Die Bundesbeauftragte
für den Datenschutz und
die Informationsfreiheit

Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)93

BfDI

Antworten

der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
Andrea Voßhoff

auf die Fragen für das Fachgespräch

„Europäische Datenschutz-Grundverordnung“

Ausschuss Digitale Agenda am 24. Februar 2016

1) *Wie sind die Ergebnisse des Trilogs zur Datenschutzgrundverordnung aus Ihrer Sicht grundsätzlich zu bewerten? Im Zusammenhang mit der Datenschutzgrundverordnung sind Big Data, Ubiquitous Computing, Cloud Computing und andere datenzentrierte Geschäftsmodelle diskutiert worden. Sind diese Möglichkeiten der modernen Datenverarbeitung - vor dem Hintergrund der getroffenen Regelungen zur Weiterverarbeitung und Pseudonymisierung - aus Ihrer Sicht weiterhin möglich? Welche Auswirkungen auf den internationalen Wettbewerb sind für europäische Anbieter zu erwarten? Inwiefern wird die Datenschutzgrundverordnung den gestiegenen Herausforderungen hinsichtlich eines effektiven Grundrechtschutzes angesichts neuer Arten der Datenerfassung, Speicherung, Verarbeitung und Weitergabe an Dritte insgesamt gerecht?*

BfDI: Die Ergebnisse des Trilogs zur Datenschutz-Grundverordnung (DSGVO) bewerte ich insgesamt positiv. Zunächst ist anzuerkennen, dass es den für

die Rechtssetzung verantwortlichen Organen der EU gelungen ist, sich auf einen gemeinsamen Rechtsakt zu verständigen. Dies war nicht zu jedem Zeitpunkt der Verhandlungen selbstverständlich. Die Einigung zeigt nicht nur, dass die EU in der Lage ist, gemeinsam wichtige Entscheidungen zu treffen. Sie hat vielmehr auch zu erkennen gegeben, dass trotz der vielfach artikulierten Partikularinteressen der einende Wille vorhanden ist, für ganz Europa ein einheitliches Datenschutzrecht zu schaffen und die heterogene Landschaft stärker zu harmonisieren.

Auch aus inhaltlicher Sicht kann sich die Einigung durchaus sehen lassen. Dabei ist zuallererst zu betonen, dass sich die DSGVO konsequent an dem durch das Primärrecht vorgegebenen grundrechtlichen Rahmen, insbesondere an Art. 8 GRCh und Art. 16 AEUV, orientiert. Damit ist auch die grundsätzliche Entscheidung gefallen, dass die bestehenden Prinzipien des Datenschutzes weiterhin gelten und im künftigen Rechtsrahmen verankert werden müssen. Dazu gehören die Anknüpfung an den Begriff des Personenbezugs ebenso wie die Aufrechterhaltung der Legitimation der Datenverarbeitung entweder durch die autonome Entscheidung des Einzelnen (Einwilligung oder vertragliche Beziehung) oder einen gesetzlichen Erlaubnistatbestand. Abgerundet wird dieser Rahmen durch die Prinzipien der Datensparsamkeit, der Angemessenheit und Erforderlichkeit, der Zweckbindung und Transparenz sowie der Kontrolle und Sanktionierung durch unabhängige Datenschutzbehörden.

Datenzentrierte Geschäftsmodelle werden unter der DSGVO weiterhin möglich sein. Die in der Frage genannten Beispiele haben sich jedoch jeweils den Grundprinzipien des Datenschutzrechts ebenso unterzuordnen wie dies hinsichtlich anderer rechtlicher Rahmenbedingungen (z. B. Verbraucherschutzrecht, Urheberrecht, Strafrecht) der Fall ist. Geschäftsmodelle sind somit immer dann möglich, wenn sie datenschutzrechtlich auch zulässig sind. Dies ist jeweils im Einzelfall zu prüfen. Ich setze darauf, dass die Digitalwirtschaft intelligente Lösungen entwickelt, um die enormen Potentiale der Datenwirtschaft auch datenschutzgerecht auf den Markt zu bringen. Klar sein muss aber auch, dass nicht jedes Geschäftsmodell nur deshalb zulässig sein kann, weil es technisch möglich ist.

Wie schon erwähnt, schreibt die DSGVO den Grundsatz der Zweckbindung fort und erlaubt wie das geltende Recht eine Änderung des ursprünglichen Verarbeitungszwecks nur dann, wenn der neue Zweck mit dem ursprünglichen vereinbar ist. Anders als die geltende Richtlinie von 1995 stellt die DSGVO jedoch in Art. 6 Abs. 3a Kriterien auf, die bei der Beurtei-

lung der Vereinbarkeit zu berücksichtigen sind. Unter anderem ist in diese Prüfung die Frage einzubeziehen, ob die Daten in pseudonymisierter Form oder verschlüsselt weiterverarbeitet werden. Ich halte diese beiden Kriterien im Zusammenhang mit der Prüfung der Zweckvereinbarkeit zwar systematisch für verfehlt, da die technischen Maßnahmen von Pseudonymisierung und Verschlüsselung keinerlei Zusammenhang mit der Zweckbestimmung der Datenverarbeitung aufweisen. Der Gesetzgeber wollte hier jedoch gerade vor dem Hintergrund datenzentrierter Geschäftsmodellen offenbar eine vorsichtige Privilegierung der Verarbeitung pseudonymisierter bzw. verschlüsselter personenbezogener Daten vornehmen.

Die Auswirkungen auf europäische Anbieter im internationalen Wettbewerb vermag ich nicht zu beurteilen. Dies wird entscheidend davon abhängen, inwieweit außerhalb Europas datenschutzfreundliche und vertrauenswürdige Geschäftsmodelle nachgefragt werden, mit anderen Worten davon, wie hoch das Datenschutzbewusstsein weltweit ausgeprägt ist. In jedem Falle führt die DSGVO jedoch zu einheitlichen Wettbewerbsbedingungen innerhalb des europäischen Marktes und das für alle Anbieter, die auf diesem Markt tätig sind. Diese Tatsache kann angesichts eines Marktes von 500 Millionen Verbrauchern nicht hoch genug eingeschätzt werden und ich verspreche mir davon natürlich eine Ausstrahlung weit über Europa hinaus.

Insgesamt glaube ich, dass die DSGVO den Herausforderungen gerecht wird und einen robusten Grundrechtsschutz ermöglicht, auch wenn ich mir in einigen Punkten durchaus mehr gewünscht hätte. Dies betrifft zum Beispiel die Anforderungen an die Einwilligung, die im Regelfall nicht ausdrücklich erteilt werden muss. Ebenso sind Regelungen zum Profiling zum Teil enttäuschend, da es nicht gelungen ist, das Anlegen und Speichern von Profilen zu regulieren, sondern weiterhin nur Entscheidungen, die auf der Grundlage von Profilen getroffen werden, von der Regulierung betroffen sind.

2) *Wird mit der Datenschutzgrundverordnung der erhoffte einheitliche und europaweite Rechtsrahmen für den Datenschutz erreicht, der europaweit einen hohen Datenschutzstandard garantiert, und kann hierdurch insbesondere auch das Marktortprinzip Wettbewerbsgleichheit für alle Anbieter, die in Europa ihre Dienste anbieten, sichergestellt werden? Wird die Umsetzung der Datenschutzgrundverordnung gleiche und faire Wettbewerbsbedingungen für deutsche und europäische Unternehmen sowie US-amerikanische Unternehmen herstellen?*

BfDI: Wie unter Frage 1. bereits ausgeführt, gewährleistet die DSGVO einen europaweit einheitlichen Rechtsrahmen für den Datenschutz und erreicht einen höheren Grad an Harmonisierung als dies derzeit der Fall ist. Dies gilt jedenfalls für den Datenschutz im Bereich der Wirtschaft. Im Bereich der Datenverarbeitung durch Behörden und öffentliche Stellen erlaubt die DSGVO durch zahlreiche zum Teil sehr weitreichende Öffnungsklauseln weiterhin eine höhere Vielfalt an national spezifischen Datenschutzvorschriften.

Ich erwarte, dass das Marktortprinzip für gleiche Wettbewerbsbedingungen für alle Unternehmen sorgen wird, die Waren und Dienstleistungen auf dem europäischen Markt anbieten. Insbesondere werden auch ausländische Unternehmen nur dann Zugang zum europäischen Binnenmarkt erhalten, wenn sie sich an die hier geltenden Regelungen halten. Die zurzeit bestehende Wettbewerbsverzerrung etwa zwischen US-amerikanischen und europäischen Unternehmen sollte damit weitgehend beendet werden können.

3) *Welcher Änderungsbedarf ergibt sich aus der Verabschiedung der Datenschutzgrundverordnung für das deutsche Datenschutzrecht und die zahlreichen bereichsspezifischen Vorgaben? Von welchen Öffnungsklauseln sollte der nationale Gesetzgeber zwingend Gebrauch machen, um über die Vorgaben der Datenschutzgrundverordnung hinausgehende Regelungen zu schaffen? In welchen Bereichen besteht zukünftig kein Spielraum mehr für den nationalen Gesetzgeber? Wo sehen Sie für den nationalen Gesetzgeber nach der Verabschiedung der Datenschutzgrundverordnung noch Möglichkeiten, Regelungen im nicht-öffentlichen Bereich zu schaffen? Sehen Sie insbesondere Handlungsbedarf seitens des Gesetzgebers im Bereich der Beschäftigtendaten? Und wenn ja, in welcher Form? Was kann man außerhalb der Gesetzgebung tun, um den Datenschutz in Umsetzung der Datenschutzgrundverordnung in Deutschland zu fördern?*

BfDI: Hinsichtlich des Anpassungsbedarfs im deutschen Datenschutzrecht ist zunächst grundsätzlich zwischen dem öffentlichen und dem nicht-öffentlichen Bereich zu differenzieren. Die bereichsspezifischen Vorschriften im öffentlichen Bereich werden aufgrund der Öffnungsklauseln in Art. 6 Abs. 2a, Art. 6 Abs. 3, Art. 9 Abs. 5, Art. 21 und in Kapitel IX zum ganz überwiegenden Teil erhalten bleiben können. Allerdings wird jeweils durch den Gesetzgeber zu prüfen sein, in welchem Umfang eine Anpassung und

Rechtsbereinigung notwendig ist. Die Bundesregierung bereitet diese Arbeiten unter Federführung des BMI zurzeit vor.

Im nicht-öffentlichen Bereich bestehen hingegen deutlich geringere Spielräume für nationale Regelungen. Eine wichtige Möglichkeit, auch in diesem Bereich nationale Bestimmungen zu erlassen, besteht im Zusammenhang mit dem Profiling: Art. 20 Abs. 1a lit. b) DSGVO erlaubt es den Mitgliedstaaten, vom Verbot der ggf. auch auf Profiling beruhenden automatisierten Einzelentscheidung abzuweichen, wenn eine Rechtsvorschrift eine solche Ausnahme vorsieht. Diese Rechtsvorschrift muss die Rechte und Freiheiten der betroffenen Personen und deren berechtigte Interessen wahren. Dies könnte etwa für die Regelungen zum Scoring (§ 28b BDSG) von Bedeutung sein.

Von welchen Öffnungsklauseln die deutschen Gesetzgeber in Bund und Ländern Gebrauch machen sollten, hängt zunächst davon ab, ob es sich um zwingend umzusetzende Regelungen handelt oder nicht. Im ersteren Falle besteht kein Spielraum und die Mitgliedstaaten müssen nationales Recht schaffen. Dazu gehören beispielsweise die Vorschriften zur Einrichtung und näheren Ausgestaltung der Aufsichtsbehörden (Art. 46 bis 49 DSGVO) einschließlich des Rechtsschutzes gegen deren Entscheidungen (Art. 53 Abs. 2 DSGVO) und eines Klagerechts für die Aufsichtsbehörden (Art. 53 Abs. 3 DSGVO) sowie deren Vertretung im Europäischen Datenschutzausschuss (EDSA – Art. 46 Abs. 2 DSGVO). Zwingender Umsetzungsbedarf besteht darüber hinaus auch beim Rechtsschutz gegen die Verhängung von Geldbußen (Art 79 Abs. 4 DSGVO) und der Regelung weitergehender Sanktionen (Art. 79b DSGVO) sowie bei der Umsetzung des Medienprivilegs (Art. 80 DSGVO).

Da die Aufsichtsbehörden auch im öffentlichen Bereich Anordnungs- und Untersagungsbefugnisse (Art. 53 Abs. 1b DSGVO) erhalten werden, müssen auch hierfür die verfahrens- und prozessrechtlichen Voraussetzungen geschaffen werden, damit insbesondere diese Maßnahmen auch gerichtlich überprüfbar sind.

Über den zwingenden Umsetzungsbedarf hinaus enthält die DSGVO eine Reihe von optionalen Öffnungsmöglichkeiten. Neben der bereits erwähnten Anpassung und Bereinigung des bereichsspezifischen Rechts möchte ich vor allem auf zwei Bereiche hinweisen, in denen aus meiner Sicht dringender Bedarf nationaler Rechtssetzung besteht:

Zum einen betrifft dies die Möglichkeit, gem. Art. 35 Abs. 4 DSGVO auch in weiteren als den in Art. 35 Abs. 1 DSGVO genannten Fällen die verpflichtende Bestellung betrieblicher und behördlicher Datenschutzbeauftragter vorzusehen. Ich halte es für unabdingbar, dass Deutschland hiervon Gebrauch macht und sein bewährtes Zwei-Säulen-Modell aus innerbetrieblichem Datenschutz und staatlicher Aufsicht beibehält. Dieses hat enorm zu dem heute vorhandenen Datenschutzbewusstsein beigetragen und gewährleistet datenschutzrechtliche Compliance auf einem unbürokratischen und effektiven Weg. § 4f Abs. 1 BDSG sollte daher weitgehend erhalten bleiben.

Zum anderen sollte Art. 82 der DSGVO zum Anlass genommen werden, endlich ein Beschäftigtendatenschutzgesetz zu schaffen, das für einen spezifischen Schutz des Einzelnen in dem durch Abhängigkeitsverhältnisse geprägten Beschäftigtenkontext sorgt.

Außerhalb der Gesetzgebung gibt es vielfältige Möglichkeiten, den Datenschutz weiter zu fördern. Dies kann einerseits unmittelbar durch die in der DSGVO vorgesehenen Instrumente wie Verhaltensregeln (Art. 38, 38a DSGVO), Zertifizierungen (Art. 39, 39a DSGVO) oder auch die Aufklärungs- und Öffentlichkeitsarbeit der Datenschutzbehörden (Art. 52 Abs. 1 lit. aa DSGVO) geschehen. Andererseits erhoffe ich mir aber auch eine gezielte Förderung datenschutzfreundlicher Technologien und Geschäftsmodelle, etwa im Bereich der Anonymisierungstechniken oder der Umsetzung von Privacy by Design und Privacy by Default.

4) *Lässt die Datenschutzgrundverordnung ausreichend Spielraum für Innovation? Leistet sie einen Beitrag dazu, dass Datenschutz sich als Wettbewerbsvorteil für europäische Unternehmen etablieren kann? Wo und warum sehen Sie in dem neuen Regelungswerk positive und wo negative Effekte für die deutsche und europäische Wirtschaft?*

BfDI: Meines Erachtens lässt die DSGVO nicht nur ausreichend Spielraum für Innovation, sondern fordert diese geradezu heraus: Nur durch Innovation und Kreativität können Geschäftsmodelle entwickelt werden, die das Potential einer immer mehr datenzentrierten Ökonomie weitgehend nutzbar machen und dabei zugleich die datenschutzrechtlichen Rahmenbedingungen beachten. Insofern bedarf es einer höheren Innovationskraft als in Rechtsordnungen, in denen die grundrechtliche Gewährleistung des Datenschutzes gar nicht oder weniger ausgeprägt ist als in Europa.

Daher bin ich mir sicher, dass die DSGVO einen Beitrag dazu leistet, Datenschutz als Wettbewerbsvorteil zu etablieren. Hierzu bedarf es eines selbstbewussten und offensiven Herausstellens der Vorteile datenschutzgerechter Geschäftsmodelle, während das lautstarke Klagen über datenschutzrechtliche Beschränkungen eher das Gegenteil bewirkt.

Im Übrigen verweise ich auf die Antworten zu den Fragen 1. und 2.

5) *Wie kann man eine flächendeckende Datenschutzaufsicht und -kontrolle im Hinblick auf das in der Verordnung verankerte „one-stop-shop"-Verfahren gewährleisten und dabei dem deutschen Föderalismus mit seinen Länderdatenschutzbeauftragten ausreichend Rechnung tragen? Welche Möglichkeiten sehen Sie, das innerstaatliche Kooperationsverfahren auszugestalten? Wie kann die Vertretung der deutschen Datenschutzaufsicht in Brüssel gewährleistet werden, ohne dass eine Doppelvertretung von Bundes- und Landesdatenschutzaufsichtsbehörden erfolgt, und wie könnte das Verfahren konkret ausgestaltet werden?*

BfDI: Die DSGVO gewährleistet, dass flächendeckend eine staatliche Datenschutzaufsicht durch die Aufsichtsbehörden ausgeübt werden kann. Der One-Stop-Mechanismus führt bei (innereuropäischer) grenzüberschreitender Verarbeitung personenbezogener Daten zu einer Zuständigkeitskonzentration bei der Aufsichtsbehörde in dem Mitgliedstaat, in dem sich die Hauptniederlassung oder die einzige Niederlassung eines Unternehmens befindet. Damit haben die Unternehmen einen zentralen Ansprechpartner an ihrem Hauptsitz, der grundsätzlich auch für die Durchsetzung des Datenschutzrechts zuständig ist. Die Abstimmung mit den anderen zuständigen Aufsichtsbehörden (in deren Mitgliedstaaten sich entweder ein weiterer Sitz des Unternehmens befindet oder erhebliche Auswirkungen auf Betroffene bestehen können) erfolgt mithilfe des One-Stop-Mechanismus', auf dessen Grundlage ggf. durch den EDSA europaweit verbindliche Entscheidungen der Aufsichtsbehörden getroffen werden. Damit können sich die Unternehmen auf eine europaweit konsistente Anwendung des Datenschutzrechts verlassen und erlangen ein deutlich höheres Maß an Rechtssicherheit. Für die Betroffenen bietet die DSGVO auch bei grenzüberschreitender Datenverarbeitung wiederum den Vorteil, dass „ihre" Aufsichtsbehörde vor Ort ihre Beschwerden bearbeitet und sie in ihrem Mitgliedstaat auch Rechtsschutz suchen können.

Für die föderale Aufsichtsstruktur in Deutschland ist die Durchführung des One-Stop-Mechanismus‘ und die Vertretung im EDSA eine besondere Herausforderung. Art. 46 Abs. 2 DSGVO schreibt für Mitgliedstaaten mit mehreren Aufsichtsbehörden vor, dass eine Aufsichtsbehörde zu bestimmen ist, die die Vertretung im EDSA wahrnimmt und dass ein Verfahren einzuführen ist, dass die Durchführung des Kohärenzverfahrens gewährleistet. Aus EG 93 ergibt sich zudem, dass eine zentrale Kontaktstelle eingerichtet werden soll, die eine wirksame Beteiligung der anderen Aufsichtsbehörden am Kohärenzverfahren sicherstellen und die reibungslose Zusammenarbeit mit dem EDSA, den Aufsichtsbehörden der anderen Mitgliedstaaten und der Europäischen Kommission gewährleisten solle. Art. 64 Abs. 3 DSGVO bestimmt erneut, dass nach dem mitgliedstaatlichen Recht ein gemeinsamer Vertreter der Aufsichtsbehörden als Mitglied im EDSA zu benennen ist.

Aus meiner Sicht müssen die grundsätzlichen Voraussetzungen in einem Bundesgesetz geregelt werden. Dieses sollte den gemeinsamen Vertreter nach Art. 64 Abs. 3 DSGVO bestimmen, die Grundzüge des Abstimmungsverfahrens zwischen den deutschen Aufsichtsbehörden regeln und die Einrichtung der zentralen Kontaktstelle festlegen. Die Außenvertretung der deutschen Datenschutzbehörden im EDSA sollte grundsätzlich durch die BfDI wahrgenommen und die zentrale Kontaktstelle bei ihr eingerichtet werden. Soweit innerstaatlich Zuständigkeiten der Datenschutzaufsichtsbehörden der Länder bestehen, ist dies entsprechend zu berücksichtigen, etwa in dem entsprechende Positionen von diesen im EDSA vertreten werden. Als Vorbild hierfür könnte das abgestufte System der Vertretung der Länderinteressen nach dem EUZBLG dienen. Jedenfalls muss sichergestellt werden, dass die deutschen Aufsichtsbehörden entsprechend der Bedeutung Deutschlands als größtem Mitgliedstaat der EU eine starke Stimme darstellen und sich wirksam und einheitlich innerhalb der EU positionieren können.

6) *Wie bewerten Sie die Datenschutzgrundverordnung vor dem Hintergrund des Safe-Harbor-Urteils des EuGH von Oktober 2015 sowie des sogenannten „EU-US Privacy Shield“ mit von der Europäischen Kommission ausgehandelten Kontrollbefugnissen und Rechten für europäische Bürger gegenüber amerikanischen Datenverarbeitern, das Anfang des Monats von der Europäischen Kommission vorgestellt wurde?*

BfDI: Die DSGVO sieht in Art. 41 Abs. 1 die Möglichkeit vor, dass die EU-Kommission im Wege eines Durchführungsrechtsaktes feststellt, dass in einem Drittstaat ein angemessenes Datenschutzniveau besteht. Die Entscheidung kann sich auch auf einen oder mehrere Sektoren eines Drittstaates beziehen. Diese Vorschriften könnten als Rechtsgrundlage für einen neuen Angemessenheitsbeschluss, etwa des „EU-US Privacy Shield“ dienen.

Ebenso wie der EuGH in seiner Entscheidung vom 6. Oktober 2015 sieht Art. 41 Abs. 2 lit. a) DSGVO u. a. vor, dass auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht und Zugang von Behörden zu personenbezogenen Daten die Einhaltung von Rechtstaatlichkeit und die Achtung der Menschenrechte und Grundfreiheiten in dem betreffenden Drittland wichtiger Maßstab für die Angemessenheitsentscheidung sind. Zudem müssen den Betroffenen wirksame und durchsetzbare Rechte sowie wirksame verwaltungsrechtliche und gerichtliche Rechtsbehelfe zur Verfügung stehen. Darüber hinaus verlangt Art. 41 Abs. 2 lit. b) DSGVO in dem betreffenden Drittland die Existenz und wirksame Funktionsweise unabhängiger Aufsichtsbehörden einschließlich angemessener Sanktionsbefugnisse und der Unterstützung der Betroffenen bei der Wahrnehmung ihrer Rechte. Insofern setzt die DSGVO die Vorgaben des EuGH auf gesetzlicher Ebene weitgehend um.

Ob das von der EU-Kommission Anfang Februar 2016 vorgestellte „EU-US Privacy Shield“ diese Bedingungen erfüllt, kann erst beurteilt werden, wenn die Einzelheiten hierzu bekannt sind. Die Art-29-Gruppe der Europäischen Datenschutzbehörden hat die Kommission um Vorlage der entsprechenden Vereinbarungen bis Ende Februar 2016 ersucht.

7) *Kann Großbritannien tatsächlich eine Ausnahmeregelung in Anspruch nehmen, der zufolge die Sperrklausel des Art. 43 a Datenschutzgrundverordnung bei der Datenübermittlung an Drittstaaten keine Anwendung findet? Falls ja, wie bewerten Sie diesen Sachverhalt und welche Konsequenzen hätte dies für den Datenaustausch innerhalb von Europa und für britische Unternehmen?*

BfDI: Nach Medienberichten falle Art. 43a DSGVO nach Ansicht der britischen Regierung unter Protokoll Nr. 21 zum AEUV. Danach beteiligt sich Großbritannien nicht an der Annahme von Maßnahmen im Bereich der polizeilichen und justiziellen Zusammenarbeit im Sinne von Titel V AEUV, sofern

Großbritannien dem nicht ausdrücklich zustimmt („opt-in“). Offiziell liegen mir hierzu allerdings weder von Seiten der EU noch von Seiten der Bundesregierung Erkenntnisse vor. Die oben zitierte Auslegung des Protokolls Nr. 21 zum AEUV halte ich für äußerst zweifelhaft. Die DSGVO trifft keine Regelungen im Bereich der polizeilichen und justiziellen Zusammenarbeit. Vielmehr ergibt sich die Regelungskompetenz der EU aus Art. 16 AEUV, einer Regelung, die nicht in Titel V AEUV verortet ist. Auch inhaltlich geht es bei Art. 43a DSGVO nicht um die polizeiliche und justizielle Zusammenarbeit, sondern um eine spezifische Übermittlungsvorschrift, die sich an verantwortliche Stellen in der EU richtet, die gerade nicht dem Polizei- und Justizbereich zuzurechnen sind. Dass auf Seiten des potentiellen Übermittlungsempfängers auch ausländische Polizei- oder Justizbehörden stehen können, ist insoweit ohne Belang, da diese von der DSGVO naturgemäß gar nicht reguliert werden.

Würde die Auffassung Großbritanniens zutreffen, würde dies eine deutliche Schwächung des Datenschutzes bedeuten, da dann Unternehmen und Behörden in Großbritannien auch ohne das Erfordernis von Rechtshilfevereinbarungen personenbezogene Daten an ausländische Behörden und Gerichte übermitteln dürften.

8) *In Erwägungsgrund 40 wird die Weiterverarbeitung von personenbezogenen Daten erlaubt, wenn es sich dabei um eine aufgrund einer Rechtsvorschrift (seitens der Europäischen Kommission oder der Mitgliedsstaaten) „notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses“ handelt. Steht diese Passage vor dem Hintergrund, dass fraglich ist, ob eine einheitliche Rechtsauslegung dieser Begriffe in den Mitgliedsstaaten stattfindet, im Widerspruch zu einem einheitlichen Handeln innerhalb der EU-Mitgliedsstaaten?*

BfDI: Entscheidende Norm ist insoweit in erster Linie der einleitende Satz des Art. 6 Abs. 3a DSGVO, der durch EG 40 ergänzt wird. Demnach sind Zweckänderungen u. a. dann möglich, wenn diese auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten beruhen, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 21 Absatz 1 Buchstaben aa bis g genannten Ziele darstellt. Damit sind Zweckänderungen bei Vorliegen bestimmter öffentlicher Interessen auch dann möglich, wenn die neue

Zweckbestimmung der Daten nicht mit der ursprünglichen Zweckbestimmung vereinbar ist.

Diese Möglichkeit der Zweckänderung ist nicht unkritisch, zumal die in Art. 21 genannten Rechtsgüter zahlreich und von sehr unterschiedlichem Gewicht sind. Allerdings muss sich eine Rechtsvorschrift, die solche Zweckänderungen erlaubt, an den Menschenrechten und Grundfreiheiten sowohl auf europäischer als auch auf nationaler Ebene ausrichten und die Zweckänderungen auf das unabdingbar notwendige Maß zur Erfüllung der in Bezug genommenen öffentlichen Interessen beschränken.

Art. 6 Abs. 3a DSGVO wird in der Tat dazu führen, dass in diesem Kontext die durch die DSGVO angestrebte Harmonisierung nicht erreicht und hier ein Stück weit eine heterogene Struktur entstehen wird. Dieser Befund gilt insgesamt für die Verarbeitung personenbezogener Daten zur Erfüllung öffentlicher Interessen und berücksichtigt die sehr unterschiedlichen Kulturen der Mitgliedstaaten. Die Herstellung gleicher Wettbewerbsbedingungen im Binnenmarkt wird hierdurch meines Erachtens aber nicht grundsätzlich in Frage gestellt.

9) *Wie bewerten Sie die Ausnahmen der Datenschutzgrundverordnung zur Rechtmäßigkeit von Datenverarbeitung ohne Einwilligung zu Zwecken von berechtigtem Interesse?*

BfDI: Soweit sich die Frage auf die Regelung des Art. 6 Abs. 1 lit. f) DSGVO bezieht, erlaubt diese – als eine von sechs Zulässigkeitstatbeständen, zu denen auch die Einwilligung gehört – die Verarbeitung personenbezogener Daten, wenn sie zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Diese Norm ist aus dem geltenden Recht (Art. 7 lit. f der Richtlinie 95/46/EG) übernommen und in Deutschland beispielsweise durch § 28 Abs. 1 Satz 1 Nr. 2 BDSG umgesetzt. Dieser Erlaubnistatbestand ist mithin seit über 20 Jahren im europäischen Recht etabliert.

Die im Entwurf des Rates vom 15. Juni 2015 in Art. 6 Abs. 4 Satz 2 DSGVO vorgesehene Möglichkeit, ohne weitere Rechtsgrundlage eine Zweckänderung bei berechtigtem Interesse des Verantwortlichen vornehmen zu dürfen, hat erfreulicherweise keinen Eingang in den geeinigten Text gefunden. Art. 6 Abs. 4 DSGVO wurde insgesamt gestrichen.

Angesichts der Unbestimmtheit des Art. 6 Abs. 1 lit. f) DSGVO wird auch in Zukunft auf die Datenschutzaufsichtsbehörden aber auch auf die Gerichte die Aufgabe zukommen, die Anforderungen zu konkretisieren.

Andrea Voßhoff Bonn, den 19. Februar 2016