WESTFÄLISCHE WILHELMS-UNIVERSITÄT
Institut für Informations-, Telekommunikations- und Medienrecht (ITM)
- Zivilrechtliche Abteilung -
Prof. Dr. Franziska Boehm
Juniorprofessur für IT-Recht

Leonardo-Campus 9
D-48149 Münster
Tel.: 02 51/83-3 86 00
Fax: 02 51/83-3 86 01
Email:
boehmf@uni-muenster.de
26. Februar 2013

Stellungnahme „EU-Datenschutzreform“

Zuziehung von Sachverständigen des Ausschusses für Europa und Eine Welt zu den Vorschlägen der EU-Kommission, Landtag Nordrhein-Westfalen

- für eine Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), KOM(2012)11 endg. (im Folgenden **DS-GVOE**)
- und für eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr, KOM(2012)10 endg. (im Folgenden **DS-RLE**)

Im Folgenden wird auf den Fragenkatalog in zusammengefasster Form geantwortet. Aufgrund der recht kurzen Zeitspanne zur Beantwortung der Fragen, wurden einige wenige Fragen außen vor gelassen.

Antworten auf den Fragenkatalog

Fragen 1, 2 und 11:

1. Halten Sie die Datenschutz-Grundverordnung für grundsätzlich zulässig hinsichtlich der Regelungskompetenz der EU?

2. Halten Sie die Rechtsform der Verordnung für sinnvoll und angemessen oder hätte man Ihres Erachtens eher auf eine Weiterentwicklung der bestehenden Datenschutzrichtlinie setzen sollen?

11. Ist der Entwurf der Kommission mit dem Subsidiaritätsprinzip (Art. 5 Abs. 3 EUV) vereinbar?

Die Kompetenz zur Regelung der Datenschutz-Grundverordnung folgt aus Art. 16 Abs. 2 AEUV. Dieser Artikel bezieht spiegelt sich in Artikel 8 der Grundrechte-Charta wider und inkorporiert das Datenschutzgrundrecht in den Regelungsbereich des AEUV. Art. 16 Abs. 2 S. 1 AEUV legt fest, dass das Europäische Parlament und der Rat Vorschriften über den Schutz von Personen bei der Verarbeitung personenbezogener Daten durch die „Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, und über den freien Datenverkehr“, erlassen dürfen. Inwieweit die EU-Institutionen dabei in mitgliedstaatliche Befugnisse eingreifen dürfen, bestimmt sich nach den der EU übertragenen Kompetenzen und der Beachtung der Prinzipien des Art. 5 EUV (der Grundsatz der begrenzten Einzelermächtigung und die Grundsätze der Subsidiarität und der Verhältnismäßigkeit). Das Protokoll über die Anwendung der Grundsätze der Subsidiarität und der Verhältnismäßigkeit regelt die Einzelheiten.

Weil der Bundesrat davon ausgeht, dass die Kommission in ihrem Vorschlag den Subsidiaritätsgedanken nicht beachtet hat, hat er mit dem Beschluss vom 30.03.2012 eine Subsidiaritätsrüge gemäß Art. 12 (b) EUV erhoben (BR-Drucksache 52/12). In diesem Beschluss werden einzelne Punkte des Verordnungsvorschlages kritisiert. *Nguyen* setzt sich mit diesem Punkten ausführlich auseinander und kommt zu dem Ergebnis, dass die Bedenken des Bundesrates hinsichtlich der Kompetenzüberschreitung der EU größtenteils unbegründet sind.[1] Dem soll sich hier angeschlossen werden.

[1] *Nguyen*, „Die Subsidiaritätsrüge des Deutschen Bundesrates gegen den Vorschlag der EU-Kommission für eine Datenschutzgrundverordnung“, ZEuS, Heft 3, 2012, S. 277-300.

Art. 16 Abs. 2 S. 1 AEUV definiert klar für welche Bereiche der EU-Gesetzgeber zuständig ist, nämlich „im Anwendungsbereich des Unionsrecht“. Dieser kann sich nur aus den der EU in den Verträgen zugewiesenen Politikbereichen ergeben und diese schließen den Datenschutz auf mitgliedstaatlicher Ebene mit ein (vgl. Art. 16 AEUV, Art. 8 Grundrechtecharta). Der vorherige einengende Bezug des EG-Vertrages (ex. Art. 95 EGV) zum Binnenmarkt ist weggefallen.[2] Stattdessen sind Politikbereiche, die der Gesetzgebung der EU vorenthalten bleiben sollen, ausdrücklich geregelt (z.B. die Bereiche nationale Sicherheit, Gefahrenabwehrrecht). Diese Bereiche nimmt der DS-GVOE daher auch bewusst von ihrem Anwendungsbereich aus (vgl. Art. 2 Abs. 2 (a) und (e) DS-GVOE).

Weiterhin sind auch die Anforderungen des Subsidiaritätsprinzips (die Ziele der Maßnahme sind nicht auf mitgliedstaatlicher Ebene erreichbar und die Maßnahme ist besser auf EU-Ebene erreichbar) erfüllt. Insbesondere die Tatsache, dass das Hauptziel des DS-GVOE – die europaweite Vereinheitlichung der Datenschutzregeln – bisher nicht erreicht wurde, auch nicht durch das Instrument der Richtlinie (Richtlinie 95/46), spricht für ein Tätigwerden der EU in diesem Bereich. Ebenso können Staaten immer weniger auf die globalen Entwicklungen in der Datenverarbeitung mit Einzelmaßnahmen reagieren. Ein europaweit einheitliches Datenschutzniveau wäre im Hinblick auf die Herausforderungen des Internetzeitalters in vielerlei Hinsicht von Vorteil. Genannt werden sollen hier die Rechte der Betroffenen auf Auskunft, Löschung und Berichtigung gespeicherter Daten. Eine einheitliche Gestaltung dieser Rechte über Staatsgrenzen hinweg könnte hier zu Verbesserungen führen.

Fragen 6 und 7

6. Welche Durchsetzungsdefizite sehen Sie im heutigen Datenschutzrecht? Inwiefern werden diese durch die Europäische Datenschutzreform gemindert oder beseitigt?
7. Welche Vor- und Nachteile sehen Sie in den durch die Europäische Datenschutzreform vorgesehenen Veränderungen in der Datenschutzaufsicht?

Durchsetzungsdefizite im heutigen Datenschutzrecht ergeben sich in verschiedener Hinsicht.

Räumlich gesehen entstehen Durchsetzungsdefizite oft dort, wo nationale Datenschutzbehörden an Staatsgrenzen stoßen. Aus diesem Blickwinkel ist der

[2] Ibid, *S. 288.*

vorgeschlagene Kohärenzmechanismus als Fortschritt zu betrachten. Verfahren, die einen länderübergreifenden Bezug mit europaweiter Bedeutung haben, können, oder müssen sogar, mit den anderen Datenschutzbehörden im Kohärenzverfahren im europäischen Datenschutzausschuss besprochen werden (vgl. Art. 57 ff. DS-GVOE). Dadurch werden von der Öffentlichkeit kritisierte Alleingänge, wie zum Beispiel der der irischen Datenschutzbehörde im Fall „Facebook“, vermieden. Auch Unterschiede in der Behandlung von grenzüberschreitenden Sachverhalten („Facebook“ etc.) würden so minimiert.

Ein Vorteil des Kohärenzmechanismus wäre also die Vereinheitlichung der Rechtsanwendung, und somit auch der Durchsetzung, von Datenschutzrecht bei Sachverhalten mit europaweitem Bezug. Die bisherige Artikel 29. Datenschutzgruppe erarbeitet vornehmlich beratende Stellungnahmen und äußert sich darin zu aktuellen Themen von europaweiter Bedeutung. Eine konkrete Zusammenarbeit findet zwar in Einzelfällen statt, allerdings gilt dies nicht für jeden Fall mit europaweitem Bezug. Da das Ziel des DS-GVOE die harmonisierte Anwendung und auch die Behebung von Durchsetzungsdefiziten ist, könnte hier die verstärkte Kooperation der Datenschutzbehörden eine positive Auswirkung auf die genannten Aspekte haben.

Der vorgeschlagene Kohärenzmechanismus führt allerdings dazu, dass die nationalen Datenschutzbehörden einen Teil ihrer Entscheidungsgewalt an das europäische Gremium abgeben. Dies ruft bei einigen nationalen Datenschutzbehörden Kritik hervor (als Beispiel kann hier die französische CNIL genannt werden) und führt zu der Befürchtung, dass viele Fälle nun im Kohärenzverfahren besprochen werden *müssen*. Dem kann entgegnet werden, dass die Datenschutzbehörden allerdings auch selbst Mitglied im europäischen Datenschutzausschuss sind und sich dieses Verfahren ausdrücklich nur auf Verarbeitungstätigkeiten bezieht, die in Art. 58 DS-GVOE aufgelistet sind (z.B. Tätigkeiten „die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen in *mehreren* Mitgliedstaaten oder mit der Beobachtung des Verhaltens dieser Personen im Zusammenhang stehen“, Art. 58 Abs. 2 (a) DS-GVOE).

Allerdings könnten präzisierende Kriterien, z.B. ab welchen Zeitpunkt genau (wie viele Mitgliedsstaaten müssen betroffen sein etc.) aus Sicht der Datenschutzbehörden eventuell Abhilfe schaffen. Weiterhin ist die starke *Rolle der Kommission* im Kohärenzmechanismus zu überdenken. Die Einwirkungsmöglichkeiten auf Entscheidungen der Datenschutzbehörden im Rahmen des Kohärenzmechanismus verstoßen möglicherweise gegen Primärrecht und führen faktisch zu einer ungerechtfertigten Besserstellung der Kommission gegenüber den eigentlich zuständigen Datenschutzbehörden (vgl. Antwort auf Frage 15).

Um auf die Durchsetzung von Datenschutzrecht in anderen Zusammenhängen zurückzukommen, sollten auch über die Personalausstattung von Datenschutzbehörden und die Möglichkeit von effektiven Strafen nachgedacht werden. Der DS-GVOE sieht höhere Geldstrafen als das LDSG NRW oder das BDSG vor. Bis zu 2 % des weltweiten Jahresumsatzes eines Unternehmens können verhängt werden. Im Hinblick auf die Aufgaben, die auf die Aufsichtsbehörden zukommen, sollte bedacht werden, dass eine konkrete Größe für die Personalausstattung in dem DS-GVOE nicht vorgesehen ist.

Fragen 15 und 22

15. Wie beurteilen die Sachverständigen die Vielzahl von Einzelermächtigungen zu bestimmten Sachbereichen des Datenschutzrechts zu Gunsten der Kommission, so dass das europäische Parlament weitgehend aus der Mitverantwortung für das Datenschutzrecht genommen wird?
22. Wie bewerten Sie die Vielzahl der delegierten Rechtsakte und Durchführungsrechtsakte in der Datenschutz-Grundverordnung, welche der Kommission, ohne die Einbindung demokratisch legitimierter Institutionen, erheblichen Ermächtigungsspielraum bei der Ausgestaltung der Verordnung einräumt?

Die Einzelermächtigungen der Kommission befinden sich am Ende fast jeden Artikels des DS-GVOE. Art. 86 und 87 Abs. 2 und 3 DS-GVOE verdeutlichen, wie viele Befugnisse zum Erlass von delegierten Rechtsakten (Art. 86 DS-GVOE) und von Durchführungsrechtsakten (Art. 87 Abs. 2 und 3 DS-GVOE) bestehen. Art. 290 und 291 AEUV enthalten die primärrechtliche Grundlage dafür. Die Vielzahl von Befugnissen ist aus verschiedenen Gründen problematisch:

- Art. 290 AEUV legt klar fest, dass sich delegierte Rechtsakte nur auf „Rechtsakte ohne Gesetzescharakter mit allgemeiner Geltung zur Ergänzung oder Änderung bestimmter *nicht wesentlicher Vorschriften* des betreffenden Gesetzgebungsaktes“ beziehen können.[3] Es ist höchst fraglich, ob die Vielzahl von Einzelermächtigungen und die damit verbundene tiefgreifende Entscheidungsgewalt der Kommission sich auf *nicht wesentliche Vorschriften* der DS-GVOE beziehen. Insbesondere dort, wo der DS-GVOE nur allgemeingültige Prinzipien nennt, ist das Ausgestaltungsrecht der

[3] Vgl. auch *Hornung*, Stellungnahme zu den öffentlichen Anhörungen des Innenausschusses des Deutschen Bundestages am 22. Oktober 2012 zu den Vorschlägen der Europäischen Kommission für eine Reform des Datenschutzes, abrufbar unter: http://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung22/Stellungnahmen_SV/Stellungnahme_05.pdf, S. 11 ff.

Kommission sehr weitgehend und kann dazu führen, dass auch wesentliche Vorschriften des DS-GVOE interpretiert werden. Als Beispiele können das Recht auf Datenübertragbarkeit (Art. 18), der Datenschutz durch Technik (Art. 23) und der Beschäftigtendatenschutz genannt werden.[4]

- Die in der Antwort auf die Fragen 6 und 7 angesprochene Rolle der Kommission im Rahmen des Kohärenzmechanismus (Art. 59 DS-GVOE) ist ebenfalls problematisch. Insbesondere im Hinblick auf den faktischen Einfluss auf die eigentlich unabhängigen Datenschutzbehörden. Das Kriterium der Unabhängigkeit ergibt sich aus dem Unionsrecht (Kapitel VI DS-GVOE und Rechtsprechung der europäischen Gerichte) und es ist nicht ersichtlich, dass die Kommission dieses Kriterium erfüllt. Es stellt sich daher die Frage, inwieweit der Einfluss der Kommission im Kohärenzmechanismus gerechtfertigt ist (*Hornung*[5] spricht hier von einer systemwidrigen Befugnis der Kommission, *Wuermeling*[6] von einer unnötigen Zentralisierung der Entscheidungsbefugnisse).

Fragen 20 und 21

20. Wie bewerten Sie das angestrebte Datenschutzniveau der Grundverordnung im Vergleich zum Richtlinienentwurf für den Sicherheitsbereich, insbesondere vor dem Hintergrund der mitunter unspezifischen Formulierungen der datenschutzrechtlichen Vorgaben für Polizei- und Justizbehörden?
21. Wie ist Ihrer Ansicht nach die im Richtlinienvorschlag vorgesehene „Erleichterung der Datenübermittlung an Drittländer und internationale Organisationen“ – man denke hier an den Zugriff US-amerikanischer Behörden auf europäische Fluggastdaten – mit der Gewährleistung eines hohen Datenschutzniveaus vereinbar? Bedarf es hier Ihrer Ansicht nach einer genaueren Definition und Begründung der vorgesehenen „Erleichterung“?

Das Datenschutzniveau der vorgeschlagenen DS-RLE bleibt weit hinter dem der DS-GVOE zurück. Der DS-RLE enthält eine Vielzahl von Ausnahmen von grundlegenden Datenschutzprinzipien. Eingeschränkt werden dadurch insbesondere die Betroffenenrechte, datenschutzrechtliche Grundprinzipien wie der Zweckbindungsgrundsatz oder die

[4] Ibid, S. 12.
[5] Ibid.
[6] *Wuermeling*, Stellungnahme zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 22. Oktober 2012 zum Vorschlag der Europäischen Kommission für eine Europäische Datenschutz-Grundverordnung (KOM (2012) 11 endg.), abrufbar unter: http://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung22/Stellungnahmen_SV/Stellungnahme_07.pdf, Punkt 5.

Anforderungen an ein angemessenes Schutzniveau bei der Übermittlung von Daten in Drittstaaten. Oft sind in den Artikeln des DS-RLE zwar die Grundprinzipien genannt, diese werden dann aber durch Ausnahmen wieder eingeschränkt. Auch fallen die Befugnisse der Datenschutzbehörden im DS-RLE im Vergleich zum DS-GVOE deutlich zurück.

In Bezug auf die in Frage 21 angesprochene „Erleichterung der Datenübermittlung an Drittländer und internationale Organisationen" ist auf die generelle Schwäche der Reglungen zum Drittstaatentransfer im DS-RLE hinzuweisen. Die Voraussetzung, dass grundsätzlich ein Angemessenheitsbeschluss der Kommission vorliegen muss, wird in Art. 35 Abs. 1 (b) des DS-RLE dadurch entwertet, dass schon ein für die Verarbeitung Verantwortlicher oder der Auftragsverarbeiter, der „alle Umstände beurteilt hat, die bei der Übermittlung personenbezogener Daten eine Rolle spielen, und zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen", Daten an ein Drittland oder eine internationale Organisation übermitteln darf. Die Entscheidung über die Übermittlung wird also nur von einem Mitarbeiter der entsprechenden Behörde oder sogar einem Auftragsdatenverarbeiter getroffen. In der Praxis wird es also in den meisten Fällen gerade nicht auf eine Angemessenheitsentscheidung der Kommission ankommen (diese existiert bisher nur für 12 Länder und 2 Sonderfälle (Fluggastdaten und Safe Harbor)), sondern auf die Entscheidung der einzelnen Behörden.

Eine einheitliche Übermittlungspraxis wird es also weiterhin nicht geben. Zusätzlich zu dieser Ausnahme sind weitere Ausnahmen in Art. 36 DS-RLE vorgesehen. Artikel 36 (d) des Entwurfs erlaubt dabei „abweichend von den Artikeln 35 und 35" des DS-RLE, dass Daten in ein Drittland oder eine internationale Organisation übermittelt werden dürfen, wenn „die Übermittlung zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Strafvollstreckung erforderlich ist". Es würde also reichen, wenn mit der Übermittlung irgendein polizeiliches oder justizielles Interesse verbunden ist. Wird dieser Vorschrift gefolgt, ist eine Angemessenheitsentscheidung der Kommission oder die Überprüfung weiterer datenschutzrechtlicher Voraussetzungen faktisch bei keinem Übermittlungsvorgang notwendig. Hier besteht dringender Nachbesserungsbedarf.

Ein weiterer Kritikpunkt bezieht sich in diesem Zusammenhang auf die Tatsache, dass die Kommission ihre eigenen Organisationen im Polizei- und Justizbereich (z.B. Europol und Eurojust) von einer Neuregelung ihrer Datenschutzrahmen zunächst verschont. Eine Einheitlichkeit der Regelungsinstrumente, auch vor dem Hintergrund des europaweiten Austausches von Polizei- und Justizdaten[7], auf EU- sowie mitgliedstaatlicher Ebene wird

[7] *Boehm,* "Information sharing and data protection in the Area of Freedom, Security and Justice – Towards

dadurch nicht erreicht.

Fragen 8, 14 und 18

8. Halten Sie es für sinnvoll, dass die Verordnung auch öffentliche Stellen erfassen soll und damit nach derzeitigem Entwurfsstand für öffentliche (auch hoheitlich im Bereich der Eingriffsverwaltung handelnde) Stellen gleiche Regelungen gelten würden, wie für Private und wirtschaftlich Handelnde ? Halten Sie eine Differenzierung für sinnvoll und erforderlich?
14. Wie beurteilen die Sachverständigen die Regelung des Datenschutzes sowohl für öffentliche als auch für nichtöffentliche Stellen in ein und demselben Rechtsetzungsakt, obgleich sich diese Bereiche erheblich voneinander unterscheiden?
18. Welche Rechtsetzungsbefugnisse verblieben den Mitgliedstaaten nach Inkrafttreten der Verordnungen im Bereich des Datenschutzes?

Grundsätzlich soll der DS-GVOE für private wie für öffentliche Datenverarbeitung gelten. In Deutschland hat sich allerdings eine Unterscheidung von Regeln für den öffentlichen und den privaten Bereich durchgesetzt. Auch wenn die grundlegenden Datenschutzregeln für beide Bereiche gelten, sind unterschiedliche Regelungen in Bundes- und Landesrecht, öffentlichem und privatem Recht sowie in bereichsspezifischen Bestimmungen enthalten.[8]

Der Regelungsbedarf bzw. die Harmonisierung der Datenschutzregeln im privaten Sektor ist unbestritten. Globale Herausforderungen und das Internetzeitalter machen eine stärkere Vereinheitlichung im Bereich der Wirtschaft notwendig. Inwieweit sich dieser Harmonisierungsbedarf auch auf die öffentliche Datenverarbeitung bezieht, ist nicht ganz so offensichtlich. Ein nachvollziehbares Argument, dass für eine Beibehaltung der bisherigen Trennung genannt wird, ist, dass die Datenschutzregeln im öffentlichen Bereich im Laufe der Jahre fortentwickelt und bereichsspezifisch ausdifferenziert wurden und teilweise nicht mehr von den jeweiligen Fachgesetzen zu trennen sind.[9]

Da der DS-GVOE gemeinsame Regeln für den öffentlichen sowie den privaten Sektor vorsieht, stellt sich in der Tat die Frage, wie viel Umsetzungsspielraum den Mitgliedstaaten bei der Ausgestaltung der Datenschutzvorschriften für den öffentlichen Bereich bleibt. Klar ist, dass die gleichen Datenschutzgrundsätze in beiden Bereichen gelten sollten. Ein Mittelweg wären die auch schon ansatzweise im DS-GVOE enthaltenen Öffnungsklauseln,

---

harmonised data protection principles for EU-internal information exchange", Springer 2012
[8] Vgl. *Rogall-Grothe*, „Ein neues Datenschutzrecht für Europa", ZRP 2012, S. 193-196.
[9] Ibid, S. 193.

die dem deutschen Gesetzgeber einen gewissen Spielraum überlassen um die Datenverarbeitung in bestimmten öffentlichen Bereichen national zu regeln (vgl. Art. 6 Abs. 1 (e), 9 Abs. 2 (j) DS-GVOE). Delegierte Rechtsakte der Kommission, die bislang für fast jeden Aufgabenkreis festgesetzt sind, dürften dann in diesen Bereichen nicht vorgesehen werden (vgl. z.B. Art. 81 Abs. 3 DS-GVOE). Eine Diskussion über die Bereiche, in denen der deutsche Gesetzgeber Sonderregelungen (z.B. zu speziellen Löschungsfristen, Datenarten etc.) beibehalten möchte, wäre daher notwendig. Diese Diskussion hätte auch Auswirkungen auf die Frage, welche Rechtsetzungsbefugnisse den Mitgliedstaaten nach Inkrafttreten der Verordnungen im Bereich des Datenschutzes verblieben. Grundsätzlich gilt, dass die Rechtsetzungsbereiche, die die DS-GVO regelt und bei denen die Kommission zum Erlass von delegierten Rechtsakten (Art. 86 DS-GVOE) und von Durchführungsrechtsakten (Art. 87 Abs. 2 und 3 DS-GVOE) befugt ist, der deutschen Gesetzgebung entzogen wären.

Wenn eine pauschale Ausklammerung des öffentlichen Sektors aus der EU-Regelung angestrebt wird, dann sollte bedacht werden, dass Datenschutz, trotz aller bereichsspezifischen Regelungen, nicht nur eine deutsche, sondern eine europäische Querschnittsmaterie ist und die Verbindungen zwischen privater und öffentlicher Datenverarbeitung eher zu- als abnehmen (auf EU- sowie auf mitgliedstaatlicher Ebene).[10] Beispiele dafür sind der Zugriff von Privaten auf Register-/Meldedaten und der staatliche Zugriff auf Verbindungsdaten oder Fluggastdaten. Der Zugriff des Staates auf Daten des Privatsektors (Fluggastdaten, Bankdaten, Verbindungsdaten etc.) ist allerdings weder im DS-GVOE noch im DS-RLE geregelt. Hier gibt es Nachbesserungsbedarf. Dies gilt insbesondere im Hinblick auf die wünschenswerte Harmonisierung der beiden von der EU vorgeschlagenen Instrumente (DS-GVOE und DS-RLE). Ebenso gilt zu bedenken, dass der Austausch zwischen Behörden verschiedener Mitgliedstaaten künftig ebenfalls ansteigen wird. Auch wenn gegenwärtig in diesem Bereich vielleicht noch kein großes Harmonisierungsbedürfnis besteht[11], ist dies für die Zukunft nicht ausgeschlossen. Diese Gesichtspunkte sollten im Hinterkopf behalten werden, wenn überlegt wird, die komplette öffentliche Datenverarbeitung aus dem DS-GVOE zu streichen.

Fragen 5, 12, und 26

5. Welche Regelungen des deutschen und des Nordrhein-Westfälischen Datenschutzrechts sollten aus Ihrer Sicht unbedingt erhalten bleiben?

12. Wie beurteilen die Sachverständigen die Umsetzbarkeit der in dem Entwurf für die EU-

[10] Vgl. *Masing*, „Herausforderungen des Datenschutzes“, NJW 2012, 2305-2312, insbesondere S. 2309.
[11] Vgl. *Rogall-Grothe*, „Ein neues Datenschutzrecht für Europa“, ZRP 2012, S. 193-196.

Datenschutz-Grundverordnung enthaltenen Vorgaben für die Datenverarbeitung in Unternehmen?

26. Sorgt die Grundverordnung für ein angemessenes Datenschutzniveau hinsichtlich absehbarer technologischer Entwicklungen wie beispielsweise „SmartMeter“?

Für Unternehmen, die den Bestimmungen des DS-GVOE unterfallen, ergeben sich Neuerungen, die unter bestimmten Bedingungen beispielsweise eine ausführliche Dokumentationspflicht vorsehen (Art. 28 DS-GVOE), Regelungen zum Datenschutz durch Technik vorschreiben (Art. 23 DS-GVOE) oder eine Meldepflichte bei Datenschutzverstößen (Art. 31 f. DS-GVOE) und das Erfordernis einer Datenschutzfolgenabschätzung (Art. 33 DS-GVOE) einführen. Viele dieser Neuerungen – insbesondere die Forderung nach einem Datenschutz durch Technik – entsprechen den in der Literatur seit langem geforderten Maßnahmen. Trotzdem lässt sich im DS-GVOE eine gewisse „Technikferne“[12] erkennen, die in der praktischen Umsetzung dazu führen kann, dass konkrete Maßnahmen, die technisch möglich wären, nur unzureichend umgesetzt werden. Konkrete Anforderungen an die Ausgestaltung der Technik werden nämlich nicht getroffen. Die Kommission behält sich zwar in Art. 23 Abs. (3) DS-GVOE vor, die technischen Vorgaben auszugestalten, jedoch ist diesem Ansinnen kein zeitlicher Rahmen gesetzt. Auch ist nicht geklärt, wie detailliert diese Vorgaben sein sollen.

Es ist daher schwer vorherzusagen, ob die oben genannten Anforderungen in der Praxis von Seite der Unternehmen wirklich als große Belastung wahrgenommen würden. Da hohe Datenschutzstandards auch als Wettbewerbsvorteil in bestimmten Branchen (z.B. Telekommunikation, Internetanbieter) angesehen werden können und die Regeln europaweit einheitlich wären, müssen diese Neuerungen nicht notwendigerweise negative Auswirkungen auf die Wirtschaftlichkeit der Unternehmen haben.

Allerdings kann sich der Kritik, die hinsichtlich der 250 Mitarbeiter Schwelle für die Einrichtung eines betriebsinternen Datenschutzbeauftragten (Art. 35 Abs. 1 (b)) geäußert wurde, angeschlossen werden. Eine Regelung, die weniger an quantitative Voraussetzungen gebunden ist oder die sich als Maßstab an den Betroffenen orientiert, wäre hier zu bevorzugen.[13] Laut DS-GVOE ist ein betrieblicher Datenschutzbeauftragter allerdings auch

[12] *Hornung*, Wortprotokoll zu den öffentlichen Anhörungen des Innenausschusses des Deutschen Bundestages am 22. Oktober 2012 zu den Vorschlägen der Europäischen Kommission für eine Reform des Datenschutzes, abrufbar unter: http://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung22/Protokoll.pdf, S. 15.

[13] Vgl. z.B. den Vorschlag des EU-Parlaments rapporteurs *Jan Philipp Albrecht*, der eine Schwelle von 500 von der Datenverarbeitung Betroffenen pro Jahr vorschlägt, Dokument 2012/0011 (COD)vom 17.12.2012.

bei denjenigen Unternehmen vorgesehen, die als Kerntätigkeit Datenverarbeitungsvorgänge vollziehen, „welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen“. Dies ist begrüßenswert, erfasst aber nicht alle Fälle, in denen ein Datenschutzbeauftragter notwendig wäre. *Hornung* nennt hier das Beispiel der Verarbeitung besonders sensibler Daten.[14] Hier besteht also Nachbesserungsbedarf.

Frage 10

Frage 10: Wie beurteilen die Sachverständigen den Entwurf der Kommission für eine EU-Datenschutz-Grundverordnung im Vergleich zur geltenden Rechtslage?

Diese Frage kann meiner Meinung nach nur aus europäischer Sicht beurteilt werden. Die Aufgabe der DS-GVO wird es sein, das Datenschutzrecht europaweit einheitlich zu gestalten. Den Entwurf nur mit der in Deutschland geltenden Rechtslage zu vergleichen greift zu kurz. Einzelne Rechtsordnungen, wie die deutsche, sind in der Datenschutzgesetzgebung im Vergleich zu vielen anderen europäischen Ländern weit fortschritten. Modernisierungsbedarf besteht allerdings auch in Deutschland.[15] Die vorgeschlagenen Vorschriften zum Datenschutz durch Technik (auch wenn hier noch Nachbesserungsbedarf besteht) oder zu den Meldepflichten bei Datenschutzverstößen wären auch für das deutsche Datenschutzrecht neu und können hier über das hinausgehen, was es zurzeit in Deutschland an gesetzlichen Regelungen gibt. Diese Argumentation soll allerdings nicht verhindern, dass in vielen zu recht kritisierten Bereichen des DS-GVOE nachgebessert wird.

Frage 13

Frage 13: Wie beurteilen die Sachverständigen die in Ziffer II.5 des Antrags erhobene Forderung, wonach die Kontrolle einzelstaatlicher Grundrechte den nationale Verfassungsgerichten erhalten bleiben soll, vor dem Hintergrund, dass das Unionsrecht ohnehin keine Kontrolle nationaler Grundrechte durch den Gerichtshof der Europäischen Union vorsieht?

---

[14] *Hornung*, „Eine Datenschutz-Grundverordnung für Europa?“, ZD 3/2012, S. 99-106 (S. 104).

[15] *Neumann*, Wortprotokoll zu den öffentlichen Anhörungen des Innenausschusses des Deutschen Bundestages am 22. Oktober 2012 zu den Vorschlägen der Europäischen Kommission für eine Reform des Datenschutzes, abrufbar unter: http://www.bundestag.de/bundestag/ausschuesse17/a04/Anhoerungen/Anhoerung22/Protokoll.pdf, S. 16.

Wenn das Instrument einer Verordnung gewählt wird und diese Verordnung abschließende Vollregelungen in einem Bereich enthält und die nationalen Gerichte solche Vorschriften der DS-GVO auslegen wollen, müssen sie diese Fragen den europäischen Gerichten vorlegen. Diese Vorschriften werden dann anhand der Grundrechte auf europäischer Ebene geprüft. Auf europäischer Ebene normiert Art. 8 der Charta der Grundrechte ein Recht auf Datenschutz. Art. 16 spiegelt dieses Recht im AEUV wider. Inwieweit dieses Grundrecht dem deutschen Grundrecht auf informationelle Selbstbestimmung entspricht, müsste die (europäische) Rechtsprechung im Laufe der Jahre klären. Eine Überprüfung von abschließenden Verordnungsbestimmungen anhand von nationalen Grundrechten wäre jedenfalls nicht europarechtskonform. Allerdings könnten Öffnungsklauseln, wie in der Antwort auf die Fragen 8, 14 und 18 angesprochen, in diesem Zusammenhang Spielraum für den deutschen Gesetzgeber eröffnen.

Frage 16

16. Welche Anwendungslücken der Datenschutzgrundverordnung bestehen im Hinblick auf die Datenerhebung und -nutzung durch Unternehmen ohne Sitz in der EU, die zudem aufgrund des gewählten Regelungsinstruments der Verordnung durch die Mittgliedstaaten nicht zu beheben wären?

Unternehmen ohne Sitz in der EU, die Daten im Anwendungsbereich der DS-GVO verarbeiten, müssen gemäß Art. 25 DS-GVOE einen Vertreter in der EU benennen. Dies gilt allerdings nicht für Unternehmen, die in einem Drittland niedergelassen sind, das laut Beschluss der Kommission einen angemessenen Schutz bietet, für Unternehmen, die weniger als 250 Mitarbeiter beschäftigen oder für Unternehmen, die nur gelegentlich Waren oder Dienstleistungen anbieten. Insbesondere die Ausnahme in Art. 25 Abs. 2 (b) (Unternehmen, die weniger als 250 Mitarbeiter beschäftigen) ist nicht an qualitative Kriterien geknüpft und könnte hier zu Nachteilen für die Betroffenen führen, wenn z.B. ein kleines Unternehmen viele personenbezogenen Daten verarbeitet. Genauso könnten große Unternehmen, die nur sehr wenige personenbezogene Daten verarbeiten, einem unverhältnismäßigen bürokratischen Aufwand unterworfen werden. Ein Kriterium, das an die Menge der verarbeiteten personenbezogenen Daten anknüpft[16], wäre hier sinnvoller um wirkungsvoll den Gefahren, die von der Nutzung personenbezogener Daten ausgehen, entgegenzutreten.

[16] Vgl. z.B. den Vorschlag des EU-Parlaments rapporteurs *Jan Philipp Albrecht*, der eine Schwelle von 500 von der Datenverarbeitung Betroffenen pro Jahr vorschlägt, Dokument 2012/0011 (COD)vom 17.12.2012.