UNIKASSEL
VERSITÄT

Fachbereich
Wirtschaftswissenschaften

Institut für Wirtschaftsrecht

Prof. Dr. Alexander Roßnagel

Universität Kassel
Fachgebiet Öffentliches Recht,
insb. Umwelt- und Technikrecht
Nora-Platiel-Straße 5
34109 Kassel

a.rossnagel@uni-kassel.de
fon +49-561 804 3130
fax +49-561 804 3737

Sekretariat: Edith Weise
fon +49-561 804 2874

Universität Kassel
Nora-Platiel-Str. 5 • D - 34109 Kassel

An den Vorsitzenden
des Ausschusses Digitale Agenda
des Deutschen Bundestags
Herrn Jens Koeppen

19. Februar 2016

Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24. Februar 2016 im Ausschuss Digitale Agenda des Deutschen Bundestags

Frage 1:
Wie sind die Ergebnisse des Trilogs zur Datenschutz-Grundverordnung aus Ihrer Sicht grundsätzlich zu bewerten? 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? Inwiefern wird die DSGVO den gestiegenen Herausforderungen hinsichtlich eines effektiven Grundrechtschutzes angesichts neuer Arten der Datenerfassung, Speicherung, Verarbeitung und Weitergabe an Dritte insgesamt gerecht?

Antwort 1:
Gemessen an den von der Europäische Kommission geschürten Erwartungen hinsichtlich eines modernen, künftigen Herausforderungen gewachsenen und unionsweit einheitlichen Datenschutzes und gemessen an den mehrere Jahre dauernden vorbereitenden Diskussionen und dem mehr als vier Jahre dauernden Gesetzgebungsverfahren ist der vorliegende Entwurf einer Datenschutzgrundverordnung enttäuschend. Er bietet keine Modernisierung des Datenschutzrechts, sondern führt grundsätzlich die Konzeptionen der Datenschutzrichtlinie weiter. Die Verordnung wird auch den künftigen Herausforderungen nicht gerecht und versucht sie nicht einmal zu adressieren. Einzelnen Verbesserungen stehen viele Verschlechterungen des Datenschutzes gegenüber. Unterm Strich führt die Verordnung für die Bundesrepublik Deutschland zu einer Absenkung des Datenschutzes, der insbesondere deshalb nicht so gravierend ausfällt, weil sie nicht zu einem einheitlichen unionsweiten Datenschutzrecht führt. Sie belässt nämlich in vielen Fragen den Mitgliedstaaten Entscheidungsspielräume, das bestehende Datenschutzrecht beizubehalten oder neue – besse-

re oder präzisere – Regelungen zu erlassen. Das aber verhindert, dass auch das zweite Ziel, ein unionsweit einheitliches Datenschutzrecht, erreicht wurde.

Das Hauptproblem der Datenschutz-Grundverordnung liegt vor allem in der hohen Diskrepanz zwischen der enormen Komplexität des Regelungsbedarfs einerseits und der Abstraktheit und damit Unterkomplexität ihrer Vorschriften andererseits. Sie will in 45 Artikeln des materiellen Datenschutzes die gleichen Probleme behandeln, für die im deutschen Datenschutzrecht Tausende von Vorschriften bestehen. Wird unterstellt, dass die vielen Spezialregelungen des deutschen Datenschutzrechts nicht alle einer Verkennung der Regelungsprobleme zu verdanken sind, wird deutlich, welche Defizite die Datenschutz-Grundverordnung aufweisen muss. Der Regelungsansatz der Verordnung verkennt die Breite und Komplexität der Aufgabe. Datenschutz ist zu einem zentralen Querschnittsthema der Informationsgesellschaft in Europa geworden. Kein Gesellschaftsbereich kann heute ohne die automatisierte Verarbeitung personenbezogener Daten auskommen. Alle Verfahrensabläufe in Verwaltung und Wirtschaft, Wissenschaft und Kultur sind durch sie geprägt. Wer Datenschutz regelt, verursacht Veränderungen in allen Gesellschaftsbereichen – vom Archivwesen bis zum Zeitungsverlag. Wer meint, die vielen und vielfältigen gesetzlichen Regelungen zum Datenschutz in den Mitgliedstaaten durch wenige generelle und abstrakte Regelungen ersetzen zu können, unterschätzt nicht nur diese Aufgabe gewaltig, sondern übersieht auch die negativen Auswirkungen, die dadurch entstehen, dass er die Vielfalt und Differenzierung bestehender Regelungen beseitigt und gewaltige Lücken der Rechtsunsicherheiten schafft.

Inhaltlich verursacht die Verordnung Defizite vor allem durch ihren spezifischen Ansatz der Technikneutralität.[1] Dieser Ansatz ist sinnvoll, wenn er bewirken soll, dass rechtliche Vorschriften so formuliert werden, dass sie technische Weiterentwicklungen nicht ausschließen. In der Datenschutz-Grundverordnung wird dieser Ansatz aber im Sinn einer Risikoneutralität genutzt: In keiner Regelung werden die spezifischen Grundrechtsrisiken z.B. von Big Data, Cloud Computing, Ubiquitous Computing oder datengetriebenen Geschäftsmodellen angesprochen oder gar gelöst. Die gleichen Regelungen wie für die Datenverarbeitung beim Bäcker um die Ecke sollen auch für diese risikoreichen Datenverarbeitungsformen gelten. Durch solche Regelungen werden gerade die spezifischen Grundrechtsrisiken verfehlt. Nur durch die Berücksichtigung typischer Risiken bestimmter Datenverarbeitungsformen im Verordnungstext hätte die notwendige Rechtssicherheit und Interessengerechtigkeit erreicht werden können.

Ubiquitous Computing verursacht vor allem dadurch Risiken für Grundrechte, dass angesichts der im Hintergrund ablaufenden, alltägliche Lebensvollzüge umfassend erfassenden Verarbeitung von Daten mit hoher Aussagekraft die Datenschutzgrundsätze der Transparenz, der Einwilligung, der Zweckbindung, der Erforderlichkeit und der Datenminimierung ihre Eignung verlieren, die informationelle Selbstbestimmung zu schützen.[2] Regelungen zu diesen Risiken fehlen in der Datenschutz-Grundverordnung. Durch die Aufgabe des ausdrücklichen Opt-in bei der Einwilligung, die Aufweichung der Zweckbindung[3] und die Stärkung des Erlaubnistatbestands der Interessenabwägung [4] werden viele Anwendungen des Ubiquitous Computing

---

1 S. zu diesem Grundsätzlich kritisch *Roßnagel*, Technikneutrale Regulierung: Möglichkeiten und Grenzen, in: Eifert/Hoffmann-Riem (Hrsg.), Innovationsfördernde Regulierung, Berlin 2009, 323.

2 S. hierzu ausführlich *Roßnagel*, Datenschutz in einem informatisierten Alltag, Berlin 2007.

3 S. hierzu genauer Richter, Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf des DSGVO, DuD 2015, 735; Roßnagel/Nebel/Richter, Was bleibt vom Europäischen Datenschutzrecht? Zum Ratsentwurf der Datenschutz-Grundverordnung, ZD 2015, 455.

4 S. näher die Antwort zu Frage 9.

durch die Datenschutz-Grundverordnung erleichtert, ohne dass risikoadäquate Schutzmaßnahmen bestehen.

Big Data verursacht vor allem dadurch Risiken für Grundrechte, dass sehr viele personenbezogene Daten, die für andere Zwecke erhoben wurden, zweckentfremdet genutzt werden, um über Betroffene mehr zu erfahren und dieses Wissen für eigene Zwecke zu nutzen. Darüber hinaus kann statistisches Wissen auch auf die Betroffenen angewendet werden, die einer Datenerhebung oder Zweckänderung nicht zugestimmt haben [5] Auch für Big Daten-Analysis verbessert die Datenschutz-Grundverordnung die Nutzungsbedingungen, in dem sie die Einwilligung erleichtert, die Zweckbindung relativiert und die berechtigten Interessen Dritter für eine Verarbeitung personenbezogener Daten ausreichen lässt. Risikoadäquate Schutzregelungen fehlen.

Cloud Computing verursacht vor allem dadurch Risiken für Grundrechte, dass personenbezogene Daten Dritten und weiteren Dritten übertragen werden und damit dem Einflussbereich und der Kontrolle des für die Datenverarbeitung Verantwortlichen entzogen werden. Für Cloud Computing passt das Modell der Auftragsdatenverarbeitung des Art. 26 DSGVO jedoch nicht. Beim Cloud Computing kann der verantwortliche Cloud-Nutzer seiner Verantwortung nicht dadurch gerecht werden, dass er den Cloud-Anbieter als Auftragnehmer persönlich anweist, kontrolliert und seine Anweisungen durchsetzt. Die Zielsetzung des Art. 26 DSGVO muss daher beim Cloud Computing auf andere Weise erreicht werden. Hierfür müsste eine spezifische Regelung dieses Modell der Auftragsdatenverarbeitung modifizieren und die datenschutzgerechte Erbringung von Cloud-Diensten z.B. an eine wiederkehrende Zertifizierung koppeln, die Auswahl, Weisung und Kontrolle durch den Auftraggeber selbst ersetzen kann. Für dieses „Ersatzmodell" hätten die wesentlichen Kriterien und Anforderungen in der Verordnung selbst festgelegt werden müssen. Dies ist aber nicht erfolgt. Die Rechtsunsicherheit, ob das Modell der Auftragsdatenverarbeitung oder die Durchsetzung berechtigter Interessen nach Art. 6 Abs. 1 f) DSGVO die Übertragung personenbezogener Daten an den Cloud-Anbieter rechtfertigen kann, bleibt bestehen.[6]

Datengetriebene Geschäftsmodelle verursachen vor allem dadurch Risiken für Grundrechte, dass sie sich für ihre Leistungen nicht in Geld bezahlen lassen, sondern Inhalts- und Nutzungsdaten zweckentfremden und aus ihnen umfassende Profile ihrer Nutzer (und Dritter) auf Vorrat anlegen, die sie für Werbe- und andere Zwecke nutzen [7] Die Datenschutz-Grundverordnung erleichtert diese Geschäftsmodelle dadurch, dass sie die Einwilligung erleichtert, die Zweckbindung relativiert und die berechtigten Interessen Dritter für eine Verarbeitung personenbezogener Daten ausreichen lässt. Dies werden die Argumente sein, um die vielfältigen Nachnutzungen der Kundendaten zu unterschiedlichen Zwecken als Gegenfinanzierung unentgeltlicher Angebote zu rechtfertigen. Diese Form der Profilbildung und -nutzung wird durch den „Schutz vor Profiling" in Art. 20 DSGVO nicht erfasst. Spezifischen Schutzmaßnahmen gegen diese Form der Datenverarbeitung sind in der Datenschutz-Grundverordnung nicht geregelt.

---

5 S. hierzu *Weichert*, Big Data und Datenschutz. Chancen und Risiken einer neuen Form der Datenanalyse, ZD 2013, 251; *Roßnagel*, Big Data – Small Privacy? Konzeptionelle Herausforderungen für das Datenschutzrecht, ZD 2013, 562; Roßnagel/Nebel, (Verlorene) Selbstbestimmung im Datenmeer – Privatheit im Zeitalter von Big Data, DuD 2015, 455.

6 S. hierzu ausführlich *Kroschwald*, ##, 2015, ##; *Roßnagel*, Datenschutzfragen des Cloud Computing, in: Roßnagel, A. (Hrsg.), Wolken über dem Rechtsstaat? Recht und Technik des Cloud Computing in Verwaltung und Wirtschaft, Baden-Baden 2015, 21.

7 S. hierzu *Roßnagel*, Regulierung – was leistet unser Datenschutzrecht (nicht)?, in: Hill, H. (Hrsg.), E-Transformation. Veränderung der Verwaltung durch digitale Medien, Baden-Baden 2014, 78.

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

Antwort 2:
Einer der Gewinne für den Datenschutz durch die Datenschutz-Grundverordnung ist die Ausweitung des räumlichen Anwendungsbereichs in Art. 3 Abs. 2 DSGVO durch das Marktortprinzip. Danach soll nicht mehr der Ort, an dem der Datenverarbeiter niedergelassen ist, für die Anwendung des Datenschutzrechts entscheidend sein, sondern ob personenbezogene Daten von Personen verarbeitet werden, die sich in der Union aufhalten. Voraussetzung ist hierfür, dass der Verarbeiter entweder der betroffenen Person Waren oder Dienstleistungen anbietet oder die Datenverarbeitung der Beobachtung ihres Verhaltens in der Europäischen Union dient. Damit gilt die Datenschutz-Grundverordnung auch gegenüber den vielen geldfreien Internetdienstleistungen, die Anbieter außerhalb der Union anbieten. Diese Erweiterung ist zu begrüßen, weil sie zur Wettbewerbsgleichheit auf dem europäischen Markt von Anbietern in der Union und außerhalb der Union führt und die Wahrnehmung von Betroffenenrechten vereinfacht. Durch die Begrenzung auf zwei Zwecke führt sie jedoch dazu, dass bestimmte Verarbeitungen von Daten von Personen, die sich in der Union aufhalten, in den Anwendungsbereich fallen und andere nicht. Dies ist weder interessengerecht noch rechtsklar und wird vielfältige schwierige Abgrenzungsfragen aufwerfen. Besser wäre es gewesen, den Anwendungsbereich auf jegliche Verarbeitung personenbezogener Daten von Personen, die sich in der Europäischen Union aufhalten, auszudehnen und damit immer, unabhängig vom Zweck der Datenverarbeitung auf den Aufenthaltsort der betroffenen Person abzustellen.

Auch für den Datenschutz in der Union und den Wettbewerb auf dem Binnenmarkt wird erwartet, dass die Datenschutz-Grundverordnung in der Union für einheitliche Datenschutzregelungen sorgt. Diese Erwartung scheint die Datenschutz-Grundverordnung auch zu erfüllen, da ihre Regelungen unmittelbar in der gesamten Union gelten. Dieser Vorteil besteht allerdings nur grundsätzlich und vielen Regelungsbereichen gerade nicht.

Die Datenschutz-Grundverordnung ist nach Art. 288 Abs. 2 Satz 1 AEUV nicht nur - wie eine Richtlinie - hinsichtlich ihrer Zielsetzung, sondern auch hinsichtlich der zu ergreifenden Formen und Mittel verbindlich. Sie wird mit ihrem Inkrafttreten Teil der Rechtsordnung eines jeden Mitgliedstaats und gilt für alle Personen und Organisationen in allen Mitgliedstaaten unmittelbar. [8]

Allerdings hat die Europäische Union keine Kompetenz, deutsche Gesetze zu verändern oder außer Kraft zu setzen. Eine Unionsverordnung hat daher keinen Geltungsvorrang.[9] Daher gelten auch nach ihrem Erlass die deutschen Datenschutzregelungen unverändert weiter. Dieses Nebeneinander kann dazu führen, dass

---

8 *EuGH*, Rs. 6/64, Costa/ENEL, Slg. 1964, 1251, Ls 3 = NJW 1964, 2371; *EuGH*, Rs. 106/77, Simmenthal II, Slg. 1978, 629, Rn. 17/18; s. näher *Schroeder*, in: Streinz (Hrsg.): EUV/AEUV, 2. Aufl., München 2012, Art. 288 AEUV, Rn. 56; *Geismann*, in: von der Groeben/Schwarze/Hatje, Europäisches Unionsrecht, 4 Bände, 7. Aufl., Baden-Baden 2015, Art. 288 AEUV, Rn. 34; *Biervert*, in: Schwarze (Hrsg.), EU-Kommentar, 3. Aufl., Baden-Baden 2012, Art. 288 AEUV, Rn. 20.

9 S. *BVerfGE* 73, 339 (375); 123, 267 (398); 126, 286 (301f.); *Ehlers*, in: Schulze/Zuleeg/Kadelbach (Hrsg.): Europarecht, 3. Aufl. Baden-Baden 2015, § 11 Rn. 48.

sich Regelungen widersprechen und sich die Frage stellt, welche Regelung anwendbar ist. In einem solchen Konflikt genießt die Unionsverordnung Anwendungsvorrang.[10] Sie ist von den nationalen Behörden und Gerichten anzuwenden. Die konfligierende – weiterhin geltende – deutsche Vorschrift darf in diesem konkreten Konfliktfall nicht angewendet werden – gleichgültig, ob sie früher oder später als die Unionsnorm ergangen ist. Dieser Anwendungsvorrang, den sowohl der Europäische Gerichtshof als auch das Bundesverfassungsgericht ihrer Rechtsprechung zugrunde gelegt haben, wurde auch in der Protokollerklärung Nr. 17 zum Vertrag von Lissabon anerkannt. Aufgrund des Vorrangs wird „jede entgegenstehende Bestimmung des geltenden staatlichen Rechts ohne weiteres unanwendbar".[11]

Ein Konflikt, der erst den Anwendungsvorrang der Unionsverordnung auslöst, kann aber nur zu einer Regelung in der Unionsverordnung bestehen, die unmittelbar anwendbar ist. Dies ist jedoch nur dann der Fall, wenn die Regelung „eine klare und unbedingte Verpflichtung begründe(t)", die „keiner weiteren Maßnahme der [Unions]Organe oder der Mitgliedstaaten" bedarf und deshalb von staatlichen Behörden und Gerichten angewendet werden kann.[12] Bedarf eine Regelung in der Verordnung zu ihrer unmittelbaren Anwendbarkeit erst der Vervollständigung durch Durchführungsmaßnahmen der Kommission oder des nationalen Gesetzgebers, genießt sie keinen Anwendungsvorrang.[13]

Kein Konflikt zum Unionsrecht besteht auch, wenn eine nationale Vorschrift in ihrer Anwendung nicht zu einem Widerspruch zu den Vorgaben der Unionsverordnung führt, weil sie diese nur ergänzt. Sie bleibt anwendbar, solange und soweit eine im Bereich geteilter Unionskompetenzen erlassene Unionsverordnung den Sachverhalt nicht abschließend regelt. Nach Art. 2 Abs. 2 AEUV können die Mitgliedstaaten im Bereich geteilter Zuständigkeiten tätig werden, „sofern und soweit die Union ihre Zuständigkeit nicht ausgeübt hat". Dies gilt auch für den Kompetenzbereich des Datenschutzes. Ob der Mitgliedstaat zur Rechtssetzung befugt ist, muss in jedem Einzelfall anhand des erlassenen Sekundärrechts geklärt werden. Entscheidend ist, in welchem Umfang die Union durch einen Sekundärrechtsakt von einer ihr zustehenden geteilten Zuständigkeit Gebrauch gemacht hat und dadurch der Akt eine Sperrwirkung gegenüber den Mitgliedstaaten entfaltet. Im Umkehrschluss ergibt sich aus dieser Analyse, „welche (Rest-)Zuständigkeit bei den Mitgliedstaaten verblieben ist".[14] Das Protokoll Nr. 25 zum Vertrag von Lissabon „Über die Ausübung der geteilten Zuständigkeiten"[15] stellt insofern klar: „Ist die Union in einem bestimmten Bereich" im Sinn des Art. 2 Abs. 2 AEUV „betreffend die geteilte Zuständigkeit tätig geworden, so erstreckt sich die Ausübung der Zuständigkeit nur auf die durch den entsprechenden Rechtsakt der Union geregelten Elemente und nicht auf den

---

10 *EuGH*, Rs. 6/64, Costa/ENEL, Slg. 1964, 1251, Ls 3 = NJW 1964, 2371; *EuGH*, Rs. 11/70, Internationale Handelsgesellschaft, Slg. 1970, 1125, Rn. 3 = NJW 1971, 343f.; *EuGH*, Rs. 106/77, Simmenthal II, Slg. 1978, 629, Rn. 17f.; *EuGH, Rs. 94/77,* Zerbone, Slg. 1978, 99, Rn. 22, 27; *BVerfGE* 31, 145 (173 ff.); 73, 223 (244); *Schroeder*, in: Streinz (Fn. 8), Art. 288 AEUV, Rn. 40; *Nettesheim*, in: Grabitz/Hilf/Nettesheim (Hrsg.): Das Recht der Europäischen Union, 3 Bände, München, Loseblatt, Art. 288 AEUV, Rn. 89; *Geismann,* in: von der Groeben/Schwarze/Hatje (Fn. 8),Art. 288 AEUV, Rn. 37; *Biervert,* in: Schwarze (Fn. 8), Art. 288 AEUV, Rn. 22; *Ruffert*, in: Calliess/Ruffert (Hrsg.,: EUV/AEUV, 4. Aufl. München 2011, Art. 288 AEUV, Rn. 20; *Jarass/Beljin*, Die Bedeutung von Vorrang und Durchführung des EG-Rechts für die nationale Rechtssetzung und Rechtsanwendung, NVwZ 2004, 1 ff.

11 *EuGH*, Rs. 106/77, Simmenthal II, Slg. 1978, 629, Rn. 17/18;

12 *EuGH*, Rs. 57/65, Lütticke, Slg. 1966, 239 (266) = NJW 1966, 1630f.; so auch für Sekundärrechtsakte Schroeder, in: Streinz (Fn. 8), Art. 288 AEUV, Rn. 60; *König*, in: Schulze/Zuleeg/Kadelbach (Fn. 9), § 2, Rn. 42*. Jarass/Beljin* (Fn. 10), NVwZ 2004, 3.

13 S. *EuGH*, Rs. 272/83, Kommission/Italien, Slg. 1985, 1057 Rn. 25; *Schroeder*, in: Streinz (Fn. 8), Art.288 AEUV, Rn. 61; *König*, in: Schulze/Zuleeg/Kadelbach (Fn. 9), § 2 Rn. 42; *Roßnagel*, Der Anwendungsvorrang der eIDAS-Verordnung. Welche Regelungen des deutschen Rechts sind weiterhin für eCommerce elektronische Signaturen anwendbar?, MMR 2015, 360.

14 S. *Pelka*, in: Schwarze (Fn. 8), Art. 2 AEUV, Rn. 14; S. *Streinz*, in: ders. (Fn. 8), Art. 2 AEUV, Rn. 8; *König*, in: Schulze/Zuleeg/Kadelbach (Fn. 9), § 2, Rn. 22.

15 EU ABl. C 115 vom 9.5.2008, 307.

gesamten Bereich." Daher sind Vorschriften der Mitgliedstaaten auch dann weiterhin anwendbar, wenn die Unionsverordnung bestimmte Themen ungeregelt lässt oder Regelungslücken lässt, auch wenn sie keine ausdrückliche Ermächtigung für ergänzende Maßnahmen enthält.[16] Dies gilt aber auch für unzureichende Konkretisierungen: „Solange und soweit" eine im Bereich geteilter Zuständigkeiten „erlassene Verordnung nicht durch Maßnahmen des Unionsgesetzgebers abschließend konkretisiert worden ist, sind auch ergänzende Maßnahmen der Mitgliedstaaten zulässig, und zwar mit oder ohne ausdrückliche Ermächtigung durch die Verordnung".[17]

Somit können Vorschriften eines Mitgliedstaats im Anwendungsbereich einer Unionsverordnung trotz ihres grundsätzlichen Anwendungsvorrangs aus drei Gründen weiterhin anwendbar sein:

Erstens ist ihre Anwendbarkeit nur insoweit eingeschränkt, als sie den Regelungen der Unionsverordnung widersprechen. Soweit kein Widerspruch vorliegt, sondern nur eine Präzisierung unbestimmter Rechtsbegriffe, eine Konkretisierung ausfüllungsbedürftiger Vorgaben oder die Ergänzung von unvollständigen Regelungen oder die Schließung von Regelungslücken, ohne das Regelungsziel der Verordnung zu verletzten, kann die mitgliedstaatliche Regelung weiter anwendbar bleiben, auch wenn ihr Wortlaut sich von der Regelung in der Verordnung unterscheidet. Ob ein solcher Widerspruch besteht ist für die Anwendung einer bestimmten Vorschrift der Unionsverordnung im Einzelfall zu prüfen. Ein schlichter Unterschied im Wortlaut reicht für die Feststellung eines solchen Widerspruchs nicht aus. Beispielsweise kann der Betroffene nach Art. 15 Abs. 1 h) DSGVO Auskunft über die „verwendete Logik" der automatisierten Entscheidungsfindung verlangen. Nach § 34 Abs. 2 und 4 BDSG kann der Betroffene u.a. Auskunft über die Berechnung und das Zustandekommen von Wahrscheinlichkeitswerten fordern. Diese Regelung ist nicht mit Art. Art. 15 Abs. 1 h) DSGVO identisch, kann aber als Präzisierung der „verwendeten Logik" verstanden werden.

Zweitens kann die mitgliedstaatliche Regelung weiter anwendbar sein, wenn die Verordnung explizite oder implizite Spielräume für nationale Regelungen lässt. So können z.B. die Mitgliedstaaten nach Art. 6 Abs. 3 DSGVO die beiden Erlaubnistatbestände der Erfüllung einer rechtlichen Verpflichtung nach (Art. 6 Abs. 1 c) DSGVO und der Wahrnehmung einer öffentlichen Aufgabe oder der Ausübung hoheitlicher Gewalt nach Art. 6 Abs. 1 e) DSGVO ausgestalten. Sie können dabei den Zweck der Datenverarbeitung näher regeln sowie Verarbeitungsbedingungen, Arten von Daten, betroffene Personen, Weitergabe von Daten, Speicherfristen sowie Verarbeitungsvorgänge und -verfahren.

Drittens kann eine von der Verordnung abweichende mitgliedstaatliche Regelung weiter angewendet werden, wenn sie einen impliziten Spielraum der Verordnung ausfüllt. Vollendet erst die mitgliedstaatliche Regelung eine unvollständige Vorschrift der Verordnung in der erforderlichen Bestimmtheit, ermöglicht sie erst den Vollzug der Verordnung durch die nationalen Behörden oder Gerichte, unterstützt sie die Umsetzung der Verordnung durch einen im nationalen Recht notwendigen Rechtsrahmen oder passt sie die Vorschrift der Verordnung in die Systematik und den Sprachgebrauch des nationalen Rechts ein, dann besteht kein Wiederspruch zur Unionsverordnung, der ihren Anwendungsvorrang aktiviert und die Nichtanwendbarkeit der nationalen Regelung zur Folge hat. Dies gilt etwa für die Ergänzung des Schutzes von Profiling in Art. 20 DSGVO. Die automatisierte Generierung von Einzelentscheidungen ist nur zulässig, wenn der Mit-

---

16 *Biervert*, in: Schwarze (Fn. 8), Art. 288 AEUV, Rn. 21; *Jarass/Beljin* (Fn. 10), NVwZ 2004, 5; *Schroeder*, in: Streinz (Fn. 8), Art. 288 AEUV, Rn. 61 – s. dort das Beispiel der EMAS-VO und des deutschen Ausführungsgesetzes.

17 *Schroeder*, in: Streinz (Fn. 8), Art. 288 AEUV, Rn. 61 unter Hinweis auf *EuGH*, Rs. 16/83, Prantl, Slg. 1984, 1299, Rn. 13 ff., 16.

gliedstaat „geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person“ geregelt hat.

Hinzukommt, dass die vielen unbestimmten Regelungen in der Praxis der Konkretisierung durch die nationalen Aufsichtsbehörden und Gerichte bedürfen. So wird etwa die Interessenabwägung für die Zulässigkeit der Datenverarbeitung nach der jeweiligen nationalen Datenschutzkultur konkretisiert und daher in der Praxis von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein.[18] Dadurch entsteht kein einheitlich durchgesetztes und gelebtes Recht.

Aufgrund der Unterkomplexität der Unionsregelungen sind mitgliedstaatliche Präzisierungen, Ausfüllungen und Ergänzungen notwendig, um die Verordnung problemadäquat und damit auf die faktischen Probleme, die es zu bewältigen gilt, anwendbar zu machen. In der Folge ist die Datenschutz-Grundverordnung kein homogenes, in sich geschlossenes Gesetzeswerk für den Datenschutz in der Union, sondern gleicht eher einem „Schweizer Käse“, der zwar einige strukturierende Elemente aufweist, vor allem aber durch die Löcher dazwischen auffällt. Anders als bei einem Schweizer Käse, werden diese Löcher aber unterschiedlich gefüllt werden. In der Folge wird kein einheitliches Datenschutzrecht in allen Mitgliedstaaten zur Anwendung kommen, sondern vergleichbar viele Unterschiede wie zuvor unter der Datenschutz-Richtlinie – nur an anderen Stellen und mit erheblicher Rechtsunsicherheit.

Frage 3:
Welcher Änderungsbedarf ergibt sich aus der Verabschiedung der Datenschutz-Grundverordnung für das deutsche Datenschutzrecht und die zahlreichen bereichsspezifischen Vorgaben? Von welchen Öffnungsklauseln sollte der nationale Gesetzgeber zwingend Gebrauch machen, um über die Vorgaben der Datenschutz-Grundverordnung hinausgehende Regelungen zu schaffen? 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? 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 DSGVO in Deutschland zu fördern?

Antwort 3:
Das Nebeneinandergelten der Rechtsordnungen der Union und des Mitgliedstaats sowie die Bedingungen für den Anwendungsvorrang können zu großen Rechtsunsicherheiten führen. Zwar greift im Konfliktfall der Vorrang zugunsten der Unionsverordnung, die deshalb kollidierende nationale Regelungen in ihrem Anwendungsbereich verdrängt. Jedoch ergeben sich aus einer solchen Situation „Unklarheiten tatsächlicher Art, weil die Normadressaten bezüglich der … Möglichkeiten, sich auf das [Unions]recht zu berufen, in einem Zustand der Ungewissheit gelassen werden“.[19] Diese Rechtsunsicherheiten können einen Bedarf an nationalen Regelungen begründen, die sie beseitigen.

---

18 S. hierzu Antwort 9.

19 *EuGH*, Rs. 74/86, Kommission/Deutschland, Slg. 1988, 2139, Rn. 10; *Schroeder*, in: Streinz (Fn. 8), Art. 288 AEUV, Rn. 62; *Biervert,* in: Schwarze (Fn. 8), Art. 288 AEUV, Rn. 21.

Widerspricht eine geplante mitgliedstaatliche Regelung der Verordnung, verhindert der Anwendungsvorrang des Unionsrechts „ein wirksames Zustandekommen neuer staatlicher Gesetzgebungsakte" der Mitgliedstaaten.[20] Der Gesetzgeber darf kein gegen Unionsrecht verstoßendes Recht setzen.

Hinsichtlich bestehender Regelungen kann der Mitgliedstaat verpflichtet sein, diese anzupassen oder aufzuheben, wenn sie keine Anwendung mehr finden können. Dadurch soll eine Ungewissheit vermieden werden, welches Recht anwendbar ist.[21] Sie dürfen daher geeignete Durchführungsmaßnahmen auch ohne Ermächtigung durch die Unionsverordnung erlassen. Sie können hierzu sogar nach Art. 291 Abs. 1 AEUV verpflichtet sein, wenn dies erforderlich ist, um die Unionsverordnung durchzusetzen. Dies gilt auch, wenn eine Lücke im Unionsrecht besteht und die Unionsverordnung durch die nationale Vorschrift abgerundet wird. Die nationale Vorschrift darf die Unionsverordnung jedoch nicht inhaltlich abändern.[22]

Dabei würde es sich anbieten, die Regelungen der Datenschutz-Grundverordnung und die Regelungen des deutschen Datenschutzrechts, die weiterhin anwendbar sind, in einem einheitlichen Regelwerk zusammenzufassen. Dies wäre für alle Beteiligten übersichtlicher und rechtssicherer als getrennte, sich ergänzende Regelwerke. Allerdings besteht für mitgliedsstaatliche Regelungen, die Unionsverordnungen unterstützen, ein Normwiederholungsverbot.[23] Würde eine Regelung einer Unionsverordnung im originär deutschen Recht wiederholt, wäre ihr nicht mehr anzusehen, welchen Ursprung sie hat und welcher Maßstab (Grundrechtecharta oder Grundgesetz) für sie entscheidend ist und welche Entscheidungsinstanz (Europäischer Gerichtshof oder Bundesverfassungsgericht) diesen Maßstab anwendet. Deshalb ist eine Umsetzung von Verordnungen durch Gesetzgeber der Mitgliedstaaten nicht nur überflüssig, sondern unzulässig, weil andernfalls die Adressaten den Unionsrechtscharakter der einschlägigen Regelung nicht mehr erkennen könnten und das Auslegungsmonopol des Europäischen Gerichtshofs ausgehöhlt würde.[24]

Dieses grundsätzliche Verbot nationaler Parallelgesetzgebung schließt jedoch nicht aus, dass mitgliedsstaatliche Bestimmungen einzelne Passagen des Wortlauts der Unionsverordnung wiederholen, um den inneren Zusammenhangs zwischen Unionsregelung und mitgliedsstaatlicher Regelung zu verdeutlichen und ihren gemeinsamen Inhalt für die Adressaten verständlich zu machen.[25] Diese Ausnahme greift Erwägungsgrund 6a DSGVO auf und weist darauf hin, dass die Mitgliedstaaten, wenn sie Vorschriften der Verordnung präzisieren oder einschränken, „Bestandteile der Verordnung in ihre jeweiligen nationalen Rechtsvorschriften aufnehmen (können), soweit dies erforderlich ist, um die Kohärenz zu wahren und die nationalen Rechtsvorschriften für die Personen, für die sie gelten, verständlicher zu machen".

Die unvollständige und unterkomplexe Datenschutz-Grundverordnung führt durch ihren nur partiellen Anwendungsvorrang und das Fortgelten des deutschen Datenschutzrechts zu einer sehr schwer zu durchschauenden Gemengelage von Unionsrecht und deutschem Recht. Daher muss der deutsche Gesetzgeber

---

20 *EuGH*, Rs. C-106/77, Simmenthal II, Slg. 1978, 629, Rn. 17/18; *Schroeder*, in: Streinz (Fn. 8), Art. 288 AEUV, Rn. 45.

21 *EuGH*, Rs. 54/91, Deutschland/Kommission, Slg. 1993, I-3399, Rn. 38; *EuGH*, Rs. 52/95, Kommission/ Frankreich, Slg. 1995, I-4443, Rn. 28; *Schroeder*, in: Streinz (Fn. 8), Art. 288 AEUV, Rn. 62; *Biervert,* in: Schwarze (Fn. 8), Art. 288 AEUV, Rn. 21; *König*, in: Schulze/Zuleeg/Kadelbach (Fn. 9), § 2, Rn. 43.

22 *EuGH*, Rs. 40/69, Hauptzollamt Hamburg/Bollmann, Slg. 1970, 69, Rn. 4 ff.; *Biervert,* in: Schwarze (Fn. 8), Art. 288 AEUV, Rn. 21; *Ehlers,* in: Schulze/Zuleeg/Kadelbach (Fn. 9), § 11 Rn. 58.

23 S. auch *Bundesministerium der Justiz,* Handbuch der Rechtsförmlichkeit, 3. Aufl. Berlin 2008, Rn. 285.

24 S. *EuGH*, Rs. 39/72, Italien, Slg. 1973, 101; *EuGH*, Rs. 34/73, Variola, Slg. 1973, 981, Rn. 9 ff.; *Schroeder*, in: Streinz (Fn. 8), Art. 288, Rn. 58;

25 S. *EuGH*, Rs. 272/83, Kommission/Italien, Slg. 1985, 1057 Rn. 27; *Schroeder*, in: Streinz (Fn. 8), Art. 288, Rn. 65.

das deutsche Datenschutzrecht, insbesondere das Bundesdatenschutzgesetz daraufhin überarbeiten, dass aus der Datenschutz-Grundverordnung und aus dem weiteranwendbaren deutschen Datenschutzrecht sowie aus zusätzlichen Regelungern, die zu erlassen sind, um die Vorschriften der Datenschutz-Grundverordnung zu präzisieren, zu konkretisieren und zu ergänzen, eine kohärente, widerspruchsfreie und vollzugsfähige Gesamtregelung des Datenschutzrechts wird.

Für ein Anpassungsgesetz zur Datenschutz-Grundverordnung ergeben sich unterschiedliche Aufgaben und Dringlichkeiten:

Um die praktische Anwendbarkeit der Datenschutz-Grundverordnung zu gewährleisten sollte bis zu ihrem Inkrafttreten eine Bereinigung des deutschen Datenschutzrechts in der Weise erfolgen, dass die Regelungen, die aufgrund der Anwendungsvorrangs der Vorgaben der Datenschutz-Grundverordnung in keiner Weise mehr angewendet werden können, aufgehoben oder angepasst werden. Nur so erlangen die betroffenen Unternehmen, Behörden, Aufsichtsstellen und Personen ausreichende Rechtssicherheit zum anwendbaren Datenschutzrecht.

Um die Vollzugsfähigkeit der Verordnung herzustellen, sind die Regelungsaufträge der Verordnung wie etwa in Art. 39 DSGVO (Zertifizierung), 53 DSGVO (ausreichende Aufsichtsbefugnisse) und Art. 79b DSGVO (Sanktionen) erforderlich.

Um für die Regelungsadressaten rechtzeitig Rechtssicherheit zu gewährleisten, muss frühzeitig geklärt werden, wie z.B. die Regelungsspielräume in Art. 9 Abs. 2 DSGVO (Ausnahmen vom Verbot der Verarbeitung sensibler Daten), Art. 9 Abs. 5 DSVGO (Verarbeitung von Gesundheits- und genetischen Daten), Art. 20 Abs. 2 DSGVO (Ausnahmen vom Verbot automatisierter Generierung von Einzelentscheidungen), Art. 35 DSGVO (Bestellung von Datenschutzbeauftragten) ausgefüllt werden sollen. Anpassungen in der Datenschutzpraxis können erst dann erfolgen, wenn klar ist, welche in der Vergangenheit geübten Praktiken auch künftig weiter zulässig oder gefordert sein sollen.

Ausgefüllt werden müssen auch die in Kapitel IX (Art. 80 bis 85 DSGVO) geregelten besonderen Verarbeitungssituationen (Meinungs- und Informationsfreiheit, Zugang zu und Weitergabe von Informationen des öffentlichen Sektors, Verarbeitung von nationalen Kennziffern, Geheimhaltungspflichten, Datenverarbeitung im Beschäftigungskontext, in Kirchen und religiösen Vereinigungen oder Gemeinschaften sowie zu wissenschaftlichen, statistischen oder historischen Zwecken). Für diese besteht allerdings kein vergleichbarer Zeitdruck. Diese Regelungsspielräume könnten auch nach Inkrafttreten der Datenschutz-Grundverordnung gefüllt werden. Bis zur Neuregelung gelten die bestehenden Regelungen etwa der §§ 32, 39 bis 42 BDSG weiter.

Dennoch besteht ein Klärungsbedarf, wie die weiter bestehenden Regelungen des deutschen Datenschutzrechts und die neuen Regelungen der Datenschutz-Grundverordnung zusammenspielen. Dieser Regelungsbedarf besteht insbesondere für den Datenschutz im Arbeitsverhältnis, der in § 32 BDSG ohnehin nur eine rudimentäre Regelung erhalten hat.

Für den Regelungsspielraum des Art. 6 Abs. 2a DSGVO gilt Vergleichbares. Er lässt alle nationalen Erlaubnistatbestände, die die Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 c) DSGVO) und die Wahrnehmung einer öffentlichen Aufgabe oder die Ausübung hoheitlicher Gewalt (Art. 6 Abs. 1 e) DSGVO) betreffen, weiter bestehen. Sie können auch nach Inkrafttreten der Datenschutz-Grundverordnung unverändert ange-

wendet werden. Dennoch ist auch für diese vielen Erlaubnistatbestände mittelfristig zu prüfen, ob ein Bedarf besteht, sie an die übrigen Vorgaben der Datenschutz-Grundverordnung anzupassen. Da der Regelungsspielraum nur die Erlaubnistatbestände betrifft, gilt für andere Regelungen des öffentlichen Datenschutzrechts – wie z.B. die Betroffenenrechte – grundsätzlich die Datenschutz-Grundverordnung.

Schließlich sollte möglichst bald geprüft werden, welche Regelungsspielräume zur Präzisierung und Konkretisierung der allgemeinen Vorgaben der Datenschutz-Grundverordnung hinsichtlich der spezifischen Risiken besonders risikoreicher Anwendungen der Informationstechnik bestehen – wie etwa bei Ubiquitous Computing, Big Data, Cloud Computing und datengetriebenen Dienstleistungen.

Unabhängig davon, ob nationale Regelungsspielräume bestehen oder nicht, wäre es sehr hilfreich, wenn staatliche Förderung von Forschung und Entwicklung Lösungen für datenschutzgerechte Technik- und Organisationsgestaltung sowie nachhaltige Geschäftsmodelle sowie Best Practice für ihre Umsetzung fördern würde.

Frage 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?

Antwort 4:
Zu Recht hat der Unionsgesetzgeber der Europäischen Kommission die geplante Selbstermächtigung durch delegierte Rechtsakte[26] verweigert. Statt 26 Ermächtigungen für delegierte Rechtsankte sieht die Verordnung nur zwei vor, nämlich in Art. 12 Abs. 4 c) DSGVO zur Festlegung von Bildsymbolen und in Art. 39a Abs. 7 DSGVO zur Bestimmung von Anforderungen und Kriterien für Zertifizierungsverfahren.

Die Fortentwicklung des Datenschutzrechts ist vor allem von der Dynamik immer wieder innovativer Informationstechniken, Anwendungen und Geschäftsmodelle geprägt, die permanent zu neuen und vielfältigen Infragestellungen informationeller Selbstbestimmung führen. Diese Dynamik verursacht immer wieder neuartige Risiken und Folgen und verstärkt zunehmend deren Komplexität. Für den Datenschutz stellen sich daher ständig neue Herausforderungen und erfordern eine permanente Suche nach geeigneten Regulierungen. Gefordert ist eine Suche nach heute noch unbekannten Lösungen. Für diese wäre es evolutorisch der absolut falsche Weg gewesen, die Fortentwicklung des Datenschutzrechts, wie von der Kommission gewollt, zu zentralisieren und zu monopolisieren. Vielmehr erfordern diese Herausforderungen eine Vielfalt der Lösungssuche, ein Experimentieren mit Konzepten und ein Erproben von Regelungen. Letztlich bewirkt die Verordnung in der Weiterentwicklung des Datenschutzrechts eine sinnvolle Arbeitsteilung zwischen Union und Mitgliedstaaten. Sie ermöglicht zumindest in beschränktem Umfang Experimente der Mitgliedstaaten. Die Verteilung der Fortentwicklung des Datenschutzrechts auf die Gesetzgeber der Union und der Mitglied-

---

26 S. zur Kritik u.a. *Hornung*, Eine Datenschutz-Grundverordnung für Europa?, ZD 2012, 104 (105); *Schild/Tinnefeld*, Datenschutz in der Union – Gelungene oder missglückte Gesetzentwürfe?, DuD 2012, 312 (314); *Roßnagel*, Datenschutzgesetzgebung: Monopol oder Vielfalt?, DuD 2012, 553; *Jaspers*, Die EU-Datenschutz-Grundverordnung – Auswirkungen auf die Datenschutzor-ganisation des Unternehmens, DuD 2012, 571; *Gießen*, Imperiale und totalitäre Züge des Kommissionsentwurfs für eine europäische Datenschutzverordnung, CR 2012, 550.

staaten bietet die Grundlage für einen Wettbewerb um Innovationen im Datenschutzrecht und die Entwicklung eines lebendigen Datenschutzes, der vielfältige Quellen hat.

Die Datenschutz-Grundverordnung leistet zumindest einen Beitrag, dass Datenschutz sich als Wettbewerbsvorteil für europäische Unternehmen etablieren kann. Sie fordert in vielen Bereichen Anstrengungen zur Realisierung von Datenschutz (etwa bei Privacy bei Design und Default in Art. 23 DSGVO), zur Aufstellung anspruchsvoller Verhaltensregeln (Art. 38 DSGVO) sowie zur Zertifizierung von Unternehmen und der Ausstellung von Datenschutzsiegeln und -prüfzeichen (Art. 39 DSGVO). Mit diesen können deutsche oder europäische Unternehmen im Binnenmarkt und auf dem Weltmarkt werben.

Positive und negative Effekte durch die Datenschutz-Grundverordnung für die deutsche und europäische Wirtschaft wurden schon in den Antworten zu den Fragen 1 bis 3 angedeutet. Für die Wirtschaft vordergründig positiv ist ein in vielen Details erweiterter Handlungsspielraum durch Verringerung des Datenschutzniveaus. Negativ dürften die erhöhte Rechtsunsicherheit und die hohe Wettbewerbsungleichheit sein.

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? 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?

Antwort 5:
Dieses Koordinationsproblem der föderalen Ordnung ist grundsätzlich in Art. 23 Abs. 4 und 5 GG geregelt. Danach ist der Bundesrat an der Willensbildung des Bundes zu beteiligen, soweit er an einer entsprechenden innerstaatlichen Maßnahme mitzuwirken hätte oder soweit die Länder innerstaatlich zuständig wären. Soweit in einem Bereich ausschließlicher Zuständigkeiten des Bundes Interessen der Länder berührt sind oder soweit im Übrigen der Bund das Recht zur Gesetzgebung hat, berücksichtigt die Bundesregierung die Stellungnahme des Bundesrates. Wenn im Schwerpunkt Gesetzgebungsbefugnisse der Länder, die Einrichtung ihrer Behörden oder ihre Verwaltungsverfahren betroffen sind, ist bei der Willensbildung des Bundes insoweit die Auffassung des Bundesrates maßgeblich zu berücksichtigen; dabei ist die gesamtstaatliche Verantwortung des Bundes zu wahren.

In einem Anpassungsgesetz zur Datenschutz-Grundverordnung sollte dieses Koordinationsproblem in vergleichbarer Weise gelöst werden. Die Vertretung der Bundesrepublik Deutschland im Europäischen Datenschutzausschuss (Art. 58 DSGVO) sollte die Beschlüsse eines noch zu errichtenden Deutschen Datenschutzausschusses der Aufsichtsbehörden nach den in Art. 23 Abs. 4 und 5 GG genannten Maßgaben berücksichtigen.

Frage 6:
Wie bewerten Sie die Datenschutz-Grundverordnung vor dem Hintergrund des Safe-Harbor-Urteils des EuGH von Oktober 2015 sowie des sogenannten „EU-US Privacy Shield", mit von der Europäischen Kommis-

sion ausgehandelten Kontrollbefugnissen und Rechten für europäische Bürger gegenüber amerikanischen Datenverarbeitern, das Anfang des Monats von der KOM vorgestellt wurde?

Antwort 6:
Die Frage ist schwer zu beantworten, weil bisher nur unklare Ankündigungen der Europäischen Kommission bekannt sind. Dargestellt werden können nur die Regelungen in der Datenschutz-Grundverordnung und die wesentlichen Gründe in der Entscheidung des Europäischen Gerichtshofs zu Unionsrechtswidrigkeit des Safe Harbor-Beschlusses der Kommission.

Wie nach Art. 25 DSRL darf eine Datenübermittlung in ein Drittland nach Art. 41 DSGVO nur erfolgen, wenn die Kommission festgestellt hat, dass das Drittland ein angemessenes Schutzniveau bietet. Bei der Prüfung der Angemessenheit muss die Kommission nach Art. 42 Abs. 2 insbesondere „die Rechtsstaatlichkeit, die Achtung der Menschenrechte und Grundfreiheiten, die in dem betreffenden Drittland geltenden einschlägigen Rechtsvorschriften sowohl allgemeiner als auch sektoraler Art – auch in Bezug auf öffentliche Sicherheit, Verteidigung, nationale Sicherheit und Strafrecht sowie Zugang der Behörden zu personenbezogenen Daten –, … die Existenz und die wirksame Funktionsweise einer oder mehrerer unabhängiger Aufsichtsbehörden, … Verpflichtungen, die sich aus rechtlich bindenden Übereinkünften oder Instrumenten“ ergeben, berücksichtigen. Insofern wird sich an den grundsätzlichen Anforderungen des Art. 25 DSRL an die Angemessenheit des Datenschutzniveaus nichts Wesentliches ändern. Die Regelungen der Datenschutz-Grundverordnung sind nur präziser gefasst.

Zur Angemessenheit des Datenschutzes in den USA hat der Europäische Gerichtshof in seinem Urteil vom 6. Oktober 2015 Folgendes Festgestellt:

Die Safe Harbor-Entscheidung 2000/520 der Kommission ermöglicht, „gestützt auf Erfordernisse der nationalen Sicherheit, des öffentlichen Interesses oder von Rechtsvorschriften der Vereinigten Staaten in die Grundrechte der Personen einzugreifen, deren personenbezogene Daten aus der Union in die Vereinigten Staaten übermittelt werden oder werden könnten. Für die Feststellung des Vorliegens eines Eingriffs in das Grundrecht auf Achtung der Privatsphäre kommt es nicht darauf an, ob die betreffenden Informationen über die Privatsphäre sensiblen Charakter haben oder ob die Betroffenen durch den Eingriff Nachteile erlitten haben könnten (Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 33 und die dort angeführte Rechtsprechung) (Rn. 87).“

„Der Schutz des Grundrechts auf Achtung des Privatlebens auf Unionsebene (verlangt jedoch) vor allem, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken (Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 52 und die dort angeführte Rechtsprechung) (Rn. 92).

„Nicht auf das absolut Notwendige beschränkt ist eine Regelung, die generell die Speicherung aller personenbezogenen Daten sämtlicher Personen, deren Daten aus der Union in die Vereinigten Staaten übermittelt wurden, gestattet, ohne irgendeine Differenzierung, Einschränkung oder Ausnahme anhand des verfolgten Ziels vorzunehmen und ohne ein objektives Kriterium vorzusehen, das es ermöglicht, den Zugang der Behörden zu den Daten und deren spätere Nutzung auf ganz bestimmte, strikt begrenzte Zwecke zu beschränken, die den sowohl mit dem Zugang zu diesen Daten als auch mit deren Nutzung verbundenen Eingriff zu rechtfertigen vermögen.“ (Rn. 83)

„Insbesondere verletzt eine Regelung, die es den Behörden gestattet, generell auf den Inhalt elektronischer Kommunikation zuzugreifen, den Wesensgehalt des durch Art. 7 der Charta garantierten Grundrechts auf Achtung des Privatlebens (vgl. in diesem Sinne Urteil Digital Rights Ireland u. a., C-293/12 und C-594/12, EU:C:2014:238, Rn. 39)." (Rn. 94)

„Desgleichen verletzt eine Regelung, die keine Möglichkeit für den Bürger vorsieht, mittels eines Rechtsbehelfs Zugang zu den ihn betreffenden personenbezogenen Daten zu erlangen oder ihre Berichtigung oder Löschung zu erwirken, den Wesensgehalt des in Art. 47 der Charta verankerten Grundrechts auf wirksamen gerichtlichen Rechtsschutz. Nach Art. 47 Abs. 1 der Charta hat nämlich jede Person, deren durch das Recht der Union garantierte Rechte oder Freiheiten verletzt worden sind, das Recht, nach Maßgabe der in diesem Artikel vorgesehenen Bedingungen bei einem Gericht einen wirksamen Rechtsbehelf einzulegen." (Rn. 95)

Aus diesen Passagen des Urteils des Europäischen Gerichtshofs ergibt sich, dass eine Anerkennung der Angemessenheit des Datenschutzniveaus der USA nicht möglich ist; wenn nicht die Zugriffsbefugnisse der US-Sicherheitsbehörden auf das „absolut Notwendige" beschränkt sind und europäische Bürger keine echten Möglichkeiten haben, bei einem Gericht einen wirksamen Rechtsbehelf einzulegen.

Frage 7:
Kann Großbritannien tatsächlich eine Ausnahmeregelung in Anspruch nehmen, der zufolge die Sperrklausel des Art. 43a 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?

Antwort 7:
Wenn Großbritannien Art. 43a DSVGO nicht anerkennt, muss es den anderen Mitgliedstaaten möglich sein, in ihren Anpassungsgesetzen zur Datenschutz-Grundverordnung den freien Datenverkehr mit Großbritannien aus diesem Grund einzuschränken. Das Verbot des Art. 1 Abs. 3 DSGVO, dass der freie Verkehr personenbezogener Daten in der Union aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden darf, kann nur gelten, soweit der Grundrechtsschutz durch die in der Verordnung geregelten Schutzklauseln gewährleistet ist.

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, das fraglich ist, ob eine einheitliche Rechtsauslegung dieser Begriffe in den Mitgliedsstaaten stattfindet, im Widerspruch zu einem einheitlichen Handeln innerhalb der EU-Mitgliedsstaaten?

Antwort 8:
Nach Art. 5 Abs. 1 b) DSGVO muss die Datenverarbeitung für einen anderen Zweck mit dem ursprünglichen Zweck „vereinbar" sein. Nach Art. 6 Abs. 3a DSGVO ist eine Regelung eines Mitgliedstaats zum Schutz der öffentlichen Sicherheit und Ordnung und zur Verhütung oder Verfolgung von Straftaten (s. die Zwecke in

Art. 21 Abs. 1 DSGVO) immer mit dem ursprünglichen Zweck der Datenverarbeitung vereinbar. Erwägungsgrund 40 DSGVO erläutert diese Vorschrift und ist bei ihrer Auslegung heranzuziehen.

Diese massive Durchbrechung des Zweckbindungsgrundsatzes kann in jedem Mitgliedstaat einen anderen Inhalt haben, je nachdem in diesem die Regelungen zum Schutz der öffentlichen Sicherheit und Ordnung und zur Verhütung oder Verfolgung von Straftaten ausgestaltet sind. Nicht nur dieser Begriff, sondern alle unbestimmten Rechtsbegriffe der Verordnung werden in den Mitgliedsstaaten eine unterschiedliche Rechtsauslegung erfahren.[27] Hier knüpft die Verordnung aber ausdrücklich an unterschiedliche Regelungen in den Mitgliedstaaten an und bewirkt in der zentralen Frage der Zweckbindung ein unterschiedliches Datenschutzrecht in den Mitgliedstaaten der Union. Dies steht in direktem Widerspruch zu einem – ursprünglich gewollten – einheitlichen Handeln innerhalb der EU-Mitgliedsstaaten. Dieses Ziel hat die Verordnung aber in vielen Fragen aufgegeben oder verfehlt. [28]

Frage 9:
Wie bewerten Sie die Ausnahmen der Datenschutz-Grundverordnung zur Rechtmäßigkeit von Datenverarbeitung ohne Einwilligung zu Zwecken von berechtigtem Interesse?

Antwort 9:
Nach dem Erlaubnistatbestand der Interessenabwägung in Art 6 Abs. 1 f) DSGVO ist die Datenverarbeitung im privatwirtschaftlichen Bereich bei einem berechtigten Interesse des Verantwortlichen oder eines Dritten erlaubt, sofern nicht Interessen, Grundfreiheiten und Grundrechte der betroffenen Person überwiegen. Diese extrem weite und unbestimmte Erlaubnis bietet weder Rechtssicherheit noch Grundrechtsschutz. Sie wird weder der Komplexität des Regelungsbedarfs noch der Schutzbedürftigkeit der betroffenen Personen (überwiegend Verbraucher) gerecht. Sie soll alle Erlaubnistatbestände abschließend ersetzen, die in den Mitgliedstaaten in vier Jahrzehnten sehr differenziert geregelt worden sind. Sie ersetzt etwa die Regelungen zum Datenschutz in der Werbung (§ 28 Abs. 3, 5 und 5 BDSG), bei der Übermittlung von Daten an Auskunfteien und zur Verarbeitung in Auskunfteien (§§ 28a, 29 und 30 BDSG), bei der Markt- und Meinungsforschung (§ 30a BDSG) und bei der Nutzung von Internetangeboten (§§ 11 bis 15 TMG). Dadurch werden nicht nur viele bisher unzulässige oder nur unter engen Bedingungen zulässige Formen des Umgangs mit personenbezogenen Daten erlaubt. Viel schlimmer ist, dass dieser offene Erlaubnistatbestand auch der alleinige Maßstab für die vielen neuen Geschäftsmodelle im Internet sein wird, die in den nächsten Jahren entstehen und auf der Ausbeutung personenbezogener Daten der Kunden beruhen.

Dieser bereits aus der Datenschutz-Richtlinie bekannte, reichlich unscharfe Tatbestand wird in der Verordnung noch weiter aufgeweicht, da die berechtigten Interessen eines jeden Dritten genügen. Die durch das Erfordernis der Interessenabwägung verursachte sehr hohe Rechtsunsicherheit zu reduzieren, sollte eigentlich Aufgabe der Mitgliedstaaten sein. Es wäre sehr hilfreich, wenn diese typische Interessenabwägungen in generalisierter Weise vornehmen würden. Solche Regelungen sind etwa vorgesehen in Art. 20 Abs. 2 DSVGO hinsichtlich automatisierter Generierung von Einzelentscheidungen, in Art. 80 und 80a DSVGO hinsichtlich der Wahrnehmung der Meinungsfreiheit, der Informationsfreiheit und des Zugangs zu amtlichen Dokumenten, in Art. 82 DSGVO hinsichtlich der Beschäftigungsverhältnisse sowie in Art. 83 DSGVO hinsichtlich Archiv-, Forschungs- und Statistikzwecken. Eine solche typisierte Interessenabwägung durch die Mitglied-

---

27 S. Antwort 9.

28 S. Antwort 2.

staaten wäre aber auch für die Werbung, für Auskunfteien, für Marktforschung und für Internetangebote sehr hilfreich.

Wegen der expliziten Ausnahmevorschrift des Art. 6 Abs. 2a DSVGO, die sich nicht auf alle Erlaubnistatbestände des Art. 6 Abs. 1 DSVGO, sondern ausschließlich auf die beiden Erlaubnistatbestände des Art. 6 Abs. 1 c) und e) DSVGO bezieht, fällt es jedoch schwer für den Erlaubnistatbestand der Interessenabwägung in Art 6 Abs. 1 f) DSGVO einen Konkretisierungsspielraum der Mitgliedstaaten anzunehmen. Es muss daher angenommen werden, dass die Verordnung diese Interessenabwägung dem für die Datenverarbeitung Verantwortlichen überlässt.

Ein unionsweit gleicher Wortlaut und der Ausschluss unterschiedlicher Konkretisierungen durch nationale Gesetzgeber werden aber nicht zu einer unionsweit gleichen Datenschutzpraxis führen. Es ist ein entscheidender Unterschied, ob eine Richtlinie fünf Erlaubnistatbestände als Ziel vorgibt, die eine bereichs- und problemspezifische Konkretisierung durch nationale Gesetze erfahren sollen, oder ob die gleichen fünf Erlaubnistatbestände in einer Verordnung unmittelbare Rechtsgeltung haben und die bestehenden ausdifferenzierten nationalen Regelungen ersetzen sollen. In diesem Fall kann Vereinheitlichung und Rechtssicherheit nur eine Illusion sein. Insbesondere die offene Abwägung berechtigter Interessen mit den schutzwürdigen Interessen der betroffenen Person wird in jedem Mitgliedstaat nach der bisherigen Datenschutzkultur erfolgen. Sie wird sich z.B. für die Videoüberwachung in Großbritannien an der bisher sehr großzügigen Praxis orientieren, in Deutschland an der Abwägung, die § 6b BDSG zugrunde liegt. Entsprechend wird man sich in Deutschland etwa für die Werbung an § 28 Abs. 3 BDSG, für Auskunfteien an § 28a BDSG, für Scoring an § 28b BDSG und für Marktforschung an § 30a BDSG und für Internetangebote an §§ 14 und 15 TMG ausrichten. Europäischer Datenschutz wird hinsichtlich der Zulässigkeit der Datenverarbeitung in jedem Mitgliedstaat praktisch einen anderen Inhalt haben. Wettbewerbsgleichheit ist so nicht zu erreichen.

Indem die Verordnung die Entscheidung über die Abwägung letztlich auf die Gerichte überträgt, entstehen aber noch viel unterschiedlichere Ergebnissen als unter der Datenschutzrichtlinie. Bisher waren die typisierten vom Gesetzgeber vorgenommenen Interessenabwägungen wenigsten für die Bundesrepublik Deutschland einheitlich. Jetzt wird es möglich sein, dass sie für lange Zeit von Gerichtsbezirk zu Gerichtsbezirk unterschiedlich ausfällt. Erst wenn die obersten Gerichte (in den jeweiligen Einzelfällen) für Rechtsklarheit sorgen, wie einzelne Interessenabwägungen vorzunehmen sind, besteht für diese Rechtssicherheit.

Zwar haben für die Anwendung der unbestimmten Rechtsbegriffe die Aufsichtsbehörden des Bundes und der Länder und aller Mitgliedstaaten einen bestimmenden Einfluss. Um diesen unionsweit zu vereinheitlichen, gibt es umständliche Koordinationsmechanismen. Da aber die Beschlüsse nach Art. 58a DSGVO nur die Aufsichtsbehörden als Adressaten verpflichten und kein allgemeinverbindliches (Exekutiv-)Recht setzen, unterliegen die divergierenden oder vereinheitlichten Interpretationsversuche der Verordnung durch die Aufsichtsbehörden der Überprüfung durch die örtlichen Gerichte. Diese können jeden vereinheitlichten Interpretationsversuch durch den Datenschutzausschuss konterkarieren. Eine Vereinheitlichung der Rechtsprechung ist allenfalls in einzelnen Fällen bezogen auf die jeweils enge Fallfrage nach jahrelangen Prozessen durch den Europäischen Gerichtshof zu erwarten.

A. Roßnagel

(Prof. Dr. Alexander Roßnagel)