Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)518

Stellungnahme

der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

zum

Vorschlag für eine EU-Datenschutz-Grundverordnung (DS-GVO-E) vom 25.01.2012 (KOM(2012) 11 endgültig)

hinsichtlich der Auswirkungen auf die Privatwirtschaft

I. Allgemeine Erwägungen

1. Vereinheitlichung und Modernisierung des europäischen Datenschutzrechts

Das Instrument der Verordnung zur Generierung eines einheitlichen Datenschutzrechts auf europäischer Ebene ist für den Bereich der Privatwirtschaft ein geeignetes Mittel zur Fortentwicklung des gemeinsamen europäischen Datenschutzrechts. In einer allgegenwärtig vernetzten Welt unterstützt ein EU-weit einheitlicher Datenschutz die Wirtschaft bei länderübergreifenden Datenverarbeitungen. Gleichzeitig werden in der EU Datenschutzstandards insbesondere für die Online-Welt geschaffen, welche auch von außerhalb der EU ansässigen Anbietern zu befolgen sind, sofern diese Daten von EU-Bürgern verarbeiten.

Mit dem Entwurf der Datenschutz-Grundverordnung (DS-GVO-E) wurden neue Datenschutzinstrumente entworfen, aber das Grundprinzip des Datenschutzrechts beibehalten.

Es ist begrüßenswert, dass der Verordnungsentwurf am Verbotsprinzip festhält, welches sich unmittelbar aus dem vom Bundesverfassungsgericht entwickelten Recht auf informationelle Selbstbestimmung ableitet. Das Verbotsprinzip, dessen Anwendung durch jahrelange Rechtsprechung und Literatur gesichert und mit Leben ausgefüllt wurde, schafft mehr Rechtssicherheit als eine grundsätzliche Erlaubnis der Datenverarbeitung mit Verbotsvorbehalt. „Modernisierung“ ist nicht mit Werteaustausch gleichzusetzen. Um einen solchen würde es sich jedoch bei der Abkehr vom Verbotsprinzip handeln. Insbesondere ein Paradigmenwechsel zum teilweise vertretenen „Sphärenmodell“ ist nicht praktikabel, weil bislang keine validen Kriterien existieren, um die nur theoretisch entwickelten Sphären von vermeintlich nicht datenschutzrelevanten öffentlich zugänglichen Informationen bis hin zur die Intimsphäre betreffenden Informationen justiziabel und grundrechtsfest abgrenzen zu können.

Die DS-GVO-E enthält zahlreiche und wesentliche Vorschläge zur Fortentwicklung des bisherigen europäischen und deutschen Datenschutzrechts. Normiert werden sollen dabei viele Überlegungen zur Modernisierung, die bisher nur als Zielvorstellungen oder Ideen vorlagen. Zu nennen sind die Instrumente „privacy by default“, „privacy by design“, „Recht auf Vergessenwerden“ und „Datenportabilität“. Zwar sind die rechtlichen Forderungen nach einem Datenschutz durch Technik und zu datenschutzfreundlichen Voreinstellungen wenig konkret ausgestaltet, in Anbetracht der dynamischen Entwicklung der Informationstechnik sind diese Prinzipien im Wege einer Datenschutzgrundverordnung aber auch nicht weiter konkretisierbar. Hier bedarf es dynamischer delegierter Rechtsakte, die jedoch ihrerseits wegen der Bußgeldbewehrung eine rechtsstaatliche Durchformung im Sinne einer hinreichenden Konkretisierung erforderlich machen. Die Vorgaben zur Technik müssen zudem den Grundsatz der Verhältnismäßigkeit wahren. Sicherzustellen ist auch, dass die Daten verarbeitenden Stellen bei der Entwicklung und Ausgestaltung der technischen Vorgaben angemessen einbezogen werden.

2. Vorbehalt wesentlicher Regelungsinhalte

Der Verordnungsentwurf enthält mehrere Dutzend Ermächtigungen zum Erlass von delegierten Rechtsakten und Durchführungsbestimmungen durch die EU-Kommission, die sämtliche Bereiche des Datenschutzes von der Zulässigkeit bis hin zu Transparenz-, Sicherheits- und Organisationsanforderungen erfassen. Problematisch ist, dass auch wesentliche Aspekte des Datenschutzes delegierten Rechtsakten überantwortet werden sollen und damit Unsicherheit über evidente Themen verbleibt.

Exemplarisch seien hier genannt:

- Art. 6 Abs. 1 Buchstabe f) i.V.m. Abs. 5 DS-GVO-E: Interessenabwägung im Rahmen der Zulässigkeit der Datenverarbeitung
- Art. 26 Abs. 5 DS-GVO-E: Kriterien und Anforderungen für die Verantwortlichkeiten im Zusammenhang mit der Verarbeitung von Daten im Auftrag sowie Pflichten und Aufgaben des Auftragsverarbeiters
- Art. 34 Abs. 8 DS-GVO-E: Kriterien und Anforderungen an die „hohen Risiken“, die eine Zurateziehung der Aufsichtsbehörde notwendig machen
- Art. 82 Abs. 3 DS-GVO-E: Datenverarbeitung im Beschäftigungskontext

Sofern sich Ermächtigungen auf wesentliche Regelungsinhalte beziehen, ist zu prüfen, ob entweder die Möglichkeit zum Erlass delegierter Rechtsakte gestrichen wird, was z.B. für die Interessenabwägung zu fordern ist (vgl. insofern im Einzelnen Abschnitt II. 2.), oder aber Leitlinien für die delegierten Rechtsakte in die DS-GVO aufgenommen werden.

3. Öffnungsklauseln für den nationalen Gesetzgeber

Die Art. 80 ff. DS-GVO-E sehen Rechtsbereiche vor, in denen mitgliedstaatliche Regelungen zum Datenschutz möglich bleiben sollen. Insbesondere der Umstand, dass der Umgang mit Beschäftigtendaten weitgehend durch das jeweilige nationale Arbeitsrecht bestimmt wird, macht eine diesbezügliche Öffnungsklausel erforderlich. Kritisch hinterfragt werden muss allerdings, ob diese Öffnungsklausel durch die Möglichkeit zum Erlass delegierter Rechtsakte in diesem Bereich nicht wieder konterkariert

wird. Die vorgesehene Ermächtigung zum Erlass delegierter Rechtsakte im Bereich des Beschäftigtendatenschutzes ist jedenfalls nicht mit dem Grundsatz zu vereinbaren, dass sich delegierte Rechtsakte nicht auf wesentliche Aspekte des Gesetzgebungsakts beziehen dürfen (vgl. dazu bereits den vorstehenden Abschnitt).

4. Bürokratieabbau

Es ist begrüßenswert, dass von der Meldepflichtigkeit von Verfahren personenbezogener Datenverarbeitung bei den staatlichen Aufsichtsbehörden, wie sie bisher im Grundsatz in der Datenschutz-Richtlinie (95/46/EG) geregelt ist, abgesehen wird. Allerdings wird bei der Datenschutz-Folgenabschätzung eine Zurateziehung der Aufsichtsbehörde erforderlich, sofern sich „hohe konkrete Risiken“ für den Betroffenen ergeben (Art. 33, 34 Abs. 2 Buchstabe a) DS-GVO-E). Die EU-Kommission wird ermächtigt, delegierte Rechtsakte zu erlassen, um die Kriterien und Anforderungen für die Bestimmung der in Bezug genommenen hohen konkreten Risiken festzulegen (Art. 34 Abs. 8 DS-GVO-E). Zusätzlich wird die nationale Aufsichtsbehörde ermächtigt, eine Liste von Verarbeitungsvorgängen festzulegen, bei denen eine vorherige Konsultation zu erfolgen hat (Art. 34 Abs. 2 Buchstabe b) i.V.m. Abs. 4 DS-GVO-E). Im Ergebnis sind damit die Fälle der Einschaltung der staatlichen Fremdkontrolle in die Geschäftsprozesse der Datenverarbeitung von Unternehmen unabsehbar. Zu befürchten steht überdies, dass sich das - nicht näher geregelte - Verfahren der vorherigen Zurateziehung in der Praxis faktisch wie ein Genehmigungserfordernis auswirkt. Denn naheliegend ist, dass in diesem Fall - anders als bei einer reinen Meldepflicht - grundsätzlich zunächst die Reaktion der Aufsichtsbehörde abgewartet werden soll.

Hier enthält der Entwurf Potenziale zum Bürokratieabbau. So könnte die Datenschutz-Folgenabschätzung auf den betrieblichen Datenschutzbeauftragten übertragen werden, der sich in Zweifelfällen mit der Aufsichtsbehörde ins Benehmen setzt. Durch diese Stärkung der betrieblichen Selbstkontrolle könnten zeitaufwendige Konsultationen der Aufsichtsbehörde auf ein notwendiges Minimum beschränkt werden. Zugleich ließen sich die Stellung des Datenschutzbeauftragten und damit seine Akzeptanz im Unternehmen stärken.

Bei der Entwicklung von „Standardvorlagen“ der EU-Kommission zur Dokumentation der Verarbeitungsprozesse (Art. 28 Abs. 6 DS-GVO-E) bzw. „Standardvorlagen und Verfahrensvorschriften“ für das Verfahren der vorherigen Genehmigung bzw. Zurateziehung der Aufsichtsbehörden gemäß Art. 34 Abs. 1 und 2 DS-GVO-E sollte auch die fachliche Expertise der Vertreter der Datenschutzpraxis, insbesondere der betrieblichen Datenschutzbeauftragten eingeholt werden, um überflüssige Bürokratie auf der operativen Ebene der Datenschutzorganisation zu verhindern.

5. Prinzip der betrieblichen Selbstkontrolle durch Datenschutzbeauftragte

a) Schwellenwert für die Bestellung eines betrieblichen Datenschutzbeauftragten und Möglichkeit einer befristeten Bestellung

Die GDD begrüßt, dass das Prinzip der betrieblichen Selbstkontrolle durch Datenschutzbeauftragte im Sinne einer europarechtlichen Bestellpflicht in den Entwurf einer Datenschutz-Grundverordnung Einzug gehalten hat. Jedoch ist dieses Prinzip geschwächt.

Zu dieser Schwächung führt zunächst der Umstand, dass gemäß Art. 35 Abs. 1 Buchstabe b) DS-GVO-E eine Bestellpflicht grundsätzlich erst ab einer Unternehmensgröße von 250 Mitarbeitern bestehen soll. Damit würde insbesondere im Mittelstand eine unabhängige interne Compliance-Instanz zum Datenschutz fehlen bzw. eine Person, die im Hinblick auf die personenbezogene Datenverarbeitung als Anwalt der Betroffenen agiert. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit geht davon aus, dass nur noch 0,3% der deutschen Unternehmen zur Bestellung eines Datenschutzbeauftragten verpflichtet wären.

Aus Sicht der GDD ist der geplante hohe Schwellenwert von 250 Mitarbeitern für die Grundrechtsposition des von der Verarbeitung Betroffenen äußerst kontraproduktiv. Zum einen ist zu befürchten, dass viele Unternehmen unterhalb des Schwellenwertes in Ermangelung einer internen Compliance-Instanz zum Thema "Datenschutz" nur unzureichend die datenschutzrechtlichen Anforderungen bei der Verarbeitung von Kunden- und Mitarbeiterdaten beachten. Zum anderen ist der Wegfall des betrieblichen Datenschutzbeauftragten auch unter Wirtschaftlichkeitsgesichtspunkten wenig sinnvoll. So müssten sich zur Befolgung der geplanten EU-Verordnung die Fachabteilungen im Unternehmen die notwendigen datenschutzrechtlichen Kenntnisse selber aneignen, die bisher beim Datenschutzbeauftragten gebündelt waren, mit der Folge, dass erhebliche Synergieeffekte verloren gingen. Insofern ist der betriebliche Datenschutzbeauftragte ein wesentliches Element zur Entbürokratisierung der Datenschutzorganisation und -kontrolle.

Die Betroffenen, vor allen Dingen Kunden und Mitarbeiter, wären gehalten, sich mit ihren Datenschutzfragen und -beschwerden unmittelbar an die staatliche Datenschutzaufsichtsbehörde zu wenden, die ihrerseits Ermittlungen im Unternehmen anstellen müsste. Diese Aufgabe wird zurzeit weitgehend von den betrieblichen Datenschutzbeauftragten wahrgenommen, die die in Rede stehenden Sachverhalte sach- und zeitnah aufklären können. Auch im Verhältnis der Unternehmensleitung zur Mitarbeitervertretung fehlt die Kompetenz des betrieblichen Datenschutzbeauftragten bei der Beurteilung von Prozessen der Mitarbeiterdatenverarbeitung mit der Folge, dass die jeweiligen Interessen ohne mögliche Moderation durch den Datenschutzbeauftragten aufeinander prallen.

Nach Art. 35 Abs. 7 DS-GVO-E soll die Bestellung des Datenschutzbeauftragten zudem auf zwei Jahre begrenzt werden können. Diese Befristungsmöglichkeit steht einer unabhängigen Aufgabenwahrnehmung entgegen. Nicht zuletzt auf Grund der Datenschutzskandale im Umgang mit Mitarbeiter- und Kundendaten ist mit der Novellierung des Bundesdatenschutzgesetzes im Jahr 2009 dem betrieblichen Datenschutzbeauftragten auf nationaler Ebene ein Kündigungsschutz eingeräumt worden. Dieser soll ihm die notwendige Unabhängigkeit bei der Prüfung und Behandlung von datenschutzrelevanten Sachverhalten ermöglichen.

Die GDD tritt dafür ein, dass die Regelungen zum betrieblichen Datenschutzbeauftragten überarbeitet und der Schwellenwert für die Bestellung von Datenschutzbeauftragten deutlich nach unten korrigiert, zumindest aber eine nationale Öffnungsklausel vorgesehen wird. Bereits Unternehmen mittlerer Größe, also solche, die mehr als 50 Mitarbeiter beschäftigen, haben in der Regel Beschäftigten- und vielfach auch Kundendatenverarbeitungen in einem kontrollbedürftigen Umfang.

b) Verpflichtung zur Bestellung eines Datenschutzbeauftragten wegen Kontrollbedürftigkeit der Verarbeitungsvorgänge

Die zweite für die Privatwirtschaft relevante Regelung zur Bestellpflicht eines Datenschutzbeauftragten in Art. 35 Abs. 1 Buchstabe c) DS-GVO-E stellt auf Datenverarbeitungsvorgänge ab, welche aufgrund ihres Wesens, ihres Umfangs und/oder ihrer Zwecke eine regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen. Die Regelung stellt damit auf die Überwachung von Personen ab und ist somit enger als der Erwägungsgrund 75 bzw. die Einleitung (Kapitel 3.4.4.4.) des DS-GVO-Entwurfs, die hinsichtlich der Pflicht zur Berufung eines betrieblichen Datenschutzbeauftragten sinnvollerweise auf die Kontrollbedürftigkeit der Verarbeitungsvorgänge abstellen. Die in Art. 35 Abs. 1 Buchstabe c) DS-GVO-E gewählte Formulierung geht an der Intention der EU-Kommission vorbei, unter dem Gesichtspunkt der Compliance für das Persönlichkeitsrecht kritische Geschäfts- und Verarbeitungsprozesse durch den Datenschutzbeauftragten fachlich kompetent überprüfen zu lassen.

Entsprechend der Formulierung im Erwägungsgrund 75 bzw. der Einleitung sollte Anknüpfungspunkt der Bestellpflicht die Kontrollbedürftigkeit der Datenverarbeitung sein. Im Hinblick auf eine mögliche Gefährdung der Persönlichkeitsrechte des Betroffenen kann dabei nicht ausschlaggebend sein, ob die kontrollbedürftige Verarbeitung betriebswirtschaftlich die Kerntätigkeit des Unternehmens darstellt. So ist etwa im Gesundheitswesen als Kerntätigkeit die medizinische Versorgung der Patienten anzusehen. Gleichwohl bestehen im Hinblick auf die Sensibilität der verwendeten Daten kontrollbedürftige Datenverarbeitungsprozesse.

Die Frage, wann eine die Bestellpflicht auslösende Kontrollbedürftigkeit der Datenverarbeitung vorliegt, sollte nicht delegierten Rechtsakten überlassen werden (Art. 35 Abs. 11 DS-GVO-E), sondern in der Verordnung selbst, sinnvollerweise in Form von Regelbeispielen beantwortet werden. Eine Bestellpflicht ist insbesondere in folgenden Fällen angezeigt:

- Das Unternehmen führt Verarbeitungsvorgänge durch, welche regelmäßig eine Datenschutz-Folgenabschätzung gemäß Art. 33 DS-GVO-E notwendig machen.

  Die Datenschutz-Folgenabschätzung würde auf Basis des aktuellen Entwurfs häufig eine vorherige Zurateziehung der Datenschutzaufsichtsbehörde nach sich ziehen (Art. 34 Abs. 2 DS-GVO-E). Dieses bürokratische und in der Praxis langwierige Verfahren könnte sachnäher und effektiver ausgestaltet werden, indem die Datenschutz-Folgenabschätzung dem Datenschutzbeauftragten als unabhängigem betrieblichem Kontrollorgan überantwortet wird, das in Zweifelsfällen die Aufsichtsbehörde kontaktiert. Die Bestellpflicht sollte aus Gründen des Bürokratieabbaus damit verbunden werden, dass im Fall der Bestellung die Pflicht zur Zurateziehung der Aufsichtsbehörde entfällt. Siehe hierzu auch vorstehend unter 5.

- Es werden besondere Kategorien personenbezogener Daten im Sinne von Art. 9 DS-GVO-E verarbeitet, es sei denn, die Verarbeitung erfolgt auf Grundlage gesetzlicher Verpflichtungen.

c) Bestellung von gemeinsamen Beauftragten und Verschwiegenheitspflicht

Art. 35 Abs. 2 DS-GVO-E ermöglicht einer Gruppe von Unternehmen einen gemeinsamen Datenschutzbeauftragten zu benennen, sofern der Schwellenwert von 250 Mitarbeitern nach Art. 35 Abs. 1 Buchstabe b) DS-GVO-E überschritten ist. Da nicht davon auszugehen ist, dass die geplanten Regelungen der DS-GVO die Bestellung eines Beauftragten für verschiedene (Konzern-) Unternehmen verbieten sollen, kommt dieser Norm eine eigenständige Bedeutung nur dann zu, wenn sie Unternehmensverbünden und Konzernen die zentrale Bestellung von (Konzern-)Beauftragten für den Datenschutz ermöglicht. Eine bürokratische Bestellung des Datenschutzbeauftragten in jedem einzelnen Unternehmen wäre nicht mehr erforderlich.

Kritisch zu hinterfragen ist der Umstand, dass die Möglichkeit zur Bestellung eines gemeinsamen Datenschutzbeauftragten gemäß Art. 35 Abs. 2 DS-GVO-E ausschließlich auf Art. 35 Abs. 1 Buchstabe b) DS-GVO-E, d.h. Unternehmen mit mindestens 250 Mitarbeitern referenziert. Auch in einer Unternehmensgruppe, in der kritische Datenverarbeitungen im Sinne des Art. 35 Abs. 1 Buchstabe c) DS-GVO-E erfolgen, kann die Bestellung eines gemeinsamen Datenschutzbeauftragten wirtschaftlich und organisatorisch sinnvoll sein, insbesondere dann, wenn gleichartige kritische Datenverarbeitungsprozesse erfolgen und damit Synergieeffekte genutzt werden können.

Die Regelungen des Vierten Abschnitts der DS-GVO-E sollten schließlich um eine Verschwiegenheitsverpflichtung des betrieblichen Datenschutzbeauftragten ergänzt werden.

II. Die einzelnen Regelungen des Entwurfs

1. Art. 4 Abs. 1 und 2 BDSG: Begriff der personenbezogenen Daten

Nach Art. 4 Abs. 2 DS-GVO-E sind „personenbezogene Daten“ alle Informationen, die sich auf eine betroffene Person beziehen. Nach Art. 4 Abs. 1 DS-GVO-E bezeichnet der Ausdruck „betroffene Person“ eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt mit Mitteln bestimmt werden kann, die der für die Verarbeitung Verantwortliche oder jede sonstige natürliche oder juristische Person nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, etwa mittels Zuordnung zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind.

Indem Art. 4 Abs. 1 DS-GVO-E nicht nur auf die Möglichkeiten des für die Verarbeitung Verantwortlichen abstellt, den Bezug zu einer konkreten natürlichen Person herzustellen, sondern die Möglichkeiten aller natürlichen und juristischen Personen einbezieht, wird im Hinblick auf die Bestimmbarkeit des Betroffenen insofern auf eine absolute (objektive) Betrachtungsweise abgestellt. Letzterer steht die relative Betrachtungsweise gegenüber, nach welcher es für den Personenbezug ausschließlich darauf ankommen soll, welche Kenntnisse und Möglichkeiten der für die Verarbeitung Verantwortliche hat, um den von der Datenverarbeitung Betroffenen zu bestimmen.

Insofern ist zunächst festzustellen, dass die Definition in Art. 4 Abs. 1 DS-GVO-E in einem Widerspruch zu den Ausführungen im Erwägungsgrund 24 steht, wonach Online-Kennungen wie IP-Adressen und Cookie-Kennungen, Standortdaten und ähnliche Informationen „nicht zwangsläufig und unter allen Umständen als personenbezogene Daten zu betrachten sind.“ Problematisch ist dies

vor allem insofern, als der Erwägungsgrund gerade die Sachverhalte anspricht, die in der Praxis zu Streitigkeiten führen, selbst allerdings – anders als die Definition in Art. 4 Abs. 1 DS-GVO-E – keine unmittelbaren rechtlichen Wirkungen erzeugt.

Ganz generell gilt, dass mit einem absoluten Begriff der Personenbeziehbarkeit nicht unerhebliche Rechtsunsicherheit entsteht, weil die betroffenen Unternehmen für die Beurteilung derselben nicht mehr auf ihre eigenen Möglichkeiten abstellen dürfen, sondern sich vielmehr ganz generell fragen müssen, ob es ggf. eine Stelle oder Person gibt, die den Betroffenen zu identifizieren vermag.

Art. 4 Abs. 1 DS-GVO-E sollte mit der Zielsetzung überarbeitet werden, mehr Rechtssicherheit im Hinblick auf die Frage der Anwendbarkeit des Datenschutzrechts, insbesondere auch bezogen auf den besonders praxisrelevanten Fall der Online-Kennungen zu erreichen.

2. Art. 6 DS-GVO-E: Rechtmäßigkeit der Verarbeitung

Art. 6 Abs. 1 Buchstabe f) DS-GVO-E lässt die Verarbeitung personenbezogener Daten zu, soweit diese zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen erforderlich ist und nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Eine Verarbeitung, insbesondere Übermittlung personenbezogener Daten im berechtigten Interesse eines Dritten, wie dies noch Art. 7 Buchstabe f) der Richtlinie 95/46/EG vorsieht, wird im Verordnungsentwurf nicht geregelt. Insoweit besteht Nachbesserungsbedarf, da es in der Praxis eine Reihe von sinnvollen Anwendungsfällen für eine derartige Regelung gibt, z.B. die Übermittlung von Daten über ausstehende Forderungen an Auskunfteien oder die Übermittlung von Informationen in sonstige anerkannte Warnsysteme. Eine entsprechende Regelung ermöglicht etwa auch Fluggesellschaften oder Hotels Informationen über den Aufenthalt von Angehörigen oder Mitarbeitern zu erteilen, wenn diese dringend erreicht werden müssen.

Im Verhältnis zu den Vorgaben der Richtlinie 95/46/EG verkürzt überdies Art. 6 Abs. 4 DS-GVO-E die Zulässigkeit nachgelagerter Datenverarbeitungsprozesse. Ist der Zweck der Weiterverarbeitung der personenbezogenen Daten mit dem Zweck, für den diese erhoben wurden, nicht vereinbar, muss danach auf die Verarbeitung mindestens einer der in Art. 6 Absatz 1 Buchstabe a bis e genannten Gründe zutreffen. Eine zweckändernde Nutzung von personenbezogenen Daten soll danach nicht mehr mit einer Interessenabwägung begründet werden können. Die geplante Beschränkung gegenüber dem bisherigen Recht engt die Daten verarbeitende Wirtschaft über Gebühr ein, indem sie ggf. umfassende Neuerhebungen bzw. den Verzicht auf eine geplante Datenverwendung erforderlich macht, obwohl diese mit den schutzwürdigen Interessen des Betroffenen durchaus vereinbar wäre. So wäre es etwa einem Unternehmen verwehrt, seine Bestandskunden im Hinblick auf die aktuelle Produktpalette werblich anzusprechen, wenn eine solche Absicht bei Erhebung der Daten noch nicht bestand und insofern ein entsprechender Hinweis unterblieben ist. In einem solchen Fall wird den Interessen des Betroffenen, der ggf. sogar ein Interesse an derartigen Informationen hat, über die Möglichkeit des Werbewiderspruchs ausreichend Rechnung getragen.

Gemäß Art. 6 Abs. 5 DS-GVO-E soll die Kommission ermächtigt werden, delegierte Rechtsakte nach Maßgabe von Artikel 86 zu erlassen, um die Anwendung von Art. 6 Absatz 1 Buchstabe f, also den Fall der Datenverarbeitung auf Grundlage einer Interessenabwägung für verschiedene Bereiche und Verarbeitungssituationen näher zu regeln. Eine derartige Ermächtigung ist abzulehnen. Mit der Möglich-

keit der Datenverarbeitung auf Grund einer Interessenabwägung sollen differenzierte Einzelentscheidungen ermöglicht werden. Kleingliedrige behördliche Definitionen können den Interessen der an der der Datenverarbeitung Beteiligten, die einer ständigen Dynamik unterliegen, nicht angemessen Rechnung tragen. Es empfiehlt sich vielmehr, es bei der allgemeinen, zukunftsoffenen Abwägungsklausel zu belassen.

3. Art. 7 Abs. 4 DS-GVO-E: Wirksamkeit der Einwilligung

Nach Art. 7 Abs. 4 DS-GVO-E bietet die Einwilligung keine Rechtsgrundlage für die Verarbeitung, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht. In Erwägungsgrund 34 wird als Beispiel für eine derartige Konstellation ohne weitere Differenzierung die Verarbeitung von personenbezogenen Daten im Beschäftigungsverhältnis genannt.

Mit der Art. 29-Gruppe ist allerdings davon auszugehen, dass eine Einwilligung grundsätzlich auch im Arbeitsverhältnis wirksam erteilt werden kann. Dies gilt insbesondere, wenn mit der Datenübermittlung Vorteile für den Mitarbeiter einhergehen. Beispielhaft seien in diesem Zusammenhang Qualifizierungsmaßnahmen, Karrierechancen und Bonusprogramme wie z.B. Stock Options zu nennen. Insofern sollten die irreführenden Ausführungen im Erwägungsgrund 34 gestrichen bzw. relativiert werden.

4. Art. 12 DS-GVO-E: Verfahren und Vorkehrungen, damit die betroffene Person ihre Rechte ausüben kann

Die in Art. 12 Abs. 2 DS-GVO-E vorgesehene feste Frist von regelmäßig einem Monat für die Antragsbearbeitung im Zusammenhang mit der Ausübung von Betroffenenrechten sollte gestrichen und stattdessen darauf abgestellt werden, ob die Bearbeitung „ohne schuldhaftes Zögern“ erfolgt. Über die vorgeschlagene Formulierung kann den individuellen Gegebenheiten beim für die Verarbeitung Verantwortlichen, insbesondere der Komplexität der Datenverarbeitung angemessen Rechnung getragen werden. Vermieden werden sollte, dass Unternehmen bislang dezentral geführte Datenbestände zusammenführen, um auf diese Weise eine möglichst schnelle und komplikationslose Antragsbearbeitung zu erreichen.

Stellt die betroffene Person den Antrag in elektronischer Form, so ist sie gemäß Art. 12 Abs. 4 Satz 4 DS-GVO-E auf elektronischem Weg zu unterrichten, sofern sich nichts anderes ergibt. Vgl. insofern die Ausführungen zum gleichlautenden Art. 15 Abs. 2 Satz 2 DS-GVO-E.

5. Art. 14 DS-GVO-E: Information der betroffenen Person

Art. 14 DS-GVO-E regelt die Information der von der Datenverarbeitung betroffenen Person und geht dabei deutlich über die Vorgaben hinaus, die § 4 Abs. 3 BDSG bislang macht. Festzustellen ist insofern zunächst, dass Transparenz für den Betroffenen selbstverständlich wünschenswert ist, mit einer Überinformation aber letztlich genau das Gegenteil erreicht wird. Zunächst besteht die Gefahr, dass auf Grund der Länge der zur Verfügung gestellten Informationen diese gar nicht erst gelesen werden. Dies gilt insbesondere, wenn, wie dies vielfach der Fall sein wird, gleichzeitig weitere rechtlich erforderliche Informationen, z.B. Allgemeine Geschäftsbedingungen oder Informationen nach Fernabsatzrecht, bereitgestellt werden müssen. Unabhängig davon sollte nicht der Blick auf das Wesentliche

verstellt werden. In diesem Sinne kann es sinnvoll sein, auf umfassende allgemeine Informationen, z.B. zur Rechtewahrnehmung und zur zuständigen Aufsichtsbehörde, im Vorfeld zu verzichten und sich auf die für den Betroffenen interessanten Kernaussagen zu beschränken, nämlich von wem und zu welchen Zwecken seine Daten verarbeitet werden sowie ob und ggf. wohin eine Weitergabe der personenbezogenen Informationen erfolgt. Bezüglich weitergehender Informationen kann dem Betroffenen ggf. ein Auskunftsrecht eingeräumt werden. Alternativ kann ein Hinweis auf die nach Art. 11 DS-GVO-E ohnedies bereitzustellenden Informationen erfolgen.

Hingewiesen sei in diesem Zusammenhang auch darauf, dass die Information des Betroffenen in der Praxis im Rahmen von Standardverfahren erfolgt, bei denen eine Individualisierung nicht möglich ist bzw. einen unverhältnismäßigen Aufwand erfordern würde. Insoweit käme nur die Bereitstellung generischer Informationen in Betracht. Dies betrifft etwa die Verpflichtung zur Angabe der Kontaktdaten der (zuständigen) Aufsichtsbehörde (Art. 14 Abs. 1 Buchstabe e) DS-GVO-E). Auch die Dauer der Datenspeicherung (Art. 14 Abs. 1 Buchstabe c) DS-GVO-E) kann im Einzelfall je nach Verlauf der Geschäftsbeziehung variieren.

6. Art. 15 Abs. 2 Satz 2 DS-GVO-E: Elektronische Auskunftserteilung

Stellt die betroffene Person den Auskunftsantrag in elektronischer Form, so ist sie gemäß Art. 15 Abs. 2 Satz 2 DS-GVO-E auf elektronischem Weg zu unterrichten, sofern sich nichts anderes ergibt. Um Rechtsverletzungen zulasten des Betroffenen zu vermeiden, können in der Praxis Eingaben auf elektronischem Weg erst bearbeitet werden, wenn die Identität des Absenders sichergestellt ist. Um eine sichere Authentifizierung zu erreichen, können insofern zusätzliche Datenerhebungen erforderlich werden.

7. Art. 17 Abs. 2 DS-GVO-E: Recht auf Vergessenwerden

Das in Art. 17 Abs. 2 DS-GVO-E normierte neue „Recht auf Vergessenwerden“ ist wesentlich durch die Diskussionen um Profile bzw. Veröffentlichungen im Rahmen von sozialen Netzwerken beeinflusst und die praktischen Schwierigkeiten, welche damit verbunden sind, wenn ein Betroffener die Preisgabe personenbezogener Daten im Internet später wieder rückgängig machen will („digitaler Radiergummi“). Die geplante Regelung ist allerdings nicht auf soziale Netzwerke beschränkt.

Insgesamt fehlt es der geplanten Regelung, vor allem auch vor dem Hintergrund, dass die Regelung bußgeldbewehrt ist (Art. 79 Abs. 5 Buchstabe g) DS-GVO-E), an einer hinreichend klaren Konturierung. Es stellt sich schon die Frage, ob ein Portalbetreiber, der seinen Nutzern das Erstellen und Pflegen von Profilen sowie das Versenden von Nachrichten ermöglicht, tatsächlich im Sinne von Art. 17 Abs. 2 Satz 1 DS-GVO-E personenbezogene Daten als für die Verarbeitung Verantwortlicher öffentlich macht. Betreiber wie z.B. Facebook stellen letztlich nur die Plattform zur Verfügung, die Entscheidung über die Veröffentlichung der Informationen über das Netzwerk trifft jedoch der Nutzer selbst.

Die zunächst angedachte Pflicht des für die Verarbeitung Verantwortlichen, selbst für die Löschung der Links und Kopien bezüglich der in Frage stehenden Daten zu sorgen, wurde durch die Verpflichtung ersetzt, alle vertretbaren Schritte zu unternehmen, die für die Datenspuren unmittelbar Verantwortlichen über das Löschungsbegehren des Betroffenen zu informieren. Angesichts der Vervielfältigungs- und Verknüpfungsmechanismen im Internet können sich Inhalte dort in kurzer Zeit auf nahezu unüberschaubare Weise verbreiten, so dass sich die in die Pflicht genommenen Unterneh-

men schnell einer kaum zu bewältigenden Aufgabe gegenüber sehen dürften. Welche Anstrengungen in diesem Zusammenhang als „vertretbar“ anzusehen sind, ist mit erheblichen Unwägbarkeiten behaftet.

Die geplante Norm sollte mit dem Ziel überarbeitet werden, eine entsprechend rechtssichere und für die Unternehmen in der Praxis auch umsetzbare Regelung zu schaffen. Jedenfalls bis erste Praxiserfahrungen mit der Regelung gesammelt wurden, erscheint es auch sinnvoll, ihren Anwendungsbereich auf soziale Netzwerke zu beschränken.

8. Art. 18 DS-GVO-E: Recht auf Datenübertragbarkeit

Das geplante Recht auf Datenübertragbarkeit stellt ebenso wie das zuvor angesprochene neue Recht auf Vergessenwerden eine substantielle Neuerung dar. Anders als bei dem Recht auf Vergessenwerden handelt es sich allerdings bei dem Recht auf Datenportabilität um eine Regelung, die weniger dem Schutz der informationellen Selbstbestimmung als dem Verbraucherschutz dient. Insofern stellt sich bereits die Frage nach der richtigen Verortung der Regelung.

Das Recht auf Datenübertragbarkeit sollte zudem - anders als Art. 18 Abs. 1 DS-GVO-E dies vorsieht, welcher insoweit lediglich auf die elektronische Verarbeitung der betreffenden personenbezogenen Daten in einem strukturierten gängigen elektronischen Format abstellt - auf Informationen beschränkt sein, die der Betroffene selbst zur Verfügung gestellt hat. Es würde einen übergebührlichen Eingriff in die Unternehmensfreiheit darstellen, wenn von der Portabilität auch solche Informationen erfasst würden, die das Unternehmen im Rahmen seiner Geschäftstätigkeit zur Person des Betroffenen speichert, z.B. Informationen zu vorhandenen Verträgen oder Werbemerkmalen in einer Kundendatenbank. Diese Informationen bzw. die dahinter stehenden Verarbeitungsprozesse (z.B. Berechnungsmodelle) unterliegen zum einen dem Geschäftsgeheimnis, das angemessen zu schützen ist. Zum anderen ist zu verhindern, dass ein neuer Anbieter des Betroffenen die Früchte der Arbeit des vorherigen Geschäftspartners erntet. Art. 18 Abs. 2 DS-GVO-E nimmt zwar eine Beschränkung auf solche personenbezogenen Daten vor, die der Betroffene „zur Verfügung gestellt“ hat, das Verhältnis von Art. 18 Abs. 2 DS-GVO-E und Art. 18 Abs. 1 DS-GVO-E ist jedoch unklar.

Art. 18 Abs. 2 DS-GVO-E geht davon aus, dass die personenbezogenen Daten dem bisherigen für die Verarbeitung Verantwortlichen „entzogen werden“. Diese Wortwahl zeigt, dass die Kommission bei der Formulierung des Regelungsvorschlags offenbar vor allem Anbieter sozialer Netzwerke vor Augen hatte, obgleich der Anwendungsbereich der geplanten Regelung nicht auf diese beschränkt ist. Außerhalb dieses Bereichs können einer vollständigen „Mitnahme“ der Daten ggf. Aufbewahrungs- und Dokumentationspflichten des bisherigen Geschäftspartners entgegenstehen.

9. Art. 22 DS-GVO-E: Strategien und Maßnahmen zur Sicherstellung des Datenschutzes

Nach Art. 22 Abs. 1 DS-GVO-E stellt der für die Verarbeitung Verantwortliche durch geeignete Strategien und Maßnahmen sicher, dass personenbezogene Daten in Übereinstimmung mit dieser Verordnung verarbeitet werden und er den Nachweis dafür erbringen kann. Insofern sollte deutlicher formuliert werden, dass sich die Nachweis- im Sinne einer Dokumentationspflicht auf das Vorliegen eines entsprechenden Datenschutzkonzepts, d.h. angemessener Strategien und Maßnahmen bezieht und nicht etwa allgemein auf die Rechtmäßigkeit jeder personenbezogenen Datenverarbeitung, für die das Unternehmen ohnedies die Beweislast trägt.

Gemäß Art. 22 Abs. 3 Satz 1 DS-GVO-E ist die Wirksamkeit der Maßnahmen durch den Einsatz geeigneter Verfahren zu überprüfen. Soweit dies angemessen ist, ist diese Prüfung von unabhängigen (internen oder externen) Prüfern durchzuführen (Art. 22 Abs. 3 Satz 2 DS-GVO-E).

Während also der Einsatz unabhängiger Prüfer einem Angemessenheitsvorbehalt unterliegt, trifft die Auditpflicht gemäß Art. 22 Abs. 3 Satz 1 DS-GVO-E ihrem Wortlaut nach jedwede Stelle, die personenbezogene Daten verarbeitet, gilt also unabhängig von deren Größe, der Sensibilität der verarbeiteten Informationen oder der eingesetzten Prozesse. Vor allem aus Sicht von kleineren Unternehmen erscheint eine solche allgemeine Verpflichtung zur Durchführung eines Datenschutzaudits aber unverhältnismäßig und bürokratisch, sofern personenbezogene Daten nur im Rahmen von wenig risikobehafteten Standardprozessen (z.B. zur Vertragsabwicklung) verarbeitet werden. Auch die Pflicht zur Auditierung sollte daher nur bestehen, sofern dies angemessen ist, was vor allem von der Größe des Unternehmens und der Sensibilität der Datenverarbeitung abhängig ist.

Art. 22 Abs. 3 DS-GVO-E sollte zudem um die Feststellung ergänzt werden, dass als unabhängiger interner Prüfer insbesondere der Datenschutzbeauftragte in Betracht kommt. Wegen seiner Fachkunde und Unabhängigkeit ist er hierzu prädestiniert.

10. Art. 23 DS-GVO-E: Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

Art. 23 Abs. 4 DS-GVO-E ermächtigt die Kommission, „technische Standards“ für die in Art. 23 Abs. 1 und 2 genannten Anforderungen festzulegen. Normative Detailregelungen sind nicht in der Lage mit dem rasanten technischen Wandel und der permanenten Entwicklung neuer Technologien schrittzuhalten. Durchführungsakte mit technischen Implikationen sollten insofern von der Kommission nicht erlassen werden.

11. Art. 24 DS-GVO-E: Gemeinsam für die Verarbeitung Verantwortliche

Der Entwurf der DS-GVO-E geht davon aus, dass mehrere Stellen bzw. Personen gemeinsam für eine Datenverarbeitung verantwortlich sein können und dementsprechend auch zusammen gegenüber dem Betroffenen haften (Art. 24 DS-GVO-E). Unter welchen Voraussetzungen eine solche gemeinsame Verantwortung entstehen kann bzw. darf, wird, abgesehen von der in Art. 26 Abs. 4 DS-GVO-E enthaltenen Regelung, nicht näher erläutert.

Die Frage nach der Zulässigkeit von gemeinsamen Verfahren personenbezogener Datenverarbeitung stellt sich in der Praxis insbesondere für Konzerne bzw. Unternehmensverbünde. Zunehmend werden unternehmerische Ziele in nationalen und multinationalen Unternehmensverbünden verfolgt, wobei die Konzerne in wachsendem Maße darauf angewiesen sind, Kunden- und Mitarbeiterdaten im Rahmen ihrer Geschäftstätigkeiten an konzernangehörige Unternehmen zu transferieren. Hinzu kommt, dass die Konzernstrukturen einer großen Dynamik unterworfen sind und konzerninterne Dienstleistungen häufig zentralisiert oder arbeitsteilig erbracht werden (z.B. bei Shared-Service-Centern bzw. Matrixstrukturen).

Vor diesem Hintergrund und insbesondere mit Blick auf den bezweckten freien Datenverkehr innerhalb der EU erachtet es die GDD als sinnvoll, den gewandelten Gegebenheiten im Rahmen einer Spe-

zialregelung zur Zulässigkeit der Datenverarbeitung durch verbundene Unternehmen unter Wahrung eines angemessenen Datenschutzniveaus Rechnung zu tragen.

12. Art. 26 DS-GVO-E: Auftragsdatenverarbeitung

Während das deutsche Recht die Verantwortlichkeiten und Aufgaben der verantwortlichen Stelle und des Auftragsdatenverarbeiters (§ 11 BDSG) klar differenziert, kennt die DS-GVO-E eine derart klare Trennung nicht. So gilt etwa gemäß Art. 26 Abs. 4 DS-GVO-E der Auftragsverarbeiter, der personenbezogene Daten auf eine andere als die vom für die Verarbeitung Verantwortlichen bezeichnete Weise verarbeitet, für diese Verarbeitung als Verantwortlicher und unterliegt den Bestimmungen des Art. 24 DS-GVO-E für gemeinsam für die Verarbeitung Verantwortliche.

Wichtig wäre insbesondere, eine eindeutigere Aufgabentrennung zwischen dem für die Verarbeitung Verantwortlichen und dem Auftragsverarbeiter vorzunehmen. Lediglich beispielhaft seien in diesem Zusammenhang folgende Punkte genannt:

- Die Datenschutz-Folgenabschätzung (Art. 33 DS-GVO-E) soll „der für die Verarbeitung Verantwortliche oder der in seinem Auftrag handelnde Auftragsverarbeiter“ durchführen. Die Durchführung einer Datenschutz-Folgenabschätzung kann aber richtigerweise, schon weil dies die haftende Stelle ist, letztlich nur Aufgabe des für die Verarbeitung Verantwortlichen sein.

- Nach Art. 28 Abs. 1 DS-GVO-E sollen auch Auftragsverarbeiter die ihrer Zuständigkeit unterliegenden Verarbeitungsvorgänge dokumentieren. Soweit ein Unternehmen als Auftragsverarbeiter tätig wird, ist es jedoch nicht Herr der von ihm durchgeführten Verfahren. Die betreffenden Verfahren wären insofern in die Dokumentation des Auftraggebers aufzunehmen. Hinsichtlich der faktisch in seinem Bereich stattfindenden Verarbeitungen ist der Auftragnehmer vielmehr zu verpflichten, dem Auftraggeber die dokumentationsrelevanten Informationen zur Verfügung zu stellen.

- Art. 42 Abs. 1 DS-GVO-E sieht eine Rechtsgrundlage für die Datenübermittlung in ein Drittland auf Grundlage geeigneter Garantien vor. Diese bezieht sich nach ihrem Wortlaut auch auf Auftragsverarbeiter. Ein Auftragnehmer ist jedoch nicht berechtigt, über die Übermittlung der im Auftrag verarbeiteten Daten zu entscheiden.

Sinnvoll wäre schließlich eine Klarstellung, dass die Einschaltung eines Auftragsverarbeiters bzw. die damit verbundene Weitergabe personenbezogener Daten an diesen keines besonderen Erlaubnistatbestandes bedarf, sofern die Vorgaben des Art. 26 DS-GVO-E eingehalten werden.

Bezüglich des in Art. 26 Abs. 2 DS-GVO-E enthaltenen Katalogs an Anforderungen an den Vertrag mit dem Auftragsverarbeiter fällt auf, dass ein wesentlicher regelungsbedürftiger Punkt fehlt, nämlich der Gegenstand des Auftrags, also Umfang, Art und Zweck der vorgesehenen Verarbeitung, die Art der Daten und der Kreis der Betroffenen.

13. Art. 28 DS-GVO-E: Dokumentation der Verarbeitungsvorgänge

Nach Art. 28 Abs. 2 Buchstabe c) DS-GVO-E sind im Rahmen der Dokumentation der Verarbeitungsvorgänge unter anderem Angaben über „die Zwecke der Verarbeitung sowie - falls sich die Verarbei-

tung auf Artikel 6 Absatz 1 Buchstabe f gründet - über die von dem für die Verarbeitung Verantwortlichen verfolgten legitimen Interessen“ aufzunehmen. Mit Blick auf eine gesonderte Dokumentationspflicht bezüglich der „legitimen Interessen“ ist diese Regelung überflüssig, da im Fall der Interessenabwägung der Verarbeitungszweck auch die verfolgten Interessen widerspiegelt. Die Forderung nach der Angabe der verfolgten Interessen ist folglich redundant. Die Regelung sollte so abgeändert werden, dass ausschließlich eine Angabe der Verarbeitungszwecke erforderlich ist.

14. Art. 31 und 32 DS-GVO-E: Meldepflicht bei „Datenschutzpannen“

Die vorgesehenen Regelungen bzgl. der Meldung von Datenschutzverletzungen gegenüber der Aufsichtsbehörde bzw. der Benachrichtigung des Betroffenen sind zu weitreichend. Die Melde- bzw. Benachrichtigungspflicht erfasst alle Arten personenbezogener Daten. Die Meldepflicht gegenüber der Aufsichtsbehörde greift überdies unabhängig davon, ob auf Grund der festgestellten Datenschutzverletzung eine Beeinträchtigung der betroffenen Person zu besorgen ist. Schließlich stellt die Verpflichtung allein auf das Vorliegen einer „Verletzung des Schutzes personenbezogener Daten“ ab. Nach ihrem Wortlaut würde die geplante Regelung damit auch bei unbefugten Zugriffen innerhalb der verantwortlichen Stelle eingreifen.

Um ein Ausufern der Informationsverpflichtung zu vermeiden, wäre es zweckmäßig, sich an der deutschen Regelung (§ 42a BDSG) zu orientieren, die eine Melde- bzw. Benachrichtigungspflicht nur bei dem Verlust bestimmter, im Gesetz näher aufgezählter Datenkategorien vorsieht und die Informationspflicht zudem daran knüpft, dass infolge der „Datenschutzpanne“ schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Die Tatbestandsvoraussetzung der unrechtmäßigen Kenntniserlangung muss sich nach deutschem Recht auf einen „Dritten“ beziehen. Keine Dritten sind Personen innerhalb der verantwortlichen Stelle oder Auftragsdatenverarbeiter. Unberechtigte Zugriffe innerhalb der verantwortlichen Stelle lösen insofern keine Informationspflicht nach § 42a BDSG aus. Auf diese Weise wird eine sinnvolle Beschränkung der Informationspflicht erreicht.

Für die Benachrichtigung der Aufsichtsbehörde sollte festgelegt werden, dass diese „ohne schuldhaftes Zögern“ zu erfolgen hat. Die vorgesehene feste Frist („nach Möglichkeit binnen 24 Stunden nach Feststellung der Verletzung“) wird insbesondere dann Schwierigkeiten bereiten, wenn die Datenschutzpanne bei einem Auftragsverarbeiter geschieht, der dann zunächst den - für die Information nach Art. 31 und Art. 32 DS-GVO-E zuständigen - für die Verarbeitung Verantwortlichen zu informieren hat. Über die vorgeschlagene Formulierung können solche und vergleichbare Praxissachverhalte angemessen aufgefangen werden. Vermieden würde zudem, dass aus Sorge vor der Verwirklichung eines Bußgeldtatbestandes (Art. 79 Abs. 6 Buchstabe s) DS-GVO-E) unqualifizierte Meldungen abgegeben werden.

Der die Verschlüsselung von personenbezogenen Daten in Bezug nehmende Art. 32 Abs. 3 Satz 2 DS-GVO-E sollte im Sinne einer besseren Verständlichkeit neu gefasst werden. Um einen entsprechenden Anreiz für die Schaffung angemessener Sicherheitsmaßnahmen zu erreichen, sollte außerdem auch die Verpflichtung zur Information der Aufsichtsbehörde hinsichtlich einer aufgetretenen Datenschutzpanne entfallen, wenn die Daten entsprechend dem Stand der Technik verschlüsselt wurden.

Schließlich sollte entsprechend § 42a Satz 6 BDSG die geplante Meldepflicht um eine verfahrensrechtliche Regelung ergänzt werden, welche die Verwendung der Benachrichtigung in Straf- und

Ordnungswidrigkeitenverfahren gegen den Benachrichtigungspflichtigen selbst und seine Angehörigen verbietet. Nur so kann dem wichtigen rechtsstaatlichen Prinzip Rechnung getragen werden, wonach niemand verpflichtet ist, sich selbst oder seinen Angehörigen zu bezichtigen („nemo tenetur se ipsum accusare“).

15. Art. 64 ff. DS-GVO-E: Europäischer Datenschutzausschuss

Um sicherzustellen, dass bei den Entscheidungen des Europäischen Datenschutzausschusses die Belange der Daten verarbeitenden Stellen in angemessener Weise berücksichtigt werden können, sollte bestimmt werden, dass vor Beschlüssen mit entsprechender Reichweite eine Anhörung der Vertreter der Privatwirtschaft obligatorisch ist.