, deren

Datenschutz ausgehöhlt wird, wären sie die Hauptleidtragenden des deutschen Sonderwegs.

III. Stellungnahme zu einzelnen Vorschriften

1. Zu Art. I §4 des Entwurfs (Videoüberwachung)

- 1.1. Mit der Vorschrift soll eine Neuregelung der Videoüberwachung öffentlich zugänglicher Räume geschaffen werden. Anders als in der Überschrift suggeriert, gehen die vorgeschlagenen Videoüberwachungsbefugnisse über § 6b BDSG-alt hinaus. Zudem differenziert die Vorschrift nicht — anders als die derzeitige Regelung — zwischen der Beobachtung mittels optisch-elektronischer Einrichtungen und der Verarbeitung und Nutzung der erhobenen Daten. Schließlich fehlt die bisherige Vorgabe, die Daten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Belange des Betroffenen entgegenstehen.
- 1.2. Mit der neuen Regelung soll vielmehr ein entsprechendes Vorhaben der Bundesregierung fortgeschrieben werden, das bereits nach derzeitiger Rechtslage verfassungsrechtlich problematisch ist (vgl. Stellungnahme der EAID zum „Videoüberwachungsverbesserungsgesetz“ v. 6. November 2016)
- 1.3. Besonders kritisch ist es, dass bei großflächigen Videoüberwachungen die verfassungsrechtlich gebotene und auch in der Datenschutzgrundverordnung vorgesehene Interessenabwägung einseitig zu Gunsten der Sicherheit und zu Lasten der Grundrechte erfolgen soll.

2. Zu Art. I §§ 17 – 19 des Entwurfs (Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle, Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder in Angelegenheiten der Europäischen Union):

- 2.1. Der Entwurf sieht vor, dass die oder der Bundesbeauftragte gemeinsamer Vertreter im Europäischen Datenschutzausschuss und zentrale Anlaufstelle sein soll (§ 17 Abs. 1 Satz 1 BDSG-neu). Es ist jedoch zweifelhaft, ob dem Bund hierfür die Gesetzgebungskompetenz zusteht. Die vom BMI angenommene Annexkompetenz berücksichtigt nicht ausreichend, dass die Datenschutzaufsicht im föderalen System der Bundesrepublik zwischen Bund und Ländern aufgeteilt ist. Das gilt nicht nur für die Gesetzgebungskompetenz, sondern insbesondere auch für die Ausführung von Bundesgesetzen durch die Länder (Art. 83 GG). Die Länder haben deshalb auch die Kompetenz zur Regelung des Verfahrens bei der Datenschutzaufsicht im Bereich der Wirtschaft (bis auf die Bereiche Telekommunikation und Post, für die aus historischen Gründen die Bundesbeauftragte zuständig ist) und der öffentlichen Verwaltung in Ländern und Kommunen. Die notwendige Zusammenarbeit zwischen Bund und Ländern legt es deshalb nahe, die oder den gemeinsamen Vertreter der Aufsichtsbehörden und die zentrale Anlaufstelle durch einen Bund-Länder-Staatsvertrag zu regeln.

- 2.2. Die vorgesehene Wahl des Ländervertreeters durch den Bundesrat ist mit der Unabhängigkeit der Datenschutzaufsichtsbehörden der Länder unvereinbar. Deren Leiter werden in Deutschland – ebenso wie die Bundesbeauftragte – von den jeweiligen Parlamenten gewählt. Damit wäre es nicht zu vereinbaren, wenn die Landesregierungen den Vertreter der Landesaufsichtsbehörden im Europäischen Datenschutzausschuss bestimmen könnten. Zumindest müssen die Landesdatenschutzbehörden das alleinige Vorschlagsrecht hierfür haben.
- 2.3. Für den Fall, dass eine Angelegenheit, die vom Europäischen Datenschutzausschuss behandelt wird, die Wahrnehmung von Aufgaben betrifft, die das Verfahren von Landesbehörden betreffen, muss die Bundesbeauftragte – falls sie gemeinsame Vertreterin ist – die Verhandlungsführung und das Stimmrecht im Ausschuss stets und nicht erst auf Verlangen des Stellvertreters – falls dies ein Ländervertreter ist – diesem übertragen.
- 2.4. § 18 des Entwurfs sieht vor, dass die deutschen Aufsichtsbehörden in allen Angelegenheiten der Europäischen Union nach einem bestimmten formalisierten Verfahren mit dem Ziel einer einheitlichen Anwendung der Verordnung 679/16 und der Richtlinie 680/16 zusammenzuarbeiten zu haben. Um den Koordinationsaufwand unter den Aufsichtsbehörden auf ein vernünftiges Maß zu begrenzen, sollte die in § 18 vorgesehene Zusammenarbeitsverpflichtung auf die Fälle des Kohärenzverfahrens und der vorgeschalteten oder unabhängig von einem Kohärenzverfahren stattfindenden Zusammenarbeit nach den Art. 60 – 62 beschränkt werden. Für die übrigen Bereiche hat sich die in Deutschland bisher praktizierte informelle Zusammenarbeit unter den Aufsichtsbehörden bewährt.

4. Zu Art. 1 § 23 des Entwurfs (Verarbeitung zu anderen Zwecken)

- 4.1. § 23 BDSG-neu enthält eine Reihe von Befugnissen für öffentliche und nicht-öffentliche Stellen, über die in der DS-GVO enthaltenen Regelungen hinaus Daten für andere Zwecke als den Erhebungszweck zu verarbeiten. Entgegen der Ankündigung, das Datenschutzniveau des Bundesdatenschutzgesetzes halten zu wollen, die auch durch die Hinweise („ex: § 28 II Nr. 1 BDSG“, etc.) suggeriert wird, werden deutliche Verschlechterungen des Datenschutzniveaus vorgeschlagen.
- 4.2. Nach Art. 6 Absatz 4 DS-GVO können Zweckänderungen nur durch eine Rechtsvorschrift der Mitgliedstaaten gerechtfertigt werden, die „in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Absatz 1 genannten Ziele darstellt.“ Die vorgeschlagenen Änderungen genügen dieser Maxime nicht, zumal die Vorschriften weitgehend keinen Bezug zur konkreten Verarbeitungssituation aufweisen.
- 4.3. Auch zu Art. 23 Abs. 2 DS-GVO stehen die vorgeschlagenen Zweckänderungsbefugnisse in Widerspruch. Dieser macht es zur Voraussetzung „jeder Gesetzgebungsmaßnahme im Sinne des Absatz 1“,

dass sie „insbesondere gegebenenfalls spezifische Vorschriften enthalten zumindest in Bezug auf a) die Zwecke der Verarbeitung und Verarbeitungskategorien, b) die Kategorien personenbezogener Daten, c) den Umfang der vorgenommenen Beschränkungen, d) die Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung, e) die Angaben zu dem Verantwortlichen oder den Kategorien von Verantwortlichen, f) die jeweiligen Speicherfristen sowie die geltenden Garantien unter Berücksichtigung von Art, Umfang und Zweck der Verarbeitung oder der Verarbeitungskategorien, g) die Risiken für die Rechte und Freiheiten der betroffenen Personen und h) das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung, sofern dies nicht dem Zweck der Beschränkung abträglich“ wäre.

- 4.4. Zudem ist zu bedenken, dass die zulässigen Verarbeitungen innerhalb eines Verarbeitungszwecks in Art. 6 Abs. 4 DS-GVO ohnehin erheblich weiter gefasst sind als die Zweckbindungsvorgaben nach dem BDSG-alt. Während nach derzeitigem deutschem Recht jede Zweckänderung einer gesetzlichen Erlaubnis bedarf, schränkt Art. 5 Abs. 1 lit. b DS-GVO die Zweckänderung generell nur dann ein, wenn die weitere Verwendung der personenbezogenen Daten in einer mit diesen Zwecken nicht zu vereinbarenden Weise erfolgt. Die in dem vorgeschlagenen § 23 Abs. 2 BDSG-neu enthaltenen Regelungen erweitern diese ohnehin weiten Zweckänderungsbefugnisse mit dem Ergebnis einer Kumulation zulässiger Zweckänderungen zu Lasten der Betroffenen.
- 4.5. Der Katalog der Zweckänderungsbefugnisse des § 23 Abs. 2 BDSG-neu für nicht-öffentliche Stellen ist pauschal und uferlos. Art. 23 DS-GVO richtet sich an die Mitgliedstaaten und verleiht ihnen Befugnisse zur Schaffung von Gesetzen. Der Gesetzesentwurf des BMI verwendet ähnliche oder gleich lautende Formulierungen im selben Abstraktionsgrad wie Art. 23 DS-GVO, um nicht-öffentlichen Stellen Datenverarbeitungsbefugnisse zu verschaffen. Damit erfüllt der Gesetzesentwurf nicht die an Gesetzgeber der Mitgliedstaaten gerichteten Konkretisierungsanforderungen der DS-GVO, insbesondere nicht diejenigen aus Art. 23 Absatz 2 DS-GVO. Die Befugnisse für die Mitgliedstaaten zu ergänzenden Regelungen im nationalen Recht stehen gerade unter dem Vorbehalt, dass die abstrakt gefassten Befugnisse zur Schaffung von mitgliedstaatlichem Recht ausgefüllt und auf konkrete Gesetzgebungsmaterien zugeschnitten werden, etwa in spezialgesetzlichen Datenschutzvorschriften. Mit den in der Vorschrift vorgesehenen bloßen Schaffung neuer Datenverarbeitungsbefugnisse entzieht sich der Gesetzgeber der ihm vorbehaltenen Konkretisierungsaufgabe und verstößt damit gegen die DS-GVO.
- 4.6. § 28 Abs. 2 des BDSG-alt enthält umfangreiche Abwägungserfordernisse des Interesses an einer beabsichtigten Zweckänderung mit schutzwürdigen Interessen des Betroffenen an dem Ausschluss der Verarbeitung. Diese Abwägung soll nach dem Entwurf teils entfallen. Keine Abwägung soll insbesondere mehr nötig sein bei Zweckänderungen zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten (§ 23 Abs. 2 Nr. 1 BDSG-neu), bei der Wahrung berechtigter Interessen des Verantwortlichen (Nr. 2) und bei der Geltendmachung,

Ausübung oder Verteidigung rechtlicher Ansprüche (Nr. 3). Diese schrankenlosen zusätzlichen Verarbeitungsbefugnisse widersprechen den Vorgaben der DS-GVO, die dazu verpflichten, bei Zweckänderungen entsprechende Garantien bzw. Sicherheitsmaßnahmen für die Rechte der betroffenen Personen vorzusehen.

5. Zu Art. 1 § 24 des Entwurfs (Verarbeitung im Beschäftigungskontext)

- 5.1. Im Hinblick auf den Beschäftigtendatenschutz begnügt sich § 24 BDSG-neu mit einem Minimalprogramm, indem es den alten § 32 BDSG unverändert übernimmt. Gem. Art. 88 Abs. 2 DS-GVO soll eine nationale Regelung zur Verarbeitung von personenbezogenen Daten im Beschäftigungskontext „angemessene und besondere Maßnahmen zur Wahrung der menschlichen Würde, der berechtigten Interessen und der Grundrechte der betroffenen Person, insbesondere im Hinblick auf die Transparenz der Verarbeitung, die Übermittlung personenbezogener Daten innerhalb einer Unternehmensgruppe oder einer Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, und die Überwachungssysteme am Arbeitsplatz“ umfassen.
- 5.2. Davon findet sich nichts im Referentenentwurf, der deshalb erneut nicht die Erwartungen an einen dringend erforderlichen modernen Beschäftigtendatenschutz erfüllt. Dies ist besonders bedauerlich, weil im Zuge der Digitalisierung der Arbeitswelt hier klare Grenzen der Datenerfassung und -verwendung immer dringlicher werden.

6. Zu Art. 1 § 26 des Entwurfs (Kontrollbefugnisse der Aufsichtsbehörden bei einer Geheimhaltungspflicht unterliegenden Daten)

- 6.1. § 26 schränkt den Datenschutz und die Kontrolle seiner Einhaltung bei geheimhaltungsbedürftigen Daten in unzulässiger Weise ein. So sollen Informations- und Auskunftsrechte der Betroffenen generell ausgeschlossen sein bei allen Daten, die aufgrund einer Rechtsvorschrift oder „ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten“ geheimhaltungsbedürftig sind. Diese pauschal und undifferenziert formulierte Ausnahme („wenn“ statt „solange und soweit“) geht deutlich über die in der Grundverordnung vorgesehenen Grenzen (Art. 23) hinaus und verletzt Art. 8 der Europäischen Grundrechte-Charta. Art. 23 Abs. 1 lit. i der Verordnung sieht zwar vor, dass durch Gesetze der Mitgliedstaaten die Informationspflichten und Auskunftsrechte zum Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen eingeschränkt werden können, sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt. Diese Voraussetzungen erfüllt der Entwurf in keiner Weise, denn er nimmt generell (aus welchem Grund auch immer) geheim zu haltende Daten von den Informations- und Auskunftspflichten aus. Zudem müssen gesetzliche Beschränkungen nach Art. 23 DS-GVO zum Ausgleich spezifische Vorschriften enthalten, die z.B. Garantien gegen Missbrauch oder unrechtmäßigen Zugang oder unrechtmäßige Übermittlung sowie

Speicherfristen vorsehen (Art. 23 Abs. 2 lit. a – h). Daran fehlt es im Entwurf völlig.

- 6.2. Auch die in § 26 Abs. 2 des Entwurfs vorgesehene Beschränkung der Kontrollbefugnisse der Aufsichtsbehörden auf technisch-organisatorische Maßnahmen ist unionsrechtswidrig. Die Mitgliedstaaten sind nach Art. 58 Abs. 6 nur befugt, die Prüfrechte der Aufsichtsbehörden zu erweitern („zusätzliche Befugnisse“), nicht aber zu beschränken.

7. Zu Art. 1 §§ 30 – 34 des Entwurfs (Betroffenenrechte)

- 7.1. Die in § 30 des Entwurfs vorgesehene Einschränkung der Informationspflicht bei einer Datenerhebung beim Betroffenen genügt ebenfalls nicht den Anforderungen der Verordnung. Hier vermengt der Entwurf in unzulässiger Weise Interessen der verantwortlichen Stelle (unverhältnismäßiger Aufwand) mit dem Schutz der betroffenen Person und der Rechte Dritter. Art. 13 sieht bewusst keine Ausnahme von der Informationspflicht bei unverhältnismäßigem Aufwand vor, auch Art. 23 tut dies nicht. Die gebotene Information auf eine Videoüberwachung soll nach § 30 Abs. 3 Satz 2 des Entwurfs „zum frühestmöglichen Zeitpunkt“ gegeben werden. Das lässt dem Verantwortlichen einen zu großen zeitlichen Spielraum, wann er über eine Videoüberwachung informieren will. Es muss – wie nach geltendem Recht – dabei bleiben, dass eine Videoüberwachung nur stattfinden darf, wenn spätestens mit der Aktivschaltung von Kameras auch über sie und die dafür verantwortliche Stelle informiert wird. Eine Einschränkung von Art. 13 der Verordnung ist auch in diesem Punkt nicht gerechtfertigt.
- 7.2. § 31 Abs. 1 Nr. 1 lit. a schränkt die Informationspflicht öffentlicher Stellen nach Art 14 DS-GVO schon dann ein, wenn die Information die ordnungsgemäße Erfüllung der in der Zuständigkeit der jeweiligen Stelle liegenden Aufgabe gefährden würde. Die Verordnung sieht eine solche Beschränkungsmöglichkeit – anders als bei einer Gefährdung der öffentlichen Sicherheit oder Ordnung (dazu § 31 Abs. 1 Nr. 1 lit. b) — nicht vor.
- 7.3. Aus diesem Grund geht auch die Beschränkung des Auskunftsrechts in § 32 Abs. 1 Nr. 1 des Entwurfs, der auf § 31 Abs. 1 verweist, zu weit.
- 7.4. Ein möglicher unverhältnismäßiger Aufwand für die Auskunftserteilung, der diese nach § 32 Abs. 3 entbehrlich machen soll, ist nach der Grundverordnung (im Gegensatz zu § 19 Abs. 1 Satz 3 BDSG-alt) kein zulässiger Grund für die Auskunftsverweigerung. Das gilt auch für das Auskunftsrecht nach Art. 14 der Richtlinie 680/16 (dennoch will § 51 Abs. 3 des Entwurfs in solchen Fällen die Auskunftspflicht entfallen lassen).
- 7.5. § 33 Abs. 1 des Entwurfs schränkt das Recht der betroffenen Person auf Löschung in einer mit dem Unionsrecht unvereinbaren Weise ein. Löschung soll stets dann nicht verlangt werden können, wenn diese „wegen der besonderen Art der Speicherung“ nicht oder nur mit unverhältnismäßigem

Aufwand möglich ist. Darauf könnten sich die Hersteller und Anbieter von Hard- oder Software berufen, deren Produkte eine Löschung nicht zulassen. Ziel der Grundverordnung ist es aber gerade, durch Technikgestaltung die Verarbeitung von personenbezogenen Daten auch in zeitlicher Hinsicht auf das erforderliche Maß zu beschränken. Art. 23 Abs. 1 lit. i der Verordnung ist deshalb nicht so zu verstehen, dass die Verwender von nicht datenschutzgerechter Hard- und Software (die eine Löschung nicht ermöglicht) von Betroffenenrechten freigestellt werden können.

- 7.6. § 34 ist unverständlich, weil die Vorschrift in Art. 22 Abs. 1 DS-GVO genannte „Zwecke“ erwähnt, die diese Vorschrift nicht benennt. Profiling ist kein Zweck, sondern eine besonders invasive Methode der Verarbeitung personenbezogener Daten. Bei ihr das Widerspruchsrecht nach Art. 21 generell auszuschließen, ist mit Unionsrecht nicht zu vereinbaren.

8. Zu Art. 8 (Änderung des Bundesstatistikgesetzes)

- 8.1. Im Bundesstatistikgesetz soll der Auskunfts- und Berichtigungsanspruch, der nur bis zur Löschung der Hilfsmerkmale besteht, dann nicht durchgreifen, wenn die Verwirklichung dieser Rechte die Erfüllung der Aufgaben der Statistikbehörden gefährden würde. Es ist nicht erkennbar, wann dies der Fall sein sollte. Im Zeitalter der Datenverarbeitung ist es ohne großen Aufwand und ohne Beeinträchtigung der Aufgabenerfüllung möglich, Auskunfts- und Berichtigungsansprüche betroffener Personen zu erfüllen. Art. 8 des Entwurfs ist ersatzlos zu streichen.

9. Zu Art. 10 (Inkrafttreten/Außerkräfttreten)

- 9.1. Das DSAnpUG-EU soll am 25. Mai 2018 in Kraft treten, dem Datum des Wirksamwerdens der Datenschutzgrundverordnung. Da das „Datenschutz-Anpassungs- und -Umsetzungsgesetz EU“ aber auch die Richtlinie für die Bereiche Justiz und Polizei umsetzen soll, deren Umsetzung bis zum 6. Mai 2018 zu erfolgen hat (Art. 63 Abs. 1 RL (EU) 2016/680), verstößt Art. 10 gegen das europäische Recht.