Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
18(24)90neu

Fragen für das Fachgespräch „Europäische Datenschutzgrundverordnung“ des Ausschusses Digitale Agenda am 24. Februar 2016

Beantwortung durch MR Dr. Waltraut Kotschy

FRAGE 1

Wie sind die Ergebnisse des Trilogs zur Datenschutz-Grundverordnung aus Ihrer Sicht grundsätzlich zu bewerten?

Gemessen an den erklärten Zielen des Vorhabens ist generell Folgendes feststellen:

1) Das Ziel einer Vereinheitlichung des Datenschutzrechts in den MS der EU wird nur sehr oberflächlich erreicht. Nicht nur gibt es viele Delegationen (- über 50 -) an die nationalen Gesetzgeber der MS, auch die wenig stringenten Formulierungen in vielen wesentlichen Punkten der DS-GVO eröffnen einen weiten Interpretations-spielraum, der einer Vereinheitlichung hinderlich ist. Der Rückgriff auf nationale spezifische Datenschutzregelungen war m.E. allerdings sinnvoll, da die Schaffung von einheitlichem EU-Recht in allen datenschutzrechtlich relevanten Spezialmaterien innerhalb kurzer Zeit nicht möglich ist und andrerseits ohne solche speziellen Regeln die Umsetzung von Datenschutz nicht funktioniert. Was aber gerügt werden muss, ist der Umstand, dass die Formulierung vieler wichtiger Bestimmungen der DSGVO nicht eindeutig ausgefallen ist. Als Beispiel kann etwa Art. 7 Abs. 4 (betreffend die Einwilligung des Betroffenen) zitiert werden, dessen eigentliche Aussage sich in klarer Weise nur im Erwägungsgrund 34 findet, woraus sich eine etwas unsichere Rechtslage in diesem für die Praxis so zentralen Punkt ergibt. Andrerseits werden die Erwägungsgründe vielfach nur zur Nacherzählung des Inhalts der zugehörigen Bestimmung benutzt anstatt Zweifelsfragen anzusprechen, z.B. dass das Recht auf Vergessen auch gegenüber Suchmaschinen auf der Grundlage des Art. 17 (1) geltend gemacht werden kann.

Die mit der Vollziehung der DS-GVO betrauten Gremien, insbesondere der EDSA, werden daher noch viel Arbeit leisten müssen, um ein einheitliches Verständnis der zahlreichen vieldeutigen Textstellen herbeizuführen.

In der öffentlichen Diskussion werden öfters auch Codes of Conduct als Mittel zur materiengerechten Spezifizierung der Regeln der DS-GVO ins Spiel gebracht. Die praktischen Erfahrungen mit diesem Instrument sind jedoch nicht unbedingt ermutigend: Im nationalen Bereich (z.B: Österreich) ist dieses Instrument ein Fremdkörper geblieben, der nur ganz selten erfolgreich verwendet wurde. EU-weite Beispiele für Codes of Conduct, die der Art. 29-Gruppe vorgelegt wurden (z.B. FEDMA Verhaltensregeln betr. Direktmarketing), haben regelmäßig nur wenig konkrete Regeln beinhaltet, sodass sie die Rechtsanwendung in der betroffenen Branche auch nicht wesentlich beeinflussen und erleichtern konnten.

2) Was die Anpassung des Rechtsrahmens an das Internet-Zeitalter betrifft, sind die diesbezüglichen Neuerungen nicht besonders zahlreich: Wirklich neu ist das Recht auf Datenportabilität und wirklich neu ist ein Recht auf Vergessenwerden, das – internetkonform – auch gegenüber Suchmaschinenbetreibern ausgeübt werden kann; (die Formulierung des Art. 17 und auch des zugehörigen Erwägungsgrunds sind diesbezüglich allerdings nicht explizit, sodass letztlich nur die Judikatur des EuGH ein Garant dafür ist, dass Art. 17 der GVO so zu verstehen ist, dass das Recht auf Vergessenwerden nicht nur gegenüber dem Primärverantwortlichen ausgeübt werden kann.

Wesentliche Aspekte der seit 1995 doch erheblich geänderten Datenverarbeitungs-gewohnheiten in unserer Gesellschaft sind jedoch unberücksichtigt geblieben. Damit meine ich vor allem Änderungen in der Rollenverteilung der wesentlichen Akteure Betroffener – Verantwortlicher - Dienstleister: Obwohl sich die Bedeutung der Privatperson als Datenverarbeiter erheblich verändert hat, seit das Internet die technischen Mittel für die Verarbeitung der eigenen Daten, aber auch der Daten von anderen in großem Stil zur Verfügung stellt, ist die sog. „Haushaltsausnahme“ unverändert geblieben. Die fortschreitende Verbreitung von ubiquitous computing wird die Frage der datenschutzrechtlich richtigen Positionierung des Betroffenen in seiner Rolle als „Nutzer“ noch dringender machen.

Für zwei Verarbeitungskategorien, die seit 1995 ebenfalls ganz wesentlich an Bedeutung gewonnen haben, nämlich „profiling“ und „big-data-Anwendungen“, enthält die DS-GVO keine wirklich neuen Regelungen, die die Zulässigkeit solcher Anwendungen betreffen. Allerdings verdient die genauere Regelung der „vereinbaren Weiterverwendung“ in Art. 6 Abs. 3a der DS-GVO Erwähnung, da damit die Voraussetzungen für viele big-data Anwendungen beeinflusst werden (- siehe dazu auch die Beantwortung der Frage 3).

Die ausdrückliche Definition der Pseudonymisierung von Daten und ihre Erwähnung als eine „geeignete Garantie“ an mehreren Stellen (z.B. im Zusammenhang mit statistischen Anwendungen) darf immerhin als Gleichziehen mit mehreren nationalen Umsetzungen in den MS gewertet werden. Eine mutige Privilegierung der Verwendung pseudonymisierter Daten – was ein Anreiz für ihre Verwendung z.B. im Zusammenhang mit medizinischer Forschung wäre – fehlt allerdings.

Im Zusammenhang mit der Datenschutz-Grundverordnung 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?

Diese Datenverarbeitungen sind nach dem vorliegenden Text zweifellos nach wie vor möglich. Die nunmehrige Regelung des Begriffs der „vereinbaren Weiterverwendung“ wird gegenüber mancher nationaler Umsetzung der DSRL sogar eine Erleichterung für Big Data Anwendungen mit sich bringen, da sich nunmehr aus dem Text der GVO doch ablesen lässt, dass die Grenze „vereinbarer Zwecke“ nicht so eng zu ziehen ist, dass eine Weitergabe von Daten an einen anderen Verantwortlichen generell ausgeschlossen ist. Gegenüber Anbietern im Drittausland, die keinen besonderen datenschutz-rechtlichen Beschränkungen unterliegen, könnte dies in der Tat eine Verbesserung der wettbewerblichen Stellung europäischer Datenverarbeiter mit sich

bringen. Wichtiger für das Wettbewerbsgleichgewicht dürfte allerdings die Ausdehnung des territorialen Geltungsbereichs der DSGVO auf grundsätzlich alle Anbieter in der EU, unabhängig von ihrer Niederlassung in der EU, sein.

Einen echten Vorteil für die datenverarbeitende Wirtschaft werden die neuen Regelungen zur Weiterverarbeitung und zur Pseudonymisierung aber erst dann bringen, wenn ihre Auswirkung im Einzelfall deutlicher feststehen: Solange der Stellenwert der z.B. in Art. 6 Abs. 3a genannten Faktoren für die Zulässigkeit eines Geschäftsmodells, das auf Weiterverarbeitung beruht, angesichts der verwendeten Formulierungen in Art. 6 Abs. 3a unsicher ist, wird diese Unsicherheit zusammen mit den drastisch erhöhten Strafen für unzulässige Datenverarbeitung ein Hindernis für die Entwicklung neuer Geschäftsmodelle bleiben. Eine Verbesserung der Wettbewerbsposition europäischer Datenverarbeiter wird daher wesentlich davon abhängen, ob es gelingt, bald Mechanismen in Gang zu setzen, die ein höheres Ausmaß an Rechtssicherheit bei der Interpratation der neuen Bestimmungen in der DS GVO zu erzeugen vermögen.

Inwiefern wird die DSGVO den gestiegenen Herausforderungen hinsichtlich eines effektiven Grundrechtschutzes angesichts neuer Arten der Datenerfassung, Speicherung, Verarbeitung und Weitergabe an Dritte insgesamt gerecht?

Die DSGVO enthält wesentlich verbesserte Informationspflichten (Art. 14 und 14a) und auch einen interessanten Ansatz zur schnelleren Erfassbarkeit von Information, indem Information in Hinkunft auch in Form von standardisierten Icons gegeben werden kann (Art. 12 (4b) und (4c)). Die Treffsicherheit von Information ist von entscheidender Bedeutung für die Fähigkeit des Betroffenen, die Auswirkung einer Datenverarbeitung auf seine rechtlichen Interessen beurteilen zu können und daher eine wichtige Voraussetzung für effektiven Grundrechtsschutz.

Auch die Durchsetzbarkeit von Schutzinteressen des Betroffenen ist gegenüber der RL (- wenn auch nicht notwendigerweise gegenüber der jeweiligen nationalen Umsetzung der RL -) erheblich verbessert. Zu erwähnen sind vor allem

das stärker determiniertes Widerspruchsrecht

das Beschwerderecht im Wohnsitzstaat auch gegenüber ausländischen Verantwortlichen,

die Popularklage,

knappe Erledigungsfristen für Beschwerden, sowohl bei den Verantwortlichen als auch bei den Datenschutzbehörden, und nicht zuletzt

Strafrahmen mit sehr hohen Obergrenzen

Als Mangel ist festzuhalten, dass gerade für die prinzipiell risikobehaftete Weiterverarbeitung von Daten für „vereinbare andere Zwecke“ zwar Informationspflicht, aber kein generelles Widerspruchsrecht gegen die Bereitstellung zur Weiterverarbeitung besteht, da dieses auf Verarbeitungen beschränkt ist, die auf Art. 6 (1) lit. e oder f beruhen, während die Weiterverwendung zu vereinbaren anderen Zwecken auf Art. 6 Abs. 3a beruht. Ein Widerspruchsrecht ist nur im Zusammenhang

mit der Weiterverarbeitung von Daten für Forschungs- und Statistikzwecke ausdrücklich eingeräumt (Art. 19 Abs. 2aa).

FRAGE 2

Wird mit der Datenschutz-Grundverordnung der erhoffte einheitliche und europaweite Rechtsrahmen für den Datenschutz erreicht, der europaweit einen hohen Datenschutzstandard garantiert und kann insbesondere auch das Marktortprinzip Wettbewerbsgleichheit für alle Anbieter, die in Europa ihre Dienste anbieten, sicherstellen?

Das erklärte Ziel der Schaffung eines einheitlichen Rechtsrahmens ist nicht erreicht angesichts von etwa 50 Bestimmungen in der DSGVO, in welchen Rechtssetzungsbefugnisse an die Mitgliedstaaten delegiert werden.

Es muss aber realistischerweise festgehalten werden, dass dieses Ziel auch nicht erreicht werden konnte: Datenschutz ist ein Musterbeispiel für eine „Querschnittsmaterie", die alle Bereiche unseres Lebens betrifft. Die Formulierung eines generellen Rechtsrahmens muss daher einen relativ hohen Abstraktionsgrad aufweisen, der der näheren Ausgestaltung für die einzelnen Sachmaterien bedarf, um den generellen Rechtsrahmen vollziehbar zu machen. Das Kapitel IX der DSGVO ist ein Versuch, einige Spezialbereiche schon in der GVO regelnd zu behandeln. Es wäre aber vollkommen unmöglich gewesen, innerhalb der zur Verfügung stehenden Zeit für sämtliche wichtige Materienbereiche angemessen detaillierte EU-rechtliche Regelungen zu schaffen. Da solche Regelungen aber gleichzeitig unverzichtbar sind, konnte sinnvollerweise nur auf bestehendes nationales Recht zurückverwiesen werden. Es wird die Aufgabe der nächsten Jahre sein zu prüfen, in welchen Bereichen doch einheitliches spezielles EU-Datenschutzrecht geschaffen werden muss, um Wettbewerbsverzerrungen hintanzuhalten. Ein Bereich, der sich z.B. sofort anbietet, ist die Weiterverwendung von Patientendaten für die medizinische Forschung. Diesbezüglich bestehen sehr unterschiedliche Zustimmungserfordernisse in den MS der EU, was für einen einheitlichen Raum der wissenschaftlichen Forschung äußerst hinderlich ist.

Wird die Umsetzung der Datenschutzgrundverordnung gleiche und faire Wettbewerbsbedingungen für deutsche und europäische Unternehmen sowie US-amerikanischen Unternehmen herstellen?

Zwischen europäischen Unternehmen jedenfalls nicht weniger als dies bisher – aus datenschutzrechtlicher Perspektive - der Fall war. Aus der nunmehr etwas detaillierteren Regelung (Art. 6 Abs. 3a) der Weiterverwendung von Daten für andere vereinbare Zwecke wird sich voraussichtlich ein vereinheitlichender Effekt ergeben, insbesondere wenn es gelingt, sich in Anwendung der DSGVO auf eine noch präzisere Festlegung der maßgeblichen Kriterien für die Vereinbarkeit von Zwecken - etwa im Hinblick auf wichtige use cases - zu einigen.

Gegenüber US-amerikanischen Unternehmen ist ein entscheidender Schritt in Richtung gleicher Wettbewerbsbedingungen schon durch die Ausdehnung des territorialen Geltungsbereichs der DSGVO getan.

Was damit freilich nicht beeinflusst werden kann, sind gleichartige Wettbewerbsbedingungen zwischen europäischen Anbietern und US-amerikanischen Anbietern auf Drittmärkten, wo US-Anbieter den EU-Datenschutzregeln nicht unterliegen.

Hier kann nur die globale Propagierung der Idee des Datenschutzes solchen Unternehmen Wettbewerbsvorteile verschaffen, die sich dieser Idee sichtbar verpflichtet fühlen.

FRAGE 3

Welcher Änderungsbedarf ergibt sich aus der Verabschiedung der Datenschutz-Grundverordnung für das deutsche Datenschutzrecht und die zahlreichen bereichsspezifischen Vorgaben?

Diese Frage kann ich für Deutschland nicht beantworten. Aber vielleicht ist es auch interessant aufzuzeigen, welcher Anpassungsbedarf sich aus österreichischer Sicht voraussichtlich ergibt: m.E. wird vor allem in zwei wichtigen Punkten zu diskutieren sein, in wie weit generell Anpassungsbedarf bestehen, und zwar

- Im Bereich des neuen Art. 6 (1) lit.f (Datenverarbeitung zu Zwecken von berechtigten Interessen), weil in Österreich bisher ein „*überwiegendes* berechtigtes Interesse“ des Verantwortlichen oder eines Dritten gegeben sein musste, um die Verarbeitung zu rechtfertigen, und
- Im Bereich des Zweckbindungsprinzips, da in Österreich die Grenzen einer „Weiterverarbeitung zu anderen, nicht unvereinbaren Zwecken“ derzeit enger gezogen sind als im künftigen Art. 6 (3a) der DSGVO.

Von welchen Öffnungsklauseln sollte der nationale Gesetzgeber zwingend Gebrauch machen, um über die Vorgaben der Datenschutz-Grundverordnung hinausgehende Regelungen zu schaffen?

Es gibt einige Punkte im organisations- und verfahrensrechtlichen Bereich, die unbedingt von der nationalen Gesetzgebung ausgefüllt werden müssen, damit Datenschutz vollzogen werden kann.

Soweit es sich um materielles Datenschutzrecht handelt, geht es wohl nicht so sehr darum, neues Recht zu schaffen, sondern bereits im MS vorhandenes spezielles Datenschutzrecht nach wie vor anzuwenden, freilich erst nach einem Kompatibilitätscheck im Hinblick auf die Bestimmungen der DSGVO.

Aus österr. Sicht etwa, besteht prima vista kaum Bedürfnis nach neuen Regelungen, sondern eher nach einem Überdenken der bestehenden speziellen Regelungen, z.B. im Bereich der Weiterverwendung von Daten für Forschung und Statistik.

In welchen Bereichen besteht zukünftig kein Spielraum mehr für den nationalen Gesetzgeber? Wo sehen Sie für nationalen Gesetzgeber nach der Verabschiedung der Datenschutzgrundverordnung noch Möglichkeiten, Regelungen im nicht-öffentlichen Bereich zu schaffen?

Die diesbezüglich durch die DSGVO für die Zukunft geschaffene Rechtslage scheint besonders diskussionswürdig. In den Ratsverhandlungen war eine gewisse Tendenz erkennbar, einen Spielraum für den nationalen Gesetzgeber im öffentlichen (staatlichen) Bereich zu ermöglichen, aber eher nicht im privaten (Business)Bereich.

Mit dieser Frage beschäftigt sich nunmehr der Art. 6 Abs. 2a. Danach dürfen die MS speziellere Regelungen (in Ausführung zur GVO) „beibehalten oder neu einführen", aber nur im Bereich des Art. 6 (1) lit. c und e, sowie im Bereich der im Kapitel IX behandelten spezifischen Verarbeitungssituationen. Von Kapitel IX sind nur einige wenige Themen betroffen - was tatsächlich den Eindruck erweckt, als ob die MS spezielle Datenschutzregelungen im Privaten Bereich grundsätzlich nicht beibehalten oder erlassen dürften.

Diesem Schluss muss allerdings widersprochen werden, da durch Verweis auf Art. 6 (1) lt. c auch alle Fälle miteinbezogen werden, in welchen Datenverarbeitung notwendig ist für die Erfüllung einer rechtlichen Verpflichtung, der der Verantwortliche unterliegt. Solche rechtlichen Verpflichtungen bestehen für Verantwortliche des privaten Bereichs in reichem Maße und dürfen in Hinkunft auch offenbar beibehalten und auch neu geschaffen werden. Daraus folgt m. E., dass spezielle Regelungen in Ausführung der DSGVO auch im privaten Bereich von den MS getroffen werden können, sie müssen allerdings die Qualität von rechtlichen Verpflichtungen der Verantwortlichen haben.

Es steht ja auch außer Zweifel, dass der Wegfall aller speziellen Regelungen des nationalen Rechts etwa über Datenschutz im Bereich des Konsumentenkredits oder des Versicherungsvertragswesens oder des Direktmarketing etc. nur Nachteile für die Betroffenen mit sich bringen würde. Solange derartige Regelungen nicht durch EU-rechtliche Regelungen gleicher Dichte (Spezialität) ersetzt worden sind, müssen sie für die Gesetzgebung auf mitgliedstaatlicher Ebene weiter offen bleiben.

Sehen Sie insbesondere Handlungsbedarf seitens des Gesetzgebers im Bereich der Beschäftigtendaten? Und wenn ja in welcher Form?

Für Österreich: Grundsätzlich nicht als spezielle Folge der DSGVO. Freilich wird zu prüfen sein, ob sich in irgendwelchen Detailfragen ein Anpassungsbedarf an die GVO ergibt

Was kann man außerhalb der Gesetzgebung tun, um den Datenschutz in Umsetzung der DSGVO in Deutschland zu fördern?

Man sollte alles daran setzen, noch innerhalb der Legisvakanz der GVO eine möglichst einheitliche Sichtweise von den Neuerungen in der DSGVO zu entwickeln. Das bedarf wahrscheinlich der Bereitstellung spezieller Ressourcen für jene Institutionen, die aus der Sicht der DSGVO vornehmlich zur Erarbeitung solcher gemeinsamen Interpretationssichtweisen berufen sind.

FRAGE 4

Lässt die Datenschutzgrundverordnung ausreichend Spielraum für Innovation? Leistet sie einen Beitrag dazu, dass Datenschutz sich als Wettbewerbsvorteil für europäische Unternehmen etablieren kann?

Soweit Innovation und neue Geschäftsmodelle auf der Nutzung (einschließlich Weiterverwendung) von Daten beruhen, ist als Positivum der DSGVO zu vermerken, dass sie sich der Frage der Bedingungen für eine zulässige Weiterverwendung von Daten für neue Zwecke deutlicher stellt als die DSRL. Ob sich aus der maßgeblichen Regelung tatsächlich ein „ausreichender" Spielraum für Innovation ergibt, wird von der Interpretation der Bedingungen für das Vorliegen von „nicht unvereinbarer Weiterverwendung" abhängen, wobei allerdings zu berücksichtigen ist, dass die Zulässigkeit von Innovation gegenüber der Einhaltung von Grundrechten keinen Vorrang genießen kann.

Dass „innovative Geschäftsmodelle", die die Weiterverwendung von Daten für einen anderen, mit dem Ermittlungszweck der Daten unvereinbaren Zweck zur Voraussetzung hätten, nicht zulässig sind, ergibt sich aus dem Zweckbindungsprinzip. In diesem Fall müssten die Daten wohl tatsächlich physisch neuerlich ermittelt werden, und zwar dann nach den Regeln des Art. 6 Abs. 1 der DSGVO.

Ob die Auswirkungen des Zweckbindungsprinzips ein Wettbewerbsvorteil oder ein -Nachteil für europäische Unternehmen auf Drittauslandsmärkten darstellt, hängt von der Einstellung der dortigen Konsumenten ab: Wenn Datenschutz dort keinerlei Stellenwert besitzt, wird eine Zusage der Einhaltung des Zweckbindungsprinzips wohl keinen Wettbewerbsvorteil bringen.

Wo und warum sehen Sie in dem neuen Regelungswerk positive und wo negative Effekte für die deutsche und europäische Wirtschaft?

An sich ist die künftige stärkere Betonung eines Risiko-orientierten Ansatzes wohl eher positiv zu bewerten. Voraussetzung für ein insgesamt positives Ergebnis wird aber sein, dass die maßgeblichen Faktoren für die Annahme eines jeweils höheren oder geringeren Datenschutzrisikos eindeutiger und greifbarer gemacht werden, als dies nach dem vorliegenden Text in vielen Punkten der Fall ist.

Es hilft der großen Anzahl von KMUs in Europa wenig, wenn Erleichterungen in den formalen Anforderungen für ordnungsgemäße Datenverarbeitung an Bedingungen geknüpft sind, deren Vorliegen jeweils erheblichen interpretationsaufwand verursacht. Das Aufstellen klarer Spielregeln würde einen der wesentlichsten Beiträge im Zusammenhang mit dem neuen Regelungswerk leisten.

FRAGE 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?

Das One-stop-shop-Verfahren gilt nur für den privaten Bereich und ist an die territoriale Zuständigkeit der lead-authority gebunden. Insofern müsste sich daraus eine klare Zuständigkeit jener Landesdatenschutzbehörde als lead-authority ergeben, in deren Bereich die Hauptniederlassung eines Verantwortlichen oder Auftragsverarbeiters gelegen ist. Dass allerdings ein gewisses Problem entstehen kann, wenn eine lead authority, die den MS im EDSA *nicht* vertritt, von einem Kohärenzverfahren im EDSA betroffen ist, ist nachvollziehbar. Vielleicht könnte in solchen Fällen eine flexible Vertretungsregelung für den MS gefunden werden.

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?

Für eine Beantwortung dieser Fragen fühle ich mich nicht berufen. In Österreich existiert trotz der föderalen Staatsstruktur nur eine Datenschutzbehörde.

FRAGE 6

Wie bewerten Sie die DSGVO 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 KOM vorgestellt wurde?

Das für den Internationalen Datenverkehr geltende Regelungsregime in der DSGVO ist nicht grundsätzlich verschieden von jenem der DS-RL. Obwohl der EuGH in seinem Safe-Harbour-Urteil dezidiert erklärt hat, dass die Beurteilung der Angemessenheit von Datenschutz beim Datenempfänger im Dritt-Ausland der zuständigen unabhängigen Datenschutzbehörde nie verwehrt ist, und zwar auch dann nicht, wenn eine positive Angemessenheitsentscheidung der EU-Kommission vorliegt, enthält auch die DS-GVO nach wie vor eine Kompetenz der EU-Kommission, die Angemessenheit des Datenschutzniveaus in Drittstaaten bzw. Teilbereichen von Drittstaaten mit Beschluss festzustellen. Der Umfang der Bindungswirkung einer solchen Feststellung ist nach Aussage des Gerichtshofs so zu sehen, dass es den unabhängigen Datenschutzbehörden möglich sein muss, die Richtigkeit eines solchen Beschlusses vor einem Gericht – offenbar nach vorangegangenem Beschwerdeverfahren – in Frage

zu stellen, sodass der EuGH angerufen werden kann, um letztendlich über den Bestand der Kommissionentscheidung zu befinden.

Die DS-GVO enthält allerdings zusätzliche Bedingungen im Zusammenhang mit Adäquanzentscheidungen der EU Kommission, indem nähere Kriterien für das Vorliegen von adäquatem Datenschutz aufgezählt werden (Art. 41 Abs. 2) und auch verpflichtend regelmäßiges Monitoring im Hinblick auf getroffene Adäquanzentscheidungen vorgeschrieben wird (Art. 41 Abs. 4a). Insofern werden die Voraussetzungen für einen Entscheidung der EU-Kommission in Hinkunft deutlicher erkennbar sein.

Was nun eine allfällige Nachfolgeregelung zur Safe-Harbour-Entscheidung angeht, kann derzeit wenig Konkretes gesagt werden, da der Inhalt der relevanten Vereinbarungen mit den befassten US-Stellen nicht bekannt ist.

Inhaltlich hat der EuGH das Safe Harbour System v.a. in zwei Punkten als ungeeignet zur Herstellung von angemessenem Datenschutz befunden:

- Es sieht einen uneingeschränkten Vorrang der US-Rechtsordnung vor den Safe Harbour Regeln vor, woraus sich im vorliegenden Verfahrenszusammenhang vor allem ein aus europäischer Sicht unverhältnismäßig weites Zugangsrecht staatlicher Stellen zu personenbezogenen Daten ergibt, die aus dem EWR an US Safe Harbour Unternehmen exportiert wurden;
- Die von diesem Datenverkehr Betroffenen haben keinen effektiven Rechtsschutz in den USA, mit welchen derartige Datenzugriffe einer gerichtlichen Prüfung unterzogen werden könnten.

Jedenfalls in diesen Hauptkritikpunkten müsste die neue Vereinbarung, die einer „privacy shield“ – Adäquanzentscheidung der EUKommission zugrunde liegen würde, Abhilfe schaffen.

FRAGE 7

Kann Großbritannien tatsächlich eine Ausnahmeregelung in Anspruch nehmen, der zufolge die Sperrklausel des Art. 43 a DS-GVO 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?

Die schriftliche Erklärung der brit. Regierung, eingebracht im brit. Parlament am 4. **Februar** 2016, betreffend Art. 43a der DS-GVO, spricht davon, dass der Wortlaut des Art. 43a mit der Anerkennung und Durchsetzung von Urteilen zu tun habe und Fragen der Art. 81 und 82 des AEUV betreffe. In der Erklärung wird daraus auf die Anwendbarkeit des Protokolls Nr. 21 zum Vertrag von Lissabon geschlossen. Dazu ist meines Erachtens Folgendes zu sagen:

➔ Titel V Kapitel 3 und 4 des AEUV betrifft die **Zusammenarbeit unter den MS der Union** in Justizangelegenheiten: Die Union entwickelt eine justizielle Zusammenarbeit in Zivilsachen mit grenzüberschreitendem Bezug (Art. 81) und in Strafsachen (Art. 82) und legt hierfür den Grundsatz der gegenseitigen Anerkennung von gerichtlichen Urteilen und Entscheidungen fest und das Streben nach Angleichung der Rechtsvorschriften der MS in gewissen Bereichen. Dies betrifft ausschließlich die Zusammenarbeit über jene Grenzen hinweg, die zwischen den MS bestehen, und gerichtliche Urteile und Entscheidungen von MS.

➔ Art. 43a betrifft gerade NICHT die Zusammenarbeit zwischen den MS der Union in Justizangelegenheiten, sondern Fragen der Zusammenarbeit von MS der Union mit Drittstaaten. Art. 43a ist somit kein Gegenstand des Titels V Kapitel 3 und 4 des AEUV.

➔ Das Protokoll Nr. 21 zum Vertrag von Lissabon ist daher nicht anwendbar.

➔ **Im** Übrigen **wäre noch folgendes Argument zu prüfen**: Unabhängig davon, ob Art. 43a der DS-GVO angewendet wird oder nicht, könnte die Berufung auf ein Urteil oder eine Entscheidung einer Drittstaatsbehörde als Rechtsgrundlage für einen Datentransfer in den Drittstaat nur dem Art. 6 Abs. 1 lit. c der DS-GVO zugeordnet werden, also als Datenverarbeitung verstanden werden, die notwendig ist aufgrund einer rechtlichen Verpflichtung, der der Verantwortliche (oder Auftragsverarbeiter) unterliegt. Gemäß Art. 6 Abs. 3 der GVO muss aber jede Berufung auf Art. 6 Abs. 1 lit.c gleichzeitig eine Berufung auf Unionsrecht oder Mitgliedsstaatsrecht sein. Schon aus diesem Grund kann sich ein für die Datenverarbeitung (den Transfer) Verantwortlicher oder ein Auftragsverarbeiter nur dann auf einen behördlichen Akt aus einem Drittstaat stützen, wenn dieser Drittstaats-Akt durch Unionsrecht oder nationales Recht des territorial zuständigen MS zu einem Akt nach Unions- oder MS-Rechts gemacht wurde, was üblicherweise eines Rechtshilfe- oder Amtshilfeabkommens oder vergleichbaren Übereinkommens bedarf.

Dieses Argument sollte auf seine Tragfähigkeit noch genauestens geprüft werden, da es vielleicht das britische opt-out zu Art. 43a gegenstandslos macht.

FRAGE 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?

Ich darf diesbezüglich auf meine bereits zu Anfang, nämlich zu Punkt 1 gemachten Ausführungen verweisen, in welchen betont wurde, dass die Erreichung eines neuen einheitlichen Rechtsrahmens ganz wesentlich davon abhängen wird, ob es gelingt, ein Gremium - naheliegender Weise die Artikel-29-Gruppe - als allgemein akzeptiertes Forum zu etablieren, das die dringend benötigte Arbeit einer vorgängigen vereinheitlichenden Interpretation der wichtigsten Bestimmungen der DS-GVO leistet. Die dem Europäischen Datenschutzausschuss in der GVO zugeteilten Kompetenzen würden eine solche Rolle wohl ermöglichen, doch sollte nicht bis zu seiner formalen Konstitution zugewartet werden. Es wird von den MS und von der EU Kommission abhängen, ob sie der Vorläuferorganisation des EDSA auch die notwendigen sachlichen und personellen Mittel zur Verfügung stellen, damit sie diese außergewöhnliche Aufgabe tatsächlich zeitgerecht erfüllen kann.

FRAGE 9

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

In der österreichischen Umsetzung der DS-RL hat die Datenverarbeitung auf der Rechtsgrundlage des Art. 7 lt. f (berechtigte Interessen des Verantwortlichen oder eines Dritten) immer eine besonderes wichtige Rolle gespielt, allerdings mit der Besonderheit, dass immer nur eine ÜBERWIEGENDES berechtigtes Interesse des Verantwortlichen (oder eines Dritten) als taugliche Rechtsgrundlage anerkannt wurde.

Die Berechtigung zu einer derartigen – von Art. 7 lit.f der RL formal abweichenden – Formulierung (in § 8 (1) DSG 2000) wurde immer aus dem Bestand der österr. Rechtsordnung vor Inkrafttreten der RL hergeleitet und aus dem Umstand, dass kein MS gezwungen werden konnte, im Zuge der Umsetzung der RL sein Schutzniveau zu senken.

Aus heutiger Sicht fragt sich jedoch, ob nicht auch der neue Art. 6 (1) lit. f der DS-GVO eigentich ohnehin so verstanden werden muss, dass nur berechtigte Interessen des Verantwortlichen (oder eines Dritten), die die Datenschutzinteressen der Betroffenen *überwiegen,* eine taugliche Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellen können: Erhebt nämlich der Betroffene Widerspruch gegen eine Datenverarbeitung gemäß Art. 19, dann hat der Verantwortliche nachzuweisen, dass zwingende Gründe für die Verarbeitung vorliegen, die gegenüber den Interessen des Betroffenen am Schutz seiner Grund- und Freiheitsrechte *überwiegen*. Es genügt also nicht, dass der Verantwortliche AUCH legitime Interessen hat, sondern es müssen von Anfang an solche legitime Interessen sein, die nach objektiven Gesichtspunkten als vorrangig gegenüber den Schutzinteressen der Betroffenen einzustufen sind.

Wenn man sich interpretativ auf ein solches Verständnis von Art. 6 (1) (f)DS-GVO verstehen könnte, wäre der datenschutzrechtliche Sprengstoff dieser Bestimmung weitestgehend entschärft, wie die österr. Praxis der letzten 15 Jahre deutlich zeigt.