

Glaser, Anika

Von: DDV Titus Goll [t.goll@ddv.de]
Gesendet: Freitag, 9. März 2012 11:18
An: Meltzian, Daniel, Dr.
Cc: Stentzel, Rainer, Dr.; Sobotta, Stefan, VII4; PGDS_
Anlagen: 120308_DDV_Stellungnahme_General Data Protection Regulation_Article 1-21.DOC

VII4 - M - 151 561 - 2 62

2. M. 13.3.

[Handwritten signature]

27.4.

Sehr geehrter Herr Dr. Meltzian,

wir hatten Ihnen vorbereitend zur RAG Sitzung am 23./24. Februar 2012 vorläufige Anmerkungen zu den Artikeln 1 bis 10 des Vorschlags der Europäischen Kommission zu Datenschutz-Grundverordnung (2012/0011 (COD)) übersendet. Nachfolgend erhalten Sie ebenfalls vorläufig die um Artikel 11 bis 21 ergänzte Fassung (E-Mailtext, unten, bzw. Dateianhang) für die RAG Sitzung am 14/15. Februar 2012 (und die heutige Ressortabstimmung). Die vollständige Stellungnahme folgt noch im März.

Für Rückfragen stehen wir Ihnen jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen

Dieter Weng

Präsident des DDV

i.A. Titus Goll

Titus Goll
Rechtsanwalt
Consultant Public Affairs



DDV
Deutscher Dialogmarketing Verband e. V.
- Hauptstadtbüro-
Charlottenstrasse 79/80
D-10117 Berlin
Tel. +49 30 28882920
Fax +49 30 28882919
Mobil: +49 1522 1921334
[mailto: t.goll@ddv.de](mailto:t.goll@ddv.de)

DDV im Netz:
www.ddv.de
[www.twitter.com/DDV_DE](https://twitter.com/DDV_DE)

Anmerkungen Artikel 1 bis 21

Artikel 1 Absatz 1: Zu der Frage der Rechtsnatur der Verordnung sind wir der Ansicht, dass grundsätzlich eine striktere europaweite Harmonisierung wünschenswert ist. Wir sind angesichts der vorgesehenen Ausnahmen aber auch der Ansicht, dass der vorliegende Entwurf hier im Grunde ein Rückschritt gegenüber der bisherigen Richtlinie (95/46/EG) ist, die ja nach der zutreffenden Auslegung des Europäischen Gerichtshofs (C-468/10 und C-469/10) bereits eine Vollharmonisierung enthält. Am Ende kommt es deshalb nicht darauf an, ob die Regelung im Wege einer Verordnung oder einer Richtlinie erfolgt. Wichtig ist nur, dass die Regelungen ausgewogen sind und sich alle Mitgliedstaaten daran halten. Unter Subsidiaritätsgesichtspunkten wären wir auch einer Lösung gegenüber aufgeschlossen, bei der die Verordnung sich auf Fragen des Drittländerdatentransfers beschränkt und die Harmonisierung ansonsten weiterhin über eine Richtlinie erfolgt. Dies würde auch der Tatsache Rechnung tragen, dass das Datenschutzrecht stark mit anderen Rechtsbereichen verwebt ist und eine europäische Verordnung hier als Fremdkörper im Verhältnis zum nationalen Recht unweigerlich zu erheblichen Auslegungsunsicherheiten führen würde.

Artikel 1 Absatz 3: Wir sind der Ansicht, dass Artikel 16 Abs. 2 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) keine Rechtsgrundlage für die Regelung des Datenschutzes im nicht-öffentlichen Bereich ist. Die Vorschrift bezieht sich ausdrücklich ausschließlich auf den öffentlichen Bereich. Die richtige Rechtsgrundlage für den nicht-öffentlichen Bereich ist allein Artikel 114 Abs. 1 AEUV, der auch am Anfang des Verordnungsentwurfs aufgeführt wird. Artikel 1 Absatz 3 ist der bisherigen Richtlinie entnommen, aber war auch dort schon unglücklich formuliert. 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 Binnenmarktes 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“ gestrichen werden. Es gibt keine Rechtsgrundlage, die es der Europäischen Union erlaubt, aus diesem Grund Regelungen im Bereich des nicht-öffentlichen Datenschutzes zu treffen. Damit würde auch deutlicher, dass die Verordnung im Ergebnis wirtschaftlichen Interessen dienen muss und diese nicht behindern soll. Weiterhin sollte stärker hervorgehoben werden, dass der grundrechtliche Schutz personenbezogener Daten nicht absolut gilt, sondern einer Abwägung mit anderen Grundrechten unterliegt, insbesondere im Hinblick auf die unternehmerische Freiheit. Dieser Aspekt liegt bisher im Erwägungsgrund 139 etwas versteckt im Hintergrund und wird im Rahmen der Verordnung auch nicht berücksichtigt.

Artikel 2 Absatz 1: Der Anwendungsbereich auf nicht-automatisierte Verarbeitungen ist bereits nach der geltenden Richtlinie problematisch, weil beispielsweise ein nach Adressaten sortierter Stapel adressierter Briefe bereits unter den Anwendungsbereich fällt. Insofern ist die Formulierung in Erwägungsgrund 13 („die in einem Ablagesystem gespeichert sind“) zu begrüßen. Leider findet sich diese Einschränkung aber

nicht in Artikel 2 Absatz 1 oder der Definition der Datei in Artikel 4 Absatz 4. Nachteilig 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 dem Wohnort sortiert ist, würde dies auch zur Anwendung der Verordnung und aller damit verbundenen Rechte und Pflichten führen. Nach der bisherigen Richtlinie muss es sich laut Erwägungsgrund 15 um „personenbezogene“ Kriterien handeln. Dies sollte beibehalten und auch ausdrücklich in der Definition des Begriff „Datei“ aufgenommen werden. Auch für die Frage der Anwendung der Vorschrift auf Akten ist dies wichtig.

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 wichtig, da insbesondere im Internet und mobil viele Dienste angeboten werden, die den Nutzern zur Verarbeitung zu persönlichen und familiären Zwecken dienen. Wenn bei diesen Diensten der Anwendungsbereich der Verordnung eröffnet würde, müssten alle Anforderungen an eine Auftragsverarbeitung eingehalten werden, was in der Praxis unmöglich ist. Das zusätzliche Merkmal „ohne jede Gewinnerzielungsabsicht“ führt hier zu unnötiger Rechtsunsicherheit darüber, was ausgenommene Verarbeitungen sind. Heute verstehen wir sehr wohl eine Reihe von Datenverarbeitungen im geschäftlichen Bereich als „persönlich“. Beispielsweise würde jedes persönliche elektronische Telefonverzeichnis, das auch geschäftliche Kontakte enthält, unter den Anwendungsbereich der Verordnung fallen. Die damit verbundenen Konsequenzen sind in der Praxis nicht umsetzbar.

Artikel 2 Absatz 3: Die Vorrangregelungen zu anderen Richtlinien (auch später in 89 zur ePrivacy Richtlinie) sind im Grundsatz problematisch, weil es eines Vorrangs des umsetzenden nationalen Rechts vor der Verordnung bedarf. Ein Vorrang der Richtlinie vor der Verordnung greift zu kurz.

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 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 sollte der Verweis auf „oder jede sonstige natürliche oder juristische Person“ in Artikel 4 Absatz 1 und auf „oder einer anderen Person“ in Erwägungsgrund 23 gestrichen werden. Sobald solche „andere Personen“ die Daten erhalten, soll die Verordnung Anwendung finden, aber nicht, wenn dies nicht erfolgt. Die Streichung des Verweises auf „andere Personen“ würde auch nicht dazu führen, dass sie 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 3: Wir würden es begrüßen, wenn – nach dem Beispiel von § 3 Abs. 6 BDSG – eine Definition der Anonymisierung aufgenommen und dann die Anonymisierung ausdrücklich von der Definition der Verarbeitung ausgeschlossen würde. Aus datenschutzrechtlicher Sicht ist eine Anonymisierung von Daten stets wünschenswert und sollte nicht datenschutzrechtlich beschränkt sein oder gar datenschutzrechtliche Verpflichtungen auslösen. Außerdem wäre eine Definition der Anonymisierung hilfreich um die Abgrenzung zur Definition der personenbezogenen Daten zu schärfen.

Artikel 4 Absatz 4: Siehe Anmerkung zu Artikel 2 Absatz 1. Die Worte „nach bestimmten Kriterien“ sollten durch „nach bestimmten personenbezogenen Kriterien“ ersetzt werden, so wie es in Erwägungsgrund 15 der bisherigen Richtlinie bestimmt wird.

Artikel 4 Absatz 5 und 6: Eines der aktuellen praktischen Probleme der Auftragsverarbeitung liegt darin, dass die Datenschutzaufsichtsbehörden in den Auftragsverarbeitungsverträgen unangemessen detaillierte Vorgaben des Auftraggebers hinsichtlich der „Mittel“ der Verarbeitung fordern. Datenschutzrechtlich haben diese Detaillierungen jedoch keinerlei Mehrwert. Sie haben aber Nachteile, denn jede Änderung der „Mittel“ erfordert dann eine Vertragsänderung, d.h. wenn beispielsweise eine bestimmte technische Infrastruktur beschrieben ist, kann der Auftragsverarbeiter diese nur noch ändern, nachdem er dies mit allen 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 „Mittel“ eingesetzt werden. Insofern sollte – auch in Abweichung zur bisherigen Richtlinie und entsprechend der deutschen Regelung in § 11 BDSG – der Verweis auf „Mittel“ gestrichen werden. Auf jeden Fall sollte der neu hinzugefügte Verweis auf „Bedingungen“ gestrichen werden. Es ist unklar, was damit überhaupt gemeint ist und würde nur zu einer weiteren Bürokratisierung der Auftragsverarbeitung führen.

Artikel 4 Absatz 7: Die Definition des „Dritten“ wurde gestrichen, so dass jetzt keine Differenzierung mehr zwischen „Empfängern“ und „Dritten“ erfolgt. Damit werden in den jeweiligen Regelungen insbesondere Auftragsverarbeiter immer mit erfasst. Dies führt insbesondere dazu, dass nach Artikel 14 Absatz 4 b) die Information gegeben werden müsste, bevor die Daten an einen Auftragsverarbeiter weitergegeben werden. Hierfür besteht kein sachlicher Grund. Auch in anderen Vorschriften (wie beispielsweise bei der Auskunft) wäre der Begriff des Dritten notwendig. Alternativ wäre zu überlegen, ob Auftragsverarbeiter nicht ausdrücklich von der Definition der „Empfänger“ ausgenommen werden.

Artikel 4 Absatz 8: Von der Verwendung von Einwilligungserklärungen sollte nicht durch übertriebene Anforderungen abgeschreckt werden. Insbesondere das Wort „explizit“ sollte hier gestrichen werden. 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 werden?

Artikel 4 Absatz 10, 11 und 12: Die Definitionen sind in einer Weise formuliert, dass ihnen ein uferloser Anwendungsbereich zukommen könnte. 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 und 15: Der Begriff der Hauptniederlassung spielt an Stellen der Verordnung eine Rolle, wo die Anwendung des Datenschutzrechts für grenzüberschreitend tätige Unternehmen geregelt wird. Es sollte überlegt werden, ob entsprechende Grundsätze auch dann gelten sollen, wenn in einem Land (wie in Deutschland) mehrere lokale Aufsichtsbehörden existieren. Außerdem wäre es wichtig, dass eine entsprechende Regelung auch dann greift, wenn es um selbständige Niederlassungen geht. 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 deutschen Steuerrecht könnte so eine Konzernregelung eingeführt 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 erfolgen. 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 dann nicht gelten. Die Grenze des 13. Lebensjahrs sollte verwendet werden.

Artikel 5: Der Regelungswert der „Grundsätze“ neben den Rechtmäßigkeitsanforderungen sollte überdacht werden. Außerdem ist zu bedenken, dass die Grundsätze im Gegensatz zum bisherigen Artikel 6 Absatz 1 ... Richtlinie nach dem Vorschlag der Verordnung ohne jede Ausnahme gelten sollen (es sei denn, die Mitgliedstaaten schaffen eine solche nach Artikel 21). Nur Artikel 5 Buchstabe b) 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 Buchstabe d): Die Qualität der Daten liegt in der Regel auch im Interesse der Unternehmen. Es sollte aber auch sichergestellt sein, dass die Maßnahmen zur Schaffung dieser Qualität auch datenschutzrechtlich zulässig sind. Dies könnte in einem der Erwägungsgründe klargestellt werden.

Artikel 5 Buchstabe f): Hier wird dem für die Verarbeitung Verantwortliche die allgemeine Beweislast für ... 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).

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 Verbotes mit Erlaubnisvorbehalt sollte in diesem Zusammenhang überdacht werden. Man könnte beispielsweise überlegen, ob die Rechtmäßigkeitsanforderungen grundsätzlich nur erforderlich sind, wenn ein überwiegendes schutzwürdiges Interesse des Betroffenen berührt ist. Nur dann besteht auch die Notwendigkeit der gesetzlichen Einschränkung.

Artikel 6 Absatz 1 Buchstabe a): Die Anforderungen an wirksame Einwilligungen werden in der Definition der Einwilligung, in Artikel 7 und in Artikel 6 Absatz 1 Buchstabe a) festgelegt und an jeder dieser Stellen verschärft. Die Formulierung „Die betroffene Person hat ihre Einwilligung gegeben.“ würde hier ausreichen. Zumindest sollte das Wort „genau“ gestrichen oder zumindest dieselbe Formulierung wie in Artikel 7 Absatz 1 verwendet werden (in der deutschen Fassung sind es sogar unterschiedliche Wörter; „genau“ und „eindeutig“).

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 rechtsgeschäftsähnliche Beziehungen mit aufzunehmen sind, die ja nicht nur vorvertraglich bestehen können. Die 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 zur Kreditauskunfteien. Die Arbeitsteilung zwischen professionellen Datenanbietern und den Empfängern der Daten wäre 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.

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 Buchstaben 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 sie 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 Buchstaben 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 ist deshalb um einen Verweis auf Buchstaben f) zu ergänzen.

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 Rechtssetzung 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 Verbreitung des Anwendungsbereichs der Einwilligung und Erhöhung ihrer Wirksamkeitsvoraussetzungen ist in der Praxis nicht verkraftbar. Nur wenn die Einwilligung tatsächlich in sensiblen Vorgängen vorbehalten bleibt, darf sie auch hohe Anforderungen haben. 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 „eindeutig“ oder „genau“ die Verwender von Einwilligungserklärungen zu Verwendung langer und unübersichtlicher Einwilligungstexte zu zwingen. Außerdem sollten auch konkludente Einwilligungen möglich sein (siehe Anmerkung zu Artikel 4 Absatz 8). Nicht zuletzt ist die jederzeitige Widerrufbarkeit von Einwilligungen 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.

Artikel 8: Es ist für uns nicht nachvollziehbar, zu welchem Ergebnis die Einschränkung von Absatz 1 durch Absatz 2 in Deutschland kommen würde. Der Ansatz, die besonderen Schutzvorschriften auf Kinder bis zum 13. Lebensjahr zu beschränken, ist jedoch zu begrüßen. Dies sollte bereits in der Definition des Begriffs „Kind“ in Artikel 4 Absatz 18 erfolgen.

Artikel 9: Wie bereits unter der geltenden Richtlinie wird die Verarbeitung von besonderen Kategorien von Daten unabhängig von ihrer individuellen Sensibilität beschränkt. Der Ansatz führt zu unangemessenen Beschränkungen von Daten. Es sollte überlegt werden, ob insbesondere Artikel 9 Absatz 2 Buchstabe e) im Anwendungsbereich erweitert werden kann. In der Verordnung sollte vermieden werden, dass unsensible besondere Kategorien von Daten besonders geschützt werden. Dies kann nicht nur davon abhängen, ob sie die betroffene Person selbst öffentlich gemacht hat.

Artikel 10: Die Vorschrift ist vom Ansatz her zu begrüßen, sollte aber so formuliert werden, dass sie sich nicht auf anonymisierte Daten beschränkt ist, sondern auch für pseudonymisierte Daten gilt. Derzeit findet

die Vorschrift nur dann Anwendung, wenn die Verordnung keine Anwendung findet, was im Ergebnis inkonsistent ist. Die Klausel sollte außerdem die Möglichkeit der Löschung identifizierender Datenelemente erlauben. Wichtig ist, dass der Grundgedanke bei späteren Vorschriften (beispielsweise im Zusammenhang mit Auskunftsrechten, die bisher ausnahmslos auch für nicht vollständig identifizierte Daten gelten) fortgesetzt werden. Insbesondere ist Erwägungsgrund 45 in den Vorschriften der Verordnung umzusetzen.

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 „jedermann leicht zugängliche Strategie“. In der englischen Sprachfassung wird diese als „Policy“ bezeichnet. Für Internetdienste sind solche Policies üblich. 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 umzusetzen, ohne dass ein besonderer Mehrwert für die betroffenen Personen erkennbar ist.

Die Regelung ist damit eines von vielen Beispielen im Verordnungsentwurf, bei denen internetspezifische Regelungen unsachgemäß auf alle anderen Wirtschaftsbereiche erweitert werden. Dies belegt auch Erwägungsgrund 46, der auf den Bereich des Internets abhebt. Außerdem enthält die Vorschrift keinerlei Ausnahmen, so dass auch über die selbstverständlichsten Dinge informiert werden muss. Die Regelung führt damit zu völlig unnötiger Datenschutzbürokratie. Sie sollte entweder in ihrem Anwendungsbereich beschränkt oder ganz gestrichen werden. Jedenfalls sollte die Vorschrift nicht gelten, wenn die betroffenen Personen nach den Umständen des Einzelfalls mit der Verarbeitung rechnen müssen. Damit würde sichergestellt, dass nicht über Selbstverständlichkeiten zu informieren ist. Die Anforderungen könnten sich dynamisch dem allgemeinen Kenntnisstand anpassen.

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. Absatz 2 bedarf keiner Änderung, aber die restliche Verordnung sollte an diesem Ziel ausgerichtet werden. Nicht zuletzt sollte auch der Text der Verordnung der Zielsetzung entsprechend einfach und verständlich gestaltet werden. Dies würde im ersten Schritt eine wesentliche Verschärfung erfordern.

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). Der Anspruch auf elektronische Auskunft sollte deshalb gestrichen oder entsprechend eingeschränkt werden, d.h. nur in Situationen verpflichtend sein, in denen die elektronische Adresse der betroffenen Person auf Grund der vorhandenen Daten zugeordnet werden kann.

Artikel 12 Absatz 2: Angesichts der unterschiedlichsten 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 keine feste Frist geben. Die Monatsfrist ist deshalb zu streichen oder die Ausnahme von der Monatsfrist ist allgemeiner zu formulieren, denn problematisch sind nicht nur Fälle von Auskunftshäufungen. Auch hier gilt, dass ein Anspruch auf elektronische Informationen nur dann bestehen darf, wenn eine entsprechende Zuordnung der elektronischen Adresse auf Grund des vorhandenen Daten möglich ist.

Artikel 12 Absatz 4: Der Grundsatz der kostenlosen Rechtewahrnehmung sollte mit Ausnahmen versehen werden, die eine Verpflichtung zur kostenlosen Erbringung wirtschaftlicher Leistungen vermeidet. Die Kostenfreiheit sollte ausdrücklich ausgeschlossen werden, wenn kostenpflichtige Leistungen unter dem Vorwand der Ausübung datenschutzrechtlicher Rechte eingefordert werden. Außerdem sollte die Kostenfreiheit auf das Auskunftsrecht beschränkt sein. Der Anspruch auf Datenportabilität, wenn er überhaupt bestehen bleiben sollte (siehe Anmerkung zu Artikel 18), ist ein kein datenschutzrechtlicher, sondern ein rein wirtschaftlicher Anspruch, der auch entsprechend vergütet werden sollte.

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

Artikel 12 neuer Absatz: 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 aufgenommen werden. Der Erwägungsgrund allein ist keine durchsetzbare Anspruchsgrundlage.

Artikel 13: Datenqualität ist im Sinne von allen Beteiligten, aber eine generelle Verpflichtung zur Mitteilung von Berichtigungen und Löschungen an Empfänger von Daten ist realitätsfremd. Der Anspruch betrifft jede Art der Übermittlung, unabhängig davon, wie lange sie her ist oder ob schutzwürdige Interessen

der betroffenen Personen berührt sind. Die Vorschrift sollte so gestaltet werden, dass dem für die Verarbeitung Verantwortlichen die Information der Empfänger erlaubt ist und eine Pflicht zu Information nur dann besteht, wenn die betroffene Person die Information gegenüber den Empfängern verlangt, schutzwürdige Interessen der betroffenen Person berührt sind und mit der Information kein unverhältnismäßiger Aufwand verbunden ist. 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.

Artikel 14: Die Informationspflichten orientieren sich an den technischen Möglichkeiten von Internetdiensten, die eigene Datenschutzinformationen in beliebiger Länge vorsehen können. Für andere Bereiche ist die Regelung 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 für Informationspflichten von Anfang an in praktikabler Weise zu regeln. Insofern kann mit Blick auf Artikel 21 nicht auf die notwendigen und sinnvollen Ausnahmen verzichtet werden.

Artikel 14 Absatz 1: Bei der allgemeinen Informationspflicht sollte bedacht werden, dass diese den betroffenen Personen völlig unabhängig von ihrem konkreten Interesse hieran aufgedrängt wird. Insofern sollte die Information entsprechend schlank gestaltbar sein. Vor allem aber sollte es erlaubt sein, auf detailliertere Informationen zu verweisen. Auch die Benachrichtigungspflichten im Bundesdatenschutzgesetz sind vor diesem Hintergrund zu weitgehend und angesichts des Automatisierungsgrades 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. Insofern sollte es ausreichen, wenn ein Hinweis darauf erfolgt, wie die betroffene Person nähere Informationen frei zugänglich erhalten kann. Im Internet wäre dies der Link auf die Datenschutzinformation.

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 Information könnte in der Weise erfolgen, dass darüber informiert wird, wo sich detaillierte Informationen hierzu finden. Die Quelle muss für die betroffenen Personen leicht erreichbar sein, beispielsweise unter einem Internetlink.

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 Ziffer c): Die Information über die Dauer der Verarbeitung (Absatz 1 Ziffer c)) kann in der Regel nicht in allgemeiner Form 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.

Artikel 14 Absatz 1 Ziffer d) und e): Die Aufklärung über Betroffenenrechte würde mit der Zeit zu einer formelhaften Information ohne Neuigkeitswert für die betroffenen Personen. Es bestehen keine Anhaltspunkte dafür, dass es in der Praxis hier ein Informationsdefizit geben würde. Die Informationspflichten sind zu streichen.

Artikel 14 Absatz 1 Ziffer f): Die bereits heute bestehende Informationspflicht über „Kategorien von Empfängern“ bereitet in der praktischen Umsetzung Probleme, die im Rahmen der Verordnung gelöst werden sollen. „Empfänger“ im Sinne der Verordnung sind auch Auftragsverarbeiter. Es besteht kein Grund dafür, dass diese in die Informationspflicht aufgenommen werden. Jeder weiß, dass sich Unternehmen in ihrer Verwaltung Dienstleister bedienen.

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 der Begriff des „Dritten“ verwendet würde (der jedoch für die Zwecke der Verordnung noch zu definieren ist; siehe Anmerkung zu Artikel 4 Absatz 7). Alternativ sind Auftragsverarbeiter ausdrücklich von der Definition der „Empfänger“ auszunehmen.

Artikel 14 Absatz 1 Ziffer 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 Information hierüber 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 Ziffer h): Die Verpflichtung zur Bereitstellung sonstiger Informationen ist ein Einfallstor für weitere 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 Rechtssetzungsbefugnisse 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 „obligatorisch“, statt „gesetzlich vorgeschrieben“. Insofern sollte die Verordnung nach dem deutschen Beispiel klargestellt werden.

Artikel 14 Absatz 3: Wenn die Daten nicht bei der betroffenen Person erhoben werden, kann es die betroffenen Personen im Einzelfall interessieren, welche Herkunft die Daten haben. Es besteht aber kein Anlass dazu, die Herkunft bereits ungefragt in die Allgemeine Datenschutzhinweise aufzunehmen. Da es sich um eine auf die konkreten Daten individuell zugeschnittene Information ist, wäre es auch nicht so einfach möglich.

Artikel 14 Absatz 4 Ziffer a): Hinsichtlich des Informationszeitpunkts sollte berücksichtigt werden, dass Erhebungen beispielsweise auf Coupons oder auf Postkarten stattfinden. Transparenz kann auch dadurch hergestellt werden, dass unmittelbar nach der Erhebung der Daten bei der betroffenen Person diese entsprechend informiert wird. Insofern sollte eine zeitnahe Information ausreichen, statt auf den Zeitpunkt der Erhebung abzustellen. Ziffer a) sollte gestrichen und Ziffer b) zur Grundregel erklärt werden.

Artikel 14 Absatz 4 Ziffer 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 „Übermittlung“ abstellt, knüpft die Verordnung an die Weitergabe an den „Empfänger“ an. Jeder Auftragsverarbeiter wäre ein solcher Empfänger (siehe Anmerkung zu Artikel 4 Absatz 7). Dies würde dazu führen, dass beispielsweise Auskunftgebern, die Auftragsverarbeitereinschalten, bereits bei jeder Erhebung von Daten informieren müssten. Dies entspricht nicht dem Sinn der Regelung. Der Begriff des Dritten ist zu definieren und entsprechend zu verwenden. Alternativ sind Auftragsverarbeiter beim Begriff der Empfänger auszunehmen.

Artikel 14 Absatz 5: Die Ausnahmen zur Benachrichtigungspflicht sind nicht ausreichend. Hier sollte sich die Verordnung an § 33 Absatz 2 BDSG orientieren. Außerdem sollte berücksichtigt werden, 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 Rechtssetzungsbefugnisse der Europäischen Kommission sind zu streichen.

Artikel 15 Absatz 1 Ziffer 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 Ziffer d): Die Dauer der Speicherung unterliegt je nach Datenart unterschiedlichen Anforderungen. Die Information kann auch im Rahmen einer Auskunftsanfrage nicht sinnvoll gegeben werden (siehe auch Anmerkung zu Artikel 14 Absatz 1 Ziffer c)).

Artikel 15 Absatz 1 Ziffer 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. Die Ziffer sollte gestrichen werden.

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

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. Statt dessen sollte ausdrücklich geregelt werden, dass der für die Verarbeitung Verantwortliche auch ohne Verlangen durch die betroffene Person das Recht hat, unzutreffende Daten zu berichtigen. Dies wäre hilfreich, um die Datenqualität auch im Sinne der betroffenen Personen dauerhaft zu fördern.

Artikel 17: Soweit das Recht auf Vergessenwerden schlicht einen Anspruch auf Löschung rechtswidrig gespeicherter Daten darstellt, ist hiergegen nichts einzuwenden. Artikel 17 geht aber wesentlich weiter und es 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.

Artikel 17 Absatz 1: Der beispielhafte Verweis auf Kinder ist nicht hilfreich und führt zu unnötigen Auslegungsfragen. Er sollte entweder gestrichen werden oder die Klausel sollte nur für diesen Fall gelten.

Artikel 17 Absatz 1 Ziffern a): Der Begriff „notwendig“ wirft Auslegungsfragen auf. Die Pflicht sollte streng an die Rechtmäßigkeitsvoraussetzungen geknüpft werden. Deshalb ist darauf abzustellen, dass die Verarbeitung nicht mehr „rechtmäßig“ ist. Die weiteren Ziffern b) bis d) können dann gestrichen werden.

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

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

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

Artikel 17 Absatz 2: Die Verpflichtung zur Weiterverfolgung der Löschung gegenüber Dritten ist einer der schwerwiegendsten Auflagen der 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.

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. Die Ziffern a) bis e) in Absatz 3 können allenfalls als Ausnahme von diesem Grundsatz formuliert werden.

Artikel 17 Absatz 4: Im Grundsatz ist es richtig, wenn zwischen Löschung und Beschränkung unterschieden wird. Der im deutschen BDSG verwendete Begriff der „Sperrung“ entspricht nicht mehr der

Wirklichkeit der Datenverarbeitungstechnik. Die in § 35 BDSG verwendeten Sperrungstatbestände sind aber grundsätzlich zu übernehmen. Insofern 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 beispielsweise bedeuten, dass eine Verwendung von Daten zu Beweis Zwecken eine Informationspflicht gegenüber dem Betroffenen auslösen würde. Da die betroffene Person bereits über die Verarbeitung an sich unterrichtet ist, besteht für die erneute Information kein angemessener Anlass. Die Erfüllung der Informationspflicht kann im Einzelfall sehr aufwendig sein. Ausnahmen unter Berücksichtigung der Aufwands fehlen. Auch dieser Absatz ist deshalb zu streichen.

Artikel 17 Absatz 7: Diese Regelung ist nicht erforderlich und sollte gestrichen werden.

Artikel 17 Absatz 8: Es ist unklar, was mit dieser Regel gemeint ist.

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

Artikel 18: Das Recht auf Datenportabilität (in 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. 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.

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 haben, 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 hervorheben, weil der Gesetzgeber an verschiedensten Stellen diese Anforderung stellt. Dies führt beispielsweise bei der Gestaltung von Bestellformularen dazu, dass die bestellte Ware und ihr Preis hinter lauter anderen hervorgehobenen oder abgegrenzten Informationen untergeht. 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 - die Worte „für nichtkommerzielle Zwecke“ zu streichen.

Artikel 20: In der Datenschutzrichtlinie wurde (gegen den Widerstand Deutschlands) eine Regelung zu automatisierten Einzelentscheidungen (Artikel 15) aufgenommen. Diese wird jetzt durch Artikel 20 weiterentwickelt, statt aus den Erfahrungen mit der alten Regelung zu lernen und diese zu streichen. Automatisierte Einzelentscheidungen sind heute alltäglich und sollten nicht grundsätzlich verboten werden. Die Regelung hat jetzt außerdem einen überzogenen 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 betroffene Person erheblich beeinträchtigt, dann sollte die für die Verarbeitung Verantwortliche Stelle verpflichtet sein, diese Entscheidung auf Anfrage der betroffenen Person zu erläutern und zu überprüfen. Darüber hinaus besteht kein Regelungsbedarf.

Artikel 20 Absatz 4: Es wird nicht klar, welche Informationen die Vorschrift zusätzlich zu den allgemeinen Auskunftsrechten verlangt. Der Verweis auf Artikel 14 ist falsch. Es müsste auf das Auskunftsrecht in Artikel 15 verwiesen werden.

Artikel 20 Absatz 5: Die Rechtsetzungsbefugnis 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.

Anmerkungen Artikel 1 bis 21

Artikel 1 Absatz 1: Zu der Frage der Rechtsnatur der Verordnung sind wir der Ansicht, dass grundsätzlich eine striktere europaweite Harmonisierung wünschenswert ist. Wir sind angesichts der vorgesehenen Ausnahmen aber auch der Ansicht, dass der vorliegende Entwurf hier im Grunde ein Rückschritt gegenüber der bisherigen Richtlinie (95/46/EG) ist, die ja nach der zutreffenden Auslegung des Europäischen Gerichtshofs (C-468/10 und C-469/10) bereits eine Vollharmonisierung enthält. Am Ende kommt es deshalb nicht darauf an, ob die Regelung im Wege einer Verordnung oder einer Richtlinie erfolgt. Wichtig ist nur, dass die Regelungen ausgewogen sind und sich alle Mitgliedstaaten daran halten. Unter Subsidiaritätsgesichtspunkten wären wir auch einer Lösung gegenüber aufgeschlossen, bei der die Verordnung sich auf Fragen des Drittländerdatentransfers beschränkt und die Harmonisierung ansonsten weiterhin über eine Richtlinie erfolgt. Dies würde auch der Tatsache Rechnung tragen, dass das Datenschutzrecht stark mit anderen Rechtsbereichen verwebt ist und eine europäische Verordnung hier als Fremdkörper im Verhältnis zum nationalen Recht unweigerlich zu erheblichen Auslegungsunsicherheiten führen würde.

Artikel 1 Absatz 3: Wir sind der Ansicht, dass Artikel 16 Abs. 2 des Vertrages über die Arbeitsweise der Europäischen Union (AEUV) keine Rechtsgrundlage für die Regelung des Datenschutzes im nicht-öffentlichen Bereich ist. Die Vorschrift bezieht sich ausdrücklich ausschließlich auf den öffentlichen Bereich. Die richtige Rechtsgrundlage für den nicht-öffentlichen Bereich ist allein Artikel 114 Abs. 1 AEUV, der auch am Anfang des Verordnungsentwurfs aufgeführt wird. Artikel 1 Absatz 3 ist der bisherigen Richtlinie entnommen, aber war auch dort schon unglücklich formuliert. 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 Binnenmarktes 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“ gestrichen werden. Es gibt keine Rechtsgrundlage, die es der Europäischen Union erlaubt, aus diesem Grund Regelungen im Bereich des nicht-öffentlichen Datenschutzes zu treffen. Damit würde auch deutlicher, dass die Verordnung im Ergebnis wirtschaftlichen Interessen dienen muss und diese nicht behindern soll. Weiterhin sollte stärker hervorgehoben werden, dass der grundrechtliche Schutz personenbezogener Daten nicht absolut gilt, sondern einer Abwägung

mit anderen Grundrechten unterliegt, insbesondere im Hinblick auf die unternehmerische Freiheit. Dieser Aspekt liegt bisher im Erwägungsgrund 139 etwas versteckt im Hintergrund und wird im Rahmen der Verordnung auch nicht berücksichtigt.

Artikel 2 Absatz 1: Der Anwendungsbereich auf nicht-automatisierte Verarbeitungen ist bereits nach der geltenden Richtlinie problematisch, weil beispielsweise ein nach Adressaten sortierter Stapel adressierter Briefe bereits unter den Anwendungsbereich fällt. Insofern ist die Formulierung in Erwägungsgrund 13 („die in einem Ablagesystem gespeichert sind“) zu begrüßen. Leider findet sich diese Einschränkung aber nicht in Artikel 2 Absatz 1 oder der Definition der Datei in Artikel 4 Absatz 4. Nachteilig 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 dem Wohnort sortiert ist, würde dies auch zur Anwendung der Verordnung und aller damit verbundenen Rechte und Pflichten führen. Nach der bisherigen Richtlinie muss es sich laut Erwägungsgrund 15 um „personenbezogene“ Kriterien handeln. Dies sollte beibehalten und auch ausdrücklich in der Definition des Begriff „Datei“ aufgenommen werden. Auch für die Frage der Anwendung der Vorschrift auf Akten ist dies wichtig.

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 wichtig, da insbesondere im Internet und mobil viele Dienste angeboten werden, die den Nutzern zur Verarbeitung zu persönlichen und familiären Zwecken dienen. Wenn bei diesen Diensten der Anwendungsbereich der Verordnung eröffnet würde, müssten alle Anforderungen an eine Auftragsverarbeitung eingehalten werden, was in der Praxis unmöglich ist. Das zusätzliche Merkmal „ohne jede Gewinnerzielungsabsicht“ führt hier zu unnötiger Rechtsunsicherheit darüber, was ausgenommene Verarbeitungen sind. Heute verstehen wir sehr wohl eine Reihe von Datenverarbeitungen im geschäftlichen Bereich als „persönlich“. Beispielsweise würde jedes persönliche elektronische Telefonverzeichnis, das auch geschäftliche Kontakte enthält, unter den Anwendungsbereich der Verordnung fallen. Die damit verbundenen Konsequenzen sind in der Praxis nicht umsetzbar.

Artikel 2 Absatz 3: Die Vorrangregelungen zu anderen Richtlinien (auch später in 89 zur ePrivacy Richtlinie) sind im Grundsatz problematisch, weil es eines Vorrangs des

umsetzenden nationalen Rechts vor der Verordnung bedarf. Ein Vorrang der Richtlinie vor der Verordnung greift zu kurz.

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 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 sollte der Verweis auf „oder jede sonstige natürliche oder juristische Person“ in Artikel 4 Absatz 1 und auf „oder einer anderen Person“ in Erwägungsgrund 23 gestrichen werden. Sobald solche „andere Personen“ die Daten erhalten, soll die Verordnung Anwendung finden, aber nicht, wenn dies nicht erfolgt. Die Streichung des Verweises auf andere Personen würde auch nicht dazu führen, dass sie 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 3: Wir würden es begrüßen, wenn – nach dem Beispiel von § 3 Abs. 6 BDSG – eine Definition der Anonymisierung aufgenommen und dann die Anonymisierung ausdrücklich von der Definition der Verarbeitung ausgeschlossen würde. Aus datenschutzrechtlicher Sicht ist eine Anonymisierung von Daten stets wünschenswert und sollte nicht datenschutzrechtlich beschränkt sein oder gar datenschutzrechtliche Verpflichtungen auslösen. Außerdem wäre eine Definition der Anonymisierung hilfreich um die Abgrenzung zur Definition der personenbezogenen Daten zu schärfen.

Artikel 4 Absatz 4: Siehe Anmerkung zu Artikel 2 Absatz 1. Die Worte „nach bestimmten Kriterien“ sollten durch „nach bestimmten personenbezogenen Kriterien“ ersetzt werden, so wie es in Erwägungsgrund 15 der bisherigen Richtlinie bestimmt wird.

Artikel 4 Absatz 5 und 6: Eines der aktuellen praktischen Probleme der Auftragsverarbeitung liegt darin, dass die Datenschutzaufsichtsbehörden in den Auftragsverarbeitungsverträgen unangemessen detaillierte Vorgaben des Auftraggebers hinsichtlich der „Mittel“ der Verarbeitung fordern. Datenschutzrechtlich haben diese Detaillierungen jedoch keinerlei Mehrwert. Sie haben aber Nachteile, denn jede Änderung der „Mittel“ erfordert dann eine Vertragsänderung, d.h. wenn beispielsweise eine bestimmte technische Infrastruktur beschrieben ist, kann der Auftragsverarbeiter diese nur noch ändern, nachdem er dies mit allen 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 „Mittel“ eingesetzt werden. Insofern sollte – auch in Abweichung zur bisherigen Richtlinie und entsprechend der deutschen Regelung in § 11 BDSG – der Verweis auf „Mittel“ gestrichen werden. Auf jeden Fall sollte der neu hinzugefügte Verweis auf „Bedingungen“ gestrichen werden. Es ist unklar, was damit überhaupt gemeint ist und würde nur zu einer weiteren Bürokratisierung der Auftragsverarbeitung führen.

Artikel 4 Absatz 7: Die Definition des „Dritten“ wurde gestrichen, so dass jetzt keine Differenzierung mehr zwischen „Empfängern“ und „Dritten“ erfolgt. Damit werden in den jeweiligen Regelungen insbesondere Auftragsverarbeiter immer mit erfasst. Dies führt insbesondere dazu, dass nach Artikel 14 Absatz 4 b) die Information gegeben werden müsste, bevor die Daten an einen Auftragsverarbeiter weitergegeben werden. Hierfür besteht kein sachlicher Grund. Auch in anderen Vorschriften (wie beispielsweise bei der Auskunft) wäre der Begriff des Dritten notwendig. Alternativ wäre zu überlegen, ob Auftragsverarbeiter nicht ausdrücklich von der Definition der „Empfänger“ ausgenommen werden.

Artikel 4 Absatz 8: Von der Verwendung von Einwilligungserklärungen sollte nicht durch übertriebene Anforderungen abgeschreckt werden. Insbesondere das Wort „explizit“ sollte hier gestrichen werden. 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 werden ?

Artikel 4 Absatz 10, 11 und 12: Die Definitionen sind in einer Weise formuliert, dass ihnen ein uferloser Anwendungsbereich zukommen könnte. 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 und 15: Der Begriff der Hauptniederlassung spielt an Stellen der Verordnung eine Rolle, wo die Anwendung des Datenschutzrechts für grenzüberschreitend tätige Unternehmen geregelt wird. Es sollte überlegt werden, ob entsprechende Grundsätze auch dann gelten sollen, wenn in einem Land (wie in Deutschland) mehrere lokale Aufsichtsbehörden existieren. Außerdem wäre es wichtig, dass eine entsprechende Regelung auch dann greift, wenn es um selbständige Niederlassungen geht. 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 deutschen Steuerrecht könnte so eine Konzernregelung eingeführt 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 erfolgen. 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 dann nicht gelten. Die Grenze des 13. Lebensjahrs sollte verwendet werden.

Artikel 5: Der Regelungswert der „Grundsätze“ neben den Rechtmäßigkeitsanforderungen sollte überdacht werden. Außerdem ist zu bedenken, 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 nach Artikel 21). Nur Artikel 5 Buchstabe b) 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 Buchstabe d): Die Qualität der Daten liegt in der Regel auch im Interesse der Unternehmen. Es sollte aber auch sichergestellt sein, dass die Maßnahmen zur Schaffung dieser Qualität auch datenschutzrechtlich zulässig sind. Dies könnte in einem der Erwägungsgründe klargestellt werden.

Artikel 5 Buchstabe f): Hier wird dem für die Verarbeitung Verantwortliche 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).

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 Verbotes mit Erlaubnisvorbehalt sollte in diesem Zusammenhang überdacht werden. Man könnte beispielsweise überlegen, ob die Rechtmäßigkeitsanforderungen grundsätzlich nur erforderlich sind, wenn ein überwiegendes schutzwürdiges Interesse des Betroffenen berührt ist. Nur dann besteht auch die Notwendigkeit der gesetzlichen Einschränkung.

Artikel 6 Absatz 1 Buchstabe a): Die Anforderungen an wirksame Einwilligungen werden in der Definition der Einwilligung, in Artikel 7 und in Artikel 6 Absatz 1 Buchstabe a) festgelegt und an jeder dieser Stellen verschärft. Die Formulierung „Die betroffene Person hat ihre Einwilligung gegeben.“ würde hier ausreichen. Zumindest sollte das Wort „genau“ gestrichen oder zumindest dieselbe Formulierung wie in Artikel 7 Absatz 1 verwendet werden (in der deutschen Fassung sind es sogar unterschiedliche Wörter; „genau“ und „eindeutig“).

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 rechtsgeschäftsähnliche Beziehungen mit aufzunehmen sind, die ja nicht nur vorvertraglich bestehen können. Die 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 zur Kreditauskunfteien. Die Arbeitsteilung zwischen professionellen Datenanbietern und den Empfängern der Daten wäre 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.

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 Buchstaben 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 sie 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 Buchstaben 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 ist deshalb um einen Verweis auf Buchstaben f) zu ergänzen.

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 Rechtssetzung 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 Verbreitung des Anwendungsbereichs der Einwilligung und Erhöhung ihrer Wirksamkeitsvoraussetzungen ist in der Praxis nicht verkraftbar. Nur wenn die Einwilligung tatsächlich sehr sensiblen Vorgängen vorbehalten bleibt, darf sie auch hohe Anforderungen haben. 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 „eindeutig“ oder „genau“ die Verwender von Einwilligungserklärungen zu Verwendung langer und unübersichtlicher Einwilligungstexte zu zwingen. Außerdem sollten auch konkludente Einwilligungen möglich sein (siehe Anmerkung zu Artikel 4 Absatz 8). Nicht zuletzt ist die jederzeitige

Widerrufbarkeit von Einwilligungen 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.

Artikel 8: Es ist für uns nicht nachvollziehbar, zu welchem Ergebnis die Einschränkung von Absatz 1 durch Absatz 2 in Deutschland kommen würde. Der Ansatz, die besonderen Schutzvorschriften auf Kinder bis zum 13. Lebensjahr zu beschränken, ist jedoch zu begrüßen. Dies sollte bereits in der Definition des Begriffs „Kind“ in Artikel 4 Absatz 18 erfolgen.

Artikel 9: Wie bereits unter der geltenden Richtlinie wird die Verarbeitung von besonderen Kategorien von Daten unabhängig von ihrer individuellen Sensibilität beschränkt. Der Ansatz führt zu unangemessenen Beschränkungen von Daten. Es sollte überlegt werden, ob insbesondere Artikel 9 Absatz 2 Buchstabe e) im Anwendungsbereich erweitert werden kann. In der Verordnung sollte vermieden werden, dass unsensible besondere Kategorien von Daten besonders geschützt werden. Dies kann nicht nur davon abhängen, ob sie die betroffene Person selbst öffentlich gemacht hat.

Artikel 10: Die Vorschrift ist vom Ansatz her zu begrüßen, sollte aber so formuliert werden, dass sie sich nicht auf anonymisierte Daten beschränkt ist, sondern auch für pseudonymisierte Daten gilt. Derzeit findet die Vorschrift nur dann Anwendung, wenn die Verordnung keine Anwendung findet, was im Ergebnis inkonsistent ist. Die Klausel sollte außerdem die Möglichkeit der Löschung identifizierender Datenelemente erlauben. Wichtig ist, dass der Grundgedanke bei späteren Vorschriften (beispielsweise im Zusammenhang mit Auskunftsrechten, die bisher ausnahmslos auch für nicht vollständig identifizierte Daten gelten) fortgesetzt werden. Insbesondere ist Erwägungsgrund 45 in den Vorschriften der Verordnung umzusetzen.

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 „jedermann leicht zugängliche Strategie“. In der englischen Sprachfassung wird diese als „Policy“ bezeichnet. Für Internetdienste sind solche Policies üblich. 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 umzusetzen, ohne dass ein besonderer Mehrwert für die betroffenen Personen erkennbar ist.

Die Regelung ist damit eines von vielen Beispielen im Verordnungsentwurf, bei denen internetspezifische Regelungen unsachgemäß auf alle anderen Wirtschaftsbereiche erweitert werden. Dies belegt auch Erwägungsgrund 46, der auf den Bereich des Internets abhebt. Außerdem enthält die Vorschrift keinerlei Ausnahmen, so dass auch über die selbstverständlichsten Dinge informiert werden muss. Die Regelung führt damit zu völlig unnötiger Datenschutzbürokratie. Sie sollte entweder in ihrem Anwendungsbereich beschränkt oder ganz gestrichen werden. Jedenfalls sollte die Vorschrift nicht gelten, wenn die betroffenen Personen nach den Umständen des Einzelfalls mit der Verarbeitung rechnen müssen. Damit würde sichergestellt, dass nicht über Selbstverständlichkeiten zu informieren ist. Die Anforderungen könnten sich dynamisch dem allgemeinen Kenntnisstand anpassen.

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. Absatz 2 bedarf keiner Änderung, aber die restliche Verordnung sollte an diesem Ziel ausgerichtet werden. Nicht zuletzt sollte auch der Text der Verordnung der Zielsetzung entsprechend einfach und verständlich gestaltet werden. Dies würde im ersten Schritt eine wesentliche Verschlankung erfordern.

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). Der Anspruch auf elektronische Auskunft sollte deshalb gestrichen oder entsprechend eingeschränkt werden, d.h. nur in Situationen verpflichtend sein, in denen die elektronische Adresse der betroffenen Person auf Grund der vorhandenen Daten zugeordnet werden kann.

Artikel 12 Absatz 2: Angesichts der unterschiedlichsten 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 keine feste Frist geben. Die Monatsfrist ist deshalb zu streichen oder die Ausnahme von der Monatsfrist ist allgemeiner zu formulieren, denn problematisch sind nicht nur Fälle von Auskunftshäufungen. Auch hier gilt, dass ein Anspruch auf elektronische Informationen nur dann bestehen darf, wenn eine entsprechende Zuordnung der elektronischen Adresse auf Grund des vorhandenen Daten möglich ist.

Artikel 12 Absatz 4: Der Grundsatz der kostenlosen Rechtewahrnehmung sollte mit Ausnahmen versehen werden, die eine Verpflichtung zur kostenlosen Erbringung wirtschaftlicher Leistungen vermeidet. Die Kostenfreiheit sollte ausdrücklich ausgeschlossen werden, wenn kostenpflichtige Leistungen unter dem Vorwand der Ausübung datenschutzrechtlicher Rechte eingefordert werden. Außerdem sollte die Kostenfreiheit auf das Auskunftsrecht beschränkt sein. Der Anspruch auf Datenportabilität, wenn er überhaupt bestehen bleiben sollte (siehe Anmerkung zu Artikel 18), ist ein kein datenschutzrechtlicher, sondern ein rein wirtschaftlicher Anspruch, der auch entsprechend vergütet werden sollte.

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

Artikel 12 neuer Absatz: 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 aufgenommen werden. Der Erwägungsgrund allein ist keine durchsetzbare Anspruchsgrundlage.

Artikel 13: Datenqualität ist im Sinne von allen Beteiligten, aber eine generelle Verpflichtung zur Mitteilung von Berichtigungen und Löschungen an Empfänger von Daten ist realitätsfremd. Der Anspruch betrifft jede Art der Übermittlung, unabhängig davon, wie

lange sie her ist oder ob schutzwürdige Interessen der betroffenen Personen berührt sind. Die Vorschrift sollte so gestaltet werden, dass dem für die Verarbeitung Verantwortlichen die Information der Empfänger erlaubt ist und eine Pflicht zu Information nur dann besteht, wenn die betroffene Person die Information gegenüber den Empfängern verlangt, schutzwürdige Interessen der betroffenen Person berührt sind und mit der Information kein unverhältnismäßiger Aufwand verbunden ist. 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.

Artikel 14: Die Informationspflichten orientieren sich an den technischen Möglichkeiten von Internetdiensten, die eigene Datenschutzinformationen in beliebiger Länge vorsehen können. Für andere Bereiche ist die Regelung 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 die notwendigen und sinnvollen Ausnahmen verzichtet werden.

Artikel 14 Absatz 1: Bei der allgemeinen Informationspflicht sollte bedacht werden, dass diese den betroffenen Personen völlig unabhängig von ihrem konkreten Interesse hieran aufgedrängt wird. Insofern sollte die Information entsprechend schlank gestaltbar sein. Vor allem aber sollte es erlaubt sein, auf detailliertere Informationen zu verweisen. Auch die Benachrichtigungspflichten im Bundesdatenschutzgesetz sind vor diesem Hintergrund zu weitgehend und angesichts des Automatisierungsgrades 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. Insofern sollte es ausreichen, wenn ein Hinweis darauf erfolgt, wie die betroffene Person nähere Informationen frei zugänglich erhalten kann. Im Internet wäre dies der Link auf die Datenschutzinformation.

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 Information könnte in der Weise erfolgen, dass darüber informiert wird, wo sich detaillierte Informationen hierzu finden. Die

Quelle muss für die betroffenen Personen leicht erreichbar sein, beispielsweise unter einem Internetlink.

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 Datenschutzzinformationen als wenig hilfreich angesehen werden. Dies gilt vor allem dann, wenn sie sehr allgemeine Informationen enthalten, die sich in jeder Datenschutzzinformation wiederholen, obwohl sie der Allgemeinheit ohnehin bekannt sind.

Artikel 14 Absatz 1 Ziffer c): Die Information über die Dauer der Verarbeitung (Absatz 1 Ziffer c)) kann in der Regel nicht in allgemeiner Form 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.

Artikel 14 Absatz 1 Ziffer d) und e): Die Aufklärung über Betroffenenrechte würde mit der Zeit zu einer formelhaften Information ohne Neuigkeitswert für die betroffenen Personen. Es bestehen keine Anhaltspunkte dafür, dass es in der Praxis hier ein Informationsdefizit geben würde. Die Informationspflichten sind zu streichen.

Artikel 14 Absatz 1 Ziffer f): Die bereits heute bestehende Informationspflicht über „Kategorien von Empfängern“ bereitet in der praktischen Umsetzung Probleme, die im Rahmen der Verordnung gelöst werden sollen. „Empfänger“ im Sinne der Verordnung sind auch Auftragsverarbeiter. Es besteht kein Grund dafür, dass diese in die Informationspflicht aufgenommen werden. Jeder weiß, dass sich Unternehmen in ihrer Verwaltung Dienstleister bedienen.

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 der Begriff des „Dritten“ verwendet würde (der jedoch für die Zwecke der Verordnung noch zu definieren ist; siehe

Anmerkung zu Artikel 4 Absatz 7). Alternativ sind Auftragsverarbeiter ausdrücklich von der Definition der „Empfänger“ auszunehmen.

Artikel 14 Absatz 1 Ziffer 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 Information hierüber 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 Ziffer h): Die Verpflichtung zur Bereitstellung sonstiger Informationen ist ein Einfallstor für weitere 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 Rechtssetzungsbefugnisse 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 „obligatorisch“, statt „gesetzlich vorgeschrieben“. Insofern sollte die Verordnung nach dem deutschen Beispiel klargestellt werden.

Artikel 14 Absatz 3: Wenn die Daten nicht bei der betroffenen Person erhoben werden, kann es die betroffenen Personen im Einzelfall interessieren, welche Herkunft die Daten haben. Es besteht aber kein Anlass dazu, die Herkunft bereits ungefragt in die Allgemeine Datenschutzhinweise aufzunehmen. Da es eine auf die konkreten Daten individuell zugeschnittene Information ist, wäre es auch nicht so einfach möglich.

Artikel 14 Absatz 4 Ziffer a): Hinsichtlich des Informationszeitpunkts sollte berücksichtigt werden, dass Erhebungen beispielsweise auf Coupons oder auf Postkarten stattfinden. Transparenz kann auch dadurch hergestellt werden, dass unmittelbar nach der Erhebung der Daten bei der betroffenen Person diese entsprechend informiert wird. Insofern sollte eine zeitnahe Information ausreichen, statt auf den Zeitpunkt der Erhebung abzustellen. Ziffer a) sollte gestrichen und Ziffer b) zur Grundregel erklärt werden.

Artikel 14 Absatz 4 Ziffer 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 „Übermittlung“ abstellt, knüpft die Verordnung an die Weitergabe an den „Empfänger“ an. Jeder Auftragsverarbeiter wäre ein solcher Empfänger (siehe Anmerkung zur Artikel 4 Absatz 7). Dies würde dazu führen, dass beispielsweise Auskunftgebern, die Auftragsverarbeitereinsetzen, bereits bei jeder Erhebung von Daten informieren müssten. Dies entspricht nicht dem Sinn der Regelung. Der Begriff des Dritten ist zu definieren und entsprechend zu verwenden. Alternativ sind Auftragsverarbeiter beim Begriff der Empfänger auszunehmen.

Artikel 14 Absatz 5: Die Ausnahmen zur Benachrichtigungspflicht sind nicht ausreichend. Hier sollte sich die Verordnung an § 33 Absatz 2 BDSG orientieren. Außerdem sollte berücksichtigt werden, 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 Rechtssetzungsbefugnisse der Europäischen Kommission sind zu streichen.

Artikel 15 Absatz 1 Ziffer 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 Ziffer d): Die Dauer der Speicherung unterliegt je nach Datenart unterschiedlichen Anforderungen. Die Information kann auch im Rahmen einer Auskunftsanfrage nicht sinnvoll gegeben werden (siehe auch Anmerkung zu Artikel 14 Absatz 1 Ziffer c)).

Artikel 15 Absatz 1 Ziffer 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. Die Ziffer sollte gestrichen werden.

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

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. Statt dessen sollte ausdrücklich geregelt werden, dass der für die Verarbeitung Verantwortliche auch ohne Verlangen durch die betroffene Person das Recht hat, unzutreffende Daten zu berichtigen. Dies wäre hilfreich, um die Datenqualität auch im Sinne der betroffenen Personen dauerhaft zu fördern.

Artikel 17: Soweit das Recht auf Vergessenwerden schlicht einen Anspruch auf Löschung rechtswidrig gespeicherter Daten darstellt, ist hiergegen nichts einzuwenden. Artikel 17 geht aber wesentlich weiter und es 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.

Artikel 17 Absatz 1: Der beispielhafte Verweis auf Kinder ist nicht hilfreich und führt zu unnötigen Auslegungsfragen. Er sollte entweder gestrichen werden oder die Klausel sollte nur für diesen Fall gelten.

Artikel 17 Absatz 1 Ziffern a): Der Begriff „notwendig“ wirft Auslegungsfragen auf. Die Pflicht sollte streng an die Rechtmäßigkeitsvoraussetzungen geknüpft werden. Deshalb ist darauf abzustellen, dass die Verarbeitung nicht mehr „rechtmäßig“ ist. Die weiteren Ziffern b) bis d) können dann gestrichen werden.

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

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

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

Artikel 17 Absatz 2: Die Verpflichtung zur Weiterverfolgung der Löschung gegenüber Dritten ist einer der schwerwiegendsten Auflagen der 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.

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. Die Ziffern a) bis e) in Absatz 3 können allenfalls als Ausnahme von diesem Grundsatz formuliert werden.

Artikel 17 Absatz 4: Im Grundsatz ist es richtig, wenn zwischen Löschung und Beschränkung unterschieden wird. Der im deutschen BDSG verwendete Begriff der „Sperrung“ entspricht nicht mehr der Wirklichkeit der Datenverarbeitungstechnik. Die in § 35 BDSG verwendeten Sperrungstatbestände sind aber grundsätzlich zu übernehmen. Insofern 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 beispielsweise bedeuten, dass eine Verwendung von Daten zu Beweis Zwecken eine Informationspflicht gegenüber dem Betroffenen auslösen würde. Da die betroffene Person bereits über die Verarbeitung an sich unterrichtet ist, besteht für die erneute Information kein angemessener Anlass. Die Erfüllung der Informationspflicht kann im Einzelfall sehr aufwendig sein. Ausnahmen unter Berücksichtigung der Aufwands fehlen. Auch dieser Absatz ist deshalb zu streichen.

Artikel 17 Absatz 7: Diese Regelung ist nicht erforderlich und sollte gestrichen werden.

Artikel 17 Absatz 8: Es ist unklar, was mit dieser Regel gemeint ist.

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

Artikel 18: Das Recht auf Datenportabilität (in 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. 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.

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 haben, 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 hervorheben, weil der Gesetzgeber an verschiedensten Stellen diese Anforderung stellt. Dies führt beispielsweise bei der Gestaltung von Bestellformularen dazu, dass die bestellte Ware und ihr Preis hinter lauter anderen hervorgehobenen oder abgegrenzten Informationen untergeht. 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 - die Worte „für nichtkommerzielle Zwecke“ zu streichen.

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

überzogenen 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 betroffenen Person erheblich beeinträchtigt, dann sollte die für die Verarbeitung Verantwortliche Stelle verpflichtet sein, diese Entscheidung auf Anfrage der betroffenen Person zu erläutern und zu überprüfen. Darüber hinaus besteht kein Regelungsbedarf.

Artikel 20 Absatz 4: Es wird nicht klar, welche Informationen die Vorschrift zusätzlich zu den allgemeinen Auskunftsrechten verlangt. Der Verweis auf Artikel 14 ist falsch. Es müsste auf das Auskunftsrecht in Artikel 15 verwiesen werden.

Artikel 20 Absatz 5: Die Rechtsetzungsbefugnis 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.