Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)584 C

Dr. Imke Sommer
Die Landesbeauftragte für
Datenschutz und Informationsfreiheit

Freie
Hansestadt
Bremen

Bremerhaven, den 16.10.2012

Öffentliche Anhörung des Innenausschusses des Deutschen Bundestages zu

a) dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)

KOM(2012)11 endg. Ratsdok.-Nr. 5853/12

b) der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen

Der Schutz der Privatsphäre in einer vernetzten Welt

Ein europäischer Datenschutzrahmen für das 21. Jahrhundert

KOM(2012)9 endg. Ratsdok.-Nr. 5852/12

c) dem Antrag der Abgeordneten Dr. Konstantin von Notz, Volker Beck (Köln), Kai Gehring, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN

EU-Datenschutzreform unterstützen

BT-Drucksache 17/9166

Schriftliche Stellungnahme

Die Kommission hat es sich mit ihrem Vorschlag zum Ziel gesetzt, auf die Herausforderungen zu reagieren, die der rasche technologische Fortschritt und die Globalisierung für den Datenschutz bedeuten. Dies entspricht dem Eintreten der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSK) für „Ein modernes Datenschutzrecht für das 21. Jahrhundert.“[1] Gemeinsam mit der Kommission wird hier die Auffassung vertreten, dass es wichtig ist, dieses Vorhaben europaweit zu verfolgen.[2]

[1] So der Titel der Eckpunkte der Konferenz der Datenschutzbeauftragten des Bundes und der Länder für „Ein modernes Datenschutzrecht für das 21. Jahrhundert“ vom 18.3.2010, siehe etwa www.baden-wuerttemberg.datenschutz.de/service/gem-materialien/modernisierung.pdf.
[2] Siehe auch die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 21./22.3.2012 „Ein hohes Datenschutzniveau für ganz Europa!“, www.datenschutz.bremen.de/konferenzbeschluesse2.php?=157.

Wie im Folgenden zu zeigen sein wird, folgt der von der Kommission vorgelegte Vorschlag für eine „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“ einseitig der Logik des Binnenmarktes. Er nimmt also **zu sehr** den **freien Datenverkehr** in den Blick.

Das durch eine Verordnung erreichbare europäische Datenschutzniveau sollte demgegenüber durch vier Maßnahmen gestärkt werden:

1) Aus Datenschutzsicht wäre eine Verordnung optimal, die möglichst detaillierte Regelungen enthält, die den Schutz der personenbezogenen Daten der Menschen in Europa in den Vordergrund stellen. Da der gegenwärtige Verordnungsvorschlag den freien Datenverkehr privilegiert, sollten daher an zahlreichen Stellen **Regelungen, die den freien Datenverkehr begünstigen, durch Regelungen ersetzt werden, die den Datenschutz zumindest mit im Blick haben oder sogar seinerseits begünstigen** (siehe dazu II.).

2) Die zahlreichen Regelungsgegenstände, für die nach dem Verordnungsentwurf Ermächtigungen für direkte Rechtsakte bestehen, sollten **in der Verordnung selbst geregelt werden, an in der Verordnung selbst normierte Voraussetzungen für strenge Datenschutzstandards gebunden oder gestrichen** werden (siehe dazu I. 3b) und II.).

3) Als Sicherungsmechanismus gegen Verordnungsregelungen, die den freien Datenverkehr privilegieren, sollte festgelegt werden, dass es sich bei allen Regelungen der Verordnung um **datenschutzrechtliche Mindeststandards** handelt und die Mitgliedstaaten frei sind, Regelungen zu treffen, die einen höheren Datenschutzstandard gewährleisten (siehe dazu I.3).

4) Die **unabhängigen Datenschutzbehörden sollten nur dem Datenschutz**, nicht jedoch dem Schutz des freien Datenverkehres **verpflichtet** werden (siehe dazu I.3c).

Damit werden Anforderungen an den Kommissionsvorschlag formuliert, die das im Verordnungsvorschlag enthaltene strukturelle Ungleichgewicht zu Lasten des Datenschutzes beseitigen könnten. Zunächst sollen hier diejenigen Forderungen dargestellt werden, die sich auf strukturelle Veränderungen im Kommissionsvorschlag beziehen (I). Im Anschluss daran werden Forderungen formuliert, die sich auf die Erhöhung des durch den Kommissionsvorschlag erreichbaren Datenschutzniveaus beziehen (II.).

I. Die Präferenz für den freien Datenverkehr durch ein Votum für die beiden Ziele freier Datenverkehr und Datenschutz ersetzen

Die Diskussion um den Vorschlag der Europäischen Kommission wird in Deutschland – wie es das vorgeschlagene Kürzel „Datenschutzgrundverordnung“ nahe legt – als Diskussion über den Datenschutz in Europa geführt. Dass dies eine Verkürzung darstellt, zeigt schon der vollständige Titel des Kommissionsvorschlages für eine Verordnung „zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.“

Die Kommission stützt ihren Vorschlag auf den Vertrag über die Arbeitsweise der Europäischen Union (AEUV), insbesondere auf Artikel 16 Absatz 2 und Artikel 114 Absatz 1. Daher handelt es sich um Regelungen „über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (...) und über den freien Datenverkehr“

(Artikel 16 Absatz 2) und gleichzeitig eine Maßnahme „zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, welche die Errichtung und das Funktionieren des Binnenmarkts zum Gegenstand“ hat (Artikel 114 Absatz 1). Diese Unentschlossenheit in der Wahl der dem Vorschlag zugrunde liegenden Ermächtigungsgrundlage wird von der italienischen Regierung in ihrer Stellungnahme kritisiert.[3] Es deutet Vieles darauf hin, dass die Wahl dieser beiden Grundlagen nicht der Unentschlossenheit geschuldet ist, sondern die Präferenz des Kommissionsvorschlages für das Ziel der Erleichterung des freien Datenverkehrs ausdrückt.

Dass der Kommission das Ziel des freien Datenverkehrs sehr am Herzen liegt, zeigt schon die Einbettung des Kommissionsvorschlages in die „digitale Agenda“[4] die unter anderem einen „digitalen Binnenmarkt“[5] anstrebt. Als Ziele des Kommissionsvorschlages werden in diesem Zusammenhang die Stärkung der Privatheitsrechte im Onlinebereich und die Ankurbelung der europäischen digitalen Wirtschaft genannt.[6] Das Verhältnis dieser beiden Ziele erschließt sich, wenn die Kommission die Problemlage beschreibt: Die kritische Überprüfung der europäischen Datenschutzregelungen sei erforderlich, weil die Konsumentinnen und Konsumenten bei Online-Aktivitäten wenig Vertrauen hätten, dass ihre Privatheit beachtet wird. Mangelndes Vertrauen bedeute weniger Onlinegeschäft, es bremse das Wachstum der europäischen Onlinewirtschaft.[7] Diese Aussagen zeigen, dass die Kommission Datenschutz vorrangig als Instrument zur Herstellung des digitalen Binnenmarktes versteht. Das auf den Datenschutz bezogene Ziel wird gerade nicht als die größtmögliche Verwirklichung dieses Grundrechtes beschrieben. Als Ziel wird vielmehr die Herstellung einer Situation definiert, in der die Grundrechtsträgerinnen und Grundrechtsträger **das subjektive Empfinden haben**, das Grundrecht werde geschützt, weil sie erst dann Konsumentscheidungen treffen, die der europäischen Onlinewirtschaft zugute kommen. Die Frage, ob diese subjektive Auffassung der Konsumentinnen und Konsumenten, ihr Vertrauen dahinein,

---

[3] Die italienische Stellungnahme in der Stellungnahme des Europäischen Rates vom 18.7.2012, 9897/2/12 REV 2, englische Version S. 69 ff, S. 70, nennt drei mögliche Varianten, zwischen denen sich die Kommission nicht entschieden habe: Der Verordnungsvorschlag könne eine Regelung sein, die sich vor allem auf den Datenschutz beziehe und dabei beiläufige Auswirkungen auf den Binnenmarkt habe. Sie könne eine Regelung sein, die sich auf den Binnenmarkt beziehe und als untergeordnete Überlegung gewisse Aspekte in Betracht ziehe, die mit dem Datenschutz zusammenhingen, oder sie könne sich schließlich ohne Unterschied auf den Schutz personenbezogener Daten in der EU und den Binnenmarkt beziehen. „(...) whether the proposal for a Regulation (...) is an act which relates above all to personal data protection and has incidental repercussions for the internal market; or whether it is an act relating to the internal market which, as an ancillary consideration, takes account of certain aspekts connected to data protection; or, finally, whether it relates without distiction to personal data protection in the EU and to the internal market.“

[4] Der Kommissionsvorschlag ist eines von 31 Gesetzesvorhaben der „digitalen Agenda.“

[5] Säule 1 der „digitalen Agenda“ der EU. Die 12. Aktion der Säule 1 lautet: Review the EU data protection rules. https://ec.europa.eu/digital-agenda/en/our-targets/pillar-i-digital-single-market

[6] „The Commission adopted a data protection Regulation to strengthen online privacy rights and boost Europe's digital economy.“ Säule 1 der “digitalen Agenda”, a.a.O. (Fn. 6).

[7] „Why is EU action needed? Lack of trust means less online business. This lack of clarity in online privacy rules triggers a lack of trust among consumers, which slows down the growth of Europe's online economy.“ Säule 1 der “digitalen Agenda”, a.a.O. (Fn. 6).

dass ihre Privatsphäre geschützt wird, richtig oder falsch ist, erscheint nach dieser Argumentation zweitrangig.

Es ist höchst zweifelhaft, ob die Betonung der dienenden Funktion des Datenschutzes als Mittel zur Verfolgung des Zieles eines digitalen Binnenmarktes auch noch nach der Verankerung des Rechtes auf Datenschutz in der Europäischen Grundrechtecharta den primärrechtlichen Wertungen der EU entspricht. Die Charta der Grundrechte der Europäischen Union gilt seit 2009, ist also erst nach Erlass der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EU-Datenschutz-Richtlinie) in Europa Bestandteil des europäischen Primärrechtes geworden. Sie formuliert die europäischen Grundrechte, die durch Verweis in den Vertrag über die Europäische Union und in den Vertrag über die Arbeitsweise der Europäischen Union einbezogen wurden. Die Europäische Grundrechtecharta gewährt nach ihrem Artikel 8 jeder Person das Recht auf den Schutz der sie betreffenden personenbezogenen Daten. Auch die unternehmerische Freiheit ist in der Grundrechtecharta genannt. Nach Artikel 16 „erkennt“ die Grundrechtecharta die unternehmerische Freiheit nach dem Unionsrecht und den einzelstaatlichen Rechtsvorschriften und Gepflogenheiten „an“. Dass diese schwächere Formulierung zur unternehmerischen Freiheit die Instrumentalisierung des Datenschutzgrundrechtes für Zwecke der unternehmerischen Freiheit zu rechtfertigen vermag, darf stark bezweifelt werden.

Für die Präferenz des Kommissionsvorschlages für das Schutzziel des freien Datenverkehres sprechen auch die im Folgenden angesprochenen Aspekte. Ihnen sollen jeweils Forderungen entgegengestellt werden, die eine grundsätzliche Gleichwertigkeit der beiden Ziele Datenschutz und freier Datenverkehr formulieren und es so ermöglichen, für jeden Sachverhalt, auf den die Verordnung Anwendung finden wird, eine spezifische Lösung zu finden, in der **beiden** Schutzzielen im Wege der praktischen Konkordanz[8] jeweils **zu einem höchstmöglichen Verwirklichungsgrad** verholfen werden kann.

1) Datenschutzrechtlich problematisch: Ausbau lediglich des Schutzzieles freier Datenverkehr

Auch die Zielformulierung des Kommissionsvorschlages weist auf die Präferenz für das Ziel der Erleichterung des freien Datenverkehres hin. In seinem Satz 5 beschreibt Erwägungsgrund 5 das Verhältnis der beiden Schutzziele. In Satz 5 heißt es: „Die Technik hat das wirtschaftliche und gesellschaftliche Leben verändert, weshalb der Datenverkehr innerhalb der Union sowie die Datenübermittlung an Drittländer und internationale Organisationen **noch weiter erleichtert** werden muss, wobei **gleichzeitig** ein **hohes Maß** an Datenschutz zu gewährleisten ist.“ Dabei wird deutlich, dass nach dem Kommissionsvorschlag das Ziel der Erleichterung des freien Datenverkehres im Vergleich zur gegenwärtigen Situation eine Steigerung erfahren soll, wohingegen das Ziel des Datenschutzes erreicht werden soll, ohne dass der Kommissionsvorschlag das Ziel verfolgt, die Situation für dieses Schutzgut im Vergleich zum gegenwärtigen Zustand zu

[8] Grundlegend zur praktischen Konkordanz als Mechanismus, kollidierende Rechtsgüter jeweils „zu optimaler Wirksamkeit gelangen zu lassen“, Konrad Hesse, Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, z.B. 14. Auflage, Heidelberg 1984, Rn. 317 ff.

verbessern. Der Verwirklichungsgrad für dieses Schutzziel soll nur möglichst hoch sein. Den freien Datenverkehr gilt es also auszubauen. Das Datenschutzziel soll (nur) so weit erreicht werden, wie es bei Erreichung des Ziels der Erleichterung des freien Datenverkehrs möglich ist. Damit genießt das Ziel der Erleichterung des freien Datenverkehrs nach dem Kommissionsvorschlag den Vorrang vor dem Ziel des Datenschutzes.

Aus Sicht des Schutzzieles Datenschutz reicht aber ein derart relativiertes „hohes Maß an Datenschutz“ nicht aus, weil es – ohne dass der Verordnungsvorschlag hiergegen Schutzmechanismen zur Verfügung stellte – sogar unter dem durch die Richtlinie 95/46 EU normierten Schutzniveau liegen könnte, falls die gesteigerte Erleichterung der Datenübermittlungen eben nur ein Maß an Datenschutz zuließe, das entsprechend niedriger läge. Datenschutzrechtlich gesehen muss es also darum gehen, angesichts der „neuen Herausforderungen“ ebenfalls einen Zugewinn für den Schutz der personenbezogenen Daten aller EU-Bürgerinnen und EU-Bürger zu erreichen oder zumindest das bisherige Schutzniveau zu halten.

In der Formulierung des Erwägungsgrundes 5 sollte daher wie an allen anderen Stellen des Verordnungsvorschlages die offene Präferenz für das Schutzziel des freien Datenverkehres durch eine Formulierung ersetzt werden, die die Gleichwertigkeit der Schutzziele ausdrückt. In Erwägungsgrund 5 müsste es heißen: **„(...) weshalb der Datenverkehr (...) noch weiter erleichtert werden muss**. **Gleichzeitig muss auch das Maß an Datenschutz erhöht werden.“**

2) Datenschutzrechtlich problematisch: Verbot von Datenschutzregelungen, die den freien Datenverkehr einschränken

Artikel 1 Absatz 1 des Kommissionsvorschlages lautet: „Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.“ Diese Formulierung suggeriert eine Gleichwertigkeit der beiden Schutzziele. In Absatz 2 heißt es: „Die Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.“ Der durch das „insbesondere“ ausgedrückte scheinbare Vorrang des Datenschutzes wird durch Absatz 3 aufgehoben, in dem es heißt: „Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt oder verboten werden.“ In Ihrer Überarbeitung vom 2. Juni 2012 hat die Kommission diesen dritten Absatz gestrichen. **An dieser bislang nur vorläufigen Streichung von Artikel 1 Absatz 3 sollte auf jeden Fall festgehalten werden**.

3) Datenschutzrechtlich problematisch: Postulat der Vollharmonisierung

Die Präferenz für das Schutzziel des freien Datenverkehres manifestiert sich am stärksten im Postulat der Vollharmonisierung. Die Kommission zielt nach ihrem Erwägungsgrund 8 auf die unionsweit kohärente und einheitliche Anwendung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten. Damit optiert sie dafür, dass in allen Mitgliedstaaten identische Regelungen gelten und in exakt identischer Weise durchgesetzt werden. Bei der Lektüre von Erwägungsgrund 8 entsteht der Eindruck, dass

diese beiden vom Kommissionsentwurf verfolgten Zielen gleichermaßen dient: „Um ein hohes Maß an Datenschutz für den Einzelnen zu gewährleisten und die Hemmnisse für den Verkehr personenbezogener Daten zu beseitigen, sollte der Schutz der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sein. Die Vorschriften zum Schutz der Grundrechte und Grundfreiheiten von natürlichen Personen bei der Verarbeitung personenbezogener Daten sollten unionsweit kohärent und einheitlich angewandt werden.“ Der Eindruck, dass der Kommissionsentwurf beiden Zielen gleichermaßen in den Blick nimmt, täuscht.

Dass die Vollharmonisierung der Erleichterung des freien Datenverkehres dient, ist einleuchtend: Wenn überall in der EU identische Regelungen gelten und durchgesetzt werden, können die Daten fließen. Eine Vollharmonisierung dient demgegenüber gerade nicht in jedem Fall dem Recht der natürlichen Personen auf Schutz ihrer personenbezogenen Daten. Für das Schutzziel Datenschutz hängt die Wirkung einer Vollharmonisierung vielmehr allein vom dadurch gewährten Datenschutzniveau ab. Vollharmonisierung bedeutet nur dann einen Vorteil, wenn die europaweit identischen Regelungen für den Datenschutz Verbesserungen bedeuten. Für das Schutzziel des Datenschutzes kann eine Vollharmonisierung sogar nachteilig sein. Das wäre dann der Fall, wenn die vollharmonisierten Regelungen den Datenschutz weniger gewährleisteten, als es zuvor der Fall war. Die Aussage in Erwägungsgrund 8, ein hohes Maß an Datenschutz für die Einzelnen sei gewährleistet, wenn der Schutz der Rechte und Freiheiten von Personen bei der Verarbeitung dieser Daten in allen Mitgliedstaaten gleichwertig sei, wenn also europaweit die gleichen Regelungen gelten, ist also vor allem dann falsch, wenn Schutzziel nicht nur ein irgendwie hohes (oder niedriges) Maß an Datenschutz, sondern ein höchstmögliches Maß an Datenschutz ist. Für den Grad der Verwirklichung des Rechtes auf Datenschutz ist also allein die Höhe des Schutzniveaus entscheidend. Ob dieses Niveau in allen Mitgliedstaaten exakt gleich hoch ist, ist für das Schutzziel Datenschutz dann unerheblich, wenn in allen Mitgliedstaaten ein höchstmögliches Datenschutzniveau zur Pflicht gemacht wird, das nur über-, aber nicht unterschritten werden darf.

Auch das Postulat der Vollharmonisierung steht damit für den Vorrang der Erleichterung des freien Datenverkehres vor dem Schutz der personenbezogenen Daten der EU-Bürgerinnen und EU-Bürger. Aus Sicht des Datenschutzes muss der Kommissionsvorschlag daher in die Richtung verändert werden, dass an die Stelle der Vollharmonisierung die Gewährleistung eines möglichst hohen Schutzniveaus für den Datenschutz tritt.

Im Verordnungsentwurf gibt es mehrere Regelungen, die dem Postulat der Vollharmonisierung zur Geltung verhelfen sollen. Daher sollen hier drei datenschutzrechtlich unhintergehbare Grundforderungen gestellt werden, die an die Stelle dieser die Vollharmonisierung begründenden Regelungen treten sollten, wenn die Verordnung ihren Namen „Datenschutzgrundverordnung“ zu Recht tragen soll. Der Anspruch auf Vollharmonisierung wird zum einen ausgedrückt durch die Wahl der Rechtsform Verordnung bei gleichzeitigem Verzicht auf Öffnungsklauseln für nationalstaatliches Recht, das den Datenschutz stärker gewährleistet, zweitens durch die Ermöglichung einer Vielzahl von delegierten Rechtsakten und drittens durch die Ermöglichung einer stark an europaweiter Einheitlichkeit orientierten Steuerung der Rechtsdurchsetzung durch die Kommission. Diesen drei Aspekten sollen hier drei Forderungen gegenübergestellt werden, die das Schutzziel des Datenschutzes bestärken, ohne das Schutzziel des

freien Datenverkehrs aus dem Auge zu verlieren. Daher werden hier **die Normierung von datenschutzrechtlichen Mindeststandards auch im nichtöffentlichen Bereich** (a) und die **Beschneidung der vorgesehenen Befugnisse der Kommission zur Rechtsetzung** (b) und **zur Rechtsdurchsetzung** (c) gefordert. Dass die Erfüllung dieser Forderungen gleichzeitig einem höheren Datenschutzniveau dienen und zu gleichen Verhältnissen in ganz Europa führen kann, soll das unter (d) genannte aktuelle Beispiel belegen.

a) stattdessen: Normierung von hohen datenschutzrechtlichen Mindeststandards auch im nichtöffentlichen Bereich

Durch die Wahl der Rechtsform Verordnung strebt die Kommission mit ihrem Vorschlag eine unmittelbare Geltung in allen Mitgliedstaaten an. Die Verordnung würde also alle in ihrem Geltungsbereich bestehenden mitgliedstaatlichen Normen verdrängen. Diese Folge bestünde sowohl für mitgliedstaatliche Regelungen, die zuvor einen geringeren Schutz für die personenbezogenen Daten gewährleisteten, als es die Verordnung vorsähe, was aus Datenschutzsicht natürlich sehr zu begrüßen ist. Die Verordnung würde aber auch mitgliedstaatliche Regelungen verdrängen, die einen höheren Schutz für diese Rechte gewährleisteten. Die letztgenannte Folge, nach der mit der aus datenschutzrechtlicher Sicht grundsätzlich begrüßten Modernisierung des Datenschutzrechtes auf europäischer Ebene auch datenschutzfreundlichere mitgliedstaatliche Regelungen verdrängt werden, wird von einigen Mitgliedstaaten[9] und von vielen Datenschützerinnen und Datenschützern vor allem für den öffentlichen Bereich abgelehnt. Stattdessen wird die Forderung erhoben, durch die Formulierung der vorgeschlagenen Regelungen als datenschutzrechtliche Mindeststandards in der Verordnung selbst den Weg für mitgliedstaatliche Normen frei zu machen, die einen höheren Datenschutzstandard zur Pflicht machen, als ihn die Verordnung festschreibt.[10] Begründet werden soll dies hier mit den Wertentscheidungen der EU-Grundrechtecharta (aa) und mit der Eigenschaft als Instrument zur Förderung von datenschutzrechtlichen Innovationen (bb). Zusätzlich soll verdeutlicht werden, warum es wichtig ist, die Normierung von datenschutzrechtlichen Mindeststandards auch für den nichtöffentlichen Bereich zu fordern (cc).

---

[9] Für die Mitgliedstaaten steht dabei allerdings eher das Argument der Unterschiedlichkeit des Verfassungs- und Verwaltungsrechtes der Mitgliedstaaten im Vordergrund. Als Begründung für die Ablehnung der Rechtsform Verordnung für die Regelung des Datenschutzes im öffentlichen Bereich in der Stellungnahme des Europäischen Rates vom 18.7.2012, a.a.O. (Fn. 4), heißt es z.B. aus Tschechien, der öffentliche Sektor der Mitgliedstaaten solle durch Richtlinie geregelt werden. Dies solle die Mitgliedstaaten befähigen, die Regeln in viele bereichsspezifische und prozedurale Gesetze zur Tätigkeit öffentlicher Stellen zu implementieren. (S. 12),„(...) public sector within the Member States should be regulated by directive. This would enable Member States to implement the rules into many sector-specific an procedural laws regulating the activity of public authorities.“ Die schwedische Stellungnahme weist auf den Bedarf hin, den Mitgliedstaaten eine gewisse Bewegungsspanne zu lassen. Dies sei im öffentlichen Sektor besonders wichtig, weil dort unterschiedliche Verfassungstraditionen und Verwaltungsstrukturen beachtet werden müssten. (S. 130), „(...) there is a need to leave a certain margin of manoeuvre for the Member States. This is especially important in the public sector, where different constitutional traditions and administrative structures must be taken into account.“ (S. 130)

[10] Siehe etwa die Entschließung der DSK, a.a.O. (Fn 2).

aa) Normierung von datenschutzrechtlichen Mindeststandards als Ausdruck der Wertentscheidung der EU-Grundrechtecharta

Die im Verordnungsvorschlag der Kommission enthaltene Entscheidung gegen Öffnungsklauseln für mitgliedstaatliches Recht, das einen strengeren Datenschutz gewährleistet, kollidiert mit Wertungsentscheidungen, die die EU im Primär- und im Sekundärrecht in anderen Bereichen getroffen hat, die ebenfalls Rechte der Grundrechtecharta betreffen.

Nach Artikel 38 der Grundrechtecharta stellt die Politik der EU ein hohes Verbraucherschutzniveau sicher. In Artikel 168 IV AEUV heißt es für den Bereich des Verbraucherschutzes: „Die nach Absatz 3 beschlossenen Maßnahmen hindern die Mitgliedstaaten nicht daran, strengere Schutzmaßnahmen beizubehalten oder zu ergreifen.“ Zu den in Artikel 37 der Grundrechtecharta normierten Zielen der Sicherstellung eines hohen Umweltschutzniveaus und der Verbesserung der Umweltqualität heißt es in Artikel 193 AEUV: „Die Schutzmaßnahmen, die aufgrund des Artikels 192 getroffen werden, hindern die einzelnen Mitgliedstaaten nicht daran, verstärkte Schutzmaßnahmen beizubehalten oder zu ergreifen.“ Selbst wenn man davon absieht, aus den Formulierungen der Rechte in der Grundrechtecharta eine Hierarchie herauszulesen, die möglicherweise dazu führen würde, dass das mit der Persönlichkeit zusammenhängende Recht auf Datenschutz auch wegen seiner unmittelbaren Nähe zur Menschenwürde und zur Achtung des Privatlebens nach der Wertung der Europäischen Grundrechtecharta stärker geschützt werden muss als die unternehmerische Freiheit, zeigt sich, dass primärrechtlich nichts dagegen spricht, auch das Schutzniveau für den Datenschutz durch einen Mindeststandard besonders hoch auszugestalten.

Für die Formulierung eines solchen Mindeststandards in der Datenschutzverordnung spricht auch der Umstand, dass die durch die Konstruktion des Verordnungsentwurfes jetzt getroffene Entscheidung die bislang auch im Bereich des Datenschutzes getroffene Entscheidung ins Gegenteil verkehrt, wonach auch das europäische Datenschutzniveau mit Mindeststandards gesichert wird. In der Richtlinie 95/46 aus dem Jahr 1995 heißt es in Erwägungsgrund 10: “Gegenstand der einzelstaatlichen Rechtsvorschriften über die Verarbeitung personenbezogener Daten ist die Gewährleistung der Achtung der Grundrechte und Grundfreiheiten, insbesondere des auch in Artikel 8 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten und in den allgemeinen Grundsätzen des Gemeinschaftsrechts anerkannten Rechts auf die Privatsphäre. Die Angleichung dieser Rechtsvorschriften darf deshalb nicht zu einer Verringerung des durch diese Rechtsvorschriften garantierten Schutzes führen, sondern muss im Gegenteil darauf abzielen, in der Gemeinschaft ein hohes Schutzniveau sicherzustellen.“ Gerade weil die Aufwertung des Schutzes personenbezogener Daten durch die Einbeziehung der EU-Grundrechtecharta in das Primärrecht erst danach erfolgte, bestand keine Veranlassung, dieses Votum der Richtlinie für ein Mindestdatenschutzniveau im Verordnungsvorschlag zurückzunehmen. Dieser Umstand hätte vielmehr dazu führen müssen, den Schutz der personenbezogenen Daten im Vergleich zur jetzt geltenden Richtlinie sogar noch auszubauen. Daher spricht alles dafür, dass die Normierung als Mindeststandard durch die EU-Grundrechtecharta sogar gefordert wird.

Angesichts des hohen Schutzgutes des Datenschutzes, der durch die Grundrechtecharta verbürgt ist und insofern den Verbraucherschutzrechten in nichts nachsteht, ist

also auch für den Bereich des Datenschutzes die Formulierung von Mindeststandards zu fordern. Anstelle des Absatzes 3 des Artikel 1, der im Kommissionsentwurf vom 2. Juni 2012 gestrichen wurde,[11] könnte dementsprechend folgende Formulierung aufgenommen werden: „**Die Regelungen dieser Verordnung hindern die Mitgliedstaaten nicht daran, strengere Schutzmaßnahmen für den Datenschutz beizubehalten oder zu ergreifen.**“ Andere Regelungsorte für eine solche Regelung könnten Artikel 6 oder Artikel 21 sein.

bb) Normierung von datenschutzrechtlichen Mindeststandards als Instrument zur Förderung von Innovationen

Die Forderung nach Mindeststandards ist ein föderales Argument, das – nebenbei bemerkt – einer Bremerin natürlich sehr sympathisch ist. Im Föderalismus zeigt sich, dass viele unterschiedliche Einheiten viele unterschiedliche Problemlösungen finden. Eine Rechtsfortbildung zur Stärkung des Datenschutzniveaus würde also erleichtert, wenn in der Verordnung Mindeststandards formuliert würden, über die alle hinausgehen, die aber niemand unterbieten dürfte. So heißt es auch im Antrag von BÜNDNIS 90/DIE GRÜNEN: „Mit einem entsprechenden Mehrebenenansatz und deren kluger Verschränkung, bei der auch Spielräume für nationale Besonderheiten sowie Verbesserungen und Innovationen erhalten bleiben, kann ein breites und zukunftsfähiges Fundament für den Datenschutz geschaffen werden.“

cc) Normierung von datenschutzrechtlichen Mindeststandards gerade auch im nichtöffentlichen Bereich

Die Forderung danach, in der vorgeschlagenen Verordnung Mindeststandards zu formulieren und damit mitgliedstaatliche Regelungen mit einem darüber hinausgehenden Datenschutzniveau zu ermöglichen, wird hier für die Bereiche des öffentlichen und des nichtöffentlichen Datenschutzes erhoben. Viele Beiträge in der europäischen Diskussion um den Kommissionsvorschlag kritisieren die dort vorgeschlagenen Regelungen für den Datenschutz im **öffentlichen** Bereich, also im Verhältnis von Mitgliedstaaten zu Bürgerinnen und Bürgern. Sehr häufig wird sogar der Geltungsanspruch des Verordnungsvorschlages für den öffentlichen Bereich selbst kritisiert.[12] Aus datenschutzrechtlicher Sicht kann dieser Kritik mit der Normierung der vorgeschlagenen Regelungsinhalte als datenschutzrechtliche Mindeststandards begegnet werden.[13] Dies würde ein einheitliches europäisches Mindestdatenschutzniveau im öffentlichen Bereich begründen, über das die Mitgliedstaaten mit Normierungen, die ihrer Verwaltungsstruktur entsprechen, hinausgehen könnten. Aus datenschutzrechtlicher Sicht wäre eine **ersatzlose Herausnahme des öffentlichen Bereiches aus dem Regelungsgegenstand der Verordnung** demgegenüber **abzulehnen**, weil auch im

[11] Dazu s.o. I 2.
[12] Siehe etwa die Stellungnahmen in Fn. 10.
[13] Siehe die Entschließung der DSK (Fn. 2). Auch die Nr. 7 des Antrages der Fraktion BÜNDNIS 90/DIE GRÜNEN fordert dies, wenn es dort für den Bereich des öffentlichen Verwaltung heißt: „Die Verordnung sollte insoweit die Möglichkeit eröffnen, durch einzelstaatliches Recht weitergehende Regelungen zu treffen, die entsprechend der jeweiligen Rechtstradition die Grundrechte der Bürgerinnen und Bürger absichern.“

öffentlichen Bereich ein im Verhältnis zur EU-Datenschutzrichtlinie 95/46/EG deutlich modernisiertes Regelungsinstrumentarium erforderlich ist, das der Verordnungsvorschlag im Vergleich zur Richtlinie enthält.

Bei der intensiv für den öffentlichen Bereich geführten Debatte scheint der **nichtöffentliche Bereich** etwas aus dem Blick zu geraten. Dabei entfaltet das Schutzziel der Erleichterung des freien Datenverkehres wegen seines starken Bezuges auf den wirtschaftlichen Binnenmarkt gerade im nichtöffentlichen Bereich starke Auswirkungen. Dieser Umstand führt dazu, dass sich die Präferenz des Kommissionsvorschlages für das Schutzziel des freien Datenverkehres am stärksten im Bereich des Datenschutzes im nichtöffentlichen Bereich auswirkt. Daher muss dem Kommissionsvotum gegen eine Öffnung der Verordnung für Regelungen mit höherem Datenschutzniveau die Forderung entgegengehalten werden, dass in der Verordnung datenschutzrechtliche Mindeststandards normiert werden, über die die Mitgliedstaaten hinausgehen können. Dem Gegenargument, eine solche Regelung behindere den freien Datenverkehr, kann durch den Hinweis auf die genannten Öffnungsklauseln für den Verbraucherschutz und den Umweltschutz begegnet werden. Die Wirtschaft erscheint im Bereich des Datenschutzes nicht schutzwürdiger als im Bereich des Umwelt- und Verbraucherschutzes. Zudem gibt es einen großen Überschneidungsbereich zwischen datenschutzrechtlichen und verbraucherschutzrechtlichen Regelungen.

In Artikel 1 Absatz 3, Artikel 6 oder Artikel 21 sollte also die sowohl für den öffentlichen als auch für den nichtöffentlichen Bereich geltende Formulierung aufgenommen werden: „**Die Regelungen dieser Verordnung hindern die Mitgliedstaaten nicht daran, strengere Schutzmaßnahmen für den Datenschutz beizubehalten oder zu ergreifen.**“ Die an vielen Stellen im Kommissionsentwurf[14] normierte Einschränkung „**in den Grenzen dieser Verordnung**“ ist jeweils zu **streichen**.

b) Stattdessen: Beschneidung der vorgesehenen Befugnisse der Kommission zur Rechtsetzung

Ein weiteres Instrument zur Durchsetzung der Vollharmonisierung sind die an vielen Stellen des Kommissionsvorschlages vorgesehenen Ermächtigungen zum Erlass von delegierten Rechtsakten, also von Normen, die die Kommission nach Artikel 290 des AEUV ermächtigen, eigene Rechtsakte zu erlassen. Im Kommissionsvorschlag findet sich eine überwältigende Vielzahl von Ermächtigungen zum Erlass von delegierten Rechtsakten. Angesichts der oben beschriebenen Präferenz der Kommission für das Schutzziel des freien Datenverkehres vor dem Schutzziel des Datenschutzes sollte darauf **verzichtet werden, der Kommission diese umfassende Möglichkeit zur Setzung von bindendem Recht für alle Mitgliedstaaten zu geben**.

Stattdessen sollten diese Regelungen **in der Verordnung selbst oder in anderen europäischen Rechtsakten mit Gesetzescharakter**, also in Verordnungen oder Richtlinien geregelt werden. Sofern diese Forderung nicht durchsetzbar ist, sollte gleichwohl auf Ermächtigungen für delegierte Rechtsakte verzichtet werden. Dies hätte zur Folge, dass – sofern der hier erhobenen Forderung nach dem Verständnis der Verordnung als Normierung von Mindeststandards gefolgt wird – an ihre Stelle Normen träten, die durch

[14] Beispielsweise in Artikel 81 (Bereichsausnahme für Gesundheitsdaten) und Artikel 82 (Bereichsausnahme für den Beschäftigtendatenschutz)

mitgliedstaatliche Parlamente verabschiedet würden, die ihrerseits an die durch die Verordnung statuierten Mindeststandards gebunden wären. Sofern der Forderung nach Mindeststandards nicht gefolgt würde, träte an die Stelle der delegierten Rechtsakte die Auslegung der Verordnung durch die datenschutzrechtlichen Kontrollbehörden und Rechtsprechung, die aufgrund dieser Entscheidungen ergangen ist.

Für entgegen dieser Forderung verbleibende Ermächtigungen zu delegierten Rechtsakten muss ein weiterer Punkt beachtet werden: Bei den in Artikel 86 des Kommissionsvorschlages genannten Ermächtigungen zu delegierten Rechtsakten sind zwei unterschiedliche Arten zu unterscheiden. Bei einem ersten Teil können Europäisches Parlament oder Rat die Ermächtigung zum Erlass der delegierten Rechtsakte widerrufen. Dies gilt für die in Artikel 86 Absatz 3 des Kommissionsvorschlages genannten Regelungsgegenstände. Bei einem zweiten Teil ist Wirksamkeitsvoraussetzung der delegierten Rechtsakte, dass weder Europäisches Parlament noch Rat Einwände gegen den delegierten Rechtsakt erheben. Dies gilt für die in Absatz 5 genannten Regelungsgegenstände. Angesichts der oben beschriebenen Neigung der Kommission, den freien Datenverkehr vor dem Datenschutz zu privilegieren, muss aus Datenschutzsicht gefordert werden, dass die Beteiligung des Europäischen Parlamentes so stark wie möglich ist. Daher **sollten die nach einer sehr kritischen Prüfung verbleibenden Ermächtigungen der Kommission zu delegierten Rechtsakten auf jeden Fall daran gebunden werden, dass Europäisches Parlament oder Rat keine Einwände erhoben haben. Die Ermächtigungen sollten also im jetzigen Absatz 5 des Artikels 86 des Kommissionsvorschlages normiert werden**.

c) Stattdessen: Beschneidung der vorgesehenen Befugnisse der Kommission zur Rechts**durchsetzung** und Verpflichtung der unabhängigen Aufsichtsbehörden allein auf den Schutz des Datenschutzgrundrechtes der natürlichen Personen

Auch die im Kommissionsvorschlag vorgesehenen Regelungen über die Aufsichtsbehörden, also zum Vollzug und zur Rechtsdurchsetzung, sind Regelungen, die dem Ziel der Vollharmonisierung dienen. Der im Kommissionsvorschlag vorgeschlagenen Konstruktion, wonach die Kommission die unabhängigen Aufsichtsbehörden steuern kann und diese auch auf den Schutz des freien Warenverkehres verpflichtet werden, sollen hier die Forderungen nach Verzicht auf Regelungen, nach denen die Kommission Rechte der Rechtsdurchsetzung erlangt aa) und nach alleiniger Verpflichtung der unabhängigen Aufsichtsbehörden auf den Datenschutz bb) gegenübergestellt werden. Daneben wird auf die Änderungsvorschläge der Konferenz der Datenschutzbeauftragten des Bundes und der Länder verwiesen.[15]

aa) Verzicht auf Steuerung der unabhängigen Aufsichtsbehörden durch die Kommission

Nach dem Kommissionsvorschlag erhält die Kommission vielfältige Kompetenzen im Verhältnis zum unabhängigen Datenschutzausschuss sowie in Bezug auf das Kohärenzverfahren, mit dem die europaweite Einheitlichkeit der aufsichtsbehördlichen

[15] Siehe die Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, etwa https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/EU-Datenschutz_DSK/EU-Datenschutzreform__Datenschutzkonferenz_nimmt_Stellung_zu_den_Entw__rfen.php, S. 24 ff

Einzelentscheidungen hergestellt werden soll, die ohne das Verständnis der in der Verordnung normierten Regelungen als Mindeststandards allein dem freien Datenverkehr zugute käme.

So hat der unabhängige Datenschutzausschuss nach Artikel 58 umfassende Informationspflichten gegenüber der Kommission. Auch kann die Kommission nach Artikel 60 Maßnahmen der unabhängigen Aufsichtsbehörden bis zu 12 Wochen aussetzen, beispielsweise um in der Zwischenzeit gemäß Artikel 62 einen Durchführungsrechtsakt in der Form eines „Beschlusses über die ordnungsgemäße Anwendung der Verordnung“ zu erlassen. Hierbei ist besonders beachtlich, dass – sofern die Maßnahme der unabhängigen Aufsichtsbehörde der Verhinderung eines Datenschutzverstoßes dient – in der Zwischenzeit schwerwiegende Verletzungen des Rechtes auf Schutz der personenbezogenen Daten geschehen können. Auch der Erlass von „sofort geltenden Durchführungsrechtsakten“ in „hinreichend begründeten Fällen äußerster Dringlichkeit“ nach Artikel 62 Absatz 2 des Kommissionsvorschlages stellt einen tiefen Eingriff in die Unabhängigkeit der Aufsichtsbehörden dar.

Dieser starken Rolle der Kommission quasi als Kontrollbehörde über die unabhängigen Aufsichtsbehörden steht die Auffassung des EuGH zur Unabhängigkeit der datenschutzrechtlichen Kontrollstellen entgegen. Nach dem EuGH dürfen die Kontrollstellen bei der Wahrnehmung ihrer Aufgaben keinerlei Weisungen unterliegen.[16] Sie müssen „vor jeglicher Einflussnahme von außen einschließlich der unmittelbaren oder mittelbaren Einflussnahme des Bundes oder der Länder sicher sein.“[17] Hiervon muss auch die Freiheit von Einflussnahmen der Kommission umfasst sein.

Aber selbst dann, wenn sich die Kommission selbst als unabhängige oberste Aufsichtsbehörde sähe, die ihre starke Rolle gegenüber den unabhängigen Aufsichtsbehörden der eigenen Unabhängigkeit und der Eigenschaft als „Hüterin der Verträge“ verdankt, würde dies in krassem Widerspruch zur Auffassung des EuGH stehen. In seinem Urteil vom 9. März 2010 zeigt der EuGH durch die Wahl der Szenarien für mögliche Beeinträchtigungen der Unabhängigkeit der datenschutzrechtlichen Kontrollstellen, dass auch er strukturell eher den Datenschutz als den freien Datenverkehr als das schutzbedürftigere Schutzgut ansieht. So bildet er Beispiele dafür, dass mitgliedstaatliche Regierungen möglicherweise ein Interesse an der Nichteinhaltung der Datenschutzvorschriften hätten, weil sie – etwa im Fall einer Kooperation von öffentlichen und privaten Stellen oder im Rahmen öffentlicher Aufträge an private Stellen – selbst involvierte Partei dieser Bearbeitung sein könnten oder ein besonderes Interesse am Zugang zu Datenbanken haben könnten. An dieser Stelle der Urteilsbegründung heißt es weiter: „Im Übrigen könnte diese Regierung auch geneigt sein, wirtschaftlichen Interessen den Vorrang zu geben, wenn es um die Anwendung der genannten Vorschriften durch bestimmte Unternehmen geht, die für das Land oder die Region wirtschaftlich von Bedeutung sind.“[18] Warum die Kommission glaubt, diese strukturellen Bedrohungen der Unabhängigkeit gälten nicht für sie selbst, ist schwer erklärlich. Dies gilt insbesondere nach der Lektüre der folgenden Urteilspassage, in der der EuGH begründet, warum „bereits die bloße Gefahr einer politischen Einflussnahme der Aufsichtsbehörden auf die Entscheidungen der Kontrollstellen ausreicht, um deren unabhängige Wahrnehmung

[16] EuGH, Urteil vom 9.3.2010, Rs. C-518/07, Rn. 28.
[17] EuGH, a.a.O. (Fn. 17) Rn. 25.
[18] EuGH, a.a.O. (Fn. 17) Rn. 35.

ihrer Aufgaben zu beeinträchtigen.“ Es könne nämlich – wie die Kommission selbst vorgetragen hat – einen „vorauseilenden Gehorsam“ der Kontrollstellen geben. Auch fordere ihre Rolle als „Hüter des Rechts auf Privatsphäre, dass ihre Entscheidungen, also sie selbst, über jeglichen Verdacht der Parteilichkeit erhaben“ ist.[19] All diese Argumente sprechen dagegen, der Kommission als derjenigen Institution der EU, die vor allem eine exekutive Funktion hat, relevante Befugnisse gegenüber den unabhängigen Aufsichtsbehörden zu geben.

Danach ist zu fordern, **Artikel 60 (Aussetzung einer geplanten Maßnahme) und Artikel 62 (Durchführungsrechtsakte) zu streichen**. Daneben sollten die **Informationspflichten an die Kommission** in den Artikeln 58, 61 und 64 ff **gestrichen** werden.

bb) Verpflichtung der unabhängigen Aufsichtsbehörden allein auf den Datenschutz

Nach der jetzt geltenden Datenschutz-Richtlinie 95/46 kommt den „unabhängigen Kontrollstellen“ die Aufgabe der Überwachung der Anwendung der von den Mitgliedstaaten zur Umsetzung der Richtlinie erlassenen Vorschriften zu. Dabei stehen die Schutzziele freier Datenverkehr und Datenschutz nach der Richtlinie in einem Verhältnis, das zugleich der Binnenmarktlogik und dem Schutz der Privatsphäre verpflichtet ist: Weil Datenschutz Kosten verursacht, wurde die Wirtschaft in Ländern mit einem höheren Datenschutzniveau vor Erlass der Richtlinie im Verhältnis zur Wirtschaft in Ländern mit einem niedrigeren Datenschutzniveau benachteiligt. Daher musste das Datenschutzniveau in Ländern mit einem niedrigeren Datenschutzniveau angehoben werden. Dabei wird dem Postulat gefolgt, wonach die Angleichung der Rechtsvorschriften in den Mitgliedstaaten nicht zu einer Verringerung des Schutzes für das Recht auf die Privatsphäre führen darf.[20] Genau dieser Logik sind die unabhängigen Kontrollstellen nach Artikel 28 Absatz 1 verpflichtet. Bei der Anwendung der angeglichenen Rechtsvorschriften zur Erleichterung des Binnenmarktes stehen sie dafür, dass keine Absenkung des Schutzniveaus für den Datenschutz erfolgt, sondern „im Gegenteil (...) in der Gemeinschaft ein hohes Schutzniveau“[21] sichergestellt ist. Insofern ist die Einrichtung unabhängiger Kontrollstellen „ein wesentliches Element des Schutzes der Personen bei der Verarbeitung personenbezogener Daten“.[22] Auch der EuGH spricht von der „Rolle der Kontrollstellen als Hüter des Rechts auf Privatsphäre.“[23] Nur mit der Ausrichtung darauf, dass bei der Erleichterung des Binnenmarktes keine Absenkung des Datenschutzniveaus erfolgt, sind die Datenschutzbehörden also nach der Datenschutz-Richtlinie 95/46 auch dem Schutz der Freiheit des Datenverkehres verpflichtet.

Nach dem Verordnungsvorschlag der Kommission sollen die Aufgaben der unabhängigen Datenschutzbehörden nunmehr auf ein anderes Ziel ausgerichtet sein: Sie sollen einen Beitrag zur einheitlichen Anwendung der scheinbar den beiden Schutzzielen Datenschutz und freier Datenverkehr gleichermaßen verpflichteten, in Wirklichkeit aber den freien Datenverkehr privilegierenden Verordnung leisten, „damit die

---

[19] EuGH, a.a.O. (Fn. 17) Rn 36.
[20] Erwägungsgrund 10.
[21] Erwägungsgrund 10.
[22] Erwägungsgrund 62, der den freien Datenverkehr nicht erwähnt.
[23] EuGH, a.a.O. (Fn. 17) Rn 36.

Grundrechte und Grundfreiheiten natürlicher Personen bei der Verarbeitung ihrer Daten geschützt und der freie Datenverkehr in der Union erleichtert werden."[24]

Angesichts der zwischenzeitlichen Verankerung des Rechtes auf Datenschutz in der Grundrechtecharta hätte es nahe gelegen, ganz darauf zu verzichten, die unabhängigen „Datenschutzbehörden" explizit auch auf das Schutzziel des freien Datenverkehres zu verpflichten. Dies scheint angesichts der Privilegierung des freien Datenverkehres durch den Kommissionsvorschlag geboten. Insofern sollten in Artikel 46 Absatz 1 Satz 1 **die Worte „und der freie Datenverkehr in der Union erleichtert" gestrichen werden.**

d) Beispiel für einen datenschutzrechtlichen Erfolg mehrerer europäischer Datenschutzeinrichtungen auf der Grundlage der heutigen Rechtslage, der bei einem höheren Mindeststandard sicherlich noch schneller erzielt worden wäre

Dass das Zusammenwirken europäischer Datenschutzeinrichtungen schon auf der Grundlage der heutigen Richtlinie sehr erfolgreich sein kann, zeigt der Fall der Rücknahme der rechtswidrigen Gesichtserkennung durch facebook. Von allen bis Juli 2012 registrierten Nutzerinnen und Nutzern hatte facebook biometrische Gesichtsmodelle erstellt, ohne dass die Nutzerinnen und Nutzer genaue Informationen über das Verfahren der Gesichtserkennung bekommen oder eingewilligt hätten. Am 21. September 2012 erklärte facebook, dieses Verfahren nicht mehr weiterzuverfolgen und die entstandene Datenbank mit den biometrischen Daten der europäischen Nutzerinnen und Nutzer zu löschen.

Seit längerer Zeit hatten es europäische Datenschutzinstitutionen mit unterschiedlichsten Methoden versucht, facebook zum Verzicht auf diese rechtswidrige Anwendung zu bringen. Die Artikel-29-Datenschutzgruppe hatte im März 2012 ein „Workingpaper" zur Gesichtserkennung veröffentlicht.[25] Die deutsche Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte in ihrer Entschließung „Datenschutz bei sozialen Netzwerken jetzt verwirklichen!"[26] klargestellt, dass sich die Anbieter von sozialen Netzwerken, die auf den europäischen Markt zielen, auch dann an europäische Datenschutzstandards halten müssen, wenn sie ihren Sitz außerhalb Europas haben. Ein österreichischer Student hatte im August 2011 mehrere Beschwerden über facebook beim irischen Datenschutzbeauftragten eingereicht. Der irische Datenschutzbeauftragte hatte im Auditverfahren gefordert, ausreichende Informationen über das Verfahren für Nutzerinnen und Nutzer bereitzustellen sowie die Datenverwertungsrichtlinien anzupassen.[27] Deutsche Datenschutzbehörden hatten das einem Anordnungsverfahren voraus gehende Anhörungsverfahren begonnen beziehungsweise angekündigt. Die Anordnung des Hamburgischen Datenschutzbeauftragten, die unter anderem auf die Verpflichtung zur Löschung aller biometrischen

[24] Artikel 46 Absatz 1 des Kommissionsvorschlages.
[25] Siehe http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf.
[26] Siehe Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Datenschutz bei sozialen Netzwerken jetzt verwirklichen!" vom 28./29.9.2011, www.datenschutz.bremen.de/konferenzbeschluesse2.php?konfid=150.
[27] http://dataprotection.ie/viewdoc.asp?DocID=1232&m=f

Muster und Informationen, die ohne Einwilligung der betroffenen Nutzerinnen und Nutzer erfasst wurden, gerichtet war, wurde am 21. September 2012 erlassen.

Welche dieser Aktivitäten für die Entscheidung von facebook mit kausal war, lässt sich nicht feststellen. Jedenfalls spricht Vieles dafür, dass es für das Erreichte sehr günstig war, dass sich die Initiativen zur Durchsetzung des Datenschutzes unterschiedlicher Instrumente bedienten und aus unterschiedlichen europäischen Ländern kamen.

Der geschilderte Fall der Durchsetzung einer datenschutzrechtlichen Forderung belegt beispielhaft, dass auf ein hohes Datenschutzniveau gerichtete Forderungen zur Ausdehnung dieses Datenschutzniveaus auf ganz Europa führten. Der Grund hierfür wird sein, dass es für global agierende Unternehmen nicht wirtschaftlich ist, in der EU national unterschiedliche Anwendungen zu programmieren. Ein höheres europäisches Mindestdatenschutzniveau hätte diesen datenschutzrechtlichen Erfolg mit Sicherheit beschleunigt. Vielleicht wäre der datenschutzwidrige Zustand sogar gar nicht erst eingetreten.

II. Erhöhung des durch den Kommissionsvorschlag erreichbaren Datenschutzniveaus

Nicht nur an den strukturellen, sondern auch an den materiellen Teilen des Kommissionsvorschlages ist die Bevorzugung des Schutzzieles des freien Datenverkehrs vor dem Schutzziel des Datenschutzes ablesbar. Daher sollen hier Forderungen erhoben werden, die das durch den Kommissionsvorschlag erreichbare Datenschutzniveau erhöhen würden.

1) Verzicht auf Angemessenheitsbeschluss nach Artikel 41, jedenfalls Bindung an schärfere Voraussetzungen

Auf das Instrument des „Angemessenheitsbeschlusses“ in Artikel 41 des Kommissionsvorschlages, der Länder als datenschutzrechtlich unbedenklich erklärt, sollte verzichtet werden. Auch er bewirkt einen Vorrang des freien Datenverkehres vor dem Datenschutz, weil Folge dieses Beschlusses ist, dass Datenübermittlungen in Drittländer ohne weitere Voraussetzung vorgenommen werden dürfen, selbst wenn diese im Einzelfall das Recht auf Datenschutz beschränken.

Beispielsweise die gegenwärtigen datenschutzrechtlichen Debatten der nationalen Datenschutzbehörden mit Unternehmen mit Sitz in den USA zeigen, dass die Forderung nach der Beachtung angemessener datenschutzrechtlicher Standards durch US-amerikanische Unternehmen konterkariert würde, wenn die Kommission die USA in dieser Weise pauschal frei zeichnen würde. Gefordert wird hier deshalb die **Streichung des Artikels 41. Hilfsweise sollte die Entscheidung der Kommission an strengere Voraussetzungen gebunden werden**, als dies nach dem Kommissionsvorschlag der Fall ist. Es reicht nicht, dass nach Absatz 2 die Rechtsstaatlichkeit, „die Existenz wirksamer und durchsetzbarer Rechte einschließlich wirksamer administrativer und gerichtlicher Rechtsbehelfe für betroffene Personen insbesondere für in der Union ansässige betroffene Personen, deren personenbezogene Daten übermittelt werden“ und andere Kriterien lediglich „bei der Prüfung der Angemessenheit des gebotenen Schutzes“ von der Kommission „berücksichtigt“ werden. Stattdessen müsste es in Absatz 2 zumindest heißen: **„Voraussetzung für eine Feststellung nach Absatz 1 ist, dass die**

folgenden Voraussetzungen erfüllt sind: (a) (...).“Auf die Änderungsforderungen zu den Artikeln 41 fortfolgende in der Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder[28] wird zusätzlich verwiesen.

2) Aufnahme der für IT-Sicherheit und technischen und organisatorischen Datenschutz erforderlichen Regelungen in den Verordnungstext

Es ist ebenfalls Ausdruck des Vorranges des Schutzzieles freier Datenverkehr vor dem Schutzziel Datenschutz, dass die für die IT-Sicherheit und den technik- und organisationsbezogenen Datenschutz erforderlichen Regelungen nicht im Verordnungsvorschlag enthalten sind, sondern dem Erlass direkter Rechtsakte vorbehalten bleiben. Das ist deshalb problematisch, weil die überwiegende Vielzahl datenschutzrechtlicher Probleme gar nicht erst entstehen würde, wenn datenschutzgerechtere technische und organisatorische Maßnahmen ergriffen würden. Da IT-Produkte gegenwärtig in der Regel so erstellt werden, dass viele, für den beabsichtigen Zweck nicht erforderliche Daten entstehen, erscheint das Ergreifen von technischen und organisatorischen Maßnahmen, die auf diese nicht erforderlichen Datenmengen reagieren, als kostenintensiv. Diese Situation sollte schon im Vorhinein verhindert werden. Insbesondere sollten folgende Formulierungen in den Verordnungstext übernommen werden:

- Die Bedeutung des technischen und organisatorischen Datenschutzes sollte durch die Aufnahme als Grundsatz der Verarbeitung personenbezogener Daten betont werden. In **Artikel 5** des Kommissionsvorschlages sollte daher als neuer Buchstabe aufgenommen werden: Personenbezogene Daten müssen „**unter Beachtung der erforderlichen technischen und organisatorischen Maßnahmen zum Datenschutz verarbeitet werden**.“

- Die Erforderlichkeit von technischen und organisatorischen Maßnahmen zum Datenschutz sollte allein an der Tiefe des Eingriffs in das Datenschutzrecht und nicht an der Höhe der Implementierungskosten gemessen werden. In Artikel 23 Absatz 1 und Artikel 30 Absatz 1 des Kommissionsvorschlages sind deshalb die Worte: „**und der Implementierungskosten“** zu **streichen**.

- Die elementaren Datenschutzziele sollten als grundsätzliche Anforderungen normiert werden. Artikel 30 Absatz 1 sollte daher folgender Satz angefügt werden: „**Verfügbarkeit, Integrität, Vertraulichkeit, Transparenz, Nichtverkettbarkeit und Intervenierbarkeit sind Zielvorgaben aller technischen und organisatorischen Maßnahmen**.“

- Es sollte klargestellt werden, dass Datenschutz durch Technik auch die Auswahl und Gestaltung von Datenverarbeitungssystemen betrifft. Artikel 5 sollte daher in folgender Weise ergänzt werden: „**Bei der Auswahl und Gestaltung von Geräten und Datenverarbeitungssystemen durch den für die Verarbeitung Verantwortlichen sind die Grundsätze der Datensparsamkeit und des Datenschutzes zu gewährleisten.**“

- Den Verantwortlichen sollten Risikoanalysen, -bewertungen und Sicherheitskonzepte zur Pflicht gemacht werden. Artikel 30 sollte daher in folgender Weise ergänzt werden: „**Die für die Verarbeitung Verantwortlichen müssen vor der Verarbeitung personenbezogener Daten Risikoanalysen, Risikobewertungen und Sicherheits-**

[28] A.a.O. (Fn. 16), S. 22 ff.

konzepte erstellen. Das Sicherheitskonzept ist Teil der Verfahrensdokumentation nach Artikel 28 Absatz 2.“

- Grundsätzlich sollten die Verantwortlichen zur weitestmöglichen Anonymisierung und Pseudonymisierung verpflichtet werden. Dafür müssten zunächst in Artikel 4 des Verordnungsvorschlages Definitionen der Begriffe Anonymisierung und Pseudonymisierung eingefügt werden (etwa die Definition in den Absätzen 6 und 6a des § 3 Bundesdatenschutzgesetz). In der Regelung in Buchstabe e) des Artikels 5 muss an die Stelle der Passage „in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht“ folgende Passage treten: "**Personenbezogene Daten müssen weitestgehend anonymisiert und pseudonymisiert werden.**“ In Artikel 23 Absatz 2 ist nach Satz 2 folgender Satz einzufügen: „**Deshalb sind personenbezogene Daten möglichst zu anonymisieren oder zu pseudonymisieren. Dies muss nach dem Stand der Technik erfolgen.**“

- Es sollte eine Verpflichtung normiert werden, Verschlüsselungen nach dem Stand der Technik vorzunehmen. Dafür müsste zunächst in Artikel 4 des Verordnungsvorschlages eine Definition des Begriffes Verschlüsselung eingefügt werden. In Artikel 30 ist ein weiterer Grundsatz anzufügen: „**Sofern Daten zu verschlüsseln sind, müssen die für die Verarbeitung Verantwortlichen Verschlüsselungen nach dem Stand der Technik vornehmen.“** Entsprechend sollte in Artikel 32 Absatz 3 folgender Satz 3 angefügt werden: „**Die Verschlüsselung muss nach dem Stand der Technik erfolgen**.“

- Für das Internet sollte ein Recht auf Nutzung von Pseudonymen statuiert werden. In Artikel 5 sollte ein weiterer Grundsatz eingefügt werden, der lautet: „**Nutzerinnen und Nutzer des Internets haben das Recht, Pseudonyme zu verwenden**.“

- Es sollten die Verpflichtungen normiert werden, Geräte und Programme datensparsam und datenschutzgerecht herzustellen (privacy by design) und Grundeinstellungen von Geräten und Programmen datensparsam und datenschutzgerecht vorzunehmen (privacy by default). Daher sollte ein neuer Artikel eingefügt werden, der folgenden Grundsatz enthält: „**Hersteller sind verpflichtet, Geräte und Datenverarbeitungssysteme datensparsam und datenschutzgerecht herzustellen und Grundeinstellungen datensparsam und datenschutzgerecht vorzunehmen.**“

- Es sollte ausdrücklich klargestellt werden, dass die Regelungen der Verordnung auch für das Tracking im Internet gelten. In Artikel 23 sollte daher folgender neuer Absatz eingefügt werden: „**Diese Regelungen gelten auch für Verhaltensbeobachtungen im Internet (Tracking)**.“

- Die grundsätzlich begrüßenswerte Entscheidung der Kommission für technikneutrale Regelungen hat dazu geführt, dass auf die spezifischen Probleme schon jetzt eingesetzter Techniken wie **Videoüberwachung** und **Chipkarten** nicht reagiert werden kann. So fehlt etwa das Postulat des antragsunabhängigen Hinweises auf die Datenverarbeitung. So sollte beispielsweise in Artikel 14 des Kommissionsvorschlages, der die **Information der betroffenen Person** regelt, festgeschrieben werden, dass diese Information antragsunabhängig zu erfolgen hat. In Absatz 1 Satz 1 sollten daher nach den Worten „zumindest Folgendes mit“ die Worte, „**ohne dass es hierfür eines Antrages bedürfte**“ eingefügt werden.

Auf die übrigen Änderungsforderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu den Regelungen über technische und organisatorische Maßnahmen[29] wird hiermit verwiesen.

3) Nur mit Datenschutzbelangen abgewogene Privilegierung von kleinsten, kleinen und mittleren Unternehmen

Ein weiterer Ausdruck des Vorranges für das Schutzziel des freien Datenverkehrs vor dem Schutzziel des Datenschutzes sind die im Verordnungsvorschlag vorgesehenen Regelungen zur Privilegierung von kleinsten, kleinen und mittleren Unternehmen, die eine Abwägung des Zieles der Schaffung von Erleichterungen für kleinste, kleine und mittlere Unternehmen mit dem Ziel des Datenschutzes vermissen lassen. So ist nicht auf die Größe des datenschutzrechtlich verantwortlichen Unternehmens abzustellen, sondern auf die Tiefe des Eingriffes in das Datenschutzrecht.

Der in Artikel 8 Absatz 3 vorgesehene Satz 2, wonach bei den Regelungen zur **Verarbeitung personenbezogener Daten eines Kindes** „spezifische Maßnahmen für Kleinst- und Kleinunternehmen sowie mittlere Unternehmen“ geregelt werden können, ist zu **streichen**. Für den Grad der Betroffenheit des Datenschutzrechtes von Kindern spielt es keine Rolle, ob ihre personenbezogenen Daten durch Kleinst-, Kleinunternehmen, mittlere Unternehmen oder größere Unternehmen verarbeitet werden. Es kommt vielmehr auf die Tiefe des Eingriffes an.

Dasselbe gilt für Artikel 12 Absatz 6 (**Verfahren und Vorkehrungen, damit die betroffene Person ihre Rechte ausüben kann**), Artikel 14 Absatz 7 (**Information der betroffenen Personen**) und Artikel 22 Absatz 4 (**Pflichten des für die Verarbeitung Verantwortlichen**). Die vorgesehenen Ausnahmen für die Datenverarbeitung durch Kleinst-, Kleinunternehmen und mittlere Unternehmen sind jeweils zu **streichen**, weil die Ausnahmen nicht auf die Tiefe des Eingriffs für die Betroffenen abstellen.

So ist es auch nicht einleuchtend, warum bei den Regelungen zur **Verpflichtung zur Benennung eines betrieblichen Datenschutzbeauftragen** in Artikel 35 Absatz 1 Buchstabe b) und zur **Verpflichtung für Datenverarbeiter mit Sitz außerhalb der EU zur Bestellung eines Vertreters** in Artikel 25 Absatz 2 Buchstabe b) des Kommissionsentwurfes darauf abgestellt wird, dass das betreffende Unternehmen mehr als 250 Mitarbeiterinnen und Mitarbeiter beschäftigt, ohne darauf zu achten, ob von diesen Beschäftigten risikobehaftete Datenverarbeitungen vorgenommen werden oder nicht. Bei der Bestellungspflicht in Artikel 35 hilft die Variante in Buchstabe c) nicht, weil es sich bei den Datenverarbeitungen, die ein Risiko für personenbezogene Daten bergen, nicht in jedem Fall um „Kerntätigkeiten“ des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters handelt. Daher sollte Artikel 35 Absatz 1 Buchstabe c) folgendermaßen gefasst werden: „**Datenverarbeitungen vorgenommen werden, die Risiken für personenbezogene Daten bergen**.“ Auf die weiteren Änderungsforderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu den Regelungen über interne Datenschutzbeauftragte[30] wird hiermit verwiesen. Artikel 25 Absatz 2 Buchstabe b) sollte **gestrichen** werden.

---

[29] Siehe Stellungnahme, a.a.O. (Fn. 16), S. 15f, 18 f

[30] Siehe Stellungnahme, a.a.O. (Fn. 16), S. 19 ff.

4) Änderungserfordernisse bei den Regelungen zu Einwilligungen

Bei der Beschreibung der Wirksamkeitsvoraussetzungen für Einwilligungen in Artikel 7 des Kommissionsentwurfes fehlt die Informiertheit der Entscheidung. Dies ist auch nach der selbstgesetzten Logik des Kommissionsvorschlages unbedingt zu korrigieren, weil die Transparenz der Datenverarbeitung eine wesentliche Voraussetzung für das Vertrauen der Betroffenen ist.[31] Sie müssen nicht nur genau wissen, was die Zwecke der Datenverarbeitung sind, sondern auch, welche Daten genau erhoben werden, woher sie gegebenenfalls stammen, was genau mit ihnen geschehen wird, wer der für die Datenverarbeitung Verantwortliche ist und wann die Daten gelöscht werden. Weiterhin ist klarzustellen, dass sich Einwilligungen nicht auf technisch-organisatorische Maßnahmen erstrecken. Daher ist folgender Absatz an Artikel 7 anzuhängen: „**Die betroffene Person ist genau darüber zu informieren, welche Daten erhoben und welche Datenverarbeitungen geschehen werden. Die Einwilligung kann sich nicht auf technisch-organisatorische Maßnahmen beziehen**."

In Artikel 19 Absatz 2 sollte – wie dies im Vorentwurf des Kommissionsvorschlages der Fall war – auch für das Direktmarketing eine Einwilligung zur Pflicht gemacht werden. Absatz 2 sollte daher lauten „**Mit Einwilligung der betroffenen Person kann Direktwerbung betrieben werden**."[32]

5) Verantwortlichkeit auch für Inhalte

In der Definition des für die Verarbeitung Verantwortlichen in Artikel 4 Absatz 5 des Kommissionsentwurfes heißt es, es handele sich um Stellen, die allein oder gemeinsam mit anderen „über die Zwecke, Bedingungen und Mittel der Verarbeitung von personenbezogenen Daten" entschieden. Hierbei **fehlt die Verantwortlichkeit für Inhalte**, obwohl der Personenbezug von Daten ja entscheidend durch deren Inhalt geprägt ist und der Berichtigungsanspruch nach Artikel 16 des Verordnungsentwurfes gegenüber dem Verantwortlichen besteht. In Artikel 4 Absatz 5 sollte nach dem Wort „Zwecke" also das Wort „**Inhalte**" **eingefügt** werden.

6) opt-in auch bei Profilbildung

Wie bei der allgemeinen Regelung in Artikel 6 Absatz 1 Buchstabe a) des Kommissionsvorschlages sollte auch bei der Profilbildung eine Einwilligung gefordert werden. Artikel 20 Absatz 2 Buchstabe a) des Kommissionsentwurfes ist daher zu **streichen**. Ergänzend wird auf die Vorschläge der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Thema Profilbildung hingewiesen.[33]

---

[31] Siehe zur Anforderung an die Transparenz auch die Eckpunkte der Konferenz der Datenschutzbeauftragten des Bundes und der Länder für „Ein modernes Datenschutzrecht für das 21. Jahrhundert," a.a.O., (Fn. 1), S. 12 ff, 21 f.

[32] Im Übrigen sei auf die Anforderungen an Einwilligungen in den Eckpunkten der Konferenz der Datenschutzbeauftragten des Bundes und der Länder für „Ein modernes Datenschutzrecht für das 21. Jahrhundert," a.a.O., (Fn. 1), S. 22 f verwiesen.

[33] Siehe Stellungnahme der DSK, a.a.O. (Fn. 16), S. 13 f, und Eckpunkte der Konferenz der Datenschutzbeauftragten des Bundes und der Länder für „Ein modernes Datenschutzrecht für das 21. Jahrhundert," a.a.O., (Fn. 1), S. 11 f

7) Verweis auf die Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Ausdrücklich soll hier auf die ausführliche Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Kommissionsvorschlag für eine Datenschutzverordnung verwiesen werden.[34]

[34] Stellungnahme der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, a.a.O. (Fn. 16).