16. Juli 2012

Stellungnahme zum Vorschlag der Europäischen Kommission für eine Datenschutz-Grundverordnung (KOM (2012) 11 endgültig)

Hinweis: Die Anmerkungen mit hoher Priorität sind umrahmt.

Rechtsnatur: Zu der Frage der Rechtsnatur der Verordnung sind wir der Ansicht, dass grundsätzlich eine europaweite Harmonisierung wünschenswert ist. Wir sind vor dem Hintergrund der vorgesehenen Ausnahmen aber auch der Ansicht, dass der vorliegende Entwurf hier im Grunde einen Rückschritt gegenüber der bisherigen Richtlinie (95/46/EG) darstellt, die ja nach der zutreffenden Auslegung des Europäischen Gerichtshofs (C-468/10 und C-469/10) bereits eine Vollharmonisierung enthält. Am Ende kommt es nicht darauf an, ob Regelungen im Wege einer Verordnung oder einer Richtlinie erfolgen. Wichtig ist nur, dass sie ausgewogen und in sich abgeschlossen sind. Außerdem müssen sich alle Mitgliedstaaten daran halten. Insbesondere unter Subsidiaritätsgesichtspunkten wären wir auch einer Lösung gegenüber aufgeschlossen, bei der die Verordnung sich auf Fragen des Drittländerdatentransfers beschränkt und die sonstige Harmonisierung weiterhin über eine Richtlinie erfolgt. Dies würde auch dem Umstand Rechnung tragen, dass das Datenschutzrecht stark mit anderen nationalen Rechtsbereichen verwebt ist und eine europäische Verordnung hier als Fremdkörper im Verhältnis zum nationalen Recht unweigerlich zu erheblichen Auslegungs- und Anwendungsunsicherheiten führen würde.

Artikel 1 Absatz 1: Wir sind der Ansicht, dass Artikel 16 Absatz 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) keine Rechtsgrundlage für die Regelung des Datenschutzes im nicht-öffentlichen Bereich bietet. Die Vorschrift bezieht sich ausdrücklich ausschließlich auf den öffentlichen Bereich und dort auch nur auf die Stellen der Europäischen Union und die Verwaltung der Mitgliedstaaten. Dabei soll die Verwaltung der Mitgliedstaaten nur betroffen sein, soweit sie im Anwendungsbereich von Unionsrecht tätig sind. Regelungen zum freien Datenverkehr werden nur erfasst, wenn sie Daten betreffen, die von diesen Stellen

verarbeitet werden (in der englischen Sprachversion sehr deutlich „such data“). Die richtige Rechtsgrundlage für den nicht-öffentlichen Bereich ist allein Artikel 114 Absatz 1 AEUV, der auch am Anfang des Verordnungsentwurfs zutreffend aufgeführt wird. Daraus ergeben sich weitreichende Konsequenzen für den Regelungsansatz der Verordnung, denn sie darf ausschließlich der Rechtsangleichung dienen. Es ist nicht Aufgabe der Europäischen Union, das Datenschutzrecht eigenständig zu verschärfen.

Artikel 1 Absatz 3 ist der bisherigen Richtlinie entnommen, aber berücksichtigt die Rechtsgrundlage ebenfalls nicht ausreichend. Es sollte deutlicher hervorgehoben werden (auch in den Erwägungsgründen 1 bis 11), dass die Verordnung im nicht-öffentlichen Bereich ausschließlich der Rechtsangleichung zum Zwecke der Verwirklichung und Herstellung der Funktionsfähigkeit des Binnenmarkts dient und dabei der Grundrechtsschutz zu berücksichtigen ist. Insbesondere sind in Erwägungsgrund 8 die Worte „ein hohes Maß an Datenschutz für den Einzelnen zu gewährleisten und“ zu streichen. Es gibt keine Rechtsgrundlage, die es der Europäischen Union erlaubt, für diesen Zweck Regelungen im Bereich des nicht-öffentlichen Datenschutzes zu treffen. Die Verordnung muss im Ergebnis der Verwirklichung des Binnenmarkts dienen und darf die Wirtschaft nicht unnötig behindern.

Artikel 1 Absatz 2: Es sollte stärker hervorgehoben werden, dass der grundrechtliche Schutz personenbezogener Daten nicht absolut gilt, sondern einer Abwägung mit anderen Grundrechten unterliegt. Dies gilt insbesondere im Hinblick auf die unternehmerische Freiheit. Dieser zentrale Grundgedanke wird bisher im Erwägungsgrund 139 nur sehr versteckt erwähnt und wird im Verordnungstext nicht berücksichtigt.

Artikel 2 Absatz 2 d): In der Ausnahme für persönliche und familiäre Verarbeitungszwecke wurde im Vergleich zur bisherigen Richtlinie der Zusatz „ohne jede Gewinnerzielungsabsicht“ eingefügt. Die Regelung ist für die Privatwirtschaft problematisch, da insbesondere im Internet und für Mobiltelefone zahlreiche Dienste angeboten

werden, die den Nutzern zu einer Verarbeitung zu persönlichen und familiären Zwecken dienen. Das zusätzliche Merkmal „ohne jede Gewinnerzielungsabsicht" führt hier zu unnötiger Rechtsunsicherheit darüber, was ausgenommene Verarbeitungen sind. Wenn bei diesen Diensten der Anwendungsbereich der Verordnung eröffnet würde, müssten alle Anforderungen an eine Auftragsverarbeitung eingehalten werden, was in der Praxis unmöglich ist. Heute verstehen wir sehr wohl eine Reihe von Datenverarbeitungen im geschäftlichen Bereich als „persönlich", auch wenn sie zumindest indirekt mit Gewinnerzielungsabsicht betrieben werden. Beispielsweise fällt ein persönliches elektronisches Telefonverzeichnis, das auch geschäftliche Kontakte enthält, bisher nicht unter den Anwendungsbereich der Richtlinie. Würde sich dies ändern, wären die sich daraus ergebenden Rechtspflichten in der Praxis nicht umsetzbar. Auch im familiären Bereich sollte eine untergeordnete Gewinnerzielungsabsicht (beispielsweise beim privaten Verkauf eines Autos) nicht zur Anwendung der Verordnung führen.

Artikel 3 Absatz 1: Es besteht unserer Ansicht nach kein sachlicher Grund dafür, die Verordnung bereits dann anzuwenden, wenn ein nicht-europäischer Auftraggeber einen Auftragsverarbeiter in der Europäischen Union einsetzt. Wir wissen zwar, dass dies auch heute schon teilweise so vertreten wird, aber es führt zu einem unnötigen Wettbewerbsnachteil europäischer Dienstleister. Wenn das Recht des Auftraggebers fordert, dass im Land des Auftragsverarbeiters ein angemessenes Schutzniveau gilt, dann kann dies vertraglich vereinbart werden. Als Alternative dazu könnten wir uns eine Lösung vorstellen, bei der Auftragsverarbeiter vertraglich die Anwendung der Verordnung ausschließen können, wenn die Verordnung auf den Auftraggeber ansonsten keine Anwendung findet. Auf diese Weise könnte der Auftraggeber nach den Vorgaben seines nationalen Rechts entscheiden, ob er den Schutz der Verordnung wünscht oder nicht. Eine ausdrückliche Regelung zu diesem Thema wäre wünschenswert. In jedem Fall sind die Worte „oder eines Auftragsverarbeiters" in Artikel 3 Absatz 1 und Erwägungsgrund 19 zu streichen.

Artikel 4: Wir gehen davon aus, dass die Definitionen in der Regel im Zusammenhang mit den Vorschriften besprochen werden, in denen sie Verwendung finden. Zu den wichtigsten Definitionen nehmen wir wie folgt Stellung:

Artikel 4 Absatz 1 und 2: Die Definitionen der „betroffenen Person" und „personenbezogener Daten" unterscheiden sich stark vom Ansatz der bisherigen Richtlinie, ohne dass für uns deutlich wird, ob im Ergebnis ein Unterschied zur bisherigen Richtlinie tatsächlich beabsichtigt ist. Auch die Erwägungsgründe 23 und 24 verdeutlichen dies nicht. Wir sind der Ansicht, dass es keinerlei Anlass für eine Änderung der bisher in Artikel 2 a) der Richtlinie enthaltenen Definition gibt. Diese sollte übernommen und die Erwägungsgründe 23 und 24 entsprechend überarbeitet werden. Jedenfalls sollten die Verweise auf „indirekte Mittel" und auf „jede sonstige natürliche oder juristische Person" in Artikel 4 Absatz 1 sowie auf „eine andere Person" in Erwägungsgrund 23 gestrichen werden. Die Erweiterung des Anwendungsbereichs auf im Grunde anonymisierte Daten würde ansonsten datenschutzfreundliche Verfahren, wie sie beispielsweise für die Markt- und Meinungsforschung, im Marketing oder in der Gesundheitsforschung in so genannten „Trustcentern" verwendet werden, verhindern. Die Streichung des Verweises auf andere Personen ist deshalb auch aus Gesichtspunkten des Datenschutzes wünschenswert, denn Trustcenterlösungen dienen dem Datenschutz und sollten durch die regulatorischen Rahmenbedingungen gefördert werden. Sie würde auch nicht dazu führen, dass die Kenntnisse Dritter in der Definition völlig unberücksichtigt blieben, denn wenn sie als „Mittel" nach allgemeinem Ermessen aller Voraussicht nach eingesetzt würden, dann würden sie auch berücksichtigt. Nur dies ist im Ergebnis auch sinnvoll.

Artikel 4 Absatz 1 a) und 2 a): Wir würden es begrüßen, wenn – nach dem Beispiel von § 3 Absatz 6 BDSG – eine Definition der Anonymisierung aufgenommen würde. Außerdem sollte der Begriff der Pseudonymisierung definiert werden. Beide Begriffe können dann entsprechend verwendet werden, um angemessene Sonderregelungen zu schaffen.

Artikel 4 Absatz 4: Der Anwendungsbereich auf nicht-automatisierte Verarbeitungen ist bereits nach der geltenden Richtlinie problematisch, weil beispielsweise ein nach Adressaten sortierter Stapel von Briefen unter den Anwendungsbereich fällt. Insofern ist die Formulierung in Erwägungsgrund 13 (Ädie in einem Ablagesystem gespeichert sindñ) zu begrüßen. Leider findet sich diese Einschränkung aber nicht in der Definition der Datei in Artikel 4 Absatz 4. Impraktikabel ist auch, dass die Verwendung jeder Art von Kriterien zur Sortierung einer Datei nun zur Anwendung der Verordnung führen soll. Wenn also beispielsweise ein Stapel adressierter Briefe nach der Postleitzahl des Wohnorts sortiert ist, würde dies bereits zur Anwendung der Verordnung und aller damit verbundenen Rechte und Pflichten führen. Nach der bisherigen Richtlinie muss es sich laut Erwägungsgrund 15 um Äpersonenbezogeneñ Kriterien handeln. Dies sollte beibehalten und auch ausdrücklich in der Definition des Begriffs ÄDateiñ aufgenommen werden. Auch für die Frage der Anwendung der Vorschrift auf Akten ist dies wichtig. Die Worte Änach bestimmten Kriterienñ sollten entsprechend durch Änach bestimmten personenbezogenen Kriterienñ ersetzt werden.

Artikel 4 Absatz 5: Eines der aktuellen praktischen Probleme der Auftragsverarbeitung liegt in Deutschland darin, dass für Auftragsverarbeitungsverträge unangemessen detaillierte Vorgaben des Auftraggebers hinsichtlich der ÄMittelñ der Verarbeitung gefordert werden. Datenschutzrechtlich haben diese bürokratischen Detaillierungen jedoch keinerlei Mehrwert. Sie haben aber Nachteile, denn jede Änderung der ÄMittelñ erfordert eine Vertragsänderung, d.h. wenn beispielsweise eine bestimmte technische Infrastruktur beschrieben ist, kann der Auftragsverarbeiter diese nur noch ändern, nachdem er dies mit allen seinen Auftraggebern vereinbart hat. Unter Datenschutzgesichtspunkten ist diese Beschränkung überflüssig. Wichtig ist nur, wer über die Zwecke der Verarbeitung entscheiden darf. Die Verpflichtung zur Schaffung angemessener technischer und organisatorischer Maßnahmen ist gesondert geregelt. Ansonsten ist es aus Datenschutzgesichtspunkten unerheblich, welche ÄMittelñ eingesetzt werden. Insofern sollte ï auch in Abweichung von der bisherigen Richtlinie und entsprechend der deutschen Regelung in § 11 BDSG ï der Verweis auf ÄMittelñ gestrichen werden. Auf jeden Fall

sollte der neu hinzugefügte Verweis auf ÄBedingungenñ gestrichen werden. Es ist unklar, was damit überhaupt gemeint ist. Die Neuregelung würde deshalb nur zu einer weiteren Bürokratisierung der Auftragsverarbeitung führen. Die Änderung sollte dann entsprechend auch in Artikel 4 Absatz 13 und Artikel 24 erfolgen.

Artikel 4 Absatz 7: Die Definition des ÄDrittenñ wurde im Vergleich zur alten Richtlinie gestrichen, so dass jetzt keine Differenzierung mehr zwischen ÄEmpfängernñ und ÄDrittenñ erfolgt. Eine solche Differenzierung ist auch nicht zwingend erforderlich. Wichtig ist aber, dass in den jeweiligen Regelungen insbesondere Auftragsverarbeiter nicht vom Begriff des ÄEmpfängersñ mit umfasst werden. Ansonsten wäre beispielsweise nach Artikel 14 Absatz 4 b) die betroffene Person zu informieren, bevor die Daten an einen Auftragsverarbeiter weitergegeben werden. Hierfür besteht kein sachlicher Grund. Auch ansonsten wird der Begriff des Empfängers so verwendet, dass eine Einbeziehung des Auftragsverarbeiters nicht sachgerecht wäre. Auch der Betroffene selbst sollte nicht hierunter fallen. In Anlehnung an die Definition zur Verarbeitung ist außerdem von einer Weitergabe durch Übermittlung zu sprechen. Ansonsten würde gegebenenfalls jede Weitergabe innerhalb eines Unternehmens mit umfasst. Dies ist auch schon bei der bestehenden Richtlinie problematisch und sollte jetzt korrigiert werden.

Artikel 4 Absatz 8: Die Voraussetzungen an eine wirksame Einwilligung sollten möglichst konsistent in Artikel 7 geregelt werden. Jedenfalls ist aber das Wort Äexplizitñ zu streichen, da auch konkludente Einwilligungen möglich sein müssen. Das zusätzliche Merkmal Äeindeutigeñ Handlung könnte ebenfalls Verhaltensweisen ausschließen, die unter zivilrechtlichen Grundsätzen eine Willenserklärung darstellen. Die Rechtsordnung sollte in diesen Punkten konsistent sein. Außerdem sollte ausdrücklich die Möglichkeit eingeräumt werden, dass ein Vertreter die Einwilligung erklärt. Des Weiteren verweisen wir auf unsere Ausführungen zu Artikel 7.

Artikel 4 Absatz 9: Zum Begriff der Verletzung des Schutzes personenbezogener Daten werden wir im Rahmen von Artikel 31 Stellung nehmen. Es sei aber schon

hier darauf hingewiesen, dass die Definition viel zu weitgehend ist. Warum soll beispielsweise die „Vernichtung", der „Verlust" oder die „Veränderung" von Daten zu einer Meldepflicht führen, solange die Daten dabei nicht einem Dritten zugänglich gemacht werden? Außerdem kann die Definition etwas klarer formuliert und verschlankt werden.

Artikel 4 Absatz 10 und 11: Die Definitionen sind in einer Weise formuliert, dass ihr Anwendungsbereich kaum noch erfassbar wäre. Sie sollten deshalb eingeschränkt werden. Ansonsten würde beispielsweise jedes Bild einer Person sowohl unter den Begriff der genetischen als auch der biometrischen Daten fallen.

Artikel 4 Absatz 12: Bei Gesundheitsdaten sollten Einschränkungen überlegt werden, denn nach der vorliegenden Definition (wie auch nach der bisherigen Richtlinie) fallen für jedermann offensichtliche Daten hierunter - wie beispielsweise die Tatsache, dass ein Brillenträger eine Sehschwäche hat. Gesundheitsdaten sollten nur besonders geschützt werden, wenn sie auch einen sensiblen Charakter haben. Dies wäre auch in Erwägungsgrund 29 zu berücksichtigen.

Artikel 4 Absatz 13: Der Begriff der Hauptniederlassung sollte auch eine Lösung für die Fallgestaltung der Benennung eines inländischen Vertreters bereithalten. Die Begriffe „Bedingungen und Mittel" sind entsprechend der Definition der Auftragsverarbeitung zu streichen (siehe Anmerkung Artikel 4 Absatz5).

Artikel 4 Absatz 13 a): Wir sind der Ansicht, dass es eine Möglichkeit für Unternehmen geben sollte, die Hauptniederlassung und die datenschutzrechtlich konsolidierten selbstständigen Niederlassungen selbst (in transparenter Weise) zu bestimmen. Ähnlich wie im Steuerrecht könnte so eine dringend erforderliche Konzernregelung geschaffen werden, die Unternehmen nutzen können, aber nicht müssen. Dies würde auch komplizierte Definitionsfragen vermeiden, denn die Abgrenzung würde durch Entscheidung der Unternehmen in klarer Weise und transparent erfolgen. Durch eine vertragliche Verpflichtungserklärung würden die internen Verhältnisse geklärt, so dass die Hauptniederlassung die datenschutz-

rechtlichen Verpflichtungen intern durchsetzen kann. Entsprechend müsste dieses Konzept in die Definition des Unternehmens einfließen.

Artikel 4 Absatz 18: An verschiedenen Stellen wird der Begriff „Kind" verwendet, obwohl er auch Jugendliche mit ausreichender Entscheidungsfähigkeit und Eigenverantwortlichkeit umfasst. Sonderregelungen zum Schutz von Kindern sollten aber nicht so weitreichend gelten. Die Grenze des 13. Lebensjahrs sollte verwendet werden. Außerdem muss entscheidend sein, ob der für die Verarbeitung Verantwortliche Kenntnis vom Alter des Kindes hat. Andernfalls müssten die Regelungen zu Kindern insbesondere im Internet immer Anwendung finden, was nicht praxisgerecht wäre.

Artikel 3 neuer Absatz 18: Der Begriff des unverhältnismäßigen Aufwands sollte einheitlich definiert werden.

Artikel 5: Der Regelungswert der „Grundsätze" neben den Rechtmäßigkeitsanforderungen sollte überdacht werden. Dabei ist zu beachten, dass die Grundsätze im Gegensatz zum bisherigen Artikel 6 Absatz 1 der Richtlinie nach dem Vorschlag der Verordnung ohne jede Ausnahme gelten sollen (es sei denn, die Mitgliedstaaten schaffen eine solche Ausnahme nach Artikel 21). Nur Artikel 5 c) ist auf „angemessene" Maßnahmen beschränkt. Wenn die Grundsätze aber ohne jede Berücksichtigung des damit verbundenen Aufwands einzuhalten sind, werden sie für die Wirtschaft zu einer unzumutbaren Belastung.

Artikel 5 b): Neben den Rechtmäßigkeitstatbeständen ist eine gesonderte Zweckbindung nicht mehr zeitgemäß und führt in der Praxis nur zu überflüssigen und für die Betroffenen belästigenden Mehrfacherhebungen von Daten.

Artikel 5 c): Hier sollte die Möglichkeit der Anonymisierung oder Pseudonymisierung in Anlehnung an § 3 a) BDSG aufgenommen werden, wobei die Frage der Verhältnismäßigkeit der Maßnahme von großer Bedeutung ist.

Artikel 5 d): Die Regelung ist auf angemessene Maßnahmen zu beschränken.

Artikel 5 e): Die Regelung ist auf angemessene Maßnahmen zu beschränken.

Artikel 5 f): Hier wird dem für die Verarbeitung Verantwortlichen die allgemeine Beweislast für die Einhaltung der Verordnung auferlegt. Dies würde bedeuten, dass jeder Vorwurf eines Verstoßes gegen irgendeine der Vorschriften der Beweislastumkehr unterliegen würde. Im Ergebnis ist ein solcher Eingriff in die nationalen Beweislastregeln nicht gerechtfertigt. Von dieser Regelung dürfen die Mitgliedstaaten auch keine Ausnahmen erlassen (siehe Artikel 21 Absatz 1, der nur auf die Buchstaben a) bis e) verweist). Die Regelung ist zu streichen.

Artikel 6 Absatz 1: Der zentrale Grundsatz des Datenschutzrechts liegt in der Abwägung der berechtigten Interessen. Es sollte überlegt werden, ob dies zur Grundregel gemacht werden sollte und Absätze a) bis e) zu Fallbeispielen eines überwiegenden Interesses des für die Verarbeitung Verantwortlichen. Auch das Prinzip des Verbots mit Erlaubnisvorbehalt sollte in diesem Zusammenhang überdacht werden. Man könnte beispielsweise überlegen, ob die Rechtmäßigkeitsanforderungen grundsätzlich nur erforderlich sind, wenn ein schutzwürdiges Interesse des Betroffenen beeinträchtigt ist. Nur dann besteht auch die Notwendigkeit der gesetzlichen Einschränkung. Die Regulierung würde auf die Bereiche beschränkt, in denen tatsächliche Risiken für die betroffenen Personen bestehen. Artikel 5 Absatz 1 d) könnte dann konsequenterweise gestrichen werden.

Artikel 6 Absatz 1 a): Die Anforderungen an wirksame Einwilligungen werden in der Definition der Einwilligung, in Artikel 7 und in Artikel 6 Absatz 1 a) festgelegt und an jeder dieser Stellen verschärft. Die Formulierung ÄDie betroffene Person hat ihre Einwilligung gegeben.ñwürde hier ausreichen. Zumindest sollte der definierte Begriff verwendet und die Einheitlichkeit der Rechtsgrundlagen sichergestellt werden. Das Wort Ägenauñist zu streichen (in der deutschen Fassung werden hier und in Artikel 7 sogar versehentlich unterschiedliche Wörter verwendet: Ägenauñund Äeindeutigñ).

Artikel 6 Absatz 1 b): Der Text zum Vertragsverhältnis entspricht dem der bisherigen Richtlinie. Vor dem Hintergrund der deutschen Erfahrungen sollte aber überlegt werden, ob Drittberechtigte und rechtsgeschäftsähnliche Beziehungen mit aufzunehmen sind, die ja nicht nur vorvertraglich bestehen können. Dies gilt beispielsweise bei Verträgen mit Schutzwirkung für Dritte.

Artikel 6 Absatz 1 f): Im Vergleich zur bisherigen Richtlinie können die Interessen „Dritter", denen die Daten übermittelt werden sollen, im Rahmen der Interessenabwägung nicht mehr berücksichtigt werden. Damit wird § 29 BDSG praktisch gestrichen und es werden alle damit verbundenen wirtschaftlichen Betätigungsfelder abgeschafft. Dies gilt für den Bereich des Marketings bis hin zu Kreditauskunfteien. Außerdem wäre die Arbeitsteilung zwischen Datenanbietern und den Empfängern der Daten nicht mehr zulässig. Die Konsequenzen einer solchen Einschränkung für die Wirtschaft wären fatal. Eine weitere neue Einschränkung besteht darin, dass die Anwendung der Interessenabwägungsklausel für Kinder (unter 18) abgeschafft wird. In der Konsequenz werden damit auch Verarbeitungen verboten, die im überwiegenden Interesse der Kinder liegen. Es ist kein Grund ersichtlich, warum eine solche Einschränkung vorgenommen wird. Außerdem sollten nur „schutzwürdige" Interessen des Betroffenen in die Interessenabwägung eingehen.

Artikel 6 Absatz 1 g): Wir halten es für dringend angeraten, eine Rechtsgrundlage zur Erfüllung der Verpflichtungen nach Artikel 5 einzufügen, um das Verhältnis zwischen den Grundsätzen und den Rechtsgrundlagen zu klären.

Artikel 6 Absatz 4: Die Zweckbindungsregelung verweist nicht auf die Interessenabwägungsklausel (es wird nur auf Absatz 1 Buchstabe a) bis e) verwiesen und nicht auf Buchstabe f). Damit wird die Zweckbindung im Vergleich zum deutschen Bundesdatenschutzgesetz erheblich verschärft, denn selbst wenn kein überwiegendes schutzwürdiges Interesse der betroffenen Person vorliegt, müsste für die Zweckänderung eine Einwilligung eingeholt werden. Auch die geltende Richtlinie wird so ausgelegt, dass bei Zweckänderungen eine neue Rechtsgrundlage nur erforderlich ist, wenn die Änderungen nicht mit den

ursprünglichen Zwecken vereinbar sind. So ist es auch im Bundesdatenschutzgesetz umgesetzt. Ein Grund für die vorgeschlagene Verschärfung ist nicht ersichtlich und gegebenenfalls handelt es sich auch um ein Verweisungsversehen. Die vorliegende Regelung könnte wegen des fehlenden Verweises auf Buchstabe f) so verstanden werden, dass die Zweckänderung zur Verwendung zu Werbezwecken nur mit Einwilligung zulässig wäre. Eine solche Beschränkung der Werbemöglichkeiten sollte aber gerade nicht erfolgen, denn sie käme zum selben Ergebnis wie der gestrichene allgemeine Einwilligungsvorbehalt für kommerzielles Direktmarketing. Die Klausel sollte deshalb insgesamt auf Absatz 1 verweisen. Wenn man die von uns vorgeschlagene Änderung in Artikel 5 b) durchführen würde, könnte man Absatz 4 auch ganz streichen.

Artikel 6 Absatz 5: Die Interessenabwägungsklausel ist ein zentrales Element im Datenschutzrecht, mit der viele sinnvolle und berechtigte Verarbeitungen erlaubt werden. Viele Geschäftskonzepte und Geschäftsprozesse beruhen hierauf. Der Europäischen Kommission für die Auslegung die Befugnis zu delegierten Rechtsakten zu geben, käme der Übertragung einer wesentlichen Gesetzgebungsbefugnis gleich. Dies ist nicht akzeptabel. Die Rechtsetzung in diesem Bereich sollte weiterhin dem ordnungsgemäßen parlamentarischen Verfahren unterworfen werden, auch um einen gewissen Grad an Investitionssicherheit für die Wirtschaft zu gewährleisten.

Artikel 7: Hohe Anforderungen an die Wirksamkeit und Nachweisbarkeit von Einwilligungserklärungen führen dazu, dass sie nur in Ausnahmefällen eine geeignete Rechtsgrundlage darstellen können. Eine gleichzeitige Verbreiterung des Anwendungsbereichs der Einwilligung und Erhöhung ihrer Wirksamkeitsvoraussetzungen ist in der Praxis nicht verkraftbar. Nur wenn die Einwilligungserklärung tatsächlich sehr sensiblen Vorgängen vorbehalten bleibt, dürfen hier auch hohe Anforderungen gestellt werden. Ansonsten kann informationelle Selbstbestimmung auch durch das Widerspruchsrecht praktiziert werden. In jedem Fall halten wir es aber für verfehlt, durch die Verwendung von Begriffen wie Ăeindeutigñ oder Ăgenauñ die Verwender von Einwilligungserklärungen zur Verwendung langer und

unübersichtlicher Einwilligungstexte zu zwingen. Außerdem sollten auch konkludente Einwilligungen möglich sein (siehe Anmerkung zu Artikel 4 Absatz 8). Besonders wichtig ist, dass mit neuen zusätzlichen Voraussetzungen nicht Milliarden von bereits eingeholten Einwilligungen plötzlich unwirksam werden. Hierfür sind zumindest Übergangsregelungen zu schaffen.

Artikel 7 Absatz 2: Die Regelung ist unklar formuliert. Wenn eine Hervorhebung erwartet wird, sollte dies auch so geregelt werden. Es sollte jedoch auch bedacht werden, ob das Erfordernis der Hervorhebung angemessen ist. Zahlreiche Gesetze fordern für unterschiedliche Regelungen Hervorhebungen, so dass diese in der Praxis kaum noch durchführbar sind.

Artikel 7 Absatz 3: Die jederzeitige Widerrufbarkeit von Einwilligungen ist problematisch, wenn die Einwilligung Teil eines gegenseitigen Geschäfts ist oder wenn auf Grund der Einwilligung Daten an Dritte weitergegeben oder veröffentlicht wurden. In der Praxis sind diese Widerrufe nicht umsetzbar. Es muss außerdem eine Umsetzungsfrist eingeräumt werden, da Widerrufe allein rein technisch nicht sofort mit ihrem Empfang berücksichtigt werden können.

Artikel 7 Absatz 4: Die Regelung zum Ungleichgewicht ist zu streichen. Die Definition der Einwilligung sieht bereits vor, dass die Einwilligung ohne jeden Zwang zu erteilen ist. Diese Grenze muss ausreichend sein. Anderenfalls würde Unternehmen mit einer starken Marktmacht gegebenenfalls vollständig die Möglichkeit genommen, für die Verarbeitung ihrer Daten Einwilligungen einzuholen (beispielsweise für E-Mail-Werbung).

Artikel 8: Es ist für uns nicht nachvollziehbar, zu welchem Ergebnis die Einschränkung von Absatz 1 durch Absatz 2 in Deutschland kommen würde. Es sollte nur die Frage der Zulässigkeit der Einwilligung geregelt werden. Die Regelung darf aber nicht in Situationen greifen, in denen überhaupt keine Kinder angesprochen werden. Ansonsten müssten alle Nutzer wie Kinder behandelt werden. Dies wäre in der Praxis unmöglich. Insofern sollte sie auf Situationen beschränkt

werden, in denen das Angebot sich speziell an Kinder richtet. Im Hinblick auf die Altersprüfung ist festzulegen, dass der für die Verarbeitung Verantwortliche berechtigt, aber nicht verpflichtet ist, Daten zu verarbeiten. Ansonsten wäre jede Art der Altersverifikation unmöglich, denn ohne die Verarbeitung personenbezogener Daten funktioniert sie nicht.

Artikel 9 Absatz 1: Wie bereits unter der geltenden Richtlinie wird die Verarbeitung von besonderen Kategorien von Daten unabhängig von ihrer individuellen Sensibilität untersagt. Der Ansatz führt zu unangemessenen Beschränkungen von Datenverarbeitungen. Es sollte überlegt werden, ob insbesondere Artikel 9 Absatz 2 e) im Anwendungsbereich erweitert werden kann. In der Verordnung sollte es vermieden werden, nicht sensiblen Daten den verstärkten Schutz für „besondere Arten von personenbezogenen Daten" zu gewähren. Dies kann nicht nur davon abhängen, ob sie die betroffene Person selbst öffentlich gemacht hat.

Artikel 9 Absatz 2: Die Ausnahmen zum Verbot der Verarbeitung besonderer Arten von Daten sind unangemessen streng. Schon die bisherige Datenschutzrichtlinie ist in dieser Hinsicht nicht praktikabel. Ausgehend von den Rechtmäßigkeitstatbeständen in Artikel 6 Absatz 1 ist zu prüfen, ob hiervon Einschränkungen angezeigt sind. Unserer Ansicht nach könnte Absatz 2 vollständig gestrichen und durch eine kurze Regelung in Absatz 1 ersetzt werden, in der festgestellt wird, wann abweichend von Artikel 6 Absatz 1 b) bis f) eine Einwilligung einzuholen ist. Die Inkonsistenz zwischen Artikel 9 Absatz 2 und Artikel 6 Absatz 1 bereitet ansonsten unnötige praktische Anwendungsprobleme.

Artikel 10: Die Vorschrift ist vom Ansatz her zu begrüßen, sollte aber so formuliert werden, dass sie nicht auf anonymisierte Daten beschränkt ist. Derzeit findet die Vorschrift nur dann Anwendung, wenn die Verordnung an sich keine Anwendung findet, was im Ergebnis inkonsistent ist. Die Klausel sollte auch klarstellen, welche Konsequenzen sie für die Einhaltung der Verpflichtungen aus der Verordnung hat.

Artikel 11 Absatz 1: Transparenz und verständliche Information sind richtige und akzeptable Grundsätze. Die Ausführung der Verpflichtungen muss sich aber auf einen angemessenen Aufwand beschränken. Absatz 1 fordert eine für Ăjedermann leicht zugängliche Strategieñ In der englischen Sprachfassung wird diese als ĂPolicyñ bezeichnet. Für Internetdienste sind Datenschutzinformationen üblich, die teilweise auch als Policies bezeichnet werden. Die vorliegende Klausel gilt aber für jedes kleine und mittelständische Unternehmen und für alle Aspekte der Verarbeitung von personenbezogenen Daten in diesen Unternehmen (insbesondere Kunden-, Lieferanten- und Mitarbeiterdaten). In der Praxis ist dies nur mit hohem Aufwand umsetzbar, ohne dass ein besonderer Mehrwert für die betroffenen Personen erkennbar ist. Die Klausel ist deshalb anzupassen.

Artikel 11 Absatz 2: Verständliche Datenschutzinformationen sind ein gutes Ziel, wobei die vorgeschlagene Detailtiefe der Informationspflichten und die Anforderungen an wirksame Einwilligungen gerade dieses Ziel in Frage stellen. Nicht zuletzt sollte auch der Text der Verordnung der Zielsetzung entsprechend einfach und verständlich gestaltet werden. Dies würde im ersten Schritt eine wesentliche Verschlankung des Verordnungsentwurfs erfordern. In Absatz 2 sollte klargestellt werden, dass sich die Vorschrift auf Informationen und Mitteilungen bezieht, die nach der Verordnung bereitzustellen sind. Andernfalls könnte der Eindruck entstehen, Absatz 2 wolle einen eigenen Informationsanspruch begründen.

Artikel 12 Absatz 1: Datenschutzrechtliche Informationsansprüche bergen ein hohes Missbrauchsrisiko. Eines der großen praktischen Probleme bei der Ausübung von Betroffenenrechten besteht deshalb in der zuverlässigen Identifizierung der betroffenen Personen. Vor diesem Hintergrund ist es äußerst problematisch, dass die Verordnung ihren Anwendungsbereich auf Daten erweitert, bei denen der für die Verarbeitung Verantwortliche die betroffene Person nicht identifizieren kann (siehe Anmerkungen zu Artikel 4 Absätze 1 und 2 sowie zu Artikel 10). Da Absatz 2 ausdrücklich elektronische Auskunftsverfahren fordert, verstärkt sich das Problem. Häufig lässt sich nur die postalische Adresse verifizieren (beispielsweise über eine

Ausweiskopie). Außerdem ist der beabsichtigte Regelungsgehalt von Absatz 1 Satz 2 nicht verständlich. Der Satz sollte gestrichen werden.

Artikel 12 Absatz 2: Angesichts der unterschiedlichen Konstellationen, in denen Unternehmen Informationspflichten nachkommen müssen, verbietet sich eine feste Frist. Es gibt auch keine Anhaltspunkte dafür, dass die bisher existierenden Regelungen in dieser Frage zu praktischen Problemen für die Auskunftsanfragenden geführt haben. Insofern besteht auch kein Anlass für die Festlegung einer festen Frist. Da die Verordnung weitgehend auch für Akten gilt und auch die Aufbereitung elektronischer Datenbestände nicht immer einfach ist (insbesondere dann, wenn Daten Dritter zu schwärzen sind), sollte es nur eine Frist für eine Statusmitteilung geben. Die Ausnahme von der Monatsfrist ist allgemeiner zu formulieren, denn problematisch sind nicht nur Fälle von Auskunftshäufungen. Ob die Auskunftserteilung schriftlich oder elektronisch erfolgt, sollte dem für die Verarbeitung Verantwortlichen überlassen bleiben. Eine Verpflichtung zur Erteilung schriftlicher Auskünfte ist sicher nicht zukunftsorientiert.

Artikel 12 Absatz 4: Der Grundsatz der kostenlosen Rechtewahrnehmung ist in der Praxis gescheitert, denn automatisierte Auskunftsanfragetools missbrauchen das Recht zur kostenlosen Auskunft. Insofern sollte der in Deutschland derzeit praktizierte Ansatz überdacht werden. Außerdem darf die Regelung nicht zur kostenlosen Erbringung wirtschaftlich nutzbarer Leistungen verpflichten, wenn solche unter dem Vorwand der Ausübung datenschutzrechtlicher Vorschriften eingefordert werden. Der Anspruch auf Datenportabilität, wenn er überhaupt bestehen bleiben sollte (siehe Anmerkung zu Artikel 18), ist kein datenschutzrechtlicher, sondern ein rein wirtschaftlicher Anspruch, der auch entsprechend vergütet werden sollte. Die Beweislastregelung ist hier unpassend, denn den für die Verarbeitung Verantwortlichen trifft die gesetzliche Beweislast, wenn er sich auf eine Ausnahme vom Auskunftsanspruch beruft.

Artikel 12 Absätze 5 und 6: Die Rechtsetzungsbefugnisse der Europäischen Kommission sollten gestrichen werden.

Artikel 12 neuer Absatz 5: In Erwägungsgrund 45 wurde ein sehr wichtiger Grundsatz aufgenommen, nach dem die betroffene Person Informationen bereitstellen muss, damit der für die Verarbeitung Verantwortliche die bei ihm zu der Person gespeicherten Daten auffinden kann. Dieser Grundsatz muss in Artikel 12 eingefügt werden. Der Erwägungsgrund allein ist keine durchsetzbare Anspruchsgrundlage.

Artikel 12 neuer Absatz 6: Es sollte keine Pflicht zur Durchführung von Unterrichtungen oder Maßnahmen bestehen, wenn der Aufwand unverhältnismäßig wäre oder überwiegende Interessen dagegen sprechen.

Artikel 13: Datenqualität ist im Sinne aller Beteiligten, aber eine generelle Verpflichtung zur Mitteilung von Berichtigungen und Löschungen an Empfänger von Daten ist realitätsfremd. Zusätzlich birgt sie die Gefahr, dass Empfänger Berichtigungen erhalten, obwohl sie die Daten bereits gelöscht haben. Dies wäre aus Datenschutzgesichtspunkten nicht wünschenswert. Der vorgeschlagene Anspruch betrifft darüber hinaus jede Art der Übermittlung, unabhängig davon, wie lange sie her ist oder ob schutzwürdige Interessen der betroffenen Personen berührt sind. Auch dies ist praxisfern. Die Vorschrift sollte stattdessen so gestaltet werden, dass dem für die Verarbeitung Verantwortlichen die Information der Empfänger grundsätzlich erlaubt ist, aber eine Pflicht zur Information nur dann besteht, wenn die betroffene Person die Erteilung der Information an die Empfänger konkret verlangt, die Übermittlung nicht länger als 12 Monate her ist und weitere Voraussetzungen erfüllt sind. Außerdem sollte sich der Anspruch auf die Berichtigung beschränken, denn ob bei einer Löschung die Rechtsgrundlage für den Empfänger entfällt, ist eine Frage des Einzelfalls. Nicht zuletzt ist auch der Begriff des ÄEmpfängersñ zu weitgehend, da er auch Auftragsverarbeiter und die betroffene Person selbst umfasst.

Artikel 14: Die vorgeschlagenen Informationspflichten orientieren sich an den technischen Möglichkeiten von Internetdiensten, die eigene Datenschutz-

informationen in beliebiger Länge in ihre Dienste integrieren können. Für andere Bereiche ist die Regelung schon in ihrem Ansatz nicht praktikabel. Dies liegt am Zeitpunkt und dem Umfang der Information sowie an den unzureichenden Ausnahmen. Artikel 21 Absatz 1 f) würde es den Mitgliedstaaten erlauben, in diesen Fragen später noch nachzubessern. Es sollte aber Ziel der Verordnung sein, die Rahmenbedingungen der Informationspflichten von Anfang an in praktikabler Weise zu regeln. Insofern kann mit Blick auf Artikel 21 nicht auf angemessene Ausnahmen verzichtet werden. Ein modernes Datenschutzrecht muss realisieren, dass elektronische Datenverarbeitung in der Informationsgesellschaft der Normalfall ist. Anders als der Gesetzgeber in den frühen Jahren des Datenschutzrechts dachte, muss vor elektronischer Datenverarbeitung nicht mehr gewarnt werden. Es muss auch nicht mehr auf Selbstverständlichkeiten hingewiesen werden. Das Instrument der Informationspflicht ist zu reformieren und auf Fälle zu beschränken, in denen auf Grund der mit der Verarbeitung verbundenen Risiken konkrete Informationsbedürfnisse bestehen. Der Vorschlag der Europäischen Kommission verweigert sich der Modernisierung, indem er die bestehenden Informationspflichten weder in Frage stellt noch mit ausreichenden Ausnahmen versieht. Stattdessen werden die Informationspflichten mit weiteren bürokratischen Anforderungen versehen. Dies wäre aus Modernisierungsgesichtspunkten ein klarer Rückschritt.

Bereits die Benachrichtigungspflichten im Bundesdatenschutzgesetz sind vor diesem Hintergrund zu weitgehend und angesichts des Automatisierungsgrads der Datenverarbeitung nicht mehr zeitgemäß. Die Regelung geht davon aus, dass elektronische Datenverarbeitung eine überraschende Besonderheit darstellt, was aber offensichtlich seit vielen Jahren nicht mehr der Fall ist. Außerdem liegt ihr die Vorstellung zugrunde, dass jede Verarbeitung klar definiert ist. Dies war noch der Fall, als sich Datenverarbeitung auf simple Datenbanken beschränkte. Für die Verarbeitung unstrukturierter Daten in E-Mail-Systemen, Word- oder Excel-Dateien ist dies aber unmöglich. Die Informationspflichten sind insofern zu modernisieren und auf ein realistisches Mindestmaß zu reduzieren.

Artikel 14 Absatz 1: Bei der allgemeinen Informationspflicht sollte bedacht werden, dass diese den betroffenen Personen völlig unabhängig von ihrem konkreten Interesse hieran oder ihrem allgemeinen Wissensstand aufgedrängt wird. Deshalb muss die Information schlank gestaltet werden. Vor allem aber sollte es erlaubt sein, auf detailliertere Informationen an anderer Stelle zu verweisen. Beispielsweise sollte ein Hinweis genügen, wie die betroffene Person nähere Informationen frei zugänglich erhalten kann. Im Internet wäre dies der Link auf die Datenschutzinformation. Auch außerhalb des Internets könnte auf Quellen im Internet verwiesen werden.

Die Regelung könnte im Ergebnis so aussehen, dass über die Tatsache der Verarbeitung und deren Zwecke zu informieren ist, soweit die betroffene Person nach den Umständen des Einzelfalls nicht mit der Verarbeitung rechnen muss. Die Frage des mit der Information verbundenen Aufwands sollte auch Berücksichtigung finden. Außerdem sollte eine weitgehende Ausnahme für den geschäftlichen Bereich (B2B) aufgenommen werden.

Weiterhin stellt sich die Frage, warum der Katalog der Informationsinhalte erweitert wurde. Es ist nicht ersichtlich, dass sich hier in der Praxis entsprechende zusätzliche Informationsbedürfnisse ergeben hätten. Im Gegenteil ist es so, dass lange und unübersichtliche Datenschutzinformationen als wenig hilfreich angesehen werden. Dies gilt vor allem dann, wenn sie sehr allgemeine Informationen enthalten, die sich in jeder Datenschutzinformation wiederholen, obwohl sie der Allgemeinheit ohnehin bekannt sind.

Artikel 14 Absatz 1 c): Die Information über die Dauer der Verarbeitung (Absatz 1 c)) kann in der Regel nicht schon bei der Erhebung gegeben werden. Man müsste für unterschiedliche Daten (wie beispielsweise Geschäftsbriefe, Rechnungen, Bestellunterlagen oder Marketinginformationen) die Aufbewahrungsfristen im Detail erläutern. In einer normalen Geschäftsbeziehung müssten damit seitenweise Informationen gegeben werden, die für die betroffene Person kaum Wert haben. Die Regelung ist zu streichen.

Artikel 14 Absatz 1 d) und e): Die Aufklärung über Betroffenenrechte würde bereits nach kurzer Zeit zu einer formelhaften Information ohne Neuigkeitswert für die betroffenen Personen. Es bestehen keine Anhaltspunkte dafür, dass es in der Praxis diesbezüglich ein Informationsdefizit gäbe. In den weitergehenden Datenschutzinformationen könnte man einen entsprechenden Passus aber aufnehmen.

Artikel 14 Absatz 1 f): Die bereits heute bestehende Informationspflicht über ÄKategorien von Empfängernñ bereitet in der praktischen Umsetzung Probleme, die im Rahmen der Verordnung gelöst werden sollten. ÄEmpfängerñ im Sinne der Verordnung sind auch Auftragsverarbeiter. Es besteht kein Grund dafür, dass diese in die Informationspflicht aufgenommen werden. Jeder weiß, dass Unternehmen in ihrer Verwaltung Dienstleister einsetzen.

In Deutschland wird das Problem bisher damit gelöst, dass mit einer grundsätzlichen Kenntnis der betroffenen Personen von der arbeitsteiligen Datenverarbeitung gerechnet wird. Besser wäre es jedoch, wenn an dieser Stelle von Anfang an Auftragsverarbeiter ausdrücklich von der Definition der ÄEmpfängerñ ausgenommen würden.

Artikel 14 Absatz 1 g): Die Information über beabsichtigte Drittlandtransfers ist angesichts der internationalen Vernetzung der Datenverarbeitung kaum durchführbar. Entscheidend ist unserer Ansicht nach, dass die Rechte der betroffenen Personen gewahrt bleiben. Dies wird durch die Drittländertransferregelungen abgesichert. Eine besondere Information über den Datentransfer ist überflüssig und würde bei entsprechender Detaillierung (insbesondere der Nennung der einzelnen Länder, der einzelnen betroffenen Daten und der Angemessenheitsentscheidungen der Europäischen Kommission) zu einem extrem aufwendigen Unterfangen ohne erkennbaren Nutzen für die betroffene Person.

Artikel 14 Absatz 1 h): Die Verpflichtung zur Bereitstellung sonstiger Informationen ist ein Einfallstor für zusätzliche Datenschutzbürokratie, die dann nach Absätzen 7

und 8 durch die Europäische Kommission festgelegt würde. Die Regelung ist zu streichen. Es sind keine Gründe dafür ersichtlich, warum es dieser Ausweitung und der dazugehörigen Rechtsetzungsbefugnisse der Europäischen Kommission bedarf. Am Ende müsste sich jedes kleine und mittelständische Unternehmen nicht nur an die bereits komplizierten Pflichten der Verordnung halten, sondern auch den in unzähligen delegierten Rechtsakten der Europäischen Kommission geregelten zusätzlichen Informationspflichten nachkommen. Die Europäische Kommission sollte stattdessen ihrem selbst gesetzten Ziel folgend bürokratische Verpflichtungen abbauen und sich nicht Rechte zu ihrem weiteren Ausbau einräumen.

Artikel 14 Absatz 2: Die Differenzierung zwischen gesetzlich vorgeschriebenen und sonstigen Angaben ist in der Praxis nicht einfach umsetzbar, findet sich aber bereits in § 4 Absatz 3 Satz 2 BDSG. Die Verordnung geht darüber hinaus und spricht von Äobligatorischñ, statt Ägesetzlich vorgeschriebenñ. Insofern sollte die Verordnung nach dem deutschen Beispiel klargestellt werden. Besser wäre es jedoch, wenn auch weitere Rechtsgrundlagen Ausnahmen von der Informationspflicht begründen würden. Dies würde dem Gedanken Rechnung tragen, dass diese Verarbeitungen der Normallfall sind, mit dem die betroffenen Personen rechnen.

Artikel 14 Absatz 3: Wenn die Daten nicht bei der betroffenen Person erhoben werden, kann es die betroffenen Personen im Einzelfall interessieren, woher die Daten stammen. Es besteht aber kein Anlass dazu, die Herkunft bereits ungefragt in jede Datenschutzinformation aufzunehmen. Da die Herkunftsangabe eine auf die konkreten Daten individuell zugeschnittene Information ist, wäre dies auch nicht so einfach möglich, weil verschiedene Herkunftsangaben für einzelne Daten möglich sind. Außerdem könnte die Information im Einzelfall sensibel sein.

Artikel 14 Absatz 4 a): Hinsichtlich des Informationszeitpunkts sollte berücksichtigt werden, dass Erhebungen beispielsweise auf Coupons oder auf Postkarten stattfinden. Transparenz muss also auch in der Weise möglich sein, dass unmittelbar nach der Erhebung der Daten bei der betroffenen Person diese entsprechend informiert wird. Insofern sollte eine Ärzeitnaheñ Information ausreichen, statt auf den

Zeitpunkt der Erhebung abzustellen. Buchstabe a) sollte gestrichen und Buchstabe b) zur Grundregel erklärt werden. Besonders bei der Erhebung von Dritten ist dies wichtig, denn die Speicherung bei dem für die Verarbeitung Verantwortlichen ist Voraussetzung für die praktische Durchführung der Information.

Artikel 14 Absatz 4 b): Der Zeitpunkt der Information im Falle der beabsichtigten Weitergabe an den Empfänger entspricht nicht der deutschen Regelung in § 33 Absatz 1 Satz 2 BDSG. Während die deutsche Regelung auf die ÄÜbermittlungñ abstellt, knüpft die Verordnung an die Weitergabe an den ÄEmpfängerñ an. Jeder Auftragsverarbeiter wäre ein solcher Empfänger (siehe Anmerkung zur Artikel 4 Absatz 7). Dies würde dazu führen, dass beispielsweise Auskunfteien, die Auftragsverarbeiter einsetzen, bereits bei jeder Erhebung von Daten informieren müssten. Dies wäre in der Praxis nicht möglich.

Artikel 14 Absatz 5: Die Ausnahmen zur Benachrichtigungspflicht sind nicht ausreichend. Es ist zu berücksichtigen, dass elektronische Datenverarbeitung heute wesentlich üblicher und allgemein bekannter ist, als dies früher noch der Fall war (siehe Anmerkung zu Artikel 14 Absatz 1). Eine generelle Ausnahme wäre angemessen, wenn die betroffene Person nach den Umständen des Einzelfalls nicht mit der Verarbeitung rechnen muss. Außerdem sollte eine Ausnahme existieren, wenn überwiegende Interessen daran bestehen, von der Auskunft abzusehen. Insofern greift auch der bestehende § 33 Absatz 2 BDSG zu kurz. Die Ausnahme in Artikel 14 Absatz 5 d) ist unverständlich.

Artikel 14 Absatz 6: Es ist nicht erkennbar, welche Maßnahmen hier erwartet werden. Die Vorschrift ist zu streichen.

Artikel 14 Absätze 6 und 7: Die Rechtsetzungsbefugnisse der Europäischen Kommission sind zu streichen.

Artikel 15 Absatz 1 und 2: Die betroffene Person sollte ihre Auskunftsverlangen spezifizieren und damit dem für die Verarbeitung Verantwortlichen die Möglichkeit

geben, die Auskunft auf den angefragten Umfang zu beschränken. Anderenfalls müssten stets sämtliche Daten im Unternehmen (inklusive Daten in Anwendungsdateien wie Word, PowerPoint oder Excel sowie Backupkopien oder E-Mails) vollständig durchsucht werden. In der Praxis ist dies unmöglich. Bereits das geltende Datenschutzrecht ist in dieser Frage nicht mehr zeitgemäß. Der Vorschlag der Europäischen Kommission lässt in diesem Punkt leider keinerlei Modernisierungsbemühung erkennen. Elektronische Datenverarbeitung erfolgt nicht mehr in einer geringen Zahl unternehmensübergreifender Datenbanken. Diese aus der Anfangszeit der Datenverarbeitung stammende Vorstellung ist lange überholt. Die Auskunftsansprüche müssen entsprechend modernisiert werden.

Artikel 15 Absatz 1 c): Die Frage, an wen Daten „weitergegeben werden müssen", ist eine komplizierte Rechtsfrage, die im Rahmen einer Auskunft nicht beantwortet werden kann.

Artikel 15 Absatz 1 d): Die Dauer der Speicherung unterliegt je nach Datenart unterschiedlichen Anforderungen. Die Information kann auch im Rahmen einer Auskunftsanfrage nicht sinnvoll gegeben werden, weil die Information bei verschiedenen gespeicherten Daten zu komplex ist (siehe auch Anmerkung zu Artikel 14 Absatz 1 c)).

Artikel 15 Absatz 1 e): Auch das Bestehen eines Rechts auf Berichtigung und Löschung ist eine Rechtsfrage, die nicht pauschal beantwortet werden kann. Die Informationspflicht ist auch insofern zu löschen.

Artikel 15 Absatz 1 h): Es ist unklar, welche Informationen über die „Tragweite der Verarbeitung" zu geben sind. Vermutlich sollte nicht auf Artikel 20, sondern auf Artikel 21 verwiesen werden. Für diese Erweiterung der Informationspflicht besteht aber auch kein erkennbarer Anlass. Der Buchstabe sollte gestrichen werden.

Artikel 15 Absätze 3 und 4: Die Rechtsetzungsbefugnisse der Europäischen Kommission sind zu streichen.

Artikel 15 neuer Absatz 3: Es sollten angemessene Ausnahmen aufgenommen werden. Insbesondere ist zu berücksichtigen, dass die Auskunftserteilung bei einem Vorliegen von unstrukturierten Daten (beispielsweise in E-Mails oder in Schutzkopien) praktisch nicht möglich ist.

Artikel 16: Das Recht auf Vervollständigung von Daten und auf ein Korrigendum ist nicht verständlich. Entweder sind die Daten unzutreffend oder nicht. Datenverarbeitungssysteme werden in vielen Fällen gar keine Möglichkeit vorsehen, bisher nicht vorgesehene Datenfelder einzufügen. Es ist nicht ersichtlich, welchen Sinn diese zusätzliche Verpflichtung haben soll. Satz 2 ist deshalb zu streichen.

Artikel 17: Soweit das Recht auf Vergessenwerden einen Anspruch auf Löschung rechtswidrig gespeicherter Daten darstellt, ist hiergegen nichts einzuwenden. Die Einführung völlig neuer Kriterien, die im Ergebnis zu einem Anspruch auf Löschung rechtmäßig gespeicherter Daten führen, ist aber nicht sachgerecht. Das Nebeneinander unterschiedlicher Voraussetzungen führt unweigerlich zu Rechtsunsicherheiten, die zu vermeiden sind. Absatz 1 sollte deshalb klar auf die Rechtmäßigkeitstatbestände verweisen. Außerdem fehlen wichtige Ausnahmeregelungen. Auch hier gilt, dass die Möglichkeit einer späteren Einführung von Ausnahmeregelungen auf Grund von Artikel 21 Absatz 1 g) nicht dazu führen sollte, dass die Verordnung in sich nicht praktikabel ausgestaltet wird. Die erforderlichen Ausnahmen sind in die Verordnung aufzunehmen.

Artikel 17 Absatz 1: Der beispielhafte Verweis auf Kinder ist nicht hilfreich und führt zu unnötigen Auslegungsfragen, denn der Löschungsanspruch gilt völlig unabhängig davon, wann die Daten gespeichert wurden. Die durch Erfahrungen mit Social Networks motivierte Formulierung führt juristisch nur zu Auslegungsunsicherheiten.

Artikel 17 Absatz 1 a): Der Begriff Ănotwendigñ wirft Auslegungsfragen auf. Die Pflicht sollte streng an die Rechtmäßigkeitsvoraussetzungen geknüpft werden.

Ansonsten ergibt sich unnötige Rechtsunsicherheit. Es ist darauf abzustellen, dass die Verarbeitung nicht mehr „rechtmäßig" ist. Die weiteren Buchstaben b) bis d) können dann gestrichen werden.

Artikel 17 Absatz 1 b): Es gibt Einwilligungen, die im Rahmen eines Vertrags gegeben und nicht jederzeit zurückgenommen werden können. Außerdem haben Einwilligungserklärungen in der Regel keine „Speicherfrist". Buchstabe b) sollte aber schon deshalb gestrichen werden, weil die Löschungspflicht schon nach Buchstabe a) besteht, wenn die Einwilligung wirksam zurückgenommen wird.

Artikel 17 Absatz 1 c): Auch hier gilt, dass ein Widerspruch, wenn er zur Rechtswidrigkeit der Verarbeitung führt, nach Buchstabe a) einbezogen ist. Deshalb sollte Buchstabe c) gestrichen werden.

Artikel 17 Absatz 1 d): Auch dieser Buchstabe ist überflüssig und sollte deshalb gestrichen werden.

Artikel 17 Absatz 2: Die Verpflichtung zur Weiterverfolgung der Löschung gegenüber Dritten ist einer der schwerwiegendsten Auflagen des Rechts auf Vergessenwerden. Es sind ohne jede Ausnahme „alle vertretbaren Schritte" zu unternehmen. Dabei hatte die Europäische Kommission offenkundig Social Networks vor Augen. Die Regelung soll aber für jede Art der öffentlichen Verbreitung gelten. Die Regelung ist nicht umsetzbar und muss gestrichen werden. Außerdem sollte berücksichtigt werden, dass in der Praxis des Direktmarketings häufig Löschungen gefordert werden, wenn die betroffenen Personen künftig keine Werbung mehr erhalten wollen. In der Praxis muss hier eine Speicherung des Widerspruchs weiterhin erlaubt sein.

Artikel 17 Absatz 3: Hier verpflichtet die Verordnung zur Löschung von Daten, die rechtmäßig verarbeitet werden. Dies ist ein elementarer struktureller Fehler. Daten sind nur zu löschen, wenn ihre Speicherung unzulässig ist. Auch hier sind angemessene Ausnahmen vorzusehen, denn in der Praxis ist die Löschung

insbesondere bei unstrukturiert gespeicherten Daten (wie beispielsweise in E-Mails) oder bei Daten in Backups nicht mehr möglich. Ein modernes Datenschutzrecht muss dies berücksichtigen.

Artikel 17 Absatz 4: Im Grundsatz ist es richtig, wenn zwischen Löschung und Beschränkung unterschieden wird. Der im deutschen Bundesdatenschutzgesetz verwendete Begriff der ÄSperrungñ entspricht nicht mehr der Wirklichkeit der Datenverarbeitungstechnik. Hinsichtlich der Sperrungstatbestände bedarf es der Erweiterung von Absatz 4.

Artikel 17 Absatz 5: Auch hier wird in unsystematischer Weise von der Struktur der Rechtmäßigkeitstatbestände abgewichen. Der Absatz ist zu streichen.

Artikel 17 Absatz 6: Die erneute Benachrichtigungspflicht würde insbesondere bedeuten, dass eine Verwendung von Daten zu Beweiszwecken eine Informationspflicht gegenüber dem Betroffenen auslösen würde. Die Erfüllung einer solchen Informationspflicht kann im Einzelfall sehr aufwendig sein. Ausnahmen unter Berücksichtigung der Aufwands fehlen. Auch dieser Absatz ist deshalb zu streichen. Anderenfalls wäre es beispielsweise so, dass die Auswertung von archivierten E-Mailbeständen im Rahmen eines Gerichtsprozesses eine Informationspflicht gegenüber allen Versendern, Adressaten und ansonsten in den E-Mails erwähnten Personen auslösen würde. Eine solche Verpflichtung wäre völlig impraktikabel.

Artikel 17 Absatz 7: Eine regelmäßige Prüfung der Rechtmäßigkeit ist sinnvoll, sollte aber wieder klar mit der Anforderung an die Rechtmäßigkeit verknüpft werden.

Artikel 17 Absatz 8: Es ist unklar, was mit einer Speicherung auf andere Weise gemeint ist. Die Regelung sollte deshalb gestrichen werden. Sie könnte so verstanden werden, dass mit der Löschung auch eine Löschung in unstrukturierten manuellen Sammlungen erfolgen muss. Gerade das ist aber in der Regel praktisch unmöglich, weshalb die Datenschutzverordnung auf solche Daten zu Recht keine

Anwendung findet. Die Regelung ist auch deshalb praxisfremd, weil sie mit keinerlei Ausnahmen verbunden ist.

Artikel 17 Absatz 9: Die Rechtsetzungsbefugnisse der Europäischen Kommission sind zu streichen.

Artikel 18: Das Recht auf Datenportabilität (in beabsichtigter Anlehnung an das Recht zur Nummernportabilität im Telekommunikationsrecht) wäre ein scharfer wettbewerbspolitischer Eingriff, der unabhängig von seinen erheblichen wirtschaftlichen Wirkungen nicht in das Datenschutzrecht gehört. Die Regelung führt zur Verbreitung von Daten und nicht zu deren Schutz. Unternehmen würden sich bei vielen Gelegenheiten Vollmachten der betroffenen Personen einholen, um die Daten von Konkurrenten abfragen zu können. Ein Missbrauch der Regelung wäre nicht zu unterbinden. Es würde massiv in wirtschaftliche Eigentumspositionen eingegriffen, die auch verfassungsrechtlich geschützt sind. Der Wettbewerb würde verfälscht und Investitionen würden vereitelt.

Die Regelung zur Datenportabilität ist auch technisch nicht umsetzbar. Auch hier wurde eine Regelung, die speziell auf Social Networks zugeschnitten ist, allgemein ausgestaltet. Für viele andere Unternehmen ist die Regelung nicht umsetzbar. Es fehlen auch Ausnahmen, die den Aufwand in vertretbaren Grenzen halten könnten. Artikel 18 ist zu streichen. Eine Regelung zur Datenportabilität sollten allenfalls eng bereichsspezifisch außerhalb des Datenschutzrechts geregelt werden.

Artikel 19 Absatz 1: Die Verordnung modifiziert die Widerspruchsregel des Artikel 14 der Datenschutzrichtlinie in einer kaum nachvollziehbaren Weise. Wieder fehlt es an einer systematischen Verknüpfung zu den Rechtmäßigkeitsvoraussetzungen. Unter der bisherigen Richtlinie ist das Widerspruchsrecht im Kern das Recht, schutzwürdige Interessen geltend zu machen, die gegenüber den berechtigten Interessen des für die Verarbeitung Verantwortlichen überwiegen. Von diesem Prinzip ist keine Abweichung angezeigt. Es ist auch nicht bekannt, dass sich in

diesem Bereich praktische Probleme ergeben hätten, die eine gesetzgeberische Änderung rechtfertigen würden.

Artikel 19 Absatz 2: Den betroffenen Personen sollte ein Widerspruchsrecht gegen die Verarbeitung ihrer Daten zu Zwecken der Direktwerbung zustehen. Darüber sollte auch informiert werden. Hiergegen ist im Grundsatz nichts einzuwenden. Problematisch sind aber die Anforderungen an die Art und Weise dieser Information. Unternehmen müssen auf Formularen zahlreiche Informationen Ähervorhebenñ, weil der Gesetzgeber an verschiedensten Stellen diese Anforderung stellt. Dies führt insbesondere bei der Gestaltung von Bestellformularen dazu, dass es kaum noch Informationen gibt, die nicht hervorzuheben sind, was im Ergebnis die Einhaltung der Pflicht unmöglich macht. Die datenschutzrechtlichen Anforderungen sollten diese Tendenz nicht weiter verstärken.

Das Widerspruchsrecht gegen die Nutzung von Daten zu Zwecken der Direktwerbung ist den Verbrauchern in der Regel ohnehin bekannt. In der Praxis sollte die Bedeutung dieser Information deshalb nicht überbewertet werden. Es gibt keinen Anlass, die Anforderungen in dieser Hinsicht zu verschärfen. In der deutschen Sprachfassung sind in Erwägungsgrund 57 - wie in der englischen Sprachfassung bereits geschehen - die Worte Äfür nichtkommerzielle Zweckeñ zu streichen.

Gegen die Forderung verständlicher Datenschutzinformationen ist nichts einzuwenden. Die Regelung ist nur doppelt (siehe Artikel 11 Absatz 2) und führt damit zu unnötiger Unklarheit darüber, was die Verordnung hier in der Praxis fordert.

Artikel 20: In der Datenschutzrichtlinie wurde (gegen den Widerstand Deutschlands) eine Regelung zu automatisierten Einzelentscheidungen (Artikel 15) aufgenommen. Anstatt aus den schlechten Erfahrungen mit der alten Regelung zu lernen und sie zu streichen, wird diese jetzt durch Artikel 20 weiterentwickelt. Automatisierte Einzelentscheidung sind heute aber alltäglich und sollten nicht grundsätzlich verboten werden. Die Regelung hat jetzt außerdem einen zu weit ausgedehnten

Anwendungsbereich. So gilt sie beispielsweise auch für Maßnahmen, die einen rechtlichen Vorteil für die betroffene Person darstellen. Das Konzept der Regelung sollte vereinfacht werden. Wenn eine automatisierte Entscheidung die schutzwürdigen Interessen der betroffenen Person erheblich beeinträchtigt, dann sollte die für die Verarbeitung verantwortliche Stelle dazu verpflichtet sein, diese Entscheidung auf Anfrage der betroffenen Person zu erläutern und zu überprüfen. Darüber hinaus besteht kein Regelungsbedarf. Das Verhältnis der einzelnen Voraussetzungen zueinander ist durch den verschachtelten Satzbau nicht klar. Deshalb sollte Absatz 1 in zwei Sätze aufgeteilt werden. Die Ausnahmen in Absatz 2 sind ebenfalls klarer zu definieren. Teilweise sind die Voraussetzungen mehrerer Ausnahmen in einer Ausnahme vermischt. Das Beispiele passen nicht mehr zum eigentlichen Anwendungsbereich der Vorschrift. Deshalb sind die Begriffe ÄIhres Aufenthaltsortsñund ÄPersönliche Vorliebenñzu löschen.

Artikel 20 Absatz 3: Die Verarbeitung besonderer Arten von Daten unterliegt bereits sehr eingeschränkten Voraussetzungen. Es ist nicht ersichtlich, warum diese im Rahmen des Artikel 20 nochmals verschärft werden sollen. Wenn beispielsweise im Versicherungsbereich Auswertungen erfolgen, können diese durchaus ausschließlich auf besonderen Arten von Daten beruhen.

Artikel 20 Absatz 4: Es wird nicht klar, welche Informationen die Vorschrift verlangt, die nicht bereits durch die Auskunftsrechte eingefordert werden können. Der Verweis auf Artikel 14 ist falsch. Es müsste auf das Auskunftsrecht in Artikel 15 verwiesen werden.

Artikel 20 Absatz 5: Die Rechtsetzungsbefugnis der Europäischen Kommission sollte gestrichen werden.

Artikel 21: Die Vorschrift entspricht in weiten Teilen Artikel 13 der Datenschutzrichtlinie. Da die Verordnung aber nicht in nationales Recht umgesetzt wird, hat die Regelung eine geänderte Bedeutung. Es spricht nichts dagegen, Artikel 21 als Notanker für spezifische Fallgestaltungen zu belassen. Wichtig ist aber, dass die

Ausnahmen von den Betroffenenregelungen bereits in die Verordnung aufgenommen werden, so dass die Verordnung in sich stimmig und praktikabel ist. Die Mitgliedstaaten sollten Artikel 21 nur in Ausnahmefällen nutzen müssen. Weiterhin sollte in Artikel 21 ausdrücklich die Möglichkeit erwähnt werden, Ausnahmen für pseudonymisierte Daten zu erlauben. Damit könnten in den Bereichen der Markt- und Meinungsforschung sowie der sonstigen statistischen Forschung wichtige nationale Ausnahmen geschaffen werden.

Artikel 22: Die relativ allgemein formulierte Forderung nach geeigneten Strategien und Maßnahmen für den Datenschutz (Absatz 1) kann je nach praktischer Ausgestaltung zu einem erheblichen bürokratischen Aufwand führen. Dieser Aufwand wird völlig unabhängig von der Frage entstehen, welche Risiken mit der jeweiligen Datenverarbeitung verbunden sind. Insbesondere die Verpflichtung eines Nachweises der getroffenen Strategien und Maßnahmen führt zu einem unverhältnismäßig hohen bürokratischen Aufwand, wenn die zugrundeliegende Datenverarbeitung keine besonderen Risiken birgt. Das Wort Ägeeignetñ sollte durch Ærforderlichñ ersetzt werden. ÄStrategienñ sowie der Halbsatz Ä(é) und er den Nachweis dafür erbringen kannñ sollten gestrichen werden. Der Begriff der Erforderlichkeit sollte in Anlehnung an § 9 Bundesdatenschutzgesetz definiert werden: ÆErforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehtñ

Die beispielhafte Aufzählung von Maßnahmen in Absatz 2 ist gesetzestechnisch überflüssig. Es stellt sich außerdem die Frage, warum es keine abschließende Liste ist. Welche Maßnahmen sollen über die dort genannten hinaus noch getroffen werden? Diese Frage will die Europäische Kommission später über delegierte Rechtsakte beantworten (Absatz 4). Damit eröffnet sie sich ein praktisch unbeschränktes Recht zur Ausweitung der technischen und organisatorischen Anforderungen. Zusätzlich werden Überprüfungsverfahren vorgeschrieben (Absatz 3), die ebenfalls von der Europäischen Kommission näher ausgestaltet werden sollen. Was geeignet und angemessen ist, will die Europäische Kommission allein

entscheiden. Damit hat sie es in der Hand, den Aufwand für Unternehmen grenzenlos zu erweitern.

Absatz 2 ist als abschließende Aufstellung zu formulieren. Das Wort „insbesondere" ist zu streichen. Absatz 3 ist auf besonders risikorelevante Verarbeitungen zu beschränken. Das Wort „unabhängigen" sollte gestrichen werden, weil es Auslegungsschwierigkeiten hinsichtlich der Anforderungen provoziert. Im ersten Satz von Absatz 3 wären nach dem Wort „setzt" die Worte „bei Verarbeitungen, die hohe konkrete Risiken für die Privatsphäre der betroffenen Personen in sich bergen," einzufügen. Absatz 4 ist zu streichen.

Artikel 23: Datenschutzfreundliche Technik ist eine wichtige Zielsetzung, bei der aber auch Aufwand und Nutzen in einem angemessenen Verhältnis stehen sollten. Artikel 23 erwähnt zwar den Stand der Technik und die Implementierungskosten, schränkt aber die Verpflichtung an sich nicht ein. Vor den Worten „technische und organisatorische Maßnahmen" sollte das Wort „erforderlich" eingefügt werden. Außerdem sollte eine Definition in Anlehnung an § 9 Bundesdatenschutzgesetz erfolgen: „Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht." Weiterhin sind die Worte „und die Rechte der Person gewahrt bleiben" zu streichen, denn gerade die sollen ja durch die Anforderungen der Verordnung sichergestellt werden. Es ist ansonsten unklar, welche zusätzlichen Anforderungen sich aus der Formulierung ergeben sollen.

Die spezifischen Anforderungen in Absatz 2 enthalten grundsätzlich richtige Zielsetzungen, sind jedoch als harte Verpflichtungen nicht umsetzbar. Außerdem wird hier über die technischen Anforderungen an die Datenverarbeitung ein neuer Maßstab für die Rechtmäßigkeit der Verarbeitung und die Löschungsverpflichtungen gesetzt. Es darf nur noch verarbeitet werden, was unbedingt nötig und erforderlich ist, selbst wenn die Zulässigkeitsvoraussetzungen erfüllt sind.

Statt einen neuen Prüfungsmaßstab aufzubauen sollte sich die Vorschrift daran orientieren, was nach der Verordnung zulässig ist. Anderenfalls führt die Vorschrift zu Widersprüchen im Hinblick auf die Rechtmäßigkeitsvoraussetzungen und die Löschungspflichten. Daten, die nach Artikel 6 verarbeitet werden dürfen, müssen auch unter Artikel 23 Absatz 2 verarbeitet werden können. Daten, die keiner Löschungspflicht nach Artikel 17 unterliegen, sollten nicht nach Artikel 23 Absatz 2 zu löschen sein. Anderenfalls entfaltet Artikel 23 ein nicht mehr zu kontrollierendes Eigenleben. Absatz 2 ist deshalb entweder strikt auf die allgemeinen Rechtsmäßigkeitstatbestände zu beziehen oder zu streichen.

Absätze 3 und 4 sind zu streichen. Festlegungen der Europäischen Kommission zu technischen und organisatorischen Maßnahmen hätten erhebliche negative Auswirkungen auf den technischen Entwicklungsprozess von Maßnahmen zur Datensicherheit. Jede Festlegung wäre schnell überaltert und würde die Weiterentwicklung bremsen.

Artikel 24: Es ist zutreffend, dass mehrere Personen oder Unternehmen für eine Datenverarbeitung gemeinsam verantwortlich sein können. Insofern ist es auch sinnvoll, wenn sich die Beteiligten in einer solchen Konstellation intern über ihre Verantwortlichkeiten abstimmen. Noch wichtiger ist aber die Frage, wie in einer solchen Konstellation die Datenübermittlungen zwischen beiden Verantwortlichen Stellen zu beurteilen sind. Die gemeinsam verantwortlichen Stellen sind weiterhin ein ÄEmpfängerñ im Sinne der Definition der Verordnung. Es ist zu überlegen, ob die gemeinsam verantwortlichen Stellen datenschutzrechtlich als eine Einheit betrachtet werden könnten. Auf diese Weise ließen sich auch Verarbeitungen im Konzern neu gestalten. Artikel 24 könnte um folgenden Satz ergänzt werden: ÄSoweit die gemeinsam für die Verarbeitung Verantwortlichen im Rahmen einer solchen Vereinbarung eine datenschutzrechtliche Konsolidierung vereinbaren, sind sie im Sinne dieser Verordnung als ein für die Verarbeitung Verantwortlicher zu betrachten.ñ

Artikel 25: Die Pflicht zur Bestellung eines Inlandsvertreters muss in einem realistischen Rahmen Anwendung finden. Wichtig ist dabei, dass der bestellte Inlandsvertreter nicht persönlich für die Verpflichtungen aus der Verordnung in die Haftung genommen werden kann. Ansonsten werden sich nur Unternehmen für diese Aufgabe finden, die keine Haftungsmasse haben. Dies wäre nicht im Sinne der Vorschrift. Wie in anderen Bereichen könnten insbesondere Rechtsanwaltskanzleien diese Aufgabe übernehmen. Sie sollten dann Empfangsvertreter für den für die Verarbeitung Verantwortlichen sein. In Satz 1 sollte es deshalb lauten: Äbenennt einen Empfangsvertreter in der Unionñ Weiterhin wäre es sinnvoll, wenn Artikel 51 die Zuständigkeit der Aufsichtsbehörde an den Sitz des Vertreters anknüpfen würde. Ansonsten bestände ein Wertungswiderspruch zu dem Fall, dass an dem Ort eine Niederlassung des für die Verarbeitung Verantwortlichen besteht.

Artikel 26: In einer arbeitsteilig organisierten Volkswirtschaft ist die Auftragsverarbeitung ein wichtiges Strukturierungsinstrument für datenschutzrechtlich relevante Sachverhalte. Die Verantwortlichkeit für die Verarbeitung wird auf eine Stelle konzentriert. Der für die Verarbeitung Verantwortliche behält über die Weisungsgebundenheit die Kontrolle und damit eben auch die Verantwortung für die Verarbeitung der Daten. Die Verordnung durchbricht dieses Prinzip jedoch an vielen Stellen, indem sie den Auftragsverarbeiter unmittelbar in die Verantwortung nimmt. Gerade das sollte eigentlich durch die Struktur verhindert werden.

Der Auftragsverarbeiter sollte nach deutschem Vorbild für die Durchführung der technischen und organisatorischen Maßnahmen verantwortlich sein. Die weiteren Pflichten ergeben sich aus dem Auftragsverarbeitungsvertrag und den Weisungen des Auftraggebers. Beispiele für eine überzogene Einbeziehung des Auftragsverarbeiters finden sich in Artikel 3, 28, 33, 34, 51. Alle Verweise auf Auftragsverarbeiter sind daraufhin zu überprüfen, ob sich die Verpflichtungen sinnvoll gegen den Auftragsverarbeiter richten können. In der deutschen Sprachfassung der Verordnung ist das Wort ÄGarantienñ durch ÄGewährñ zu ersetzen, um einen Bezug zu Garantien im zivilrechtlichen Sinne zu vermeiden. Zuletzt kann dem für die Verarbeitung Verantwortlichen nicht auferlegt werden, für

die Einhaltung der technischen und organisatorischen Maßnahmen beim Auftragnehmer Sorge zu tragen. Allenfalls kann ihm auferlegt werden, dass er sich von Zeit zu Zeit von der Einhaltung Äüberzeugtñ

Bei den Anforderungen an die Auftragsverarbeitung ist zu differenzieren, ob es sich um die Auslagerung eines Rechenzentrums handelt oder um die Beauftragung eines externen IT-Beraters oder eines Aussenders für Werbebriefe. Die in der Verordnung vorgeschlagene Regelung trifft diese Unterscheidung nicht, so dass einfache und wenig riskante Verarbeitungen umfassenden bürokratischen Anforderungen unterliegen. Ein Problem, das sich auch unter den deutschen Regeln in Artikel 11 Bundesdatenschutzgesetz stellt. Hier sollte überlegt werden, ob die Anforderungen in zwei Absätze aufgeteilt werden, d.h. in solche für einfache Verarbeitungen und in solche für Verarbeitungen mit hohen Risiken für die Persönlichkeitsrechte der betroffenen Personen. Weiterhin verweisen wir auf unsere Anmerkungen zur Definition des ÄAuftragsverarbeitersñ

In Absatz 2 sind die einzelnen Anforderungen an die Vertragsgestaltung zu überdenken. Unter a) könnte klargestellt werden, dass die ÄWeisungenñ des Auftraggebers auch im Vertrag selbst enthalten seinen können, was in der Praxis der Regelfall ist. Buchstabe b) sollte so formuliert werden, dass nicht nur Beschäftigte im arbeitsrechtlichen Sinne eingesetzt werden können. Buchstabe d) sollte vorsehen, dass die Zustimmung bereits im Vertrag gegeben werden kann. Dies gilt auch für Buchstaben e), denn die Festlegung der technischen und organisatorischen Maßnahmen erfolgt in der Regel im Vertrag und nicht im Wege einer gesonderten ÄAbspracheñ Buchstabe g) ist nicht realistisch, denn der Pflicht einer ÄAushändigungñ von ÄErgebnissenñ liegt ein völlig veraltetes Bild von Datenverarbeitung zugrunde (Batchläufe auf einem Großrechner, die aus Daten ein Ergebnis errechnen, das dann in eine Datei gespeichert wird). Datenschutzrechtlich ist nur erheblich, dass die vorhandenen Daten irgendwann gelöscht werden. Hierzu sind Regelungen zur ÄÜbermittlung oder Löschung von Daten nach Vertragsendeñ vorzusehen. Eine vertragliche Verpflichtung zur Aushändigung von Unterlagen an

ÄAufsichtsbehördenñ ist vor dem Hintergrund der gesetzlichen Auskunftsrechte der Aufsichtsbehörde nicht erforderlich.

In Absatz 4 wird die Konstruktion der gemeinsam für die Verarbeitung Verantwortlichen als Regelfolge angesehen, wenn der Auftragsverarbeiter den Weisungen des Auftraggebers nicht folgt. Dies entspricht aber nicht dem Leitbild von Artikel 24, denn danach ist ja gerade Voraussetzung, dass die Beteiligten die Zwecke, Bindungen und Mittel Ägemeinsamñ bestimmen. Gerade das passiert ja nicht, wenn der Auftragsverarbeiter die Daten auf andere Weise verarbeitet. Absatz 4 ist deshalb zu streichen. Absatz 5 ist ebenfalls zu streichen.

Artikel 27: Das Konzept der ÄVerarbeitung unter Aufsichtñ sollte noch klarer von dem der Auftragsverarbeitung abgegrenzt werden. Dies gilt insbesondere im Hinblick auf Dienstleister, die unmittelbar im Hoheitsbereich des für die Verarbeitung Verantwortlichen tätig werden. Auf diese Weise könnten freie Mitarbeiter, Wartungsmitarbeiter und andere Dienstleister erfasst werden, die im technischen oder örtlichen Hoheitsbereich des für die Verarbeitung Verantwortlichen tätig werden.

Artikel 28: Die Verordnung will Unternehmen dadurch entlasten, dass insbesondere die Pflichten zur Registrierung bei den Aufsichtsbehörden abgeschafft werden. Dabei folgt die Verordnung dem deutschen Beispiel. In der Praxis entlasten die vorgeschlagenen Änderungen aber nur die Verwaltung bei den Aufsichtsbehörden, denn die Verpflichtung zur Führung eines internen Verarbeitungsregisters entspricht für die Unternehmen dem Aufwand einer Meldung. Die Unternehmen ersparen sich nur die Übermittlung der Eintragung an die Aufsichtsbehörde und die Meldegebühren. Die Detaillierungsrechte der Europäischen Kommission (Absatz 5 und 6) bergen außerdem das Risiko, dass die bürokratischen Anforderungen unsachgemäß erweitert werden.

Ungelöst bleibt das Problem, dass interne Verarbeitungsregister schon heute nicht mehr praktikabel umsetzbar sind. In Deutschland gibt es zwei Tendenzen, wie

hiermit umgegangen wird: Entweder werden die einzelnen Verarbeitungen im Register nur sehr allgemein beschrieben, so dass zwar alle Verarbeitungen abgedeckt sind, das Register aber ohne praktischen Nutzen ist. Oder die Unternehmen versuchen, ihre Verarbeitungen detailliert zu erfassen, was in der Praxis aber in der Regel dazu führt, dass im Register nur eine Auswahl der wesentlichen Verarbeitungen enthalten ist. So oder so stößt die Führung von Verarbeitungsregistern heute an ihre praktischen Grenzen, weil die Vielfalt der Datenverarbeitungsvorgänge in den Unternehmen zugenommen hat. Ein richtiger Ansatz wäre es, unternehmensinterne Meldungen von Datenverarbeitungen auf Bereiche mit besonderen Risiken zu beschränken. Die in Absatz 4 vorgesehenen Einschränkungen genügen nicht.

Artikel 29: Der Sinn der Vorschrift erschließt sich nicht, denn Artikel 53 findet auch unmittelbar auf den Auftragsverarbeiter Anwendung. Die Vorschrift ist zu streichen.

Artikel 30: Die Abgrenzung zwischen Artikel 22, 23 und 30 ist unklar. Grundsätzlich sollten die technischen und organisatorischen Maßnahmen einheitlich und an einer Stelle der Verordnung geregelt werden. Im Gegensatz zu Artikel 23 wird jedoch in Artikel 30 auf die Angemessenheit der Maßnahmen abgestellt. Dies sollte in Anlehnung an die deutsche Definition der ÄErforderlichkeitñ (§ 9 BDSG) auch definiert werden.

Absatz 2 fordert Maßnahmen gegen Zerstörung und Verlust von Daten. Es ist nicht ersichtlich, warum solche Regelungen aus Gründen des Schutzes der Privatsphäre erforderlich sind. Stattdessen sollte allein auf die Äunrechtmäßige Verarbeitungñ verwiesen werden. Absätze 3 und 4 sind zu streichen. Eine Regelung technischer und organisatorischer Anforderungen durch die Europäische Kommission würde wegen der Trägheit solcher Regelungen unweigerlich die Innovation von Sicherheitstechnik bremsen, die für einen wirksamen Schutz unerlässlich ist.

Artikel 31 und 32: Die Praxis der Benachrichtigungspflichten über Datenschutzverstöße zeigt, dass die Entscheidung über das ob, wie und wann eines Hinweises

einer sensiblen Abwägung bedarf. Weder die Aufsichtsbehörden noch die betroffenen Personen sind an einer Unzahl von überflüssigen oder falschen Hinweisen interessiert. Außerdem sollten Hinweise erst dann erfolgen, wenn ausreichende Klarheit über den Sachverhalt besteht. Der Begriff der ĂVerpflichtungñ sollte nicht so definiert werden, dass nur Ăim Zweifelñ informiert wird. Weder die betroffenen Personen noch die Aufsichtsbehörden haben hieran ein Interesse. Starre zeitliche Fristen führen zwingend dazu, dass übereilt und ohne ausreichende Aufklärung informiert wird.

Die weite Definition des Begriffs ĂVerletzung des Schutzes personenbezogener Datenñ (siehe Anmerkung zu Artikel 4 Absatz 9) und die wiederum kaum eingeschränkte Meldepflicht zur Aufsichtsbehörde würden in der Praxis zu einer Flut an Meldungen führen, von denen nur wenige tatsächlich beachtenswert wären. So müsste jede Fehlkonfiguration der Zugangsberechtigungen in einem Unternehmen an die Aufsichtsbehörde gemeldet werden. Besonders erstaunlich ist die Meldepflicht im Falle der Vernichtung von Daten, denn vernichtete Daten können nicht missbraucht werden.

Artikel 31 und 32 sollten vor dem Hintergrund ihres Schutzzwecks überdacht werden. Sie sollten klar auf Fälle der tatsächlichen widerrechtlichen Übermittlung von Daten an Dritte beschränkt sein. Nur wenn von einer solchen Übermittlung hohe konkrete Risiken für die Privatsphäre ausgehen, ist eine Melde- und Benachrichtigungspflicht vorzusehen. Die Meldepflicht sollte auch nur dann bestehen, wenn seitens der betroffenen Person Maßnahmen zur Eindämmung etwaiger negativer Auswirkungen möglich sind. In Zweifelsfällen sollten Unternehmen eine Meldung an die Aufsichtsbehörde vornehmen können, damit diese entscheiden kann, ob eine Benachrichtigung der betroffenen Personen erfolgen muss. Auf diese Weise könnte sichergestellt werden, dass Hinweise auf Verletzungen immer nur dann erfolgen, wenn diese für die betroffene Person sinnvoll sind. Außerdem würde sichergestellt, dass sie Beachtung finden und nicht in unzähligen überflüssigen Hinweisen untergehen.

Der **Deutsche Dialogmarketing Verband e.V. (DDV)** ist der größte nationale Zusammenschluss von Dialogmarketing-Unternehmen in Europa und einer der Spitzenverbände der Kommunikationswirtschaft in Deutschland. Im DDV sind Auftraggeber von Dialogmarketing und ihre Dienstleister vertreten, u. a. Dialogmarketing-und Online-Agenturen, Adress- und Informationsdienstleister, E-Mail-Dienstleister, Call-Center-Services und Telemedien-Dienstleister, Direct-Mail-Unternehmen sowie Werbungtreibende aus verschiedenen Wirtschaftszweigen. Der Verband sorgt für den Interessenausgleich zwischen Wirtschaft, Politik, Wissenschaft und Verbraucher - für die Freiheit der Kommunikation und die Möglichkeiten, Dialogmarketing in seiner Vielfalt gestalten und einsetzen zu können. Schwerpunkte des Verbandsengagements sind politische Arbeit, Informationsaustausch, Qualitätssicherung und Nachwuchsförderung.

Bei Fragen kontaktieren Sie bitte publicaffairs@ddv.de oder +49 (30) 28882920.