Stellungnahme

LANDTAG
NORDRHEIN-WESTFALEN
16. WAHLPERIODE

STELLUNGNAHME
16/535

Alle Abg

Zum Vorschlag der EU-Kommission für eine EU-Datenschutz-Grundverordnung vom 25.01.2012
18. Mai 2012

Der BITKOM vertritt mehr als 1.700 Unternehmen, davon über 1.100 Direktmitglieder mit 135 Milliarden Euro Umsatz und 700.000 Beschäftigten. Nahezu alle Global Player sowie 800 Mittelständler und zahlreiche gründergeführte Unternehmen werden durch BITKOM repräsentiert. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Susanne Dehmel
Bereichsleiterin
Datenschutz
Tel.: +49.30.27576-223
Fax: +49.30.27576-51-223
s.dehmel@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Einleitung

BITKOM begrüßt nachdrücklich die Initiative der EU Kommission zur Modernisierung und Harmonisierung des Europäischen Datenschutzrechts. Insbesondere die weitere Harmonisierung des Rechtsrahmens sowie ein Ansatz zur Schaffung einer einheitlichen Rechtsdurchsetzung ohne eine Erweiterung bürokratischer Strukturen sind für ein innovationsfreundliches Klima in Europa dringend notwendig. Der deutsche ITK-Markt soll in diesem Jahr erstmals die 150-Milliarden-Euro-Marke überschreiten[1]. Über alle Wirtschaftssektoren in Deutschland hinweg nutzen 40 Prozent aller Produktinnovatoren ITK, um neue Marktangebote hervorzubringen[2]. Um die Weiterentwicklung dieser „Querschnittstechnologie" und damit die Innovationskraft der Gesamtwirtschaft zu unterstützen bedarf es moderner, praxisgerechter Datenschutzregelungen.

Der am 25.01.2012 vorgelegte Entwurf enthält zahlreiche Verbesserungsansätze gegenüber der geltenden Gesetzeslage, berücksichtigt jedoch noch nicht konsequent genug die unterschiedlichen Regelungsbereiche, um zukünftig ein jeweils angemessenes Datenschutzniveau zu gewährleisten.

Dabei ist neben den nachfolgend angesprochenen Themen auch der grundsätzliche Ansatz des Verbotsprinzips mit Erlaubnisvorbehalt zu überdenken. In der jetzigen Ausgestaltung führt dieses Prinzip zur Behinderung legitimer Datenverarbeitung und nicht zum eigentlichen Ziel der Vermeidung des Missbrauchs. Dagegen sollte die Datenverarbeitung im Rahmen einer „Datenverkehrsordnung" grundsätzlich erlaubt und durch „Leitplanken" eingegrenzt werden.[3]

Darüber hinaus würde es sich der BITKOM wünschen, dass sich der Verordnungsentwurf mehr auf die Ziele eines modernen und effektiven Datenschutzes in der Informationsgesellschaft fokussiert und weniger Vorgaben im Detail macht. Wir regen daher an, den Verordnungsentwurf mit Blick auf die nachfolgend erläuterten Aspekte und anhand des Prinzips der Verantwortlichkeit[4] weiterzuentwickeln, um einen effektiven und zukunftsfähigen europäischen Datenschutzrahmen zu schaffen.

---

[1] http://www.bitkom.org/de/markt_statistik/64090_70702.aspx
[2] Studie des ZEW zum IT-Gipfel 2010 http://www.it-gipfel.de/Dateien/BBA/PDF/it-gipfel-2010-informations-telekommunikationstechnologien,property=pdf,bereich=itgipfel,sprache=de,rwb=true.pdf
[3] Siehe hierzu schon die Vorschläge des Deutschen Juristentages von 1998
[4] OECD Leitsätze für multinationale Unternehmen http://www.oecd.org/dataoecd/38/35/48808708.pdf

Die wichtigsten Aspekte für die ITK-Branche im Überblick:

1 Differenzierte Anwendung des Datenschutzrechts
Es sollte darauf verzichtet werden, den Personenbezug so zu definieren, dass das Datenschutzrecht künftig auf jede denkbare Information anzuwenden wäre. Vielmehr sollte von einem relativen Begriff des Personenbezugs ausgegangen werden und die Anwendbarkeit des Datenschutzrechts von vornherein auf die wirklich relevanten Datenverarbeitungsvorgänge begrenzt werden. Außerdem sollten mehr Anreize für die Pseudonymisierung und Anonymisierung von zu verarbeitenden personenbezogenen Daten gesetzt werden, indem noch deutlicher herausgestellt wird, dass anonymisierte Daten keine personenbezogenen Daten sind und indem für die Verarbeitung pseudonymisierter Daten gezielt erleichterte Bedingungen geschaffen werden, wie dies teilweise im deutschen Datenschutzrecht schon heute der Fall ist (Bsp. § 5 (3)).

2 Rechtsgrundlage der Datenverarbeitung
Erforderliche Datenverarbeitung im wirtschaftlichen Umfeld muss unkompliziert – d.h. auf der Basis von Interessenabwägung (auch zugunsten von Dritten) – möglich sein. Die momentan vorgesehenen Erlaubnistatbestände sind zu eng und unflexibel für die erforderlichen Datenverarbeitungsvorgänge heute und in Zukunft. Der Persönlichkeitsschutz des Betroffenen ist auch im Rahmen einer allgemeinen Interessenabwägung realisierbar.

3 Zukunftsfähige Einwilligung
Die Fälle, in denen es einer Einwilligung anstelle einer gesetzlichen Erlaubnis bedarf, sollten nicht ausgeweitet werden. Ferner fehlt noch eine praxisgerechte Definition der Einwilligung. Ziel sollte es sein, dass die Anforderungen an die Einwilligung nicht zu formalistisch sind. Insbesondere müssen die Anforderungen an die Einwilligung technische Gegebenheiten und das tatsächliche Risiko für den Betroffenen berücksichtigen. Es sollte mit Blick auf zukünftige Produkte bei ausreichender Transparenz auch möglich sein, eine Einwilligung implizit zu erteilen, nicht spezifisch ausdrücklich oder schriftlich.

4 Regelung für gesellschaftsübergreifende Datenübermittlung
In Bezug auf die Übermittlung personenbezogener Daten hat der aktuelle Entwurf der Verordnung viele Punkte aufgenommen, um die grenzübergreifende Nutzung und Verarbeitung von Daten flexibler zu gestalten, und gleichzeitig mehr Rechtssicherheit für international agierende Unternehmen zu schaffen. Allerdings fehlt nach wie vor eine klare Regelung zur gesellschaftsübergreifenden Weitergabe von Daten, obwohl diese von allen am Konsultationsprozess beteiligten Gruppen gefordert wurde.

5 Differenzierte Regelung zur Profilbildung
Die Änderung des Wortlautes des bisherigen Artikels 15 der Datenschutz-Richtlinie 95/46 im Verordnungsentwurf wirft die Frage auf, welche bisher zulässigen Profilbildungen weiterhin zulässig sind. Aus unternehmerischer Sicht sollte Profilbildung möglich sein, wenn es ein berechtigtes Interesse des Verantwortlichen gibt und im Rahmen einer Interessenabwägung kein überwiegendes Interesse auf der Seite des Betroffenen festgestellt werden kann bzw. wenn keine belastende Entscheidung für ihn zu befürchten ist.

6 Zuständigkeit der Aufsichtsbehörden und Kohärenzverfahren
Die Einführung eines One-Stop-Shop-Prinzip für die Zuständigkeit der Aufsichtsbehörden (Art. 51) wird ebenso begrüßt wie im Grundsatz das Kohärenzverfahren für die Aufsichtsbehörden. Die jetzige Ausgestaltung der Regelungen dazu erscheint jedoch noch nicht geeignet, um das Ziel eines echten One-Stop-Shops sowie eine konsistente Rechtsdurchsetzung zu erreichen.

7 Selbstverpflichtung und Zertifizierung
Die Verordnung sollte die Themen Selbstverpflichtung und Zertifizierung noch stärker verankern und einen praxisgerechten Rechtsrahmen dafür schaffen. Ein wichtiger Anwendungsfall ist die Auftragsdatenverarbeitung. Hier sind Auftraggeber verpflichtet Kontrollen durchzuführen. Für die Anbieter großer (Cloud-) Dienstleistungen ist es daher von besonderer Bedeutung, diese zertifizieren zu können, um so zahlreiche Einzelkontrollen zu vermeiden.

8 Auftragsdatenverarbeitung
Klare Regelungen zur Auftragsdatenverarbeitung - insbesondere zur Aufteilung der Zuständigkeiten und Verantwortlichkeit - sind essentiell für die Weiterentwicklung von Cloud Computing und die Wertschöpfung der gesamten europäischen Wirtschaft. Von der Praxistauglichkeit dieser Vorgaben hängt es ab, ob neue Geschäftsmodelle durch den Rechtsrahmen eher gefördert oder behindert werden. Die vorgeschlagenen Vorschriften zur Auftragsverarbeitung passen strukturell nicht auf einige Formen des Cloud Computings und würden diese daher erschweren. Um Praxistauglichkeit zu erreichen, sollten die vorgeschlagenen Regelungen noch sorgfältig überarbeitet und klargestellt werden, dass die Auftragsverarbeitung grundsätzlich zulässig ist.

9 „Recht auf Vergessen“
Der Verordnungsentwurf gibt jeder Person das Recht zu verlangen, „vergessen zu werden“. Ziel dieses Rechts ist es, den Betroffenen zu ermöglichen, insbesondere auch mit Blick auf das Internet, die einmal geschaffene Verfügbarkeit oder Verwendungsmöglichkeit ihrer Daten wieder aufzuheben. Die Datenverarbeitung wird ausschließlich in die Dispositionsbefugnis des Betroffenen gestellt. Aus Sicht der Branche ist dieser – sehr internetbezogene – Ansatz zwar nachvollziehbar, wirft aber die Frage auf, inwieweit dieser Ansatz auf Datenverarbeitungsvorgänge der „old Economy“ passt. Dort sind Fälle denkbar, in denen – nach entsprechender Interessenabwägung – eine Datenverarbeitung auch gegen den Willen des Betroffenen zulässig sein kann und muss.

10 Delegierte Rechtsakte / Sanktionsrahmen / Bürokratie
Die große Anzahl der im Verordnungsentwurf vorgesehenen delegierten Rechtsakte führt zu erheblicher Rechtsunsicherheit und sollte daher reduziert werden. Zusätzlich sollten die strengeren Sanktionen vor dem Hintergrund geprüft werden, dass der Großteil der Unternehmen Datenverarbeitung als notwendiges Instrument zur Durchführung seiner Geschäfte betreiben muss und nur wenige das Sammeln und Verwerten von Daten als Geschäftszweck betreiben. Daher stehen existenzgefährdende Sanktionen nicht in Relation zur Schwere von fahrlässigen Verstößen. Zudem sind viele Vorgaben zu unbestimmt, um daran scharfe Sanktionen zu knüpfen, und es besteht ein Missverhältnis zur Sanktionierung im öffentlichen Bereich. Außerdem enthält der Verordnungsentwurf zu viele Dokumentationspflichten und unnötig aufwändige Verfahren, die Kosten verursachen und nicht zu einem besseren Datenschutz führen.

Nachfolgend werden die aufgeführten wichtigsten Aspekte für die ITK-Branche sowie weitere problematische Vorgaben im Einzelnen erläutert.

Inhalt

1 Differenzierte Anwendung des Datenschutzrechts & Anreiz für Datensparsamkeit 5

2 Rechtsgrundlage der Datenverarbeitung 6

3 Zukunftsfähige Einwilligung 8

4 Regelung für gesellschaftsübergreifende Datenübermittlung 10

5 Differenzierte Regelung zur Profilbildung 11

6 Zuständigkeit der Aufsichtsbehörden und Kohärenzverfahren 11

7 Selbstverpflichtung und Zertifizierung 13

8 Auftragsdatenverarbeitung 13

9 „Recht auf Vergessen“ 16

10 Delegierte Rechtsakte / Sanktionsrahmen / Bürokratie 17

10.1 Rechtsunsicherheit durch „delegierte Rechtsakte“ 17
10.2 Sanktionsrahmen 18
10.3 Bürokratie 19

11 Modell des betrieblichen Datenschutzbeauftragten 22

12 Recht auf Datenübertragbarkeit („Data Portability“) 23

13 Kinder und Jugendliche Art. 4 (18) und Art. 8 24

1 Differenzierte Anwendung des Datenschutzrechts & Anreiz für Datensparsamkeit

Es sollte darauf verzichtet werden, den Personenbezug so zu definieren, dass das Datenschutzrecht auf jede denkbare Information anwendbar ist. Vielmehr sollte weiter von einem relativen Begriff des Personenbezugs ausgegangen werden und die Anwendbarkeit des Datenschutzrechts von vornherein auf die wirklich relevanten Datenverarbeitungsvorgänge begrenzt werden. Außerdem sollten mehr Anreize für die Pseudonymisierung und Anonymisierung von zu verarbeitenden personenbezogenen Daten gesetzt werden, indem klargestellt wird, dass anonymisierte Daten keine personenbezogenen Daten sind und indem für die Verarbeitung pseudonymisierter Daten erleichterte Bedingungen gelten.

- Nach der Definition in Art. 4 wäre das Datenschutzrecht praktisch auf jedes Datum anwendbar. Es stellt sich dabei die Frage, wo dann noch Raum für Anonymisierung und Pseudonymisierung sein soll, obwohl die Anonymisierung in Erwägungsgrund 23 ausdrücklich genannt wird. Es erscheint vor dem Hintergrund des weit definierten Personenbezugs kaum vorstellbar, dass ein Datum nicht als personenbeziehbar durch Dritte behandelt werden kann. Die verantwortliche Stelle muss im Grunde – unabhängig von ihren eigenen Fähigkeiten – den Personenbezug stets unterstellen (s. auch Art. 5e). Die hohen Anforderungen, die an den Umgang mit personenbezogenen Daten gestellt werden, würden dann für die Verarbeitung aller Daten gelten und zu einer Reihe von Folgeproblemen führen. Anstelle auf „jedwede natürliche Person“ sollte daher auf die verantwortliche Stelle abgestellt werden.

- Weiter weisen reine Produktionsnummern (z.B. IMEI Nummern) keinen Personenbezug auf und sind von der Regelung auszunehmen, solche Produktions- und Herstellernummern werden für das Management von Produktionsprozessen benötigt.

- Es fehlt ferner eine Definition von Standortdaten, obwohl dieser Begriff in den Vorschlägen gebraucht wird. Dies ist insb. deshalb problematisch, weil die Richtlinie 2002/58/EC eine Definition kennt.

- IP-Adressen sind ein Beispiel dafür, welche Probleme bei einer Ausweitung des Personenbezugs entstehen können. Zum einen gibt es bereits verschiedene Gerichtsurteile, die sich gegenseitig bezüglich der Aussage, ob IP-Adressen persönliche Daten sind, widersprechen. Im Verordnungsvorschlag dagegen ergibt sich ein Widerspruch zwischen den Definitionen in Art. 4 (1) und (2) und Erwägungsgrund 24, welcher feststellt, dass Online-Kennungen wie IP-Adressen nicht zwangsläufig als personenbezogene Daten zu betrachten sind. In Art. 4 werden sie dennoch als ein Beispiel für personenbezogene Daten genannt. Das liegt in der Natur der IP Adresse selbst, mit der ein Webseiten-Betreiber in der Regel nicht auf eine individuelle Person schließen kann, während das für einen Zugangs-Provider in der Regel möglich ist. Meist können mit IP-Adressen persönliche Daten nur indirekt identifiziert werden. Sie sollten deshalb durchaus geschützt werden. Sie ermöglichen es aber einem Webseiten-Betreiber nicht unmittelbar, auf eine Person rückzuschließen, da auch mehrere Personen eine IP-Adresse benutzen können. Einer Person alle Datenschutzrechte nur aufgrund einer IP-

Adresse einzuräumen, kann daher die Privatsphäre von anderen Personen verletzen.

- Die derzeitige Weite des Anwendungsbereichs nimmt Unternehmen auch die Chance, dort wo es möglich ist, auf die Verarbeitung personenbezogener Daten zu verzichten. So ist es denkbar, dass sich für das Unternehmen wichtige Erkenntnisse auch durch die Verarbeitung anonymer Daten gewinnen lassen. Mit gruppenbezogenen Auswertungen, denen eine bestimmte Mindestanzahl von Mitarbeitern zugrunde liegen, lässt sich beispielsweise eine Abteilungsperformance ermitteln, ohne mitarbeiterbezogene Auswertungen tätigen zu müssen. Auch im Bereich der Sicherstellung von Unternehmens-Compliance lassen sich Verhaltensauffälligkeiten zunächst auch durch anonymisierte Daten feststellen. Durch die jetzige Textfassung werden die Anreize zu solcher statistischen – nicht personenbezogener -Datenverarbeitung geradezu unterdrückt.

In einem ersten Schritt bedarf es deshalb einer Präzisierung und Eingrenzung des Begriffs der personenbezogenen Daten in Abgrenzung zu anonymen bzw. anonymisierten Daten. Der jetzt verfolgte Ansatz der „absoluten Theorie" des Personenbezugs muss zurückgeführt werden auf den Ansatz der „relativen Theorie", welcher die konkreten Instrumente und faktischen Zugriffsmöglichkeiten des verantwortlichen Verarbeiters oder mit ihm verbundener Institutionen bzgl. der Möglichkeit der Bestimmung der betroffenen Person berücksichtigt. In diesem Zusammenhang können auch technische Maßnahmen der Selbstbeschränkung im Sinne einer gezielten „Anonymisierung" einbezogen werden. Andernfalls vergibt die Verordnung die Chance, konkrete Anreize für Anonymisierung zu setzen.

Darüber hinaus muss dringend angedacht werden, auch innerhalb der Schwelle des Personenbezugs weitere Differenzierungen zu ermöglichen und gezielt ökonomische Anreize zur Selbstbeschränkung, etwa im Wege der Pseudonymisierung, zu setzen. Das deutsche Datenschutzrecht kann hier partiell als Vorbild dienen. Es enthält entsprechende Ansätze bereits heute und sie spielen eine bedeutende Rolle in der Praxis. Verzichtet man stattdessen, wie der aktuelle Verordnungsentwurf, auf solche weiteren Abstufungen, besteht für Anbieter faktisch der Anreiz für ein "fishing for consent" im Sinne einer möglichst weitgreifenden und umfassenden Einholung von Einwilligungen. Nur dieses Verfahren würde aus Sicht des Verarbeiters die notwendige Rechtssicherheit erzeugen, die gerade vor dem Hintergrund der geplanten weitreichenden Sanktionen notwendig ist. Der Datenschutzrahmen vergäbe hiermit die Möglichkeit einer selbstbeschränkenden Datensparsamkeit der Anbieter, da ein rein einwilligungszentriertes System ein Verhalten belohnt, bei dem der Anbieter möglichst für alle denkbaren Zwecke Einwilligungen einholt.

2 Rechtsgrundlage der Datenverarbeitung

Erforderliche Datenverarbeitung im wirtschaftlichen Umfeld muss unkompliziert – d.h. auf der Basis von Interessenabwägung - möglich sein. Die momentan vorgesehenen Erlaubnistatbestände sind zu eng und unflexibel für die erforderlichen Datenverarbeitungsvorgänge heute und in Zukunft.

Schon heute sind im bloßen Büro- und Geschäftsalltag alle Unternehmen auf funktionierende Datenverarbeitungssysteme angewiesen, die von der Personalverwaltung über die Bürokommunikation bis hin zur Logistikkette reichen. Praktisch kein Unternehmen kommt ohne irgendeine Form von Marketingaktivitäten aus. Jedes Unternehmen nutzt Email und Internet. Dabei werden zwangsläufig auch personenbezogene Daten verarbeitet. Zukünftig, und wenn es darum geht, die Europäische Informationsgesellschaft weiter erfolgreich voranzubringen, wird in vielen Bereichen wie z.B. dem Energiesektor oder dem Gesundheitswesen die Verarbeitung sehr großer (auch personenbezogener) Datenmengen notwendig, um Ressourcenprobleme zu lösen. So ist die Stromversorgung mit erneuerbaren Energiequellen nicht denkbar, ohne die Erhebung und Verarbeitung einer Vielzahl von Verbrauchs- und Erzeugungsdaten. Auch im Gesundheitswesen wird die Übertragung von mehr Gesundheitsdaten notwendig werden, um eine gute und effiziente Gesundheitsversorgung sicherzustellen. Ferner wird der Gebrauch von Verkehrsdaten, „remote learning informations" oder auch sensorischen Informationen stark zunehmen und eine Voraussetzung dafür bilden, dass sich im Interesse der Gesellschaft mehr Geschäftsmodelle am Markt durchsetzen. Die Weiterentwicklung von Verfahren zur Verarbeitung von Daten ist Voraussetzung für Innovation und damit ein Schlüssel für wirtschaftliches Wachstum in Europa.

Der Tatsache, dass das Funktionieren von Wirtschaft und Gesellschaft auch von der Verarbeitung personenbezogener Daten abhängt, muss ein zukunftsgerichteter Regelungsentwurf Rechnung tragen. Dabei kann man schon daran zweifeln, ob es noch zeitgemäß ist, die Verarbeitung personenbezogener Daten grundsätzlich zu verbieten. Aber unabhängig davon, ob man von einer grundsätzlichen Zulässigkeit der Verarbeitung personenbezogener Daten ausgeht oder von einer grundsätzlichen Unzulässigkeit, muss der gesetzliche Rahmen so ausgestaltet werden, dass er nur dort Hürden für die Datenverarbeitung aufstellt, wo berechtigte Interessen der Betroffenen entgegenstehen. Ohne die Zulässigkeit der Datenverarbeitung auf Basis einer Interessenabwägung werden sich in Zukunft viele Fälle nicht lösen lassen. Dies gilt schon deshalb, weil es Lebenssituationen gibt, in denen sich mangels persönlichen Kontakts mit dem Betroffenen eine vorherige Einwilligung nicht immer einholen lässt, wie dies beispielsweise im Rahmen von Werbemaßnahmen oder der Datenverarbeitung im Interesse Dritter (Auskunfteien) typischerweise der Fall ist. Eine Einwilligung lässt sich nur in bestimmten Fallkategorien vorweg nehmen. Im Rahmen einer Interessenabwägung sollte es möglich sein, dass Unternehmen selbst Maßnahmen zum Schutz des Betroffenen ergreifen (z.B. Pseudonymisierung), was dann zulässigkeitsbegründend zu berücksichtigen wäre. Der Vielzahl und Vielfältigkeit von Fallkonstellationen, die in der Praxis auftreten können, kann jedoch nur im Wege von flexiblen Erlaubnistatbeständen, die auch eine Interessensabwägung vorsehen, Rechnung getragen werden. Andernfalls würde eine Regulierung erwünschte Innovation verhindern.

Im vorgelegten Verordnungsentwurf verursachen vor allem folgende Punkte in der Praxis Probleme:

- **Art. 5 a)**[5] Da nicht klar wird, wie die geforderte „Nachvollziehbarkeit" der Verarbeitung für den Betroffenen umgesetzt werden soll, entsteht durch diese Vorgabe erhebliche Rechtsunsicherheit.

- **Art. 5 b)** und **c)** formulieren den Grundsatz einer strengen Zweckbindung. Gleichwohl kann es Situationen geben, in denen eine spätere zweckändernde Verarbeitung und Nutzung sachgerecht ist und keine gegenstehenden Interessen des Betroffenen dagegen sprechen. Der Zweck sollte zum einen so weit definiert werden können, dass eine Weiterentwicklung von Produkten und Verfahren im Rahmen der ursprünglichen Verwendung möglich bleibt. Außerdem sollte eine Zweckänderung möglich sein, wenn ein berechtigtes Interesse dazu besteht und kein entsprechendes Interesse des Betroffenen dagegen steht. Art. 6 (4) sieht bei den Voraussetzungen für eine mögliche Zweckänderung bislang nur die Fälle Art. 6 (1) a) bis e) vor, nicht aber das berechtigte Interesse des Verantwortlichen (Art. 6 (1) f)). Das sollte entsprechend der auch im deutschen Bundesdatenschutzgesetz geltenden Regelung ergänzt werden.

- In **Art. 6 (1) f)** ist die Zulässigkeitsvariante entfallen, wonach die Datenverarbeitung und Nutzung wegen berechtigter Interessen Dritter zulässig sein kann. Damit ist die Rechtsgrundlage, insbesondere für die sogenannten geschäftsmäßigen Daten verarbeitenden Stellen wie z.B. die in der Verbraucherkreditrichtlinie vorausgesetzten Auskunfteien – ohne erkennbaren Grund - entfallen. Sie werden in aller Regel nicht im eigenen Interesse, sondern im Interesse Dritter tätig.

- Der als allgemeine Öffnungsklausel für mitgliedsstaatliche gesetzliche Legitimationsklauseln konzipierte Artikel 21 des Entwurfs ist in seiner Zweckbeschränkung zu eng auf rein öffentliche Schutzzwecke beschränkt. Er bleibt auf diese Weise letztlich hinter der bestehenden Systematik des deutschen Datenschutzrechts zurück und sollte dringend um Zweckbestimmungen, auch für den nichtöffentlichen Bereich, ergänzt werden – auch um die allg. Klausel der Artikel 6 b) und f) auf diese Weise mittelbar zu konkretisieren.

3 Zukunftsfähige Einwilligung

Die Fälle, in denen es einer Einwilligung anstelle einer gesetzlichen Erlaubnis bedarf, sollten nicht ausgeweitet werden. Ferner fehlt noch eine praxisgerechte Definition der Einwilligung. Es sollte mit Blick auf zukünftige Produkte bei ausreichender Transparenz möglich sein, eine Einwilligung implizit zu erteilen, nicht nur spezifisch ausdrücklich oder schriftlich. Ziel sollte es sein, dass die Anforderungen an die Einwilligung nicht zu formalistisch sind. Insbesondere müssen die Anforderungen an die Einwilligung technische Gegebenheiten und das tatsächliche Risiko für den Betroffenen berücksichtigen.

Es sollte auch im Blick behalten werden, dass es Dienste gibt (insbesondere soziale Netzwerke), deren Zweck es gerade ist, dass die Nutzer dort Informationen austauschen und teilen. Die Zustimmung zur Datenverarbeitung sollte mit der Registrierung für den Dienst gegeben sein. Der Dienstleister sollte darüber

[5] Nicht näher bezeichnete Artikel sind solche des Vorschlags für eine Datenschutz-Grundverordnung der EU-Kommission vom 25.01.2012

hinaus umfassende Informationen darüber zur Verfügung stellen, wie der Dienst funktioniert und wie die Informationen verwendet werden.

- Ausdrücklichkeit der Einwilligung (Art. 4 Abs. 8):
  Der Verordnungsentwurf fordert anders als die geltende Datenschutz-Richtlinie bei der Einwilligung als Rechtsgrundlage stets die Ausdrücklichkeit unabhängig vom Kontext. Die Voraussetzungen für die Einholung der Einwilligung sind zu starr vorgeschrieben und berücksichtigen nicht, in welchem Zusammenhang die Einwilligung eingeholt wird oder welche Risiken bestehen. Das bedeutet, es wird schwieriger, eine gültige Einwilligung zu bekommen, ohne die Nutzererfahrung zu beeinträchtigen (Notwendigkeit einer Check box, pop up, log-in, Registrierung). Stattdessen sollte ein flexibleres Konzept für die Einwilligung, abhängig vom Inhalt und den Risiken der Datenverarbeitung, eingeführt werden. Nutzer werden ausreichend durch das Erfordernis geschützt, dass die Einwilligung informiert und freiwillig gegeben wird. Eine Erhöhung der Fallkonstellationen, in denen eine Einwilligung eingeholt werden muss, hat auch direkte (negative) Auswirkungen auf die Transparenz. Um für die Zukunft auch innovative technische Lösungen zu ermöglichen, dürfen keine übermäßigen formalen Anforderungen an die Einwilligung gestellt werden.

- Im Interesse der Rechtssicherheit sind eindeutige Beweislastregeln für die Einwilligung erforderlich, die das Risiko nicht einseitig auf die Unternehmen übertragen. Dies ist schon deshalb nicht geboten, da die Betroffenen in aller Regel erteilte Einwilligungen ebenfalls in ihren Vertragsunterlagen haben. Bei einer protokollierten Einwilligung sollte sich das Unternehmen grundsätzlich darauf berufen können und nicht zusätzlich die Identität des Betroffenen nachweisen müssen. Die anonymen Nutzungsmöglichkeiten im Internet dürfen nicht einseitig zu Lasten der Unternehmen gehen.

- Problematisch ist das Verbot der Einwilligung bei „erheblichem Ungleichgewicht“ zwischen Verarbeiter und Betroffenen nach Art. 7 (4). Diese Norm schafft erhebliche Rechtsunsicherheit, da unklar ist, wann von einem entsprechendem Ungleichgewicht ausgegangen werden kann/muss. Liegt es z.B. vor, wenn ein Behandlungsbedürftiger vor der Behandlung im Krankenhaus eine Einwilligungserklärung unterschreiben muss? Oder ist gar bei jedem Verbrauchervertrag im Massengeschäft, in dessen Rahmen eine datenschutzrechtliche Einwilligung eingeholt wird, bereits von einem erheblichen Ungleichgewicht der Vertragsparteien auszugehen? Problematisch ist die Regelung insbesondere auch für den Arbeitnehmerdatenschutz, weil gemäß Art. 82 (1) die Mitgliedsstaaten nur „in den Grenzen dieser Verordnung“ Regelungen zum Beschäftigtendatenschutz erlassen können. In Deutschland ist die Einwilligung im Beschäftigungsverhältnis (Über- Unterordnungsverhältnis) unter strengen Voraussetzungen aber durchaus zulässig und die konkrete Ausgestaltung des Beschäftigtendatenschutzes basiert in vielen Unternehmen auf Betriebsvereinbarungen, für die die Einwilligungsmöglichkeit Voraussetzung ist.

- Befristete Einwilligung: Aus Art 6 (1) a) mit Art. 17 (1) b) ergibt sich, dass der Betroffene seine Einwilligung nur für eine befristete Speicherdauer erteilen kann. Sobald diese abgelaufen ist, besteht ein Löschungsanspruch für die verarbeiteten Daten. Da die befristete Speicherdauer nur in Art. 17 erwähnt

wird, ist nicht ganz klar, ob hiermit nur der Fall gemeint ist, dass der Verantwortliche in seinem Einwilligungsformular eine begrenzte Speicherdauer angegeben hat, oder ob der Betroffene seine Einwilligung individuell befristen können soll. Letzteres würde das Hinterlegen individueller Löschregeln hinter jeden einzelnen Kundendatensatz erfordern und dürfte technisch kaum abbildbar sein. Das Vorsehen einer Befristung erscheint außerdem nicht notwendig, weil die Speicherungs- und Verarbeitungsdauer schon bisher durch den Erforderlichkeitsgrundsatz ausreichend begrenzt war.

- Nach Art. 7 (3) berührt der Widerruf der Einwilligung die ursprüngliche Zulässigkeit der Datenverarbeitung nicht. Allerdings sind nach Art. 17(1) b) offenbar die auf Basis einer Einwilligung überlassenen Daten zu löschen, wenn der Betroffene dies verlangt. Nach den allgemein zivilrechtlichen Regelungen wirkt ein Widerruf einer erteilten Einwilligung ex nunc. Daher sollte an den Widerruf der erteilten Einwilligung keine Löschungsverpflichtung und damit faktisch eine ex tunc-Wirkung verknüpft werden. Vielmehr sollte sich die Zulässigkeit der Weiterverarbeitung der ursprünglich auf Basis einer Einwilligung überlassenen Daten nach den allgemeinen Zulässigkeitsregeln, insbesondere nach dem Erforderlichkeitsgrundsatz, richten.

4 Regelung für gesellschaftsübergreifende Datenübermittlung

In Bezug auf die Übermittlung personenbezogener Daten in Drittländer oder internationale Organisationen hat der aktuelle Entwurf der Verordnung viele Punkte aufgenommen, um die grenzübergreifende Nutzung und Verarbeitung von Daten flexibler zu gestalten und gleichzeitig mehr Rechtssicherheit für international agierende Unternehmen zu schaffen. Allerdings fehlt nach wie vor eine klare Regelung zur gesellschaftsübergreifenden Weitergabe von Daten, obwohl diese von allen am Konsultationsprozess beteiligten Gruppen gefordert wurde. Da das Schutzniveau im Vergleich zur bisherigen Richtlinie steigt, müssen auch die Schutzmaßnahmen bei internationaler Datenübermittlung nachgezogen werden. Das Fehlen einer speziellen Regelung für die gesellschaftsübergreifende Datenverarbeitung im Konzern und der Umstand, dass das Datenschutzrecht dieses arbeitsteilige Zusammenwirken im Konzern und dessen wirtschaftliche Einheit nicht anerkennt, kann zu erheblichen Umsetzungsproblemen und Schwierigkeiten bei globalen Aktivitäten der Unternehmen führen. Organisationsstrukturen in Konzernen sind zunehmend gesellschaftsübergreifend nach Produktgruppen oder Projektaktivitäten ausgestaltet. Innerhalb von Matrixstrukturen sind Beschäftigte dabei zunehmend Vorgesetzten unterstellt, die nicht Beschäftigte derselben Gesellschaft sind.

- Es sollte dringend eine neue Regelung aufgenommen werden, die die Zulässigkeit der Weitergabe von Daten zwischen rechtlich selbständigen Unternehmen innerhalb eines Konzernverbundes praxisgerecht regelt und entsprechende Voraussetzungen festlegt.

- Die Regelungen zu Angemessenheitsbeschlüssen (Artikel 41), Standardschutzklauseln (Artikel 42) und BCR (Artikel 43) basieren richtigerweise auf sachlichen Kriterien und Verantwortlichkeit, und verzichten dabei auf zusätzliche nationale Kriterien. Des Weiteren gelten die Bedingungen für die Über-

mittlung personenbezogener Daten in Drittländer nun ausdrücklich sowohl für die Verarbeitung Verantwortlichen als auch für Auftragsverarbeiter (Artikel 40).

- Art. 42 (4) schafft eine neue bürokratische Ebene. Dies bezieht sich auf die Situation, in der die Vertragsklausel in die Datenverarbeitungsabkommen nicht standardmäßig sind und die verantwortliche Stelle vorab verpflichtet ist, die Autorisierung von einer leitenden Behörde (Art. 34) oder vom Europäischen Datenschutz Board (Art. 57,58) zu erhalten.

- Wir begrüßen die explizite Anerkennung verbindlicher unternehmensinterner Vorschriften. Jedoch ist es wenig praktikabel und kann in der Praxis zu erheblichen Verzögerungen führen, durch das Kohärenzverfahren die Zustimmung des Europäischen Datenschutzausschusses für solche Vorschriften festzuschreiben (Artikel 43 (1), 58 f).

5 Differenzierte Regelung zur Profilbildung

Die Änderung des Wortlautes des bisherigen Artikel 15 der Datenschutz-Richtlinie 95/46 im jetzigen Artikel 20 des Verordnungsentwurfs führt zu erheblicher Rechtsunsicherheit darüber, welche bisher zulässigen Profilbildungen weiterhin zulässig sind und was zukünftig nicht mehr erlaubt sein soll.

- Schon der Titel des Artikels 20, der von „Profilbildung“ im Gegensatz zur automatisierten Einzelentscheidung spricht, lässt darauf schließen, dass der Anwendungsbereich erweitert werden soll. Aus der Formulierung geht jedoch nicht genau hervor, in welchem Umfang. Der Artikel 15 zur automatisierten Einzelentscheidung in der Richtlinie enthält das Merkmal der „erheblich beeinträchtigenden Entscheidung“. Artikel 20 des Verordnungsentwurfs spricht dagegen von einer „Maßnahme, die die betroffene Person in maßgeblicher Weise beeinträchtigt“. Dieser Begriff ist unbestimmter als der bisherige und wirft die Frage auf, was damit über die bisherigen Fallkonstellationen hinaus gemeint sein könnte.

- Bislang gültige Erlaubnistatbestände aus nationalem Recht wie z.B. § 28b) BDSG zum Scoring im deutschen Recht finden sich in dem Verordnungsentwurf jedenfalls nicht direkt wieder und der Verweis in Artikel 20 (2) b) steht unter dem Vorbehalt, dass die Vorschrift geeignete Maßnahmen zu Wahrung der berechtigten Interessen der betroffenen Person enthält.

- Aus unternehmerischer Sicht sollte Profilbildung grundsätzlich möglich sein, wenn es ein berechtigtes Interesse des Verantwortlichen gibt und im Rahmen einer Interessenabwägung mit den Interessen des Betroffenen kein überwiegendes Interesse auf der Seite des Betroffenen festgestellt werden kann bzw. wenn keine belastende Entscheidung für ihn zu befürchten ist.

- Profilbildungen auf anonymisierter Basis sollten zulässig sein (s.o.).

6 Zuständigkeit der Aufsichtsbehörden und Kohärenzverfahren

Die Einführung eines One-Stop-Shop-Prinzip für die Zuständigkeit der Aufsichtsbehörden (Art. 51) wird ebenso begrüßt wie im Grundsatz das Kohärenzverfah-

ren für die Aufsichtsbehörden. Die jetzige Ausgestaltung der Regelungen dazu erscheint jedoch noch nicht geeignet, um das Ziel eines echten One-Stop-Shops sowie eine konsistente Rechtsdurchsetzung tatsächlich zu erreichen, u.a. da eine Reihe von Artikeln die Stellung der zuständigen Datenschutzbehörde unterminiert.

- Die Zuständigkeit der Aufsichtsbehörde setzt nach Art. 51 Nr. 2 an der Niederlassung eines Verantwortlichen oder Auftragsdatenverarbeiters an und regelt, wo die Zuständigkeit für die Aufsicht bei mehreren Niederlassungen liegt. Es geht aber immer um einen „Verantwortlichen". Verantwortlicher ist aber die juristische Person, also die einzelne Gesellschaft. Mit anderen Worten: Besteht ein Unternehmensverbund (z.B. ein Konzern) aus mehreren rechtlich selbstständigen Gesellschaften, etwa zwei GmbHs in Deutschland, einer S.A. in Frankreich, einer Ltd. in UK und einer SpA in Italien, so sind dies fünf Verantwortliche und es bleibt bei einer Beaufsichtigung durch vier bis fünf Aufsichtsbehörden. Notwendig wäre eine Regelung, nach der bei Unternehmen, die im Sinn von § 18 AktG aneinander beteiligt oder voneinander abhängig sind, die Aufsichtsbehörde der Obergesellschaft, hilfsweise der (nach Umsatz, MA-Zahl, Umfang der IT) größten Gesellschaft, in der EU zuständig ist. Es sollte außerdem klargestellt werden, dass für eine Gruppe von Unternehmen die führende Aufsicht für die Hauptniederlassung verantwortlich ist für die Überwachung aller Datenverarbeitungen, die von der Gruppe der Unternehmen ausgeführt wird.

- Das Grundprinzip, eine einzige Aufsichtsbehörde für multinational tätige Unternehmen in der EU zu etablieren, ist ebenfalls willkommen. Dies sollte sich jedoch auch auf mögliche co-verantwortliche Stellen beziehen, die außerhalb der EU liegen, wenn bereits eine verantwortliche Stelle des gleichen Unternehmens ihren Sitz innerhalb der EU hat.

- Entgegen dem erklärten Ziel führt das System mit einer führenden Aufsichtsbehörde nicht zu einem richtigen One-Stop-Shop, weil andere Aufsichtsbehörden ebenfalls ermitteln und sanktionieren können. Die Rolle der Aufsichtsbehörde der Hauptniederlassung ist tatsächlich beschränkt auf Genehmigungen und die Koordinierung von gemeinsamer Durchsetzung. Daher sollte der Kohärenz-Mechanismus auch greifen, wenn lokale Aufsichtsbehörden Maßnahmen ergreifen sollen oder wo sie sanktionieren möchten. Die Rolle von lokalen Datenschutzbehörden sollte es sein, Beschwerden an die führende Behörde weiterzugeben und als Verbindungsstelle zwischen verantwortlicher Stelle und Betroffenen agieren.

- Bei der Definition der "Hauptniederlassung" (Art. 51 (2), Art. 3, Art. 4 (13), Erwägungsgrund 27) wird bei der verantwortlichen Stelle darauf abgestellt, wo die Grundsatzentscheidungen hinsichtlich der Verarbeitung personenbezogener Daten getroffen werden. Passiert dies nicht in der EU, ist es der Ort, an dem die Datenverarbeitung hauptsächlich stattfindet. Bei Auftragsdatenverarbeitern dagegen ist Hauptniederlassung der Ort, an dem er seine Hauptverwaltung in der EU hat. Diese Zuständigkeitsregelung lässt zu viel Interpretationsspielraum bei der Entscheidung, wo die Grundsatzentscheidungen über die Datenverarbeitung getroffen werden. Es wäre besser, immer auf das gleiche Kriterium für die "Hauptniederlassung" abzustellen und das

sollte immer die Hauptverwaltung sein (die Regelung sollte gleich für Auftragsverarbeiter und Verantwortliche sein).

- Entsprechend der Amtshilfe (Art. 55 (8)) kann eine Aufsichtsbehörde vorläufige Maßnahmen ergreifen, wenn die führende Behörde deren Anfrage nicht binnen eines Monats beantwortet. Die Aufsichtsbehörde im Land der Hauptniederlassung könnte jedoch legitime Gründe für den Aufschub dieser vorläufigen Maßnahmen haben, daher sollten die vorläufigen Maßnahmen diese Kompetenz nicht unterminieren.

- Rolle des Europäischen Datenschutzausschusses (Art. 64ff)
  Der Europäische Datenschutzausschuss nimmt im Rahmen des Kohärenzverfahrens (Art. 57 ff) Stellung zu den Entscheidungen der Datenschutzbehörden und jedem Akt der Rechtsdurchsetzung, welcher für die anderen Aufsichtsbehörden relevant sein könnte. Damit spielt er eine gewichtige Rolle bei der Auslegung und Durchsetzung des EU-Datenschutzrechts. Gleichzeitig gibt es weder Anhörungspflichten für den Ausschuss, noch gibt es Instrumente, um seine Entscheidungen anzufechten. Wir sehen daher ein erhebliches Risiko, dass nachteilige Auflagen eingeführt werden könnten, ohne dass es angemessene Möglichkeiten gäbe, praktische Erfahrungen einzubringen oder Widerspruch zu erheben (abgesehen von langwierigen verwaltungsrechtlichen Verfahren). BITKOM erkennt die entscheidende Rolle eines Kohärenzverfahrens mit einer herausragenden Rolle des Datenschutzausschusses an. Gerade deswegen sollte ein transparenter Kontrollmechanismus installiert werden, der den betroffenen Unternehmen Gelegenheit bietet, Stellung zu nehmen oder Entscheidungen anzufechten. Die Verordnung sollte eine ausdrückliche Verpflichtung des Ausschusses enthalten, transparent zu handeln, die Wirtschaft anzuhören und die Anfechtung von Entscheidungen durch die von ihnen betroffenen zuzulassen.

7 Selbstverpflichtung und Zertifizierung

Die Verordnung sollte die Themen Selbstverpflichtung und Zertifizierung noch stärker verankern und einen praxisgerechten Rechtsrahmen dafür schaffen. Wünschenswert wäre hier ein Modell, das folgende Elemente vorsieht:

- Schaffung einer Plattform, auf der ein konstruktiver und zügiger Dialog zwischen den Beteiligten (insbesondere Unternehmen/Verbände und Aufsichtsbehörden) ermöglicht wird.
- Konfliktlösungsmechanismen
- Anreize für die Unternehmen in Form der Anerkennung von Selbstverpflichtungen durch die EU/Aufsichtsbehörden und damit mehr Rechtssicherheit
- Überprüfbarkeit ablehnender Entscheidungen der Aufsichtsbehörden

Für die Zertifizierung sollten gemeinsame Maßstäbe entwickelt werden, insbesondere im Hinblick auf Auftragsverarbeitung und Cloud Computing.

8 Auftragsdatenverarbeitung

Kaum ein Unternehmen führt seine Datenverarbeitung heute allein mit eigenen Mitteln durch, weil das nicht effizient wäre. Professionelle Anbieter von Datenverarbeitungsdienstleistungen übernehmen Aufgaben, für die das nötige Know-

How oder die erforderlichen Kapazitäten im eigenen Unternehmen nicht zur Verfügung stehen. Cloud Computing ist momentan der wichtigste Technologie- und Markttrend der Branche, der es ermöglicht, noch mehr Technik und Know-How auszulagern und zu skalieren. Fast alle dieser Konstellationen stellen aus datenschutzrechtlicher Sicht Fälle der Auftragsdatenverarbeitung dar. Daher sind die Regelungen zur Auftragsdatenverarbeitung essentiell für die Weiterentwicklung von Cloud Computing und die Wertschöpfung der gesamten europäischen Wirtschaft. Vor diesem Hintergrund erscheint Folgendes notwendig:

- Die vollharmonisierten europäischen Vorgaben sollen für Auftragsdatenverarbeiter gelten, die in Europa Dienste anbieten, unabhängig davon, ob diese Anbieter auch in einem Mitgliedsstaat die Auftragsdatenverarbeitung betreiben. Der jetzige Artikel 3 des Verordnungsentwurfs erfasst nur Auftragsverarbeiter mit einer Niederlassung in der Europäischen Union.

- Die Verantwortlichkeiten von Verantwortlichem und Auftragsverarbeiter sollten weiterhin klar getrennt sein und der Auftragsverarbeiter nur in dem vertraglich bestimmten Rahmen für die Datenverarbeitung verantwortlich sein. Das beinhaltet auch die Bestimmungen über die Sicherheit der Auftragsverarbeitung. Allein der Verantwortliche kann bestimmen, wie wichtig die Daten für ihn sind und wie sie geschützt werden müssen. Die Verteilung der Verantwortlichkeit zwischen Verantwortlichem und Auftragsverarbeiter (Art. 22, 24, 26, 27, 28 des Verordnungsentwurfs) wird aus dem Entwurf nicht ausreichend deutlich. In zahlreichen Vorschriften werden der Verantwortliche und der Auftragsverarbeiter gleichzeitig genannt. Im Sinne einer klaren Verantwortlichkeitszuordnung auf die verantwortliche Stelle müssten in den entsprechenden Vorschriften der Bezug zum Auftragsverarbeiter gestrichen werden.

  Aus den Art. 26 und 27 wird nicht hinreichend deutlich, dass die Auftragsdatenverarbeitung zulässig ist. Dies wäre in Art. 27 entsprechend klarzustellen, wobei zu überlegen wäre, ob die Artikel nicht möglicherweise getauscht werden sollten.

  Eine klare Aufteilung der Verantwortlichkeiten, die den faktischen Gegebenheiten entspricht, ist Voraussetzung für eine effektive Umsetzung der Datenschutzvorgaben. Bislang ist sowohl in der EU-Richtlinie als auch im deutschen Recht[6] geregelt, dass die gesamte datenschutzrechtliche Verantwortung bei dem für die Datenverarbeitung Verantwortlichen liegt. Er darf die Verarbeitung der Daten, für die er verantwortlich ist, nach außen geben, aber er bleibt der alleinige Ansprechpartner für die Geltendmachung von Betroffenenrechten und gegenüber der Aufsichtsbehörde, z.B. zur Meldung von Datenpannen. Damit er dieser Verantwortung gerecht werden kann, darf umgekehrt der Auftragsdatenverarbeiter nur auf seine Weisung hin tätig werden[7] und es muss vertraglich sichergestellt werden, dass er seine Pflichten erfüllen kann.

  In Erwägungsgrund 62 stellt der Verordnungsentwurf zwar fest, dass es einer klaren Zuteilung der Verantwortlichkeiten durch diese Verordnung in Fällen

[6] Artikel 17 EU-RL 95/46, § 11 (1) BDSG
[7] Art. 17 (3) EU-RL 95/46, Art. 11 (3) BDSG

der gemeinsamen Verantwortlichkeit sowie in Fällen der Auftragsverarbeitung bedarf. In den Artikeln 24, 26, 27 und 28 wird diese klare Zuteilung jedoch nicht deutlich.

- Artikel 22 führt neue Verantwortlichkeiten für die verantwortliche Stelle ein. Diese beinhalten die Pflicht, die Einhaltung der Regulierung durch interne Prozesse sowie durch interne Verantwortlichkeiten und durch den Nachweis der Konformität zu demonstrieren. Diese Regelungen sind grundsätzlich sinnvoll, jedoch kann es einige schwierige Situationen geben, in denen der Grad der Beschreibung in der Verordnung so gestaltet ist, dass diese nicht die Praxis widerspiegelt, die zur Sicherheit der persönlichen Daten angemessen ist. Dieser Artikel sollte daher noch einmal überarbeitet werden.

- Es ist unklar, für welche Konstellationen die gemeinsame Verantwortlichkeit in Art. 24 gedacht ist und welche Vorteile sich für die Beteiligten an einem gemeinsamen Datenverarbeitungsvorgang ergeben sollen.

- In Artikel 26 und 28 werden dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter zum Teil parallel die gleichen Pflichten zur Einhaltung bestimmter gesetzlicher Vorgaben auferlegt. Der Auftragsverarbeiter wird z.B. in Art. 28 für alle „seiner Zuständigkeit unterliegenden" Verarbeitungsvorgänge zu sämtlichen Dokumentationspflichten verpflichtet, zu denen der Verantwortliche ebenfalls verpflichtet ist. Es wird also eine doppelte Dokumentation verlangt, das ist nicht effizient. Offen bleibt in Art 26 (1), auch, was sich die Kommission unter hinreichenden Garantien vorstellt, welche bestätigen, dass die technisch-organisatorischen Maßnahmen so durchgeführt werden. Da es bisher weder der deutsche noch der europäische Gesetzgeber geschafft haben, anwendbare Datenschutzanforderungen zu normieren, ist es schwierig abzusehen, nach welchen Kriterien hier vorgegangen werden soll.

- In Artikel 26 (2)a) wird klargestellt, dass der Auftragsverarbeiter nur auf Weisung des für die Verarbeitung Verantwortlichen tätig werden muss. In Artikel 27 wird das relativiert, indem der Auftragsverarbeiter „nur auf Anweisung des Verantwortlichen Daten verarbeiten darf", sofern er keinen anders lautenden, aus dem Unionsrecht oder dem mitgliedsstaatlichen Recht erwachsenden Pflichten unterliegt. Damit gerät der Auftragsverarbeiter in die Gefahr einer Zwickmühle, wenn sich seiner Meinung nach die Weisungen des Verantwortlichen mit den gesetzlichen Vorgaben widersprechen. Im deutschen Recht hat er in diesem Fall nur eine Hinweispflicht an den Verantwortlichen[8]. Im Verordnungsentwurf geht er nach Art. 26 (4) das Risiko ein, selbst zum Verantwortlichen zu werden, wenn er die ihm überlassenen Daten auf eine andere als die ihm von dem für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet. Andererseits haftet er nach Artikel 77 gegenüber dem Betroffenen direkt auf Schadenersatz, wenn ein Schaden durch Verstoß gegen die Verordnung entsteht.

Diese Ausweitung der Verantwortlichkeiten auf die Auftragsverarbeiter macht das ohnehin komplexe Verhältnis von Verantwortlichem und Auftragsverar-

[8] § 11 (3) BDSG

beiter in der Praxis noch komplizierter und ist mit dem neuen Geschäftsmodell der IT-Industrie, der Cloud, noch weniger vereinbar als die bisherigen Lösungen. Besonders in der Cloud haben die Auftragsverarbeiter oft keine Kenntnis über die Bedeutung der Daten für den Verantwortlichen sowie die Risiken, die mit ihnen verbunden sind. Sie können von daher auch keine Risikoprüfungen oder ähnliches durchführen und auch nicht Genehmigungen bei der Aufsichtsbehörde einholen.

9 „Recht auf Vergessen“

Der Verordnungsentwurf gibt jeder Person das Recht, zu verlangen „vergessen zu werden“. Betroffene sollen ihre personenbezogenen Daten durch einen Verantwortlichen löschen lassen können, wenn die Verarbeitung dieser Daten nicht (mehr) zulässig oder vom Betroffenen nicht mehr gewünscht ist. Ziel dieses Rechts ist es, den Betroffenen insbesondere auch mit Blick auf das Internet, die einmal geschaffene Verfügbarkeit oder Verwendungsmöglichkeit ihrer Daten wieder aufzuheben. Aus Sicht der Branche ist dieser Ansatz nachvollziehbar, trägt in der jetzigen Ausgestaltung des Artikels 17 des Verordnungsentwurfs aber nicht zu einem effektiv besseren Datenschutz bei. Zudem lässt es Zweifel am Recht zur freien Meinungsäußerung im Internet aufkommen. Auch aus technischer Sicht besteht das Risiko, dass die Maßnahmen nicht umsetzbar sind. Daher sollte eine Balance gefunden werden zwischen dem Recht des Einzelnen, seine eigenen Daten zu löschen bzw. löschen zu lassen und den fundamentalen Rechten anderer Personen, sowie der Realität in der Online-Umgebung.

- Das „Recht auf Vergessen“ und Löschen ist insgesamt zu konturenlos und von zu wenig präzisen Voraussetzungen abhängig. Das Verhältnis der bestehenden Löschpflichten zum Recht auf Vergessen, welches im Wesentlichen das Recht des Betroffenen bedeutet, nachträglich seine Daten löschen zu lassen, wird nicht ganz klar. Ob und worin ein Mehr in diesem Recht bestehen soll, ist unklar. Angesichts der Schwierigkeit, Daten umfassend aus dem Internet zu löschen, erscheint der Begriff eher irreführend denn hilfreich und sollte daher überdacht werden.

- Das Recht auf vergessen werden sollte vielmehr durch die Schaffung klarer Löschpflichten und damit korrespondierender Löschungsansprüche realisiert werden. Dabei sollte der Löschungsanspruch an die Zulässigkeit der Datenverarbeitung – insbesondere an den Erforderlichkeitsgrundsatz - geknüpft werden. Es muss ein ausgewogenes Verhältnis zwischen dem Interesse des Betroffenen, vergessen zu werden, und der verantwortlichen Stelle, die auf die Zulässigkeitsnormen vertrauen können muss, geschaffen werden. Danach kann aber eine Datenverarbeitung auch zulässig sein, wenn sie nicht im Interesse des Betroffenen ist. Auf dieser Zulässigkeitsebene sind dann die Interessen gegeneinander abzuwägen, wie dies in Art. 6 f) auch grundsätzlich vorgesehen ist. Eine generelle einseitige Dispositionsbefugnis des Betroffenen würde zu weit gehen.

- Gleichwohl stellt sich die Frage, in welchen Fällen eine einseitige Dispositionsbefugnis Sinn machen kann. Dies ist dann der Fall, wenn der Betroffene von sich aus Daten entäußert hat und diese nun gleichsam „zurückholen“ möchte (Soziale Netzwerke). Die Verantwortung für diese öffentlich zugänglichen Daten liegt beim Nutzer selbst, da Hosting Plattformen zum Beispiel

keine spezifische Kenntnis darüber haben, wer diese öffentlichen Daten wie verarbeitet hat. Diese Fälle dürfen aber nicht gleichgesetzt werden mit den Fällen, in denen der Betroffene einer Datenverarbeitung aufgrund einer Einwilligung zugestimmt hat. Dies gilt insbesondere dann, wenn die Einwilligung zum Regelfall der zulässigen Datenverarbeitung gemacht werden soll. Die verantwortliche Stelle könnte dann mit auf Basis von Einwilligungen erlangten Daten nicht mehr zuverlässig arbeiten. Es sind daher klar abgrenzbare Fallgruppen zu bilden.

- Mit Blick auf die Löschung von Daten in sozialen Netzwerken sind drei Punkte relevant:
  - Nutzer sozialer Netzwerke sollten das Recht haben, die von ihnen eingestellten persönlichen Informationen zu jedem späteren Zeitpunkt zu löschen.
  - Art. 17(2) sieht auch die Löschung von Daten vor, nachdem diese zu einem anderen Dienst kopiert wurden. Solche Verpflichtungen sind nicht sinnvoll. Um dieser Anforderung gerecht zu werden, müssten die Anbieter die Aktivitäten der Nutzer im Internet überwachen, was höchst bedenklich ist und diametral der Art und Weise, wie das Internet funktioniert, widerspricht.
  - Schließlich ist die Idee, darauf bestehen zu können, dass Informationen, die von Dritten über einen selbst veröffentlicht wurden, gelöscht werden müssen, umstritten, wenn es keinen rechtlichen Tatbestand gibt. Im Übrigen ist die Definition der freien Meinungsäußerung in Artikel 80 und die weitere Darlegung in Erwägungsgrund 121 ziemlich eng gefasst und sollte stärker die Art der neuen Kommunikationsformen berücksichtigen.

10 Delegierte Rechtsakte / Sanktionsrahmen / Bürokratie

10.1 Rechtsunsicherheit durch „delegierte Rechtsakte“

Die große Anzahl der im Verordnungsentwurf vorgesehenen delegierten Rechtsakte führt zu erheblicher Rechtsunsicherheit und sollte daher reduziert werden.

- Es sollte zum einen geprüft werden, welche Vorschriften direkt im Verordnungsvorschlag konkretisiert werden können oder gar müssen. Dies ist insbesondere in den Fällen sinnvoll, wo noch unbestimmte Rechtsbegriffe und Regelungen näher zu definieren sind. Wo delegierte Rechtsakte beibehalten werden, sollte geprüft werden, ob eine beratende Einbeziehung von Unternehmen sinnvoll ist.

- Wo sich die Kommission vorbehält, über technische Standards und ähnliches zu entscheiden, sollte darüber nachgedacht werden, diese im Rahmen von bestehenden oder neu einzuführenden Standardisierungs- oder Selbstregulierungsprozessen unter Einbeziehung aller Beteiligten/Betroffenen zu entwickeln. Damit würde sichergestellt, dass die technischen Vorgaben den Anforderungen der Praxis entsprechen und in den Unternehmen Akzeptanz finden.

- Bei Regelungen ohne direkte Auswirkungen auf den Binnenmarkt könnte auch darüber nachgedacht werden, auf bestehende nationale Regelungen zurückzugreifen, bzw. die Mitgliedsstaaten zum Erlass solcher Regelungen zu ermächtigen.

- Weitere Rechtsunsicherheiten sollten beseitigt werden, indem das Verhältnis EU-Verordnung zu speziellen Richtlinien wie E-Commerce-Richtlinie und E-Privacy-Richtlinie umfassend geklärt wird. Bislang ist dies nicht der Fall und es finden sich teilweise Widersprüche in den Vorschriften. Z.B. verweist die E-Privacy-Richtlinie auf Sanktionshoheit der Mitgliedsstaaten, während der Verordnungsentwurf selbst Bußgeldniveau festsetzt. Auch bei der Einwilligung sehen E-Privacy-Richtlinie und Verordnungsvorschlag unterschiedliche Anforderungen vor.

10.2 Sanktionsrahmen

Die Einführung strikterer Sanktionen für Datenschutzverstöße ist nachvollziehbar und könnte die Durchsetzung höherer Datenschutzstandards unterstützen. Allerdings ist die konkrete Ausgestaltung des verwaltungsrechtlichen Sanktionsrahmens in mehrerlei Hinsicht problematisch.

- Berücksichtigt man, dass der Großteil der Unternehmen Datenverarbeitung als notwendiges Instrument zur Durchführung seiner Geschäfte betreiben muss und nur in wenigen Fällen das Geschäftsmodell allein im Sammeln und Verwerten von personenbezogenen Daten besteht, stehen existenzgefährdende Sanktionen nicht in Relation zur Schwere von fahrlässigen Verstößen gegen die aufgeführten Vorschriften.

- Vor diesem Hintergrund ist auch die Anlehnung an die Sanktionierung im Wettbewerbsrecht fragwürdig. Denn es gibt sicherlich Konstellationen, in denen sich Unternehmen durch Datenschutzverstöße größere Einnahmen verschaffen können, der Regelfall ist das jedoch nicht. Ob damit Unternehmen, die zu ihrem wirtschaftlichen Vorteil bewusst gegen Datenschutzvorschriften verstoßen, bestraft werden könnten ist ebenfalls fraglich, weil sie durch geschickte Ausgründungen hohe Strafen umgehen könnten.

- Die Schärfe der Sanktionen ist umso problematischer, als die Vorschriften, deren Missachtung die Sanktion auslösen kann, teilweise so unpräzise und voller unbestimmter Rechtsbegriffe[9] sind, dass es für die Unternehmen im Vorhinein schwer abzuschätzen ist, ob sie mit ihren Maßnahmen aus Sicht der Aufsichtsbehörden den Vorgaben der Verordnung tatsächlich genügen. Damit werden die Unternehmen einer teilweise existenzbedrohenden Rechtsunsicherheit ausgesetzt, die nicht gerechtfertigt ist.

- Die Höhe der potenziellen Strafen kann als eine Bremse für neue Innovationen und der damit verbundenen Schaffung von Arbeitsplätzen unter Internetdienstleistern verstanden werden. Denkbar ist, dass dadurch das Wachstum in der Internetwirtschaft in der EU ausgebremst wird.

[9] z.B. Art. 79 (5) e) „Auskünfte nicht in hinreichend transparenter Weise erteilt" oder Art. 79 (5) g) „alle erforderlichen Schritte".

- Das Sanktionsniveau bei Verstößen gegen die Regulierung riskiert, dass das Verhältnis zwischen Unternehmen und zuständiger Datenschutzbehörde gefährdet und ein konstruktiver Lösungsfindungsprozess erschwert wird. In einer sich schnell entwickelnden Branche wie der IT-Branche kann dies zum echten Innovationshemmnis werden.

- Für identische Verstöße sollte nur eine Behörde zuständig bleiben.

- Im Übrigen besteht ein Missverhältnis der Strafen im privaten Bereich zu den Befugnissen und Verstößen im öffentlichen Bereich.

10.3 Bürokratie

Insgesamt enthält der Verordnungsentwurf zu viele Dokumentationspflichten und unnötig aufwendige Verfahren. Die vorgesehenen Dokumentationspflichten und –verfahren sollten dahingehend überprüft werden, ob sie nur für bestimmte Fallkonstellationen sinnvoll sind, ob sie tatsächlich ein „Mehr“ an Datenschutz schaffen und ob es schlankere Verfahren geben kann.

- Verfahren und Vorkehrungen (Art. 12)
  Bei der Beantragung von Auskunfts- und anderen Rechten, die nach Art. 12 (1) auch elektronisch ermöglicht werden muss, bleibt offen, wie durch den für die Verarbeitung Verantwortlichen die Identität sichergestellt werden soll. Wenn die Kommission hierbei den elektronischen Personalausweis im Blick hat, sollte dies auch in der Verordnung als Möglichkeit dargestellt werden. Denn bislang ist es heute gängige Praxis, dass auch bei elektronischen Auskunftsbegehren die Auskunft per Brief erteilt wird, weil dadurch verifiziert werden kann, dass der Antragsteller auch der Betroffene ist. Das ist bei E-Mail-Adressen allein oft nicht möglich. Das rein elektronische Verfahren erscheint nur dort unproblematisch machbar, wo der Betroffene einen Account mit Emailadresse direkt beim Verarbeiter hat und diese dort entsprechend verifiziert werden kann.

- Transparenzpflichten (Art. 12-16)
  Art. 14 dehnt die gesetzliche Benachrichtigung unnötig aus, da diese ja nur eine Eingangsinformation darstellen soll. Die Vorschriften über die Rechte der Betroffenen sollten in einem Stufenverhältnis stehen. Die Information nach Art. 14 sollte nur die wesentlichen, für den Betroffenen wichtigen Angaben (Identität der verantwortlichen Stelle, Zweck der Datenverarbeitung sowie Kategorien von Empfängern) enthalten. In einigen Fällen wäre anstelle einer Benachrichtigung auch lediglich eine Hinweispflicht sinnvoll (z.B. bei der Videoüberwachung, wo anderes gar nicht möglich ist). Möchte sich der Betroffene daraufhin tiefer informieren, steht ihm das weitergehende Auskunftsrecht nach Art. 15 zu. Im Anschluss an die erteilte Auskunft können dann die Rechte auf Berichtigung und Löschung geltend gemacht werden. Mit diesem Stufenverhältnis der Transparenznormen lassen sich das individuelle Informationsbedürfnis des Betroffenen und die Begrenzung unnötigen Aufwandes auf Seiten der verantwortlichen Stellen interessengerecht in Einklang bringen.

- Generelles Accountability-Prinzip (Art. 22)
  Wenn für Rechtmäßigkeit der Verarbeitung jedes kleinsten Verarbeitungsvorgangs eine Strategie entworfen und dokumentiert werden muss, verursacht das großen Aufwand, der zu wenig Mehrwert führt. Hier wäre eine Konzentration auf das Wesentliche dringend erforderlich. Die im deutschen BDSG festgelegten Dokumentationspflichten werden bislang als ausreichend angesehen, um die Rechtmäßigkeit der Verarbeitung in einem Unternehmen gegebenenfalls prüfen zu können. Daran sollte sich möglichst auch die Verordnung orientieren.

- Dokumentationspflichten aus Art. 28
  Die in Art. 28 (1) vorgesehene umfangreiche Dokumentationspflicht ist nicht ausreichend zwischen den Beteiligten aufgeteilt/abgestimmt, so dass möglicherweise drei parallele Dokumentationen mit der Gefahr von Widersprüchen und unnötiger Mehrarbeit entstehen. Die Verantwortungssphären des Verantwortlichen und des Auftragsverarbeiters sind deutlicher abzugrenzen und die entsprechenden Dokumentationspflichten darauf zu begrenzen. Problematisch ist auch die in Art. 37 (1) d) vorgesehene Verantwortlichkeit des Datenschutzbeauftragten dafür, dass die Dokumentation vollständig, richtig und aktuell ist, während die Erstellung und Pflege der Dokumentation nicht direkt bei ihm, sondern allgemein bei der verantwortlichen Stelle liegt. Der betriebliche Datenschutzbeauftragte wird damit für etwas in die Pflicht genommen, was er nicht verantworten kann und selbst bei bestem Willen auch nicht ohne interne Unterstützung gewährleisten kann.

- Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (by Design und by Default Art. 23)
  Dass Unternehmens sich schon beim Design neuer Produkte und Verfahren Gedanken zum Datenschutz machen sollten, ist ein richtiger Ansatz. Es stellt sich aber grundsätzlich die Frage, ob sich diese Prinzipien als konkrete gesetzliche Vorgabe eignen, da die verwendeten Begriffe nur grob definiert und die Regelung insgesamt unpräzise ist. Damit taugt die Regelung zumindest nicht, um an eine Verletzung Bußgeldfolgen zu knüpfen. Konkreter kann sie jedoch kaum sein, weil es sehr schwer würde, eine konkrete, technikneutrale Regelung zu finden und sich hieraus auch ein Eingriff in grundrechtlich geschützte Freiheiten der Unternehmen ergäbe, der kaum zu rechtfertigen wäre. Denn zum einen gibt es bereits etablierte Prinzipien (technisch-organisatorische Maßnahmen, Datensparsamkeit), die jedenfalls einen Teil der nun angestrebten Vorgaben bereits abdecken und zum anderen ist fraglich, ob es wirklich zu rechtfertigen ist, Sanktionen bereits an Vorgänge zu knüpfen, die lange vor einer möglicherweise erfolgenden Datenverarbeitung liegen. Abzulehnen ist auch, dass die Kommission eigenständig technische Standards in Bezug auf die konkrete Umsetzung vorgibt. Der sinnvollere Weg, auf die flächendeckende Umsetzung dieser Prinzipien hinzuwirken, scheint es zu sein, im Dialog der Beteiligten sektorspezifische Standards zu entwickeln und diese möglicherweise im Rahmen von Selbstverpflichtungen oder Zertifizierungen umzusetzen. Das Prinzip des „Privacy by default“ ist ebenfalls zu überdenken. Es trägt zum Beispiel der Natur sozialer Netzwerke, Menschen miteinander zu verbinden und Informationen miteinander zu teilen, nicht hinreichend Rechnung. Die Verordnung sollte in dieser Hinsicht den Kontext, in dem Daten gesammelt und verarbeitet werden, berücksichtigen. Die Menschen sollten über jeden Inhalt, den sie in einem sozialen Netzwerk

veröffentlichen, Kontrolle besitzen. Hierzu sind die notwendigen Instrumente zur Verfügung zu stellen, die sicherstellen, dass die Menschen mit denjenigen ihre Informationen austauschen, mit denen sie möchten.

- Melde- und Benachrichtigungspflichten (Art. 31 und 32)
  Der vorgesehene Zeitrahmen und der Detaillierungsgrad der Meldepflicht sind unrealistisch. Die Schwelle für Meldungen und Benachrichtigungen von Betroffenen ist zu niedrig. Hier sollte man die Erfahrungen aus den USA und die Gefahr einer „notification fatigue" berücksichtigen. Ferner gilt es zu verhindern, dass sich Unternehmen auf die „Melde- und Benachrichtigungspflicht" konzentrieren und nicht auf das Problem an sich. Zur Anzeige gebracht werden sollten nur solche Fälle, in denen tatsächlich schwerwiegende Beeinträchtigungen für die Interessen der Betroffenen drohen. Ansonsten werden die Aufsichtsbehörden mit einer Vielzahl von Meldungen kleiner und unbedeutender Verstöße überschwemmt, die niemandem nützen. Die in Deutschland eingeführte Regelung des § 42a BDSG erscheint hier als sinnvolles Vorbild, weil sie die Melde- und Informationspflicht auf ein sachgerechtes Maß begrenzt.

- Datenschutz-Folgenabschätzung (Art. 33)
  Jede Verarbeitung personenbezogener Daten sollte geplant sein um mögliche Risiken bereits im Vorfeld zu identifizieren. Da nicht jede Verarbeitung einer Folgenabschätzung zugeleitet werden kann und dies auch erkennbar einen weder gewollten noch durchzuführenden administrativen Aufwand bedeuten würde, muss darauf geachtet werden, den Anwendungsbereich klar auf solche Fälle zu begrenzen, in denen schwerwiegende Risiken und auch die Gefahr von Schäden für die Betroffenen bestehen. Nicht jede im Entwurf angesprochene Segmentierung oder Verarbeitung von Positionsdaten wird sinnvollerweise hierunter fallen müssen.

- Art. 34 Vorherige Genehmigung und vorherige Zurateziehung
  Es ist begrüßenswert, dass die Genehmigungspflicht eingeschränkt wurde. Allerdings ist eine weitere Präzisierung wünschenswert und erforderlich. Außerdem sollten für die Datenschutzbehörden und das Kohärenzverfahren Antwortfristen eingeführt werden, damit die Vorteile für die Wirtschaft, die in geringeren Kosten für Bürokratie sowie in der zügigen Durchführung von internationalen Prozessinnovationen liegen, nicht wieder zunichte gemacht werden. In einigen EU Ländern kann es mehrere Jahre dauern, bis eine Reaktion der Behörde erfolgt oder gar die Genehmigung erteilt ist. Zudem wird sicherzustellen sein, dass die Kriterien darüber, welche Handlungen besondere Risiken beinhalten, innerhalb der EU einheitlich interpretiert werden, andernfalls würde eine Fragmentierung erreicht, die dem Ziel der Harmonisierung nicht entspricht. Art. 34 Abs. 4, wonach die Aufsichtsbehörde eine Liste der Verarbeitungsvorgänge erstellt, die nach ihrer Auffassung der vorherigen Zurateziehung zu unterziehen sind, könnte ein echtes Innovationshemmnis werden.

  Beispiel: Eine Aufsichtsbehörde ist der Auffassung, dass für den Anbieter einer Internetplattform, der seinen Nutzern den Austausch von Nachrichten (Messaging, Mail) ermöglicht, wegen der Gefährdung des Fernmeldegeheimnisses eine vorherige Zurateziehung erforderlich ist. Heute werden in der Regel zumindest einfache Messagingfunktionen bei jeder Internetplatt-

form, die dem Austausch oder der Information von/zwischen Nutzern dient, angeboten. Jeder Anbieter müsste dann vor Einführung des betreffenden Features die Aufsichtsbehörde informieren und eine entsprechende Stellungnahme einholen. Die Kommunikation mit der betreffenden Aufsichtsbehörde wird nach heutiger Erfahrung mehrere Wochen, wenn nicht eher sogar mehrere Monate betragen. Diensteanbieter entwickeln und wenden ihre Services heute aber in der Regel „agil" an, also in kurzen Sprints und sehr kurzen Entwicklungs- und Anpassungszyklen, um wettbewerbsfähig zu bleiben. Die Innovations- und Wettbewerbsfähigkeit wird durch diese Reglementierung der Verarbeitung jedoch erheblich gefährdet. Es ist insbesondere zu erwarten, dass nicht nur die Einführung neuer, sondern auch die Änderung an bestehenden Features wiederum der vorherigen Zurateziehung unterliegen, was entweder Entwicklungsstillstand oder Vollzugsdefizite nach sich ziehen könnte. Die vorherige Zurateziehung ist unserer Auffassung rechtstechnisch nicht geboten. Sie würde auch zu einer erheblichen Mehrbelastung der Aufsichtsbehörden führen. Es ist sinnvoller, die notwendigen Vorabkontrollen intern verpflichtend vorzunehmen und zu dokumentieren und für den Fall der Unterlassung entsprechende Bußgelder vorzusehen, die ggf. auch „empfindlich" sein können.

11 Modell des betrieblichen Datenschutzbeauftragten

Die Einführung des betrieblichen Datenschutzbeauftragten wird begrüßt. Denn das Modell, welches deutsche Unternehmen bereits seit Jahren aus dem BDSG kennen, hat sich bewährt. Für die erfolgreiche Etablierung dieses Selbstregulierungsmodells sind jedoch folgende Punkte zu beachten:

- Um die Vorteile dieses Modells tatsächlich zum Tragen zu bringen, sollte es konsequent im Sinne der Selbstregulierung umgesetzt werden und es sollten keine zusätzlichen Meldepflichten eingeführt werden. Das ist auch notwendig, um die Akzeptanz des Modells zu fördern. Es sollte ernsthaft darüber nachgedacht werden, das Modell der Vorabkontrolle durch den Datenschutzbeauftragten als Ersatz für Meldepflichten an die Aufsichtsbehörde auch in der EU Verordnung zu verankern. Wenn die Unternehmen sehen, dass sie durch die Ernennung eines betrieblichen Datenschutzbeauftragten nicht nur weiteren Aufwand haben, sondern sich gleichzeitig administrative Bürden ersparen, wird sich das positiv für den Datenschutz auswirken.

- Ersetzt der Datenschutzbeauftragte Meldepflichten an die Aufsichtsbehörden, ist es grundsätzlich auch für kleinere Unternehmen zumutbar und sinnvoll, einen betrieblichen Datenschutzbeauftragten zu benennen. Das gilt jedenfalls dann, wenn das Unternehmen in nennenswertem Umfang Datenverarbeitung betreibt. Eine rein an der Mitarbeiterzahl eines Unternehmens orientierte Pflicht zur Ernennung eines Datenschutzbeauftragten ist insofern nicht sachgerecht, als die Mitarbeiterzahl wenig über die potentiellen Datenschutzrisiken in einem Unternehmen aussagt (z.B. Schraubenfabrik mit 300 Mitarbeitern versus medizinisches Labor mit 20 Personen).

- Unter dem Akzeptanz- und Effizienzgesichtspunkt sollten auch die Aufgaben des Datenschutzbeauftragten so ausgestaltet werden, dass sein Schwerpunkt auf der Selbstkontrolle des Unternehmens und der Beratung der Geschäftsführung liegt. Er sollte nicht zu einer Hilfsstelle der Aufsichtsbehörden

gemacht werden, sondern im Unternehmen selbst auf einen guten Datenschutz hinwirken. „Sicherstellung" nach Ar. 37d) sollte durch „Überwachung" ersetzt werden, weil ein Datenschutzbeauftragter das gar nicht allein sicherstellen kann, die Verpflichtung der Dokumentation liegt bei der verantwortlichen Stelle.

12 Recht auf Datenübertragbarkeit („Data Portability")

Die Überlegungen, die zum „Recht auf Datenübertragbarkeit" geführt haben, sind jedenfalls mit Blick auf soziale Netzwerke ein Stück weit nachvollziehbar. Die Ausgestaltung der Regelung und die Verankerung in der Datenschutz-Verordnung sollten aus folgenden Gründen jedoch nochmals überdacht werden:

- Die Pflicht, Kunden- und Interessentendaten auf Wunsch der betroffenen Personen vollständig elektronisch so zu übermitteln, dass sie auf einen Mitbewerber übertragen werden können („Right to Data Portability", Artikel 18, geht wesentlich weiter als die Auskunfts- und Löschungsrechte, welche dem Betroffenen die Kontrolle über seine Daten geben sollen. Soweit die Pflicht darüber hinausgeht, dem Betroffenen die Daten in einem gängigen Format zugänglich zu machen, sondern auch explizit die weitere Verwendbarkeit für andere Systeme fordert, hat sie eine starke wettbewerbsrechtliche Dimension. Ob das datenschutzrechtlich zu rechtfertigen ist, ist fraglich. Gerade Kundendatenbestände können ein wesentliches Betriebsmittel darstellen, welches für das Unternehmen geradezu existenzielle Bedeutung hat. Die freie Übertragbarkeit würde diese Unternehmen ihrer Existenz berauben.

- Der Formulierung nach gilt die Regelung außerdem nicht nur für bestimmte Fallgruppen wie soziale Netzwerke, sondern für alle Unternehmen, die Kundendaten speichern. Das könnte zu absurden Ergebnissen führen (Bsp. Online-Shop muss alle Unterlagen aus seinem Bestellvorgang mit Daten des Kunden in ein für die Konkurrenz verarbeitbares Format bringen. Dabei würde er möglicherweise auch Geschäftsgeheimnisse offenbaren). Es sollte daher noch einmal genau überdacht werden, ob die Regelung in dieser Form und in diesem Gesetz sinnvoll ist. Zumindest müsste die Formulierung klar stellen, auf welche Sachverhalte das Recht auf Datenübertragbarkeit tatsächlich anwendbar sein soll und es müsste eine Interessenabwägung eingeführt werden, über die auch die Interessen des Verantwortlichen berücksichtigt werden können.

- Aus datenschutzrechtlicher Sicht immer problematisch ist die vermutlich erforderlich werdende systematische Zusammenführung von Daten aus verschiedenen Systemen, in denen sie üblicherweise von den Verantwortlichen bzw. ihren Auftragsverarbeitern verarbeitet werden.

- Es erscheint außerdem nicht sinnvoll, die in Art. 18 (3) vorgesehenen Standards und Verfahren durch delegierten Rechtsakt zu bestimmen. Solch technische Fragen können nur im Dialog mit den Beteiligten – etwa im Rahmen einer Selbstregulierung - gelöst werden.

13 Kinder und Jugendliche Art. 4 (18) und Art. 8

Da die Grundrechtsfähigkeit und auch eine beschränkte Geschäftsfähigkeit schon vor dem 18. Lebensjahr besteht, ist eine Beschränkung der Rechte von Kindern/Jugendlichen unter 18 Jahren schon grundsätzlich problematisch und sollte nochmals überdacht werden. Auch unter 13-Jährige können in Deutschland bereits gültige Verträge schließen. Sollen sie z.B. zukünftig keine Online-Bestellung im Rahmen ihres Taschengeldes mehr vornehmen dürfen? Unklar ist auch, ob Art. 8 (1) nur für Fälle vorgesehen ist, in denen generell die Einwilligung zur Datenverarbeitung eingeholt werden muss oder ob speziell bei Kindern immer der Einwilligungsvorbehalt der Eltern gelten soll. Bei der Verarbeitung personenbezogener Daten eines Kindes gibt es außerdem in vielen Fällen die rein praktische Schwierigkeit, das Alter sicher festzustellen. Daher müsste klargestellt werden, was vom Anbieter verlangt werden kann, um das Alter festzustellen.

Berlin, den 18. Mai 2012

Zuziehung von Sachverständigen des Ausschusses für Europa und Eine Welt

„EU-Datenschutzreform"
Drucksachen 16/1626 und 16/1674

Dienstag, 5. März 2013, 14.00 — 17.00 Uhr, Raum E 3 — A 02

Fragenkatalog

---

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

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?

Eine Verordnung ist jedenfalls für den nicht-öffentlichen Bereich notwendig und angemessen, weil der Versuch einer Vollharmonisierung durch eine Richtlinie bislang misslungen ist. Eine Vereinheitlichung ist jedoch für die effektive Durchsetzung des Datenschutzes sowie für die weitere wirtschaftliche Entwicklung in Europa unabdingbar.

3. Welche konkreten Verbesserungen sehen Sie hinsichtlich der Europäischen Datenschutzreform für die Bereiche
a) Datenschutz im Internet
b) Arbeitnehmerdatenschutz
c) Verbraucherdatenschutz?

Sieht dazu die beigefügte BITKOM Stelllungnahme vom 18.5.2012

4. In welchen Bereichen — insbesondere mit Blick auf die unter Frage 3 genannten Spezialgebiete — sehen Sie die Gefahr einer Absenkung von Datenschutz-Standards gegenüber dem deutschen Datenschutzrecht?

Wir sehen in den momentanen Entwürfen keine Absenkung, sondern im Gegenteil, an einigen Stellen eine Verschärfung der Vorgaben bzw. eine Einschränkung der erlaubten Datenverarbeitung.

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

§ 15 TMG – Anreize zur Anonymisierung und Pseudonymisierung von Daten
§ 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz Datenverarbeitung aufgrund eines berechtigten Interesses (auch im Interesse Dritter)
Ausgestaltung des betrieblichen Datenschutzbeauftragten

6. Welche Durchsetzungsdefizite sehen Sie im heutigen Datenschutzrecht? Inwiefern werden diese durch die Europäische Datenschutzreform gemindert oder beseitigt?

Wir haben heute keine einheitliche Rechtsdurchsetzung, Landesbehörden gehen unterschiedlich vor. Kohärenzverfahren könnte zu einer europaweit einheitlicheren Vorgehensweise bei der Durchsetzung führen. Generell sind die Aufsichtsbehörden zu knapp ausgestattet, um ihren Aufgaben flächendeckend umfänglich nachzukommen?

7. Welche Vor- und Nachteile sehen Sie in den durch die Europäische Datenschutzreform vorgesehenen Veränderungen in der Datenschutzaufsicht?

Vorteile:
-One-Stop-Shop ist für Unternehmen eine große Verwaltungsvereinfachung und mehr Rechtssicherhit
-Einheitlicher Rechtsdurchsetzung

Nachteile:
-Organisatorische Herausforderung für Aufsichtsbehörden mit viel Bedarf für Amtshilfe

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?

9. Wie beurteilen Sie die Auswirkungen der unterschiedlichen Regelungen für die Gefahrenabwehr (Verordnung: nicht-straftatenbezogen, Richtlinie: straftatenbezogen)? Lässt sich insbesondere in der Praxis sachgerecht abgrenzen?

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

Siehe BITKOM Stellgungnahme

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

12. Wie beurteilen die Sachverständigen die Umsetzbarkeit der in dem Entwurf für die EU-Datenschutz-Grundverordnung enthaltenen Vorgaben für die Datenverarbeitung in Unternehmen?

Siehe BITKOM Stellungnahme

13. Wie beurteilen die Sachverständigen die in Ziffer 11.5 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. 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?

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?

Schwer zu begründen, sollte miteinbezogen werden.

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?

Soweit EU diese regeln kann, tut das der VO-Entwurf. Zusätzlich sind jedoch Vereinbarungen zwischen EU und anderen Staaten notwendig, um weiteren Schutz der Daten von EU-Bürgern bei Verarbeitung von Daten im nicht-europäischen Ausland sicherzustellen.

17. Schließt die in der Datenschtzgrundverordnung enthaltene Legaldefinition des Begriffs der "personenbezogenen Daten" bestimmte Bereiche, die bisher nach mitgliedstaatlichem Recht dem Datenschutzrecht unterlagen -. wie z.B. die Videoüberwachung - vom Anwendungsbereich der Datenschutzverordnungen aus?

Nein, Anwendungsbereich wird nach den bisherigen Vorschlägen sogar eher

erweitert.

18. Welche Rechtsetzungsbefugnisse verblieben den Mitgliedstaaten nach Inkrafttreten der Verordnungen im Bereich des Datenschutzes?

    Das ist insbesondere in Bezug auf den Arbeitnehmerschutz und einige andere Spezialbereiche noch unklar. In Bezug auf die allgemeinen Bestimmungen zum Datenschutz, die die Verordnung regelt, bleiben nur wenige Befugnisse, die in der VO ausdrücklich genannt sind.

19. Welche Auswirkungen erwarten die Sachverständigen hinsichtlich des zu erwartenden Verwaltungs- und Kontrollaufwands nach Maßgabe der Datenschutzgrundverordnung auf kleine und mittelständische Unternehmen (KMU)?

    Momentan erheblichen Mehraufwand, weil eine Fülle von zusätzlichen Dokumentations-, Prüf- und Informationspflichten statuiert wird.

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"?

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?

Ist in dieser Fülle problematisch. Siehe dazu auch Ausführungen in BITKOM Stellungnahme.

23. Wie beurteilen Sie die Nichtdifferenzierung zwischen behördlichen Datenschutzbeauftragter und Datenschutzbeauftragter privatwirtschaftlicher Unternehmen?

24. Wie beurteilen Sie das Spannungsfeld zwischen dem Anspruch auf Daten-Portabilität und das im Kommissionsvorschlag enthaltene „Recht auf Vergessen"? Unterbreitet die Kommission in diesem Zusammenhang angemessene Lösungsansätze?

Aus unserer Sicht noch nicht praktikabel. Siehe näheres in der BITKOM Stellungnahme

25. Inwieweit beurteilen Sie das Datenschutzniveau der Grundverordnung in

Bezug auf die Widerspruchs- und Auskunftsrechte der Verbraucher (bezgl. der über sie erhobenen Daten) als ausreichend?

Siehe BITKOM Stellungnahme.

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

Problematisch ist weniger das Niveau als die Ausgestaltung. Es werden zu wenige Anreize für die Anonymisierung und Pseudonymisierung von Daten gesetzt. Das wäre gerade für die Entwicklung vieler zukünftiger Technologien wichtig.