reuschlaw
Legal Consultants

Stellungnahme

anlässlich der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 27. März 2017

zum

Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)

BT-Drucksache 18/11325

begrenzt auf ausgewählte Regelungen der §§ 1 – 85 BDSG-E

von

Dr. Carlo Piltz, Rechtsanwalt
Reusch Rechtsanwälte, Berlin

Berlin
Rosenthaler Straße 40–41
10178 Berlin
T +49 30 2332895-0
F +49 30 2332895-11

Saarbrücken
Hochstraße 63
66115 Saarbrücken
T +49 681 859160-0
F +49 681 859160-11

info@reuschlaw.de
www.reuschlaw.de

Inhaltsverzeichnis

A. Zusammenfassung der Ergebnisse

Zur Anpassung an die EU Datenschutz-Grundverordnung (DSGVO):

- Auch neben der DSGVO sind nationale Regelungen möglich und zum Teil sogar verpflichtend vorgeschrieben. Der deutsche Gesetzgeber kommt mit dem vorliegenden Gesetzentwurf dieser Pflicht nach und versucht den eröffneten Gestaltungsrahmen zu nutzen. Dies ist zu begrüßen.
- Leitprinzip des nationalen Anpassungsgesetzes sollte die Schaffung von Rechtssicherheit und -klarheit sein. Widersprüche zu europäischen Vorgaben müssen vermieden werden. Andernfalls besteht das Risiko eines Verstoßes gegen das europäische Primärrecht (Art. 4 Abs. 3 des Vertrags über die Europäische Union).
- Im Rahmen der „Öffnungsklauseln" der DSGVO ist der deutsche Gesetzgeber ausdrücklich befugt, Betroffenenrechte einzuschränken. Jedoch müssen in diesen Fällen die Voraussetzungen für Beschränkungen genau beachtet werden. Teilweise gehen die vorgeschlagenen Regelungen über die eröffneten Gestaltungsspielräume hinaus und sollten daher punktuell angepasst werden.
- Nach der Rechtsprechung des Europäischen Gerichtshofs dürfen deutsche Behörden nationales Recht, welches im Konflikt mit unmittelbar geltenden europäischen Normen steht, nicht anwenden. Für die Praxis entsteht in solchen Situationen jedoch ein Zustand rechtlicher Unsicherheit, da die Kriterien, wann eine nationale Norm nicht anzuwenden ist, umstritten sind.
- Die Vorgaben zum räumlichen Anwendungsbereich des BDSG-E sollten konkretisiert und Art. 3 Abs. 1 DSGVO angepasst werden.
- Die Regelung zur Videoüberwachung mutet wie ein exklusiver Erlaubnistatbestand an. Sie sollte angepasst werden, um klarzustellen, dass die Erlaubnistatbestände der DSGVO nicht ausgeschlossen sind.
- Das vorgeschlagene Verfahren der Zusammenarbeit der nationalen Aufsichtsbehörden und deren Vertretung im Europäischen Datenschutzausschuss sollte noch mehr an die Regelungen der DSGVO angeglichen werden. Zudem bestehen offene Fragen zur Zusammenarbeit zwischen Vertreter und Stellvertreter.
- Die vorgesehenen Möglichkeiten zur zweckändernden Weiterverarbeitung gehen derzeit teilweise über die Grenzen der Art. 6 Abs. 4, 23 Abs. 1 DSGVO hinaus und sollten daher angepasst werden.
- Die angedachten „Spezifizierungen" im Bereich des Beschäftigtendatenschutzes bleiben zum Teil hinter den Erfordernissen des Art. 88 Abs. 1 DSGVO zurück, gehen andererseits aber darüber hinaus. Auch hier sollte der deutsche Gesetzgeber entsprechende Angleichungen vornehmen.

- Die Beschränkung der Untersuchungsbefugnisse der Aufsichtsbehörden gegenüber Berufsgeheimnisträgern ist zweckmäßig und sollte beibehalten werden.
- Im Rahmen der Beschränkung der Informationspflicht werden im Gesetzesentwurf zum Teil Verarbeitungssituationen und darauf bezogene Einschränkungsmöglichkeiten entgegen den Vorgaben der DSGVO vermengt. § 32 Abs. 1 BDSG-E sollte diesbezüglich überarbeitet werden.

Zur Anpassung an die Richtlinie 2016/680 (JI-RL):

- Die Einführung der Definition der Einwilligung ist zu begrüßen und sollte beibehalten werden.
- Die Einschränkung des Auskunftsrechts sollte mit Blick auf die Erreichung eines in § 15 Abs. 1 JI-RL bestimmten Zieles konkretisiert werden.
- Für Schadensersatzansprüche sollten, wie vom Gesetzgeber vorgesehen, keine Haftungshöchstgrenzen festgelegt werden. Anderenfalls besteht das Risiko, das Ziel zur Schaffung eines „wirksamen Schadenersatzes“ zu verfehlen.

B. Allgemein – Einordnung des BDSG-E und Vorgaben für den Gesetzgeber

Das Ziel der EU Datenschutz-Grundverordnung (DSGVO) ist die Vollharmonisierung der Regelungen bei der Verarbeitung personenbezogener Daten in allen Mitgliedstaaten der Europäischen Union (EU).[1] Die oft zitierte Zielvorgabe „One continent, one law" wird jedoch mit der DSGVO nicht in Gänze erreicht. Zwar wird ab dem 25. Mai 2018 ein unmittelbar anwendbares „Datenschutzgesetz" in der EU existieren. Jedoch erlaubt es die DSGVO den Mitgliedstaaten an vielen Stellen weiterhin nationale Regelungen vorzusehen. Die DSGVO ähnelt in Teilen daher eher einer europäischen Richtlinie, deren Regelungen nicht unmittelbar anwendbar sind, sondern erst nationalstattlich umgesetzt werden müssen.[2] Über diese Öffnungsklauseln, die zum Teil einen obligatorischen Regelungsauftrag erteilen, zum Teil fakultative Handlungsmöglichkeiten eröffnen, wird das Datenschutzrecht in Zukunft in Europa also auch von einer Gemengelage aus europäischem und nationalem Recht geprägt sein. Ab dem 25. Mai 2018 werden datenverarbeitende Stellen, betroffene Personen, Aufsichtsbehörden und auch Gerichte bei ihrer Anwendung der Vorschriften mit dieser Mischung aus europäischen und nationalen Vorgaben (nicht nur jenen in Deutschland) umgehen müssen. Ob dies im Ergebnis zu mehr oder weniger Rechtssicherheit in der Praxis führen wird, dürfte auch maßgeblich davon abhängen, wie die Regelungen der nationalen Datenschutzgesetze ausgestaltet sind und wie sich diese in das Gesamtregelungskonzept der DSGVO einfügen. Wichtig ist daher bereits hier darauf hinzuweisen, dass das vorgeschlagene deutsche Gesetz das Ziel haben sollte, harmonische, verständliche und praxistaugliche Regelungen zu schaffen, um Rechtsanwender und Betroffene nicht mit noch mehr Rechtsunsicherheit (die bereits allein mit Blick auf die Anwendung der DSGVO besteht) zu belasten.

I. Anwendungsvorrang von EU-Recht

Für eine adäquate Bewertung des vorgeschlagenen BDSG (BDSG-E) und auch der aus meiner Sicht noch vorzunehmenden Ergänzungen am Gesetzentwurf im Hinblick auf sein Verhältnis zur DSGVO (vgl. unter C.) ist es unerlässlich, die Grenzen zu kennen, in denen sich der deutsche Gesetzgeber bewegt, wenn er die Öffnungsklauseln der DSGVO mit Leben füllen möchte.

Treffen in der Praxis nationale und europäische Regelungen aufeinander, gilt ein Anwendungsvorrang des europäischen vor nationalem Recht.[3] Bei einem Widerspruch der nationalen Norm gegenüber der unmittelbar anwendbaren europäischen Regelung genießt letztere Anwendungsvorrang.

---

[1] ErwG 10 DSGVO.
[2] *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016 S. 1.
[3] Grundlegend hierzu: EuGH, Urt. v. 15.07.1964, C-6/64 - Costa / E.N.E.L.; vgl. auch *Terhechte*, JuS 2008, 403.

Nationales Recht ist nicht nichtig, aber nationale Stellen (sowohl Behörden und auch Gerichte) müssen im Fall einer Kollision nationales Recht unangewendet lassen.[4]

Für den deutschen Gesetzgeber wird sich beim Entwurf des BDSG-E daher stets die Frage stellen, ob bei den vorgeschlagenen Regelungen eine solche Kollision vorliegt und damit das BDSG-E nicht anwendbar wäre. Es dürfte klar sein, dass es das Ziel sein sollte, diese Situation zu vermeiden.

Dieser Konflikt europäischen Rechts mit nationalem Recht und der damit einhergehende Anwendungsvorrang des EU-Rechts entsteht dann, wenn eine direkte oder auch indirekte Kollision gesetzlicher Regelungen vorliegt.[5] Damit eine solche Kollision vorliegt, muss die europäische Norm unmittelbar anwendbar sein, was bei der DSGVO nach Art. 288 Abs. 2 AEUV der Fall ist. Zudem muss aber auch die Regelung selbst (im Sinne des konkreten Artikels und seines Wortlauts) derart gestaltet sein, dass sie im Mitgliedstaat unmittelbar angewendet werden kann. Hierzu ist erforderlich, dass die Norm hinreichend bestimmt und unbedingt formuliert ist. Für einige der Öffnungsklauseln der DSGVO trifft dieses Merkmal nicht zu, da dem nationalen Gesetzgeber, etwa hinsichtlich bestimmter Verarbeitungssituationen, nur der Rahmen an die Hand gegeben wird, den er bei der Schaffung nationaler Regelungen zu beachten hat. Innerhalb dieses Rahmens können und müssen aber nationale Datenschutzregelungen geschaffen werden, die zur Konkretisierung und Spezifizierung neben der DSGVO zur Anwendung kommen. Solange eine europäische Norm einen Sachverhalt nicht abschließend regelt, können auch nationale Regelungen bestehen bleiben und insbesondere auch eigene Vorgaben vorsehen. Ein Konflikt mit europäischem Recht existiert dann also nicht, wenn die EU-Norm einen Sachverhalt gar nicht selbst regelt bzw. aufgrund mangelnder Gesetzgebungskompetenz auf europäischen Ebene nicht selbst regeln darf. Kein Konflikt besteht auch dann, wenn kein Widerspruch zwischen nationaler und europäischer Norm existiert.

Zudem muss bei der Frage, ob ein Konflikt von europäischem und nationalem Recht besteht, stets der Anwendungsbereich der DSGVO beachtet werden. Ein Konflikt mit Ihren Regelungen ist nur möglich, soweit sich eine nationale Norm innerhalb des sachlichen Anwendungsbereich der DSGVO bewegt, der sich konkret aus Art. 2 DSGVO ergibt.

---

[4] Hierzu näher unter B. IV.
[5] Umfassend zur Situation vor dem Hintergrund der DSGVO: *Roßnagel*, in: Roßnagel, Europäische Datenschutz-Grundverordnung, 2017, S. 69 ff.; *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 3 ff.

Es bleibt mithin festzuhalten, dass unter Geltung der DSGVO weiterhin nationale Regelungen möglich sind, ja teilweise sogar verpflichtend vorgeschrieben werden. Soweit diese nationalen Regelungen die Gestaltungsspielräume der DSGVO (und die dort jeweils aufgestellten Voraussetzungen, etwa in Art. 6 Abs. 3 und Abs. 4 oder Art. 23 Abs. 1 DSGVO) erfüllen und nicht im Widerspruch zu den Zielvorgaben der DSGVO stehen, können sie angewendet werden.[6]

Die nachfolgende Stellungnahme zu den Regelungen des BDSG-E wird sich daher insbesondere auf Situationen konzentrieren, in denen ein solcher Widerspruch möglicherweise vorliegt und/oder die bindenden Vorgaben der DSGVO zum nationalen Gestaltungsspielraum nicht (in Gänze) eingehalten werden. Aufgrund des Umfangs des Gesetzesentwurfs und der für die Erarbeitung dieser Stellungnahme knapp bemessenen Bearbeitungszeit, beschränke ich meine Ausführungen auf ausgewählte Regelungsbereiche des BDSG-E.

II. Möglicher Verstoß gegen den EU-Vertrag durch Schaffung rechtlicher Unsicherheit

Aus dem Anwendungsvorrang des unmittelbar anwendbaren europäischen Rechts ergibt sich für den deutschen Gesetzgeber eine im Rahmen des hier vorliegenden Gesetzentwurfs besonders zu beachtendes Risiko. Nach der Rechtsprechung des EuGH ergeben „*sich aus der Einführung oder unveränderten Beibehaltung einer gegen eine Vorschrift des Gemeinschaftsrechts verstoßenden Bestimmung in den Rechtsvorschriften eines Mitgliedstaats, selbst wenn diese Gemeinschaftsvorschrift in der Rechtsordnung der Mitgliedstaaten unmittelbar gilt, Unklarheiten tatsächlicher Art, weil die betroffenen Normadressaten bezüglich der ihnen eröffneten Möglichkeiten, sich auf das Gemeinschaftsrecht zu berufen, in einem Zustand der Ungewissheit gelassen werden. Eine solche Beibehaltung stellt deshalb eine Verletzung der Verpflichtungen des genannten Mitgliedstaats aus dem EWG-Vertrag dar*“.[7] Nach Art. 4 Abs. 3 des Vertrags über die Europäische Union (EUV) sind die Mitgliedstaaten verpflichtet, die Union bei der Erfüllung ihrer Aufgabe zu unterstützen und müssen alle Maßnahmen unterlassen, die die Verwirklichung der Ziele der Union gefährden könnten. Eine solche Gefährdung kann sich aus gegen DSGVO verstoßende Normen im neuen BDSG ergeben, sollten diese im Widerspruch zur Verordnung stehen.[8]

III. Handlungsmöglichkeiten der Mitgliedstaaten im Rahmen von Öffnungsklauseln

[6] *Roßnagel*, in: Roßnagel, Europäische Datenschutz-Grundverordnung, 2017, S. 73.
[7] EuGH, Urt. v. 26.04.1988 – C-74/86, Rn. 10 (Kommission ./. Bundesrepublik Deutschland).
[8] So auch: *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 3.

Das hier zu bewertende DSAnpUG-EU dient mit seinem Vorschlag für ein neues BDSG in Artikel 1 der Umsetzung der fakultativen und obligatorischen Regelungsaufträge der DSGVO und auch der Richtlinie 2016/680 (zu dieser unter D.). Die Öffnungsklauseln der DSGVO stellen sich in verschiedenen Varianten dar. Sie erlauben die Konkretisierung, die Ergänzung und auch die Modifikation der Vorgaben der DSGVO.

Im Rahmen dieser Öffnungsklauseln ist es den nationalen Gesetzgebern jedoch nicht gestattet, Spezifizierungen in der Art vorzunehmen, dass ein höheres Schutzniveau als jenes der DSGVO geschaffen wird. Dies zumindest soweit, wie eine Erhöhung des Schutzniveaus nicht durch die Vorgaben der DSGVO selbst vorgesehen ist.[9] Dies ergibt sich zum einen aus den Arbeitsdokumenten des Rates zur DSGVO.[10] Insbesondere Art. 6 Abs. 2 und 3 DSGVO erlauben es den Mitgliedstaaten nicht, ein gegenüber der DSGVO höheres Schutzniveau zu schaffen.[11] Die Europäische Kommission weist zum anderen in ihrer Mitteilung zum Standpunkt des Rates darauf hin, dass die Einigung den Mitgliedstaaten Spielraum für eine Spezifizierung der Datenschutzvorschriften für den öffentlichen Sektor lässt.[12] Ein höheres Schutzniveau, insbesondere durch strengere Regelungen als sie in der DSGVO existieren, ist damit vor allem für Verarbeitungen im öffentlichen Sektor nicht gestattet. Diese Schlussfolgerungen lassen sich auch mit Blick auf den Sinn und Zweck der DSGVO und insbesondere ihren Verordnungscharakter begründen. Die Verordnung soll gerade ein einheitliches Schutzniveau schaffen, von dem nicht jeder Mitgliedstaat beliebig, sondern nur in ausdrücklich gesetzlich geregelten Fällen nach unten[13] abweichen darf. Andernfalls hätte es des Instruments der Verordnung nicht bedurft. Selbst für EU-Richtlinien hat der Europäische Gerichtshof anerkannt, dass bei einer intendierten Vollharmonisierung strengere Vorschriften nicht angewendet werden dürfen.[14] Schutzbereich und –niveau nationaler Umsetzungsregelungen müssen in diesem Fall identisch oder

---

[9] Vgl. etwa Art. 9 Abs. 4 DSGVO, mit dem Mitgliedstaaten gestattet wird, zusätzliche Beschränkungen bei der Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten einzuführen.
[10] In Ratsdokument 14732/12, 24.10.2014 wurde eine sog. Minimumharmonisierungsklausel (Art. 1 Abs. 2a) vorgeschlagen, in der es den Mitgliedstaaten ausdrücklich gestattet werden sollte, „strengere“ nationale Regelungen für die Verarbeitung personenbezogener Daten durch öffentliche Stellen vorzusehen. Dieser Vorschlag wurde nicht in den finalen Text übernommen. In Ratsdokument 9398/1/13 REV 1 ADD 1, 27.05.2013, S. 48 dort Fn. 47 forderten die deutsche und die dänische Delegation, dass Mitgliedstaaten nicht nur die Möglichkeit haben sollten, spezifischere sondern umfassendere Regelungen vorzusehen. Auch dieser Vorschlag wurde nicht übernommen.
[11] Ratsdokument 15389/14, 13.11.2014, S. 5 f.
[12] Mitteilung der Kommission an das Europäische Parlament betreffend den Standpunkt des Rates im Hinblick auf den Erlass einer Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten sowie zum freien Datenverkehr (Datenschutz-Grundverordnung) und zur Aufhebung der Richtlinie 95/46/EG, COM(2016) 214 final, 11.04.2016, S. 4.
[13] Eine solche gesetzliche Erlaubnis zur Abweichung vom aufgestellten Schutzniveau findet sich insbesondere in Art. 23 (Beschränkungen); vgl. hierzu: Stellungnahme des Juristischen Dienstes des Rates, Ratsdokument 15712/14, 18.11.2014.
[14] EuGH, Urt. v. 08.04.2003 – C-44/01, Rn. 44 (Pippig Augenoptik).

zumindest gleichwertig sein.[15] Ähnlich stellt sich die Situation unter der DSGVO dar, die dem Grunde nach eine verbindliche Verordnung ist, jedoch an eine Richtlinie erinnernde Umsetzungsmöglichkeiten für Mitgliedstaaten eröffnet.[16] Der Harmonisierungscharakter der DGSVO kann aber nur mit jenem der Vollharmonisierung einer Richtlinie verglichen werden, in deren Grenzen und nicht darüber hinausgehend, nationale Spezifizierungen möglich sind.

In der öffentlichen Diskussion um den vorliegenden Gesetzesentwurf wurde oft kritisiert, dass die Bundesregierung das Datenschutzniveau der DSGVO absenken möchte und dass dies nicht zulässig sei. Man muss es noch einmal klar sagen: die Absenkung des Schutzniveaus (so man überhaupt von einer „Absenkung" sprechen kann, wenn nationale Vorschriften den durch die DSGVO eröffneten Regelungsrahmen ausfüllen) bei der Verarbeitung personenbezogener Daten nach unten, insbesondere durch die Einschränkung der Betroffenenrechte (Art. 23 DSGVO), ist vom europäischen Gesetzgeber, auch im Bereich der Datenverarbeitung durch private Stellen, vorgesehen, gewollt und nicht unzulässig, solange die Vorgaben der DSGVO eingehalten werden. Der juristische Dienst des Rates der Europäischen Union stellt hierzu fest:[17]

„*...the Commission has accepted that there will be different levels of data protection in the draft regulation as it has proposed, and this has been accepted, that Member States could be allowed to derogate from the harmonised level of protection* ***by providing a lower protection*** *in certain cases*". (Hervorhebung durch den Autor)

Mit den Vorschlägen der Beschränkung von Betroffenenrechten im BDSG-E wird also per se nicht gegen die DSGVO verstoßen. Dem nationalen Gesetzgeber sind beschränkende Maßnahmen nach Art. 23 DSGVO ausdrücklich gestattet. Die Frage ist freilich, ob die Beschränkungen die in der DSGVO hierfür aufgestellten Anforderungen erfüllen.

IV. Dürfen die deutschen Aufsichtsbehörden das BDSG unangewendet lassen?

Aus dem vorstehend beschriebenen Anwendungsvorrang des europäischen Rechts im Konfliktfall kann sich für deutsche Datenschutzbehörde das Problem ergeben, mit, zumindest ihrer Meinung nach, europarechtswidrigen Regelungen des BDSG-E konfrontiert zu sein, die sie, aufgrund ihrer Bindung an die Gesetze (Art. 20 Abs. 3 GG), eigentlich anwenden müssten. Die Vorsitzende der Datenschutzkonferenz von Bund und Ländern, Barbara Thiel, hat hierzu kürzlich festgestellt, dass

[15] *Nils Wahl*, Schlussanträge v. 15.05.2013 – C-184/12, Rz. 42.
[16] *Kühling/Martini*, EuZW 2016, 448, 449.
[17] Ratsdokument 15712/14, 18.11.2014, S. 10.

für die Aufsichtsbehörden das Europarecht in jedem Fall bindend ist und die Aufsichtsbehörden sich in ihren Auslegungsprinzipien deshalb an der Datenschutz-Grundverordnung zu orientieren haben.[18]

Diese Problematik der (Nicht)Anwendung von möglicherweise europarechtswidrigen Normen durch nationale Behörden ist nicht neu. Wichtig ist jedoch zunächst hervorzuheben, dass es nicht um die Frage geht, ob eine Behörde eine nationale Norm als ungültig erklären darf, also etwa in einem Verwaltungsakt, sondern um die Frage der Nichtanwendung nationaler Regelungen, die ihrer Ansicht nach gegen europäisches Recht verstoßen.

Es geht mithin um die Frage, ob und gegebenenfalls unter welchen Voraussetzungen einer nationalen Behörde prinzipiell die Befugnis zusteht, Vorschriften nationalen Rechts im Falle der von ihr so beurteilten Gemeinschaftswidrigkeit außer Anwendung zu lassen.[19]

Der EuGH hat sich in der Vergangenheit oft mit dieser Frage befasst. In seiner Entscheidung vom 22.06.1989 ist er, im Fall einer EU-Richtlinie und einer damit nicht in Einklang stehenden nationalen Regelung, zu dem Ergebnis gelangt, dass eine Nichtanwendungspflicht jedenfalls dann besteht, wenn sich der Einzelne auf die gemeinschaftsrechtliche Bestimmung berufen kann.[20] Im Fall der hier vorliegenden DSGVO kann sich jeder Adressat bereits ipso iure auf ihre Regelungen berufen. Der Vorrang des Gemeinschaftsrechts bedeutet im Fall der Normenkollision eine Verpflichtung zur Nichtanwendung des nationalen Rechts und auch die öffentlichen Verwaltung ist verpflichtet, nationale Regelungen, die mit den europäischen unvereinbar sind, nicht anzuwenden.[21]

In einem weiteren Verfahren vor dem EuGH ging es um die italienische Wettbewerbsbehörde, die nationale Regelungen zum gesetzlichen Zündholzsystem Italiens auf deren Vereinbarkeit mit den Vorgaben des EU-Rechts prüfte, und die italienischen Regelungen, dies ist besonders hervorzuheben, vor jeder gerichtlichen Feststellung eines italienischen Gerichts als gemeinschaftswidrig einstufte.[22] Der EuGH entschied in diesem Fall, dass „*die Pflicht, eine dem Gemeinschaftsrecht entgegenstehende nationale Rechtsvorschrift unangewendet zu lassen, nicht nur den nationalen Gerichten obliege, sondern allen staatlichen Organen einschließlich der Verwaltungsbehörden*“.[23]

---

[18] Heise online vom 17.03.2017, Datenschutzaufsicht: Entwurf zum Bundesdatenschutzgesetz teilweise europarechtswidrig, abrufbar unter: https://www.heise.de/newsticker/meldung/Datenschutz-aufsicht-Entwurf-zum-Bundesdatenschutzgesetz-teilweise-europarechtswidrig-3657607.html.
[19] Vgl. hierzu etwa: OVG Saarlouis, Beschl. v. 22.01.2007 – 3 W 14/06; OVG Lüneburg, Urt. v. 28.11.2016 – 9 LC 335/14.
[20] EuGH, Urt. v. 22.06.1989 – C-103/88, Rn. 28 ff. (Fratelli Costanzo).
[21] *Dámaso Ruiz-Jarabo Colomer*, Schlussanträge v. 25.06.2009 – C-205/08, Rn. 51.
[22] EuGH, Urt. v. 09.09.2003 – C-198/01 (CIF).
[23] EuGH, Urt. v. 09.09.2003 – C-198/01, Rn. 49 (CIF).

Aus der Formulierung „alle Verwaltungsbehörden“ folgt, dass die genannte Nichtanwendungspflicht sich an alle zuständigen staatlichen Träger richtet.[24] Gehen also etwa in Zukunft die deutschen Datenschutzbehörden von der Europarechtswidrigkeit einer Norm des BDSG-E aus, so ist es ihnen gestattet, die nationale Regelung unangewendet zu lassen.[25] Jedoch ist darauf hinzuweisen, dass eine solche Situation und Vorgehensweise wohl insbesondere für datenverarbeitende Unternehmen ein erhebliches rechtliches Risiko darstellt und der effektiven Umsetzung des neuen Datenschutzrechts in Deutschland einen Bärendienst erweisen würde. Zudem besteht aus Sicht der Behörde das Risiko, eine nationale Norm unangwendet zu lassen, die im Ergebnis, etwa in einem anschließenden Verwaltungsgerichtsprozess mit Vorlage an den EuGH, als europarechtskonform eingestuft wird.

Im Übrigen geht auch das Bundesverwaltungsgericht davon aus, dass der Anwendungsvorrang von EU-Recht es für die Zeit des „Widerspruchs“ zwischen nationalen und europäischen Recht verbietet, die entgegenstehenden Bestimmungen des nationalen Rechts einer behördlichen oder gerichtlichen Entscheidung zugrunde zu legen.[26]

Aus Art. 20 Abs. 3 GG lässt sich nicht herleiten, dass eine Verwaltungsbehörde unmittelbar geltendes Gemeinschaftsrecht unangewendet lassen muss, um entgegenstehendem nationalem Recht den Vorrang zu verschaffen.[27] Bindung an Recht und Gesetz bedeutet im Falle des Anwendungsvorrangs von unmittelbar geltendem Gemeinschaftsrecht eine Bindung (auch) an das europäische Recht. Wie beschrieben, sind alle nationalen Behörden an unmittelbar geltendes EU-Recht gebunden. Hieraus folgt auch, dass das Gewaltenteilungsprinzip des Art. 20 GG nicht verletzt sein kann.[28]

Natürlich lässt sich diese Rechtsprechung des EuGH auch kritisieren, da es, mit Blick auf die fehlende Möglichkeit von Behörden im Vergleich zu den Gerichten, ein Vorabentscheidungsersuchen an den EuGH zu stellen, zweifelhaft erscheinen kann, warum sie dennoch verpflichtet sind, inländische Bestimmungen nicht anzuwenden.[29] Die Exekutive ist nicht befugt, gesetzliche Regelungen für ungültig zu erklären. Dies obliegt der Legislative. Es wird daher vermittelnd vorgeschlagen, nationalen Behörden die Nichtanwendung nationaler Normen dann zu gestatten, wenn die Gemeinschaftsrechtswidrigkeit evident ist.[30] Dennoch ist festzuhalten, dass die Rechtsprechung des EuGH in die-

[24] OVG Saarlouis, Beschl. v. 22.01.2007 – 3 W 14/06.
[25] So auch für deutsche Behörden in anderen Fällen: OVG Lüneburg, Urt. v. 28.11.2016 – 9 LC 335/14; OVG Saarlouis, Beschl. v. 22.01.2007 – 3 W 14/06.
[26] BVerwG, Urt. v. 29.11.1990 – 3 C 77/87.
[27] OVG Saarlouis, Beschl. v. 22.1.2007 – 3 W 14/06.
[28] OVG Saarlouis, Beschl. v. 22.1.2007 – 3 W 14/06.
[29] *Dámaso Ruiz-Jarabo Colomer*, Schlussanträge v. 25.06.2009 – C-205/08, Rn. 51; *Ruffert*, in: Calliess/Ruffert/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV Art. 288 Rn. 73.
[30] *Ruffert*, in: Calliess/Ruffert/Ruffert, EUV/AEUV, 5. Aufl. 2016, AEUV Art. 288 Rn. 73 f. mwN.

ser Frage zur Nichtanwendung nationaler Normen gefestigt erscheint. Ich tendiere für derartige Situationen, in denen eine deutsche Datenschutzbehörde in Zukunft möglicherweise Bestimmungen des BDSG-E nicht anwenden möchte, zu der eben zitierten vermittelnden Ansicht. Möchte eine Datenschutzbehörde nationale Normen nicht anwenden, sollte in jedem Fall eine Überzeugungsgewissheit über den Verstoß nationaler Bestimmungen gegen vorrangiges Gemeinschaftsrecht als erforderlich, wohl aber auch als ausreichend erachtet werden. Nicht ausreichend wäre eine bloße Vermutung der Gemeinschaftswidrigkeit.[31]

C. Rechtliche Würdigung ausgewählter Vorschriften des BDSG-E mit Bezug zur DSGVO (§§ 1 – 44 BDSG-E)

Nachfolgend werden ausgewählte Regelungen des Gesetzentwurfs vor dem Hintergrund des Anwendungsvorrangs der DSGVO insbesondere auf ihre Vereinbarkeit und Widerspruchsfreiheit mit deren Vorgaben der DSGVO untersucht. Ziel des BDSG-E muss es, wie bereits erwähnt, sein, mit der DSGVO konsistente und ihr nicht widersprechende nationale Normen zu schaffen. Nur so kann Rechtssicherheit für die datenverarbeitende Praxis (Behörden als auch private Stellen) und Betroffene hergestellt und die Gefahr einer Verletzung des EUV vermieden werden.

I. § 1 Abs. 4 – Räumlicher Anwendungsbereich

Zwar macht die DSGVO selbst keine Vorgaben dazu, wann welches nationale Datenschutzrecht, welches in Ausübung der eröffneten Spielräume der diversen (obligatorischen als auch fakultativen) Öffnungsklauseln entsteht, Anwendung findet. Bereits dieses Fehlen einer europarechtlich einheitlichen Vorgabe in der DSGVO ist zu kritisieren, aber nicht dem Bundesgesetzgeber anzulasten. Jedoch sind die Vorgaben zum räumlichen Anwendungsbereich des BDSG-E auch selbst nicht in Gänze mit der Regelung des Art. 3 DSGVO kongruent.

In Abweichung zu den Regelungen des Art. 3 Abs. 1 DSGVO bestimmt § 1 Abs. 4 S. 2 BDSG-E, dass die Vorschriften dieses Gesetzes bereits dann Anwendung finden, sofern der Verantwortliche oder Auftragsverarbeiter personenbezogen Daten im Inland verarbeitet. Nach Art. 3 Abs. 1 DSGVO findet die DSGVO Anwendung „*auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet*“.

[31] OVG Saarlouis, Beschl. v. 22.1.2007 – 3 W 14/06.

In § 1 Abs. 4 S. 2 Nr. 1 BDSG-E fehlt der Bezug zu einer Niederlassung. Auf die Verarbeitung im Rahmen der Tätigkeiten einer inländischen Niederlassung wird zwar in § 1 Abs. 4 S. 2 Nr. 2 BDSG-E Bezug genommen, der jedoch alternativ neben den anderen Varianten des § 1 Abs. 4 S. 2 BDSG-E. Anders als in Art. 3 Abs. 1 DSGVO, fehlt in § 1 Abs. 4 S. 2 Nr. 2 BDSG-E (in dem die Niederlassung angesprochen wird) aber der Zusatz, dass es irrelevant ist, ob die Datenverarbeitung technisch in der Union bzw. hier im Gebiet der Bundesrepublik Deutschland stattfindet. Es ließe sich also der Schluss ziehen, dass der deutsche Gesetzgeber es durchaus für die Frage der Anwendbarkeit des Gesetzes für relevant hält, wo personenbezogene Daten technisch verarbeitet werden, da der Hinweis „unabhängig davon, ob die Verarbeitung in der Union stattfindet“ fehlt.

Hierfür spricht die Regelung in § 1 Abs. 4 S. 2 Nr. 1 BDSG-E, wonach das Gesetz Anwendung findet, sofern der Verantwortliche oder Auftragsverarbeiter personenbezogen Daten im Inland verarbeiten. Der Regelungsbereich dieser Norm scheint sich gerade allein auf den physischen Ort der Datenverarbeitung zu beziehen, denn ansonsten (wenn es also um eine Niederlassung gehen würde) wäre er deckungsgleich mit der Vorgabe des § 1 Abs. 4 S. 2 Nr. 2 BDSG-E.

Verwirrend ist zudem die Erläuterung hierzu in der Gesetzesbegründung (S. 80). Dort wird davon gesprochen, dass die Vorschriften des BDSG-E bereits bei einer Datenverarbeitung im Inland zur Anwendung kommen, unabhängig davon, ob eine Niederlassung im Inland existiert. Der räumliche Anwendungsbereich des BDSG-E ist damit also, bei einer entsprechenden Interpretation, weiter als jener der DSGVO nach Art. 3 Abs. 1 DSGVO, da dort in jedem Fall Bezug auf eine Niederlassung genommen wird.

Inkongruent mit den Vorgaben des Art. 3 Abs. 1 DSGVO ist, zumindest wenn man sich die Gesetzesbegründung hierzu betrachtet, die Regelung des § 1 Abs. 4 S. 2 Nr. 2 BDSG-E. Laut der Gesetzesbegründung (S. 80) kommt das BDSG-E zur Anwendung, wenn eine Datenverarbeitung durch eine in Deutschland ansässige Niederlassung vorliegt. Diese Umschreibung des Anwendungsbereichs weicht jedoch entscheidend von den Vorgaben des Art. 3 Abs. 1 DSGVO bzw. § 1 Abs. 4 S. 2 Nr. 2 BDSG-E ab, wo es darauf ankommt, dass eine Datenverarbeitungen im Rahmen der Tätigkeiten einer Niederlassung vorgenommen wird. Mit Blick auf Rechtsprechung des Europäischen Gerichtshofs zu dem Merkmal „im Rahmen der Tätigkeiten“ lässt sich feststellen, dass es hierbei eben gerade nicht, wie in der Gesetzesbegründung angeführt, darum geht, dass eine Datenverarbeitung „durch“ eine Niederlassung (also faktisch von ihr selbst) vorgenommen werden muss.[32] Die Datenverarbeitung muss nur im Rahmen ihrer Tätigkeiten erfolgen und damit im Zusammenhang stehen.

[32] EuGH, Urt. v. 13.05.2014 – C-131/12, Rn. 52 (Google Spain); EuGH, Urt. v. 01.10.2015 – C-230/14, Rn. 35 (Weltimmo); *Piltz*, K&R 2014, 566, 567.

II. § 3 – Verarbeitung personenbezogener Daten durch öffentliche Stellen

Nach § 3 BDSG-E ist die Verarbeitung personenbezogener Daten durch öffentliche Stellen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

Mit § 3 BDSG-E möchte der Gesetzgeber eine Rechtsgrundlage entsprechend den Vorgaben der Art. 6 Abs. 3 S. 1, Art. 6 Abs. 1 lit. e) DSGVO schaffen. Nach Art. 6 Abs. 3 S. 2 DSGVO muss der Zweck der Verarbeitung in der Rechtsgrundlage festgelegt oder hinsichtlich einer Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, erforderlich sein. Diese Voraussetzungen sind in § 3 BDSG-E nicht in Gänze erfüllt. Denn eine Verarbeitung soll danach bereits zulässig sein, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe erforderlich ist. Kein Bezug wird auf die „öffentlichen Interessen" genommen. Grundsätzlich wäre mithin eine Verarbeitung durch eine Behörde also auch dann zulässig, wenn damit eine Aufgabe wahrgenommen wird, die nicht im öffentlichen Interesse liegt.

Nicht teilen kann ich die Kritik des Landesbeauftragten für den Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern (LfDI MV),[33] dass § 3 BDSG-E den datenschutzrechtlichen Grundsatz des Verbots mit Erlaubnisvorbehalt aufheben würde. Denn auch nach § 3 BDSG-E ist die Datenverarbeitung dem Grunde nach verboten und nur zulässig, wenn bestimmt Voraussetzungen erfüllt sind. Im Übrigen sieht die DSGVO, wie oben erwähnt, einen solchen Erlaubnistatbestand für die Verarbeitung personenbezogener Daten in Art. 6 Abs. 1 lit. e) DSGVO gerade vor.

III. § 4 – Videoüberwachung öffentlich zugänglicher Räume

Dem Wortlaut nach mutet § 4 Abs. 1 S. 1 BDSG-E wie ein exklusiver Erlaubnistatbestand an („ist nur zulässig"). Die Schaffung eigener Erlaubnistatbestände ist dem nationalen Gesetzgeber jedoch nur im Rahmen des Art. 6 Abs. 3 DSGVO gestattet, wenn es um Verarbeitungen für die in Art. 6 Abs. 1 lit. c) oder e) DSGVO bezeichneten Zwecke geht. § 4 Abs. 1 S. 1 Nr. 3 BDSG-E deckt aber auch die Datenverarbeitung durch optisch-elektronische Geräte ab, welche auf der Grundlage einer Interesseabwägung erfolgt. Für den Erlaubnistatbestand der Interessenabwägung in Art. 6 Abs. 1 lit. f) DSGVO sieht jedoch Art. 6 Abs. 3 DSGVO nicht die Möglichkeit vor, nationale Erlaubnistatbestände zu schaffen. Auch ist es dem deutschen Gesetzgeber nicht möglich, eine Legitimation der Datenver-

[33] Stellungnahme des LfDI M-V zum DSAnpUG-EU, 25.01.2017, S. 1.

arbeitung im Rahmen der Videoüberwachung über andere in der DSGVO vorgesehene Erlaubnistatbestände (etwa die Einwilligung) auszuschließen. Dem Wortlaut nach wird mit § 4 Abs. 1 BDSG-E aber gerade ein solcher Ausschluss bezweckt. Ich empfehle daher, das Wort „nur“ zu streichen und durch „insbesondere“ zu ersetzen. So wird deutlich, dass auch andere Erlaubnistatbestände eingreifen können, um die Datenverarbeitung zu legitimieren.

Der Gesetzgeber möchte in § 4 Abs. 1 S. 2 BDSG-E konkrete Vorgaben für die zu treffende Abwägungsentscheidung im Rahmen der Interessenabwägung machen. Bei der Abwägungsentscheidung sollen der Schutz von Leben, Gesundheit oder Freiheit von Personen als ein besonders wichtiges Interesse gelten. Die vorzunehmende Interessenabwägung wird damit zumindest in eine Richtung gelenkt bzw. möchte der Gesetzgeber die bei der Interessenabwägung gedanklich zum Einsatz kommende Waage bereits einseitig vorbeladen. In seinem Urteil in Sachen „Breyer“ hat der Europäische Gerichtshof festgestellt, dass die Mitgliedstaaten in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten keine anderen als die in Art. 7 der geltenden EU-Richtlinie (RL 95/46/EG) (jetzt Art. 6 DSGVO) aufgezählten Grundsätze einführen und auch nicht durch zusätzliche Bedingungen die Tragweite der sechs in Art. 7 vorgesehenen Erlaubnistatbestände verändern dürfen.[34] Ein Mitgliedstaat kann daher für diese Kategorien das Ergebnis der Abwägung der einander gegenüberstehenden Rechte und Interessen nicht abschließend vorschreiben, ohne Raum für ein Ergebnis zu lassen, das aufgrund besonderer Umstände des Einzelfalls anders ausfällt. Vorliegend dürfte man gut vertretbar argumentieren können, dass die Vorgabe in § 4 Abs. 1 Nr. 2 S. 2 BDSG-E noch nicht die Schwelle zur Unzulässigkeit einer Einschränkung der vorzunehmenden Interessenabwägung überschreitet. Denn ein Ergebnis wird nicht vorgegeben. Jedoch kann man durchaus darüber diskutieren, inwiefern mit einer solchen gesetzlichen Vorgabe noch eine unvoreingenommene und freie Interessenabwägung möglich ist.

Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind nach § 4 Abs. 2 BDSG-E durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen. Nach Art. 13 Abs. 1 DSGVO müssen Informationen bereits zum Zeitpunkt der Erhebung der Daten mitgeteilt werden. Der „frühestmögliche“ Zeitpunkt nach dem BDSG-E muss freilich in der Praxis nicht immer der Zeitpunkt der Erhebung selbst sein. Die Information des Betroffenen könnte nach § 4 Abs. 2 BDSG-E also, abweichend von Art. 13 Abs. 1 DSGVO, später erfolgen. Im Ergebnis wird hierdurch das Recht der Betroffenen auf Informationserteilung aus Art. 13 Abs. 1 DSGVO beschränkt. Man könnte überlegen, diese Beschränkung der Betroffenenrechte unter die entsprechende Gestattung zur Beschränkung nach Art. 23 Abs. 1 DSGVO zu fassen. Jedoch müsste dann

[34] EuGH, Urt. v. 19.10.2016 – C-582/14, Rn. 57 (Breyer).

geprüft werden, welche dort abschließend aufgezählten Ziele der nationalen Beschränkungsmaßnahme hier mit § 4 Abs. 2 BDSG verfolgt werden. Der Schutz von Leben, Gesundheit oder Freiheit von Personen wird in Art. 23 BDSG-E nicht genannt. Jedoch wird in Art. 23 Abs. 1 lit. i) DSGVO das Ziel des Schutzes der betroffenen Person genannt. Diesem Ziel dient wohl § 4 Abs. 1 BDSG-E. Ob jedoch auch § 4 Abs. 2 BDSG-E diesem Ziel dient, darüber lässt sich diskutieren. Denn die Information Betroffener bereits bei der Erhebung der Daten verpflichtend vorzusehen, dürfte dem intendierten Zweck des Gesetzgebers, die Videoüberwachung und damit verbundene Datenverarbeitung zu legitimieren, nicht entgegenstehen. Man sollte daher überlegen, § 4 Abs. 2 BDSG-E entsprechend anzupassen.[35]

IV. § 17 – Vertretung im Europäischen Datenschutzausschuss, zentrale Anlaufstelle

§ 17 BDSG-E regelt die Vertretung der deutschen Aufsichtsbehörden (sowohl jene des Bundes also auch der Länder) im neu zu gründenden Europäischen Datenschutzausschuss. Diese Regelungen zur Vertretung im Europäischen Datenschutzausschuss sind insbesondere deshalb relevant, weil dieser Ausschuss in Zukunft mit einer eigenen Rechtspersönlichkeit ausgestattet sein wird und die Befugnis besitzt, bindende Beschlüsse zu erlassen (vgl. 65 DSGVO).

Nach Art. 51 Abs. 3 DSGVO bestimmt ein Mitgliedstaat, in dem mehr als eine Aufsichtsbehörde existiert (also wie in Deutschland), „*die Aufsichtsbehörde, die diese Behörden im Ausschuss vertritt*“. Dem Wortlaut nach („die Aufsichtsbehörde“) kann also nur eine Aufsichtsbehörde als gemeinsamer Vertreter im Europäischen Datenschutzausschuss bestimmt werden.

Des Weiteren sieht ErwG 119 DSGVO vor, dass ein Mitgliedstaat, in dem mehrere Aufsichtsbehörden vorhanden sind, mittels Rechtsvorschriften sicherstellen soll, „*dass diese Aufsichtsbehörden am Kohärenzverfahren wirksam beteiligt werden. Insbesondere sollte dieser Mitgliedstaat eine Aufsichtsbehörde bestimmen, die als zentrale Anlaufstelle für eine wirksame Beteiligung dieser Behörden an dem Verfahren fungiert und eine rasche und reibungslose Zusammenarbeit mit anderen Aufsichtsbehörden, dem Ausschuss und der Kommission gewährleistet*“.

Nach § 17 Abs. 1 S. 1 BDSG-E soll die BfDI sowohl gemeinsamer Vertreter im Ausschuss (Art. 51 Abs. 3 DSGVO) als auch zentrale Anlaufstelle für die anderen nationalen Aufsichtsbehörden (ErwG 119 DSGVO) werden. Die Vertretung erfolgt für alle deutschen Behörden also durch eine Behörde:

[35] So such: Stellungnahme des LfDI M-V zum DSAnpUG-EU, 25.01.2017, S. 2.

die BfDI. § 17 Abs. 1 S. 2 BDSG-E sieht jedoch zusätzlich vor, dass ein Stellvertreter des gemeinsamen Vertreters durch den Bundesrat gewählt werden muss. Dieser Stellvertreter ist gleichzeitig Leiter einer Landesaufsichtsbehörde.

Mit Blick auf diese Regelungen wird man durchaus diskutieren können, ob, entsprechend den Vorgaben der DSGVO, tatsächlich allein eine einzige Aufsichtsbehörde bestimmt wird, die die anderen Behörden im Ausschuss vertritt. Diese Problematik muss aber insbesondere auch mit Blick auf die Vorgaben des § 17 Abs. 2 BDSG-E gesehen werden, der regelt, wann der gemeinsame Vertreter (also die BfDI) die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss an den Stellvertreter übertragen muss.

§ 17 Abs. 2 BDSG-E bestimmt, dass der gemeinsame Vertreter in Angelegenheiten, die die Wahrnehmung einer Aufgabe betreffen, für welche die Länder alleine das Recht zur Gesetzgebung haben, oder welche die Einrichtung oder das Verfahren von Landesbehörden betreffen, dem Stellvertreter auf dessen Verlangen die Verhandlungsführung und das Stimmrecht im Europäischen Datenschutzausschuss überträgt.

Grundsätzlich stellt sich mit Blick auf die Vorgaben des Abs. 2 die Frage, ob es einen Anspruch des Stellvertreters auf Übertragung der Verhandlungsführung gibt. Was geschieht etwa, wenn es zum Streit zwischen dem gemeinsamen Vertreter und seinem Stellvertreter kommt? Dem Wortlaut der Regelung nach ist die Verhandlungsführung und das Stimmrecht allein dann zu übertragen, wenn der Stellvertreter dies verlangt. Was geschieht aber etwa in Fällen, in denen die Kompetenz der Länder betroffen ist, unter Stellvertreter die Übertragung nicht verlangt? Kann in einem solchen Fall der gemeinsame Vertreter im Namen der Aufsichtsbehörden der Länder sprechen? Kann der Stellvertreter, etwa durch die Landesbehörden verpflichtet werden, die Übertragung der Verhandlungsführung zu verlangen?

Die Regelung des § 17 Abs. 2 BDSG-E macht die Übertragung des Stimmrechts und der Verhandlungsführung zudem zum einen davon abhängig, dass eine Aufgabe betroffen ist, für welche die Länder alleine das Recht zur Gesetzgebung haben oder aber alternativ dann, wenn es sich um eine Aufgabe handelt, welche die Einrichtung oder das Verfahren von Landesbehörden betreffen. Diese letzte Alternative scheint aber nicht im Sinne einer Exklusivität für das Vorhandensein der Landeskompetenz zu sprechen. Was geschieht also etwa in Fällen, wenn im Ausschuss eine Aufgabe bzw. Materie verhandelt wird, die sowohl die Einrichtung oder das Verfahren von Landes- als auch Bundesbehörden betreffen?

Insgesamt sollte das Verfahren zwischen gemeinsamen Vertreter und Stellvertreter entweder genauer ausgestaltet und die Übertragungsvoraussetzungen für die Verhandlungsführung genauer festgeschrieben werden oder aber es sollte allein tatsächlich ein gemeinsamer Vertreter aus den Reihen der BfDI und der Landesdatenschutzbehörden festgelegt werden.

V. § 18 – Verfahren der Zusammenarbeit der Aufsichtsbehörden des Bundes und der Länder

Nach § 18 Abs. 1 S. 1 BDSG-E arbeiten die oder der Bundesbeauftragte und die Aufsichtsbehörden der Länder (Aufsichtsbehörden des Bundes und der Länder) in Angelegenheiten der Europäischen Union mit dem Ziel einer einheitlichen Anwendung der DSGVO zusammen. Dies entspricht der Vorgabe des Art. 51 Abs. 3 DSGVO nach der, wenn in einem Mitgliedstaat mehrere Aufsichtsbehörden vorhanden sind, „*sichergestellt wird, dass die anderen Behörden die Regeln für das Kohärenzverfahren nach Artikel 63 einhalten*“. Danach arbeiten die Aufsichtsbehörden im Rahmen des in Abschnitt 2 (ab Art. 63 DSGVO) beschriebenen Kohärenzverfahrens untereinander und gegebenenfalls mit der Kommission zusammen.

Nach § 18 Abs. 1 S. 2 BDSG-E müssen sich die Aufsichtsbehörden des Bundes und der Länder vor der Übermittlung eines gemeinsamen Standpunktes an die Aufsichtsbehörden der anderen Mitgliedstaaten, die Kommission oder den Europäischen Datenschutzausschuss, „*frühzeitig Gelegenheit zur Stellungnahme*“ geben. Fraglich ist jedoch, was konkret mit „frühzeitig“ gemeint ist. Hierzu fehlt es an genauen Vorgaben. Diesbezüglich ist insbesondere zu beachten, dass in den Art. 63 ff. DSGVO teilweise bestimmte Fristen für Stellungnahmen des Europäischen Datenschutzausschuss vorgesehen sind. So etwa in Art. 64 Abs. 3 DSGVO. Insbesondere ist auch auf die Frist von 4 Wochen in Art. 60 Abs. 4 DSGVO hinzuweisen, innerhalb derer eine betroffene Aufsichtsbehörde Einspruch gegen einen Beschlussentwurf der federführenden Behörde einlegen kann. Diese in der DSGVO vorgesehenen Fristen werden leider nicht auf das Abstimmungsverfahren zwischen den deutschen Aufsichtsbehörden übertragen. So verständlich das Absehen von der Vorgabe für konkrete Fristen gegenüber den deutschen Datenschutzbehörden ist, lässt die Offenheit der Begrifflichkeiten jedoch Interpretationsspielräume, die in der Praxis zu Unsicherheiten führen können.

§ 18 Abs. 2 S. 1 BDSG-E sieht für zwischen den Aufsichtsbehörden des Bundes und der Länder streitige Fälle vor, dass, soweit die Aufsichtsbehörden des Bundes und der Länder kein Einvernehmen über den gemeinsamen Standpunkt erzielen, die federführende Behörde oder in Ermangelung einer solchen der gemeinsame Vertreter und sein Stellvertreter einen Vorschlag für einen gemeinsamen Standpunkt vorlegt. Im Grunde wird in diesem § 18 Abs. 2 BDSG-E das Verfahren der Zusammenarbeit zwischen federführender Aufsichtsbehörde und anderen betroffenen Aufsichtsbehörden des Art. 60 DSGVO kopiert. Dieser Ansatz ist durchaus auch begrüßenswert und richtig.

Jedoch fehlt in § 18 Abs. 1 und 2 BDSG-E eine dem Art. 60 Abs. 3 S. 2 DSGVO entsprechende Regelung. Danach ist die federführende Aufsichtsbehörde dazu verpflichtet, den anderen betroffenen Aufsichtsbehörden „*unverzüglich einen Beschlussentwurf zur Stellungnahme*“ vorzulegen und zusätzlich ihren „*Standpunkten gebührend Rechnung*“ zu tragen. Die Vorlage des Beschlussentwurfs ist im § 18 Abs. 1 S. 2 und Abs. 2 S. 1 BDSG-E enthalten, wenn auch das Merkmal „unverzüglich“ fehlt. Gänzlich fehlt jedoch die Pflicht, den Standpunkten der anderen betroffenen Aufsichtsbehörden (im hiesigen Fall also anderen Landesdatenschutzbehörden) gebührend Rechnung zu tragen.

§ 18 Abs. 2 S. 2 und 3 BDSG-E sehen vor, dass für den Fall, dass sich der gemeinsame Vertreter und sein Stellvertreter „*nicht auf einen Vorschlag für einen gemeinsamen Standpunkt*“ einigen, entweder der gemeinsame Vertreter oder der Stellvertreter (wenn Landesangelegenheiten betroffen sind) einen Vorschlag festlegt.

Auch bei dieser Regelung ist jedoch unklar, welche konkreten Situationen umfasst sind, wenn davon gesprochen wird, dass Aufgaben betroffen sind, „*welche die Einrichtung oder das Verfahren von Landesbehörden betreffen*“. Soll dies bedeuten, dass es um Aufgaben geht, die allein und ausschließlich die Einrichtungen betreffen oder sollen auch solche Aufgaben umfasst sein, die die Einrichtung oder das Verfahren von Landesbehörden „auch betreffen“? Falls die zweitgenannte Alternative umfasst ist, stellt sich die Frage, warum in einem solchen Fall der Stellvertreter (also der vom Bundesrat gewählte Leiter einer Landesaufsichtsbehörde) die Letztentscheidungsbefugnis haben soll, wenn eventuell auch die Einrichtung oder das Verfahren von Bundesbehörden betroffen sind.

§ 18 Abs. 2 S. 4 BDSG-E sieht vor, dass grundsätzlich der nach den Sätzen 1-3 vorgeschlagene Standpunkt den Verhandlungen im Europäischen Datenschutzausschuss zu Grunde zu legen ist, „*wenn nicht die Aufsichtsbehörden von Bund und Ländern einen anderen Standpunkt mit einfacher Mehrheit beschließen*“. Hinsichtlich dieser Regelung stellt sich die Frage, warum der deutsche Gesetzgeber nicht im Sinne eines Stufenverhältnisses, wie dies im Rahmen der Streitbeilegung durch den Europäischen Datenschutzausschuss in Art. 65 Abs. 2 DSGVO vorgesehen ist, zunächst eine Zweidrittelmehrheit bei der Stimmenabgabe der Aufsichtsbehörden verlangt. Dem Grunde nach handelt es sich ja bei dem in § 18 Abs. 2 BDSG-E geregelten Verfahren um nichts anderes, als das Streitbeilegungsverfahren auf europäischer Ebene im Europäischen Datenschutzausschuss nach Art. 65 DSGVO. Dort wird aber, wie beschrieben, zunächst eine Zweidrittelmehrheit verlangt, um streitige Angelegenheiten zwischen Aufsichtsbehörden zu klären und erst in einem zweiten Schritt, wenn eine Zweidrittelmehrheit nicht erreichbar ist, eine Abstimmung mit einfacher Mehrheit für aus-

reichend erachtet (vgl. Art. 65 Abs. 3 DSGVO). Vorteil dieser Regelung wäre, dass einem gemeinsamen Standpunkt mit Zweidrittelmehrheit (insbesondere nach Außen) ein deutlich robusteres Unterstützungsbild zugrunde liegen würde.

VI. § 19 – Zuständigkeiten

§ 19 BDSG-E trifft Regelungen zur innerstaatlichen Zuständigkeit der Aufsichtsbehörden des Bundes und der Länder im Verfahren der Zusammenarbeit und Kohärenz nach Kapitel VII DSGVO.

Nach § 19 Abs. 1 S. 3 BDSG-E findet im Falle des Streits über die Frage, welche nationale Aufsichtsbehörde als federführende Aufsichtsbehörde agiert, „*für die Festlegung der federführenden Aufsichtsbehörde…§ 18 Absatz 2 entsprechende Anwendung*“. Diese Regelung ist in der Tat erforderlich, da die DSGVO nicht die Frage der innerstaatlichen Bestimmung der federführenden Aufsichtsbehörde im Fall des Bestehens mehrerer Aufsichtsbehörden regelt. Nach der Gesetzesbegründung (S. 92) wird auf den in § 18 Abs. 2 BDSG-E vorgesehenen Mechanismus der Mehrheitsentscheidung aller Aufsichtsbehörden verwiesen.

Ein ähnlicher Mechanismus existiert auch innerhalb des Europäischen Datenschutzausschusses (Art. 65 Abs. 1 lit. b) DSGVO). Jedoch weicht das BDSG-E hier von der DSGVO in der Weise ab, dass der entsprechende Mechanismus in der DSGVO zu der Frage, wie ein Streit über die federführende Aufsichtsbehörde entschieden werden soll, von einer Abstimmung und einer Entscheidungsfindung durch Zweidrittelmehrheit abhängig gemacht wird (vgl. Art. 65 Abs. 2 S. 1 DSGVO). Hiervon weicht die Regelung des § 19 Abs. 1 S. 3 BDSG-E ab, indem sie allein die einfache Mehrheit ausreichen lässt. In der Konsequenz bedeutet dies, dass bereits eine Stimme den Ausschlag darüber gibt, welche Behörde innerhalb Deutschlands als federführende Aufsichtsbehörde gilt. Für mehr Sicherheit in der Praxis und um nach einer Wahl weitere Zwistigkeiten zwischen den Behörden möglichst zu begegnen, würde es sich anbieten, wenn man eine Zweidrittelmehrheit festschreiben würde. Freilich kann dies auch bedeuten, dass die Entscheidungsfindung schwieriger wird.

VII. § 21 – Antrag der Aufsichtsbehörde auf gerichtliche Entscheidung bei angenommener Europarechtswidrigkeit eines Angemessenheitsbeschlusses der Kommission

§ 21 BDSG-E ist Folge des EuGH-Urteils zur Ungültigkeit der Safe Harbor-Entscheidung der Europäischen Kommission.[36] Dort hatte der Gerichtshof geurteilt, dass der nationale Gesetzgeber

[36] EuGH, Urt. v. 06.10.2015 – C-362/14 (Schrems).

Rechtsbehelfe vorsehen muss, die es nationalen Kontrollstellen ermöglichen, die von ihnen als begründet erachteten Rügen gegen Angemessenheitsentscheidung der Kommission (wie etwa derzeit das EU-US Datenschutzschild) vor den nationalen Gerichten geltend zu machen. § 21 BDSG-E beruht dem Grunde nach auf einem Antrag des Landes Hamburg im Bundesrat.[37] Der damals vorgeschlagene Gesetzesentwurf enthielt noch einige kritische Regelungen.[38] Diese wurden in dem nun vorliegenden Entwurf verbessert.

Grundsätzlich zu beachten ist bei einer solchen Regelung zu einem Rechtsbehelf gegen Angemessenheitsbeschlüsse der Europäischen Kommission (dabei handelt es sich um für die Behörden bindende Beschlüsse), dass die Feststellung der Ungültigkeit eines solchen Unionsrechtsaktes allein durch den EuGH erfolgen darf.[39] Aus diesem Grund wird in § 21 BDSG-E auch nicht die Möglichkeit vorgesehen, dass das Bundesverwaltungsgericht die Ungültigkeit eines Angemessenheitsbeschlusses feststellen kann. Nach § 21 Abs. 6 S. 3 BDSG-E ist das Bundesverwaltungsgericht bei vorhandenen Zweifeln über die Gültigkeit eines Angemessenheitsbeschlusses dazu verpflichtet, die Frage der Gültigkeit im Wege des Vorabentscheidungsersuchen (Art. 267 AEUV) dem Europäischen Gerichtshof vorzulegen. Zu der in § 21 BDSG-E vorgesehenen Prüfung der Gültigkeit eines Angemessenheitsbeschlusses der Europäischen Kommission sind die nationalen Gerichte befugt.[40] Jedoch dürfte weder das Bundesverwaltungsgericht noch eine Datenschutzaufsichtsbehörde die Ungültigkeit eines Angemessenheitsbeschlusses feststellen.[41] Die vorgesehene Möglichkeit für das Bundesverwaltungsgericht, die Gültigkeit des Angemessenheitsbeschlusses der Europäischen Kommission selbst festzustellen, ist rechtlich jedoch nicht zu beanstanden und wurde so vom EuGH auch schon bestätigt.[42] Mit einer Entscheidung, dass der europäische Rechtsakt in vollem Umfang gültig ist, stellt ein nationales Gericht nämlich die Existenz des Gemeinschaftsrechtsakts nicht infrage.

Nicht völlig deutlich wird jedoch, welche verwaltungsgerichtliche Klageart in § 21 Abs. 1 BDSG-E angesprochen ist. Nach Abs. 1 „*hat die Aufsichtsbehörde ihr Verfahren auszusetzen und einen Antrag auf gerichtliche Entscheidung zu stellen*“. Es wird jedoch nicht spezifiziert, worauf genau dieser Antrag inhaltlich gerichtet sein muss, also etwa auf Feststellung der Gültigkeit/Ungültigkeit oder aber Prüfung der Gültigkeit/Ungültigkeit oder Vorlage an den Europäischen Gerichtshof. In § 21 Abs. 6 S. 1 BDSG-E wird auf § 47 Abs. 5 S. 1 VwGO verwiesen, bei dem es um die Normenkontrolle und um

[37] BR Drs. 171/1/16.
[38] Vgl. hierzu: *Piltz*, Bundesrat: Gesetzesvorschlag für ein neues Klagerecht der Datenschutzbehörden gegen Privacy Shield, abrufbar unter: https://www.delegedata.de/2016/05/bundesrat-gesetzesvorschlag-fuer-ein-neues-klagerecht-der-datenschutzbehoerden-gegen-privacy-shield/.
[39] EuGH, Urt. v. 06.10.2015 – C-362/14, Rn. 61 (Schrems).
[40] EuGH, Urt. v. 06.10.2015 – C-362/14, Rn. 62 (Schrems).
[41] EuGH, Urt. v. 06.10.2015 – C-362/14, Rn. 62 (Schrems).
[42] EuGH, Urt. v. 10.01.2006 – C-344/04, Rn. 29 (IATA und ELFAA).

ein „Antrag über die Gültigkeit“ von Satzungen oder Rechtsverordnungen geht. Aus dieser Gesamtschau kann sich ergeben, dass der Antrag tatsächlich auf die Gültigkeit Bezug nehmen muss. Wünschenswert wäre jedoch eine Klarstellung.

VIII. § 22 – Verarbeitung besonderer Kategorien personenbezogener Daten

Wie auch derzeit gilt für die Verarbeitung besonders „sensibler“[43] Daten, die besonderen Kategorien personenbezogener Daten, ein Verarbeitungsverbot, das nur in eng begrenzten Ausnahmefällen (vgl. Art. 9 Abs. 2 DSGVO) durchbrochen werden darf. Diese personenbezogenen Daten dürfen nicht verarbeitet werden, es sei denn, die Verarbeitung ist in den in der DSGVO dargelegten besonderen Fällen zulässig.[44] Hierbei ist zu berücksichtigen, dass der europäische Gesetzgeber es ausdrücklich gestattet, dass im Recht der Mitgliedstaaten besondere Datenschutzbestimmungen festgelegt werden können, um die Anwendung der Bestimmungen der DSGVO anzupassen, damit die Einhaltung einer rechtlichen Verpflichtung oder die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, möglich ist.[45] Zusätzlich zu den speziellen Anforderungen an eine derartige Verarbeitung sind aber stets die allgemeinen Grundsätze und andere Bestimmungen der DSGVO zu beachten.

Solche „besonderen Datenschutzbestimmungen“ sieht der deutsche Gesetzgeber in § 22 BDSG-E vor. Er nutzt zulässigerweise die ausdrücklichen Regelungsmöglichkeiten der Art. 9 Abs. 2 lit. b), lit. h), lit. i) und lit. g) DSGVO, um die Vorgaben der DSGVO an das nationale Recht anzupassen.

In § 22 Abs. 2 S. 1 und 2 BDSG-E setzt der Gesetzgeber das Erfordernis um, entweder „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ oder „angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person“ vorzusehen. Hinsichtlich der Vorgabe in § 22 Abs. 2 S. 2 Nr. 1 BDSG-E („technisch organisatorische Maßnahmen“) ist jedoch unklar, was konkret mit dieser Formulierung gemeint ist: sind es technische und organisatorische Maßnahmen oder schafft der deutsche Gesetzgeber eine eigene Begrifflichkeit? Dies sollte durch eine entsprechende Ergänzung klargestellt werden.

---

[43] „Sensibel“ ist nicht als Rechtsbegriff zu verstehen, wird jedoch auch vom europäischen Gesetzgeber genutzt, um das besondere Schutzbedürfnis von Daten hervorzuheben.
[44] ErwG 51 DSGVO.
[45] ErwG 51 DSGVO.

Die Kritik des Bundesrates, dass die Pflicht zur Umsetzung von Maßnahmen zum Schutz der Rechte und Interessen der Betroffenen in § 22 Abs. 2 S. 1 BDSG-E durch eine Bezugnahme auf die Einwilligung in Art. 9 Abs. 2 lit. a) DSGVO erweitert werden sollte,[46] teile ich nicht. Die Einwilligung als Erlaubnistatbestand wird durch den deutschen Gesetzgeber nicht in § 22 Abs. 1 BDSG-E als Ausnahme für die Verarbeitung besonderer Kategorien personenbezogener Daten näher ausgestaltet. Für eine auf der Grundlage der Einwilligung nach Art. 9 Abs. 2 lit. a) DSGVO erfolgende Datenverarbeitung gelten bereits die allgemeinen Bestimmungen und Grundsätze der DSGVO, mithin etwa auch Art. 32 DSGVO zur Sicherheit der Verarbeitung.

IX. § 24 – Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen

Im Gegensatz zum Referentenentwurf[47] wurden im vorliegenden Gesetzesentwurf die Möglichkeiten einer zweckändernden Weiterverarbeitung deutlich reduziert. Generell ist es zu begrüßen, dass der deutsche Gesetzgeber im Bereich der zweckändernden Weiterverarbeitung Gebrauch von der Öffnungsklausel in Art. 6 Abs. 4 DSGVO macht. Denn auch im geltenden Recht sind solche zweckändernden Datenverarbeitungen zulässig (vgl. 28 Abs. 2 BDSG).

Mit Blick auf eine Weiterverarbeitung für andere Zwecke ist durchaus umstritten, ob Mitgliedstaaten im nationalen Recht eine eigene Rechtsgrundlage für diese Weiterverarbeitung schaffen dürfen und ob Art. 6 Abs. 4 DSGVO eine solche Ermächtigung enthält. Für eine solche Ermächtigung spricht insbesondere der Wortlaut von Art. 6 Abs. 4 DSGVO. Dieser unterscheidet zwei Situationen: zum einen jene, wenn die Verarbeitung zu einem anderen Zweck auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten beruht und zum anderen, wenn dies nicht der Fall ist, welche Kriterien der Verantwortliche zu berücksichtigen hat, um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. Der erste Teil des Abs. 4 geht davon aus, dass entweder eine Einwilligung der betroffenen Person vorliegt oder, dieser Einwilligung gleichgestellt, eine Rechtsvorschrift der Mitgliedstaaten existiert, auf der die Verarbeitung zu einem anderen Zweck beruht. Bei der Einwilligung handelt es sich unstreitig um eine Rechtsgrundlage bzw. ein Erlaubnistatbestand (vgl. Art. 6 Abs. 1 lit. a) DSGVO). In der Aufzählung des Art. 6 Abs. 4 wird die „Rechtsvorschrift der Union oder der Mitgliedstaaten“ dem Erlaubnistatbestand der Einwilligung

[46] BR Drs. 110/17 (B), S. 19.
[47] Zu den dort noch viel weitergehenden Möglichkeiten für eine Verarbeitung zu anderen Zwecken: *Piltz*, Referentenentwurf zum BDSG-neu – Kurzanalyse zur zweckändernden Weiterverarbeitung nach § 23 BDSG-neu, abrufbar unter: https://www.delegedata.de/2016/11/referentenentwurf-zum-bdsg-neu-kurzanalyse-zur-zweckaendernden-weiterverarbeitung-nach-§-23-bdsg-neu/.

gleichgestellt. Dies spricht meines Erachtens dafür, dass auch der Bezug auf die „Rechtsvorschrift“ einen Erlaubnistatbestand umfasst, der sich aus dem Recht der Mitgliedstaaten ergibt.

Art. 6 Abs. 4 DSGVO stellt gewisse Anforderungen an die nationale Rechtsvorschrift, die eine zweckändernde Weiterverarbeitung gestattet. Die Rechtsvorschrift muss eine in einer demokratischen Gesellschaft notwendige und verhältnismäßige Maßnahme zum Schutz der in Art. 23 Abs. 1 DSGVO genannten Ziele darstellen. Zu diesen Zielen gehören: die nationale Sicherheit; die Landesverteidigung; die öffentliche Sicherheit; die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit; den Schutz sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses der Union oder eines Mitgliedstaats, insbesondere eines wichtigen wirtschaftlichen oder finanziellen Interesses der Union oder eines Mitgliedstaats, etwa im Währungs-, Haushalts- und Steuerbereich sowie im Bereich der öffentlichen Gesundheit und der sozialen Sicherheit; den Schutz der Unabhängigkeit der Justiz und den Schutz von Gerichtsverfahren; die Verhütung, Aufdeckung, Ermittlung und Verfolgung von Verstößen gegen die berufsständischen Regeln reglementierter Berufe; Kontroll-, Überwachungs- und Ordnungsfunktionen, die dauernd oder zeitweise mit der Ausübung öffentlicher Gewalt für die unter den Buchstaben a bis e und g genannten Zwecke verbunden sind; den Schutz der betroffenen Person oder der Rechte und Freiheiten anderer Personen; die Durchsetzung zivilrechtlicher Ansprüche.

Im Ergebnis muss man, möchte man die Vereinbarkeit des vorgeschlagenen § 24 BDSG-E mit der DSGVO feststellen, prüfen, ob alle in § 24 BDSG-E aufgeführten Tatbestände diese Anforderungen erfüllen. Zudem müssen die Erlaubnistatbestände jeweils notwendig und verhältnismäßig sein, um die oben benannten Ziele zu schützen.

Nach § 24 Abs. 2 Nr. 1 BDSG-E ist die Weiterverarbeitung zulässig, wenn sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist. Diese Regelung ist von Art. 23 Abs. 1 DSGVO abgedeckt. Nach § 24 Abs. 2 Nr. 2 BDSG-E ist die Weiterverarbeitung zulässig, wenn sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche. Diese Ausnahme ist nur zum Teil von Art. 23 Abs. 1 lit. j) DSGVO abgedeckt. Dort wird auf die „*Durchsetzung* ***zivilrechtlicher*** *Ansprüche*“ (Hervorhebung durch den Autor) verwiesen.[48] § 24 Abs. 2 Nr. 2 BDSG-E geht jedoch dem Wortlaut nach darüber hinaus, indem allgemein „rechtliche“ Ansprüche umfasst sind und nicht nur zivilrechtliche.[49] Die Norm sollte entsprechend den Vorgaben des Art. 23 Abs. 1 lit. j) DSGVO angepasst werden.

---

[48] Diese Formulierung geht im Übrigen auf den Vorschlag der deutschen Delegation im Rat der Europäischen Union zurück, vgl. Ratsdokument 14270/1/14 REV 1, 24.20.2014, dort Fn. 100.
[49] So auch die Kritik des Bundesrates, BR Drs. 110/17 (B), S. 21 f.

Für nicht gerechtfertigt halte ich die Kritik des Bundesrates und den damit zusammenhängenden Änderungsvorschlag, in § 24 Abs. 1 Nr. 2 nach dem Wort „Ansprüche“ die Wörter „gegenüber der betroffenen Person“ einzufügen.[50] Weder aus dem Wortlaut des Art. 21 Abs. 1 lit. j) DSGVO noch aus den Erwägungsgründen ergibt sich, dass zivilrechtliche Ansprüche allein gegenüber der betroffenen Person bestehen sollen.

X. § 26 – Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses

§ 26 Abs. 1 BDSG-E entspricht dem bekannten § 32 BDSG. In § 26 BDSG-E wird im Ergebnis für den Beschäftigtendatenschutz nur das festgeschrieben, was bisher in Deutschland gilt.

§ 26 BDSG-E stützt sich auf Art. 88 DSGVO. Dabei handelt es sich um eine fakultativ nutzbare und keine verpflichtende Öffnungsklausel. Nach Art. 88 Abs. 1 DSGVO können die Mitgliedstaaten durch Rechtsvorschriften oder durch Kollektivvereinbarungen „*spezifischere Vorschriften zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext*“ vorsehen.

Es stellt sich jedoch die Frage, ob es sich bei § 26 Abs. 1 BDSG-E tatsächlich um „spezifischere Vorschriften“ handelt oder ob der Entwurf nicht dahinter zurückbleibt. Der europäische Gesetzgeber hatte, dies wird aus der beispielhaften Aufzählung von Verarbeitungssituationen in Art. 88 Abs. 1 DGVO deutlich, tatsächlich Konkretisierungen der allgemeinen Datenschutzvorgaben der DSGVO für bestimmte Lebenssachverhalte und damit zusammenhängende Datenverarbeitungen angedacht. So etwa für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz. Regelungen zu solch spezifischen Situationen und Verarbeitungszwecken enthält § 26 BDSG-E jedoch nicht. § 26 Abs. 1 S. 1 BDSG-E nennt nur allgemein die „Zwecke des Beschäftigungsverhältnisses“. Dieser allgemeine Zweck ist aber ohnehin von Art. 88 DSGVO vorausgesetzt, in dessen Rahmen dann speziellere Zweck und zugrundliegende Datenverarbeitungen und damit zusammenhängende Rechte der Betroffenen festgelegt werden sollen. Möglicherweise erfüllt § 26 Abs. 1 BDSG-E also nicht die Voraussetzungen der Öffnungsklausel des Art. 88 Abs. 1 DSGVO, da eine Spezifizierung nicht im Sinne der DSGVO erfolgt. Diesbezüglich wird eine klarstellende Überarbeitung der Vorschrift angeregt.

[50] Vgl. BR Drs. 110/17 (B), S. 22 f.

Zudem gilt es auch hier die jüngste Rechtsprechung des EuGH zur Beschränkung der Verarbeitungsmöglichkeiten im nationalen Recht zu beachten.[51] Mitgliedstaaten dürfen die Tragweite der Erlaubnistatbestände nicht national verändern. Zwar spricht der Wortlaut von § 26 Abs. 1 S. 1 BDSG-E nicht absolut eindeutig dafür, dass die Datenverarbeitung im Beschäftigungskontext allein zulässig sei soll, wenn die in § 26 Abs. 1 BDSG-E vorgesehenen Voraussetzungen gegeben sind. Denn es wird, anders als etwa in § 4 Abs. 1 S. 1 BDSG-E, nicht vorgeschrieben, dass die Verarbeitung „nur" zulässig ist. Jedoch sollte der Gesetzgeber darüber nachdenken, klarstellend darauf hinzuweisen, dass mit § 26 Abs. 1 BDSG-E nicht ausgeschlossen ist, dass eine Datenverarbeitung im Beschäftigungskontext stets auf einen der Erlaubnistatbestände des Art. 6 Abs. 1 DSGVO gestützt werden kann.

Ob der deutsche Gesetzgeber die Vorgaben der DSGVO wirklich nur „spezifiziert" oder über eine Spezifizierung hinausgeht, könnte man im Hinblick auf die Regelung in § 26 Abs. 2 S. 3 BDSG-E in Frage stellen. Danach bedarf die Einwilligung grundsätzlich der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der deutsche Gesetzgeber kreiert damit eine formelle Voraussetzung für die Einwilligung im Beschäftigungsverhältnis.[52] Begründet wird diese Regelung damit, dass hierdurch die Nachweispflicht des Arbeitgebers im Sinne von Art. 7 Abs. 1 DSGVO konkretisiert werde. Jedoch erscheint fraglich, ob die Schaffung einer zusätzlichen Voraussetzung für die Wirksamkeit der Einwilligung tatsächlich noch als „Spezifizierung" angesehen werden kann. Zudem gesteht auch der Gesetzgeber in der Begründung ein, dass es sich nicht um eine Spezifizierung im Sinne des Art. 88 Abs. 1 DSGVO handelt, sondern um eine solche des Art. 7 Abs. 1 DSGVO. Auch der Bundesrat empfiehlt die Streichung des Schriftformerfordernisses, wenn auch aus Gründen eines potentiell erhöhten bürokratischen Aufwandes.[53] Die gleiche Kritik lässt sich für die Vorgabe in § 26 Abs. 2 S. 4 BDSG-E vorbringen, nach dem der Arbeitgeber die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 DSGVO in Textform aufzuklären hat. Auch diese Regelung scheint über eine reine Spezifizierung der Vorschriften der DSGVO für Datenverarbeitungen im Beschäftigungsverhältnis hinauszugehen und tatsächlich eher zusätzlicher Voraussetzungen für die Datenverarbeitung aufzustellen. Die Information der betroffenen Person in Textform ist in Art. 7 Abs. 3 DSGVO nicht vorgesehen.

Für sinnvoll erachte ich den Vorschlag des Bundesrates, § 26 Abs. 1 S. 2 BDSG-E in der Weise anzupassen, dass nach den Wörtern "Zur Aufdeckung von Straftaten" die Wörter "oder anderer schwerer Verfehlungen" sowie nach den Wörtern "eine Straftat" die Wörter "oder eine andere

---

[51] EuGH, Urt. v. 19.10.2016 – C-582/14 (Breyer); vgl. hierzu auch die Anmerkungen zu § 4 BDSG-E unter C. III.
[52] So ausdrücklich die Gesetzesbegründung, BT Drs. 18/11325, S. 97.
[53] BR Drs. 110/17 (B), S. 24.

schwere Verfehlung" eingefügt werden.[54] Hierdurch würde insbesondere für die Praxis rechtliche Sicherheit bei internen Ermittlungsmaßnahmen und damit zusammenhängende Datenverarbeitungen geschaffen, ohne dass damit eine besondere Einschränkung der Betroffenenrechte verbunden wäre.

XI. § 29 – Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten

In § 29 Abs. 3 S. 1 BDSG-E macht der Gesetzgeber von der Öffnungsklausel des Art. 90 DSGVO Gebrauch und beschränkt die Untersuchungsbefugnisse der Datenschutzbehörden, soweit die Inanspruchnahme der Befugnisse die Geheimhaltungspflicht verletzen würde.

Entgegen anderen Ansichten ist diese Beschränkung verhältnis- und zweckmäßig.[55] In Art. 90 Abs. 1 DSGVO sieht der europäische Gesetzgeber gerade die Möglichkeit vor, ausgewählte Untersuchungsbefugnisse (jene nach Art. 58 Abs. 1 lit. e) und f) DSGVO) zu beschränken. Ohne diese Einschränkung der Befugnisse der Aufsichtsbehörden kann es in der Praxis zu einer Kollision mit Pflichten des Geheimnisträgers kommen. Ausdrücklich nur für diesen Fall sieht § 29 Abs. 3 S. 1 BDSG-E eine Beschränkung vor. Die Ausgestaltung dieser Beschränkung in der Form eines gänzlichen Ausschlusses der Untersuchungsbefugnisse in konkreten Situationen ist von der Regelungsmöglichkeit des Art. 90 Abs. 1 DSGVO gedeckt.[56]

XII. § 32 – Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person

Die Beschränkungen der Informationspflichten (§§ 32, 33 BDSG-E) stützt der Gesetzgeber auf Art. 23 Abs. 1 DSGVO. Wie auch im Fall der zweckändernden Weiterverarbeitung, sind in diesem Fall die Anforderungen des Art. 23 Abs. 1 und Abs. 2 DSGVO zu beachten.

Nach § 32 Abs. 1 Nr. 1 BDSG-E besteht die Pflicht zur Information der betroffenen Person gemäß Art. 13 Abs. 3 DSGVO (Fall der Weiterverarbeitung) ergänzend zu der in Art. 13 Abs. 4 DSGVO

---

[54] BR Drs. 110/17 (B), S. 23 f.
[55] Kritisch: Stellungnahme des LfDI M-V zum DSAnpUG-EU, 25.01.2017, S. 25; Unabhängigen Datenschutzbehörden der Länder: Entwurf zum Bundesdatenschutzgesetz verspielt Chance auf besseren Datenschutz!, abrufbar unter: https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/pm_der_DSBen_zum_BDSG-neu.pdf.
[56] *Piltz*, in: Gola, DS-GVO, 2017, Art. 90 Rn. 10.

genannten Ausnahme nicht, wenn die Erteilung der Information einen unverhältnismäßigen Aufwand erfordern würde und das Interesse der betroffenen Person als gering anzusehen ist.

Zunächst ist darauf hinzuweisen, dass diese Beschränkung im BDSG-E sich nicht auf die „normale“ Informationspflicht nach Art. 13 Abs. 1 und 2 DSGVO bezieht, sondern spezifisch nur den Fall der Weiterverarbeitung betrifft. Dennoch ist die Beschränkung kritisch zu sehen.

Der Gesetzgeber scheint in § 32 Abs. 1 Nr. 1 BDSG-E auf den Grundgedanken des Art. 14 Abs. 5 lit. b) DSGVO („die Erteilung dieser Informationen sich als unmöglich erweist“) abstellen und diesen in den Regelungsbereich des Art. 13 DSGVO übertragen zu wollen. Es handelt sich bei den Ausnahmen des Art. 13 und Art. 14 DSGVO jedoch um strukturell unterschiedliche Situationen.[57] Art. 14 Abs. 5 DSGVO erfasst Situationen, wenn Daten nicht beim Betroffenen erhoben werden. Art. 13 DSGVO bezieht sich jedoch auf Fälle der Direkterhebung, um die es auch in der Ausnahmevorschrift des § 32 Abs. 1 BDSG-E gehen soll. Im Endeffekt setzt sich der Gesetzgeber damit in § 32 Abs. 1 BDSG-E über die Vorgaben von Art. 13 Abs. 4 und Art. 14 Abs. 5 DSGVO hinweg.

Es hat durchaus seinen Sinn, dass die Ausnahme des Art. 14 Abs. 5 lit. b) DSGVO nicht in Art. 13 DSGVO genannt ist. Bei einer Direkterhebung beim Betroffenen soll es verständlicherweise weniger Ausnahmen von der Informationspflicht geben, denn für den Verantwortlichen ist es in dieser Situation (direkter Kontakt mit dem Betroffenen) einfacher, die Informationen zu erteilen. Dieses Prinzip unterläuft § 32 Abs. 1 BDSG-E.

Gegen die in § 32 Abs. 1 Nr. 1 BDSG-E vorgeschlagene Ausnahme spricht zudem die Systematik der DSGVO. In Art. 13 Abs. 4 DSGVO (im Fall der Direkterhebung) existiert allein eine Ausnahme (wenn der Betroffene die Informationen bereits besitzt). Diese Ausnahme gibt es auch im Art. 14 Abs. 5 lit. a) DSGVO (der Fall, wenn Daten nicht beim Betroffenen erhoben werden). Dies zeigt, dass der europäische Gesetzgeber manche Ausnahmen in beiden Situationen als begründbar und vertretbar ansah und entsprechend aufnahm, andere Ausnahmen, die alleine in Art. 14 Abs. 5 lit. b) DSGVO existieren, aber explizit nicht in Art. 13 Abs. 4 DSGVO für Situationen der Direkterhebung geltend lassen wollte.

Wie schon im Rahmen der vorgeschlagenen Regelungen zur Weiterverarbeitung (vgl. unter C. IX.), sollte auch in § 32 Abs. 1 Nr. 4 BDSG-E das Wort „rechtlicher“ durch „zivilrechtlicher“ ersetzt werden. Der Wortlaut des insoweit zu beachtenden Art. 23 Abs. 1 lit. j) DSGVO bezieht sich ausdrücklich

[57] Vgl. auch die Kritik des Bundesrates, BR Drs. 110/17 (B), S. 34 f.

allein auf „zivilrechtliche“ Ansprüche.[58] Das Abstellen auf „rechtliche“ Ansprüche würde über den in der Ausnahmevorschrift des Art. 23 Abs. 1 lit. j) DSGVO festgelegten Regelungsbereich für nationale Vorschriften hinausgehen. Ebenfalls wie im Rahmen der Stellungnahme zu § 24 BDSG-E halte ich jedoch die Kritik und den Anpassungsvorschlag des Bundesrates, in § 32 Abs. 1 Nr. 4 BDSG-E nach dem Wort „Ansprüche“ die Wörter „gegenüber der betroffenen Person“ einzufügen, nicht für angebracht. Weder aus dem Wortlaut des Art. 21 Abs. 1 lit. j) DSGVO noch aus den Erwägungsgründen ergibt sich, dass zivilrechtliche Ansprüche allein gegenüber der betroffenen Person bestehen sollen.

XIII. § 35 – Recht auf Löschung

In § 35 Abs. 1 S. 1 BDSG-E schränkt der Gesetzgeber das Recht der betroffenen Person auf Löschung und die damit korrespondierende Pflicht des Verantwortlichen aus Art. 17 Abs. 1 DSGVO ein. Zwar ist eine nationale Beschränkung des Betroffenenrechts der Löschung aus Art. 17 Abs. 1 DSGVO grundsätzlich über die Regelung des Art 23 Abs. 1 DSGVO vorgesehen und möglich. Jedoch wird aus dem Gesetzesentwurf und insbesondere auch der Gesetzesbegründung nicht deutlich, welches der in Art. 23 Abs. 1 DSGVO abschließend aufgezählten Ziele mit dem Vorschlag in § 35 Abs. 1 S. 1 BDSG-E erreicht werden soll. Der Gesetzgeber verweist in der Begründung auf Art. 23 Abs. 2 lit. c) DSGVO. Dieser Verweis geht jedoch zur Begründung der Beschränkung fehl, da in Art. 23 Abs. 2 DSGVO die Anforderungen an die nationale Maßnahme festgelegt werden, jedoch nicht das in jedem Fall erforderliche Ziel, welches eine solche Maßnahme erreichen will. Diese Ziele finden sich allein in Art. 23 Abs. 1 DSGVO.

Welches der in Art. 23 Abs. 1 DSGVO genannten Ziele mit § 35 Abs. 1 S. 1 BDSG-E erreicht werden soll, bleibt unklar und es steht zu befürchten, dass mit dieser Beschränkung des Löschungsrechts keines der dort aufgezählten Ziele verfolgt wird. Der in § 35 Abs. 1 S. 1 BDSG-E benannte Grund für die Beschränkung, dass die Löschung wegen der besonderen Art der Speicherung überhaupt nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist, findet sich in dieser Form nicht als Ziel in der Auflistung in Art. 23 Abs. 1 DSGVO. § 35 Abs. 1 S. 1 BDSG-E sollte vor diesem Hintergrund, um einen Verstoß gegen die DGSVO zu vermeiden, entsprechend auf eine Zielvorgabe angepasst oder gestrichen werden.[59]

XIV. Einwilligung Minderjähriger

[58] So auch der Bundesrat, BR Drs. 110/17 (B), S. 35 f.
[59] So auch der Bundesrat mit einem Anpassungsvorschlag, BR Drs. 110/17 (B), S. 39 f.

Macht der deutsche Gesetzgeber, meines Erachtens dem Grunde nach durchaus berechtigterweise, von vielen Öffnungsklauseln der DSGVO Gebrauch, so wird die Regelungsmöglichkeit des Art. 8 Abs. 1 DSGVO hinsichtlich der Festlegung einer Altersgrenze bei der Einwilligung durch Minderjährige jedoch nicht genutzt. Mir ist durchaus bewusst, dass es schwierig erscheint, eine fixe Altersgrenze festzulegen, ab der davon ausgegangen werden darf, dass Minderjährige selbst über die Verwendung ihrer personenbezogenen Daten entscheiden können. Anderseits existiert hier die Möglichkeit, eine im Datenschutzrecht bisher kontrovers diskutierte und bisher letztendlich unbeantwortete Frage anzugehen. Die Festlegung einer Altersgrenze würde in diesem Bereich für Rechtssicherheit sorgen. Dass eine verbindlich gesetzliche Entscheidung zur Altersgrenze nicht auf allseitigen Zuspruch stoßen wird, dürfte klar sein. Meines Erachtens überwiegen jedoch die Vorteile, eine (insbesondere für die datenverarbeitenden Stellen, aber gerade auch die betroffenen Minderjährigen und Eltern) verbindliche Vorgabe hinsichtlich der Altersgrenze zu etablieren. Bestenfalls sollte eine solche Festlegung im gegenseitigen Einvernehmen mit europäischen Mitgliedstaaten erfolgen, um auf diese Weise einen EU-weiten Gleichlauf der Altersgrenze zu statuieren.

Falls der Bundesgesetzgeber bewusst keine Regelung zur Einwilligung Minderjähriger getroffen hat und damit implizit zu verstehen gibt, dass seiner Ansicht nach wirksame Einwilligungen erst mit Vollendung des 16. Lebensjahres abgegeben werden können (vgl. Art. 8 Abs. 1 DSGVO), sollte darüber nachgedacht werden, zumindest diese Erwägung in der Gesetzesbegründung aufzunehmen.[60] Jedoch sollte hierbei im Blick behalten werden, dass sich der deutsche Gesetzgeber in weit sensitiveren Lebensbereichen dazu entschlossen hat, eine niedrigere Altersgrenze anzusetzen. So etwa nach § 36 Abs. 1 S. 1 SGB I, wonach Personen, die das 15. Lebensjahr vollendet haben, Anträge auf Sozialleistungen stellen können. Oder in § 2 Abs. 2 Transplantationsgesetz, nach dem mit Vollendung des 16. Lebensjahres in die Organspende eingewilligt werden kann und bereits ab dem vollendeten 14. Lebensjahr ein entsprechender Widerspruch erklärt werden kann.

D. Rechtliche Würdigung einzelner Aspekte der Vorschriften zur Umsetzung der Richtlinie (EU) 2016/680

Neben der von der Öffentlichkeit mit weitaus mehr Aufmerksamkeit bedachten DSGVO wurde gleichzeitig auch die Richtlinie (EU) 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (JI-RL) verabschiedet. Mit

[60] In der deutschen Literatur wird derzeit, soweit keine gesetzliche Vorgabe existiert, jedoch wohl zumeist von einer Altersgrenze von 14 Jahren ausgegangen, wobei es auf die Einsichtsfähigkeit im Einzelfall ankommt, vgl. *Schulz*, in: Gola, DS-GVO, 2017, Art. 8 Rn. 10.

den §§ 45 bis 85 BDSG-E setzt der deutsche Gesetzgeber die Regelungen der JI-RL gemeinsam mit den Anpassungen zur DSGVO im neuen BDSG-E um.

Erstmals wird mit der JI-RL eine Unionsregelung für Datenverarbeitungen im Bereich der Gefahrenabwehr und Strafverfolgung existieren.[61] Anders als bei der DSGVO, sind die Regelungen der JI-RL zwingend durch den deutschen Gesetzgeber in nationales Recht zu überführen. Die JI-RL ist „nur" hinsichtlich des zu erreichenden Ziels verbindlich (Art. 288 Abs. 3 AEUV). Ziele der JI-RL sind nach ErwG 93 JI-RL die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz ihrer personenbezogenen Daten und den ungehinderten Austausch personenbezogener Daten im Verkehr zwischen den zuständigen Behörden innerhalb der Union zu gewährleisten. Diese Ziele werden in Art. 1 Abs. 2 JI-RL noch einmal ausdrücklich wiederholt und dem deutschen Gesetzgeber damit quasi als Leitlinie bei seiner Umsetzungsarbeit mit auf den Weg gegeben.

I. Mindestharmonisierung durch die JI-RL

Im Gegensatz zur DSGVO (vgl. oben B. III.) bezwecken die Vorgaben der JI-RL nur eine Mindestharmonisierung (wenn auch auf hohem Niveau) der Datenschutzvorgaben in ihrem Anwendungsbereich. Betroffene Personen sollen damit einen unionweit einheitlichen Schutz genießen (ErwG 15 JI-RL). Mitgliedstaaten ist es aber ausdrücklich gestattet (Art. 1 Abs. 3 JI-RL), Garantien (also gesetzliche Regelungen) festzulegen, die strenger sind also jene der JI-RL (vgl. auch ErwG 15). Die Mitgliedstaaten dürfen also bei der Umsetzung der JI-RL das Schutzniveau[62] nach oben „durchbrechen".[63] Diese Möglichkeit der Schutzniveauerhöhung spielt auch im Rahmen des hier vorliegenden Gesetzesentwurfs eine Rolle.

II. § 46 Nr. 17 – Einwilligung

In § 46 Nr. 17 JI-RL definiert der Gesetzgeber die datenschutzrechtliche Einwilligung legal, indem er die Definition aus Art. 4 Nr. 11 DSGVO übernimmt. Die JI-RL selbst enthält keine Definition der Einwilligung, schließt sie als Erlaubnistatbestand für die Verarbeitung in ihrem Anwendungsbereich aber auch nicht aus. Dies ergibt sich aus ErwG 35 JI-RL, der Situationen benennt, in denen die Einwilligung nicht als freiwillig erteilt angesehen werden kann. Jedoch wird auch ausdrücklich darauf verwiesen, dass es Situationen geben kann, in denen die Einwilligung als Erlaubnistatbestand in

---

[61] *Kühling/Martini et al.*, Die DSGVO und das nationale Recht, 2016, S. 5.
[62] Wobei es meines Erachtens teilweise schwierig sein kann, datenschutzrechtliche Normen danach zu bewerten, ob das Schutzniveau gesenkt oder erhöht wird; denn es kommt bei einer solchen Bewertung, wie so oft, auf die Perspektive an.
[63] Stellungnahme des Juristischen Dienstes des Rates, Ratsdokument 15712/14, 18.11.2014.

Betracht kommt. Dass der deutsche Gesetzgeber hier auf die Definition der DSGVO zurückgreift, halte ich (insbesondere im Hinblick auf eine Vereinheitlichung der Anforderungen) für richtig. Nicht teilen kann ich daher die Kritik des Bundesrates, der die Übernahme der Definition aus der DSGVO mit dem Hinweis bemängelt, dass bei der Normierung von Anforderungen an eine wirksame Einwilligung der strenge Maßstab der DSGVO auf den Anwendungsbereich der Richtlinie übertragen wird.[64] Gerade wenn sich Betroffene den Strafverfolgungsbehörden gegenüber sehen und in die Verarbeitung ihrer Daten einwilligen sollen, halte ich hohe rechtliche Anforderungen für die Rechtsmäßigkeit der Verarbeitung durch die Behörden für sinnvoll. Auch die Kritik, dass durch die neue Definition „noch striktere Vorgaben" gemacht werden, verfängt nicht. Wie oben erläutert, ist es dem deutschen Gesetzgeber ausdrücklich gestattet, das Schutzniveau im Vergleich zu den harmonisierten Vorgaben der JI-RL zu erhöhen.

III. § 49 – Verarbeitung zu anderen Zwecken

In § 49 S. 2 BDSG-E regelt der Gesetzgeber die Weiterverarbeitung von zu Zwecken des § 45 BDSG-E erhobenen Daten (also jenen, die in den Anwendungsbereich der JI-RL fallen) zu anderen als in § 45 BDSG-E genannten Zwecken. Es handelt sich mithin um Zwecke, die außerhalb des Anwendungsbereichs der JI-RL liegen. Für diese Weiterverarbeitung ist grundsätzlich die DSGVO einschlägig, vgl. ErwG 34 JI-RL. § 49 S. 2 BDSG-E verweist aber nicht auf die DSGVO, sondern allein auf eine „Rechtsvorschrift". Eventuell sollte der Gesetzgeber, wie in ErwG 34 JI-RL spezifiziert, klarstellen, dass es sich sowohl um eine nationale als auch insbesondere eine Rechtsvorschrift des EU-Rechts handeln kann.

IV. § 57 – Auskunftsrecht

In § 57 Abs. 2 BDSG-E legt der Gesetzgeber fest, wann keine Auskunft gegenüber Betroffenen erteilt werden muss. Dem Wortlaut nach („Absatz 1 gilt nicht…") nimmt der Gesetzgeber personenbezogene Daten in bestimmten Verarbeitungssituation per se aus dem Anwendungsbereich des Auskunftsrechts heraus. Ob eine solche Herausnahme bestimmter personenbezogener Daten von der JI-RL gedeckt ist, erscheint zumindest fraglich. Selbst wenn man aber grundsätzlich von der Anwendbarkeit des Auskunftsrechts ausgeht, begegnet § 57 Abs. 2 BDSG-E Bedenken. Mit der Vorschrift wird das Auskunftsrecht in jedem Fall vollständig eingeschränkt. Eine solche vollständige Einschränkung ist grundsätzlich möglich und in Art. 15 Abs. 1 JI-RL vorgesehen.

[64] BR Drs. 110/17 (B), S. 43.

Jedoch muss die einschränkende gesetzliche Maßnahme einem der in Art. 15 Abs. 1 lit. a) bis e) JI-RL aufgeführten Zwecke dienen. Die Gesetzesbegründung zu § 57 Abs. 2 BDSG-E verhält sich aber nicht dazu, welcher Zweck mit der Einschränkung verfolgt wird. Eine Einschränkung in Fällen, in denen die Auskunftserteilung einen unverhältnismäßigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist, findet sich in der Aufzählung des Art. 15 Abs. 1 JI-RL nicht. Ich würde daher anregen, den mit der Einschränkung verfolgten Zweck i.S.d. Art. 15 Abs. 1 JI-RL genau zu bezeichnen oder aber § 57 Abs. 2 BDSG-E zu überarbeiten.

V. § 65 – Meldung von Verletzungen des Schutzes personenbezogener Daten an die oder den Bundesbeauftragten

Abweichend von Art. 30 Abs. 1 JI-RL bezieht sich der deutsche Gesetzgeber in § 65 Abs. 1 BDSG-E (und auch in anderen Regelungen) nicht auf ein „Risiko“, sondern die „Gefahr“ für Rechtsgüter natürlicher Personen. In allgemeinen Sprachgebrauch mögen diese Begrifflichkeiten synonym verwendet werden. In der Wissenschaft und Fachkreisen, werden beide Begriffe jedoch unterschiedlich verstanden und definiert.[65] Warum der Gesetzgeber vom Begriff „Risiko“ Abstand nimmt, ergibt sich aus der Gesetzesbegründung nicht. Ich schlage daher entweder die Aufnahme einer Erläuterung zur Abweichung gegenüber der JI-RL oder eine entsprechende Anpassung des § 65 BDSG-E (und auch anderer betroffener Vorschriften) vor.

VI. § 83 – Schadensersatz und Entschädigung

Meiner Auffassung nach zurecht sieht § 83 BDSG-E keine Begrenzung des Schadensersatzbetrages der Höhe nach vor. Ein solcher Höchstbetrag wird in Art. 56 JI-RL nicht festgelegt und auch nicht als Regelungsoption für die Mitgliedstaaten vorgesehen. Der Anregung des Bundesrates, im weiteren Gesetzgebungsverfahren zu prüfen, ob unter Geltung der JI-RL Spielräume für eine gesetzliche Höchstgrenze verbleiben,[66] würde ich vor dem Hintergrund eines möglichen Verstoßes gegen die Vorgaben der JI-RL nicht entsprechen. So gibt ErwG 88 JI-RL generell vor, dass Schäden, die einer Person aufgrund einer Verarbeitung entstehen, von dem Verantwortlichen oder einer anderen nach dem Recht der Mitgliedstaaten zuständigen Behörde ersetzt werden sollen. Zudem verlangt der europäische Gesetzgeber in ErwG 88 JI-RL, dass die betroffenen Personen einen vollständigen und

[65] Bundesinstitut für Risikobewertung, „Risiko“ oder „Gefahr“? Experten trennen nicht einheitlich, abrufbar unter: http://www.bfr.bund.de/de/presseinformation/2010/04/_risiko__oder__gefahr___experten_trennen_nicht_einheitlich-48560.html.
[66] BR Drs. 110/17 (B), S. 43 f.

wirksamen Schadenersatz für den erlittenen Schaden erhalten müssen. Jede Schaffung eines Höchstbetrages birgt das Risiko, dem Ziel eines „wirksamen Schadenersatzes“ entgegenzustehen.

Berlin, den 22. März 2017

Dr. Carlo Piltz