VDZ Verband Deutscher Zeitschriftenverleger

Haus der Presse
Markgrafenstraße 15
10969 Berlin

BDZV

Haus der Presse
Markgrafenstraße 15
10969 Berlin

Position der deutschen Zeitschriften- und Zeitungsverleger zum Vorschlag der Europäischen Kommission für eine EU-Datenschutzverordnung vom 25.01.2012 (KOM(2012)11 endg.)

(Vorläufige Version v1, Stand 09.05.2012)

I. Vorbemerkung

Das Datenschutzrecht und insbesondere die derzeit geltende Richtlinie 95/46/EG sind seit jeher für wesentliche Bereiche der Pressetätigkeit relevant. Redaktionelle Pressefreiheit ist ohne Ausnahmen vom Datenschutzrecht nicht möglich. Adressiertes Direktmarketing klassischer wie digitaler Presseabonnements ist für den Erhalt der Leserschaft unverzichtbar. Die Digitalisierung und die damit einhergehenden strukturellen Herausforderungen erfordern einen verstärkten Ausbau der digitalen Angebote der Verlage. Die Überarbeitung des geltenden Rechtsrahmens ist daher von elementarer Bedeutung für die Presse. Im Zusammenhang mit der Überarbeitung sind die Hauptanliegen der Zeitschriften- und Zeitungsverleger daher folgende:

- **Robuste und direkt anwendbare Bereichsausnahme für die journalistische Datenverarbeitung erforderlich.** Die Anwendung der Datenschutzvorschriften auf die journalistische Datenverarbeitung würde eine freie redaktionelle Berichterstattung in weiten Teilen unmöglich machen. Ein Großteil aller Informationen über Politik, Wirtschaft und sonstige Gesellschaft, die eine freie Presse frei sammeln, speichern und auswerten sowie veröffentlichen können muss, sind personenbezogen (siehe auch II. Ziffer 16).

- **Direktmarketing als wesentliche Voraussetzung freier und unabhängiger Presse muss weiter sachgerecht möglich bleiben.** Die freie und unabhängige Presse sowie die Medienvielfalt hängen in hohem Maße von der Möglichkeit ab, effektiv für Zeitschriften und Zeitungen zu werben. Es ist daher insbesondere unabdingbar, dass die Datenverarbeitung für zentrale Bereiche des Direktmarketings weiterhin ohne Einwilligung, aber mit Information und Widerspruchsmöglichkeit, zulässig bleibt (siehe auch II. Ziffern 4, 5, 10, 12, 15, 17).

- **Digitale Geschäftsmodelle dürfen nicht belastet werden.** Digitale Geschäftsmodelle von der Werbung in der digitalen Presse über die Bewerbung digitaler Abonnements bis hin zum E-Commerce sind unverzichtbar**.** Die Überarbeitung der Datenschutzrichtlinie darf daher nicht dazu führen, die Nutzung und weitere Entwicklung solcher Geschäftsmodelle unverhältnismäßig zu beeinträchtigen oder gar unmöglich zu machen (siehe auch II. Ziffern 1 – 7, 12, 15, 17, 18).

II. Konkrete Aspekte

1. Definition personenbezogener Daten (Art. 4 Nr. 1 und 2). Nach der in dieser Vorschrift enthaltenen Definition können als personenbezogener Daten all diejenigen Daten verstanden werden, die direkt oder indirekt auf eine bestimmte Person bezogen werden *können*. Diese Definition stellt damit lediglich auf die *generelle Möglichkeit der Bestimmbarkeit* der betroffenen Person ab, was einen extrem weiten Anwendungsbereich eröffnet. Dies führt in Kombination mit den damit einhergehenden Pflichten für die Verarbeitung praktisch aller Daten zu einem nicht mehr überschaubaren Aufwand für die Unternehmen. Diese Problematik wird durch Erwägungsgrund 24 nur noch unterstrichen, in dem darauf hingewiesen wird, dass Kennnummern, Standortdaten, Online-Kennungen oder sonstige Elemente als solche zwar nicht zwangsläufig und unter allen Umständen als personenbezogene Daten zu betrachten seien, dies jedoch auch nicht ausgeschlossen wird.

Auch bei einer Anonymisierung von ursprünglich personenbezogenen Daten werden regelmäßig „Elemente“ oder Kennziffern“ verwendet, so dass selbst solche Daten womöglich als „personenbezogen im Sinne dieser Definition angesehen würden.

Des Weiteren lässt die weite Definition personenbezogener Daten die Möglichkeit der Pseudonymisierung der Nutzerdaten außer Acht. Diese ist im Bundesdatenschutzgesetz vorgesehen, um die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren (§ 3 Abs. 6a BDSG). Eine solche Möglichkeit der Nutzung von pseudonym erstellten Nutzerprofilen unter Einräumung eines Widerspruchsrechts des Betroffenen sollte auch weiterhin ohne Einwilligung möglich bleiben (§ 15 Abs. 3 TMG).

Dieser ausgedehnte Anwendungsbereich erscheint angesichts der möglicherweise betroffenen unterschiedlichen Kategorien von Daten in vielen Fällen aufgrund geringer Schutzbedürftigkeit auch aus Verbraucherschutzgesichtspunkten nicht gerechtfertigt.

2. Explizite Einwilligung (Art. 4 Abs. 8). Ausweislich Art. 4 Abs. 8 soll die Einwilligung nun „explizit“ abgegeben werden. Dies könnte bewährte und den Umständen des jeweiligen Einzelfalles angepasste Möglichkeiten zur Einwilligung – sowohl im Rahmen traditioneller Kommunikationswege als auch im digitalen Bereich – erheblich beeinträchtigen.

> **a) Konkludente Einwilligung weiter möglich?** Unklar ist insbesondere, ob auch eine konkludente Einwilligung weiterhin möglich ist (z. B. durch Einwerfen einer Visitenkarte in eine entsprechend gekennzeichnete Box). Auch einem konkludenten Tun oder Unterlassen kann der eindeutige Erklärungsgehalt einer Zustimmung beigemessen werden. Dabei muss den jeweiligen Charakteristika des gewählten Kommunikationsweges Rechnung getragen werden können. So werden Angebote wie Applikationen und Internetseiten auf mobilen Endgeräten vom Endkunden typischerweise anders genutzt als etwa Postkarten, Formulare oder auch stationäre Internetseiten. Die Möglichkeit zur Einwilligungserteilung muss daher dem jeweiligen Medium entsprechend, ggf. auch in Form einer konkludenten Einwilligungsmöglichkeit, umgesetzt werden können. Eine pauschale Forderung nach einer expliziten Einwilligung ist daher nicht nur für traditionelle Kommunikationswege problematisch, sondern steht auch künftigen technischen Neuerungen entgegen.

b) Forderung nach expliziter Einwilligung bevorteilt große, international tätige Unternehmen. Bei der Diskussion über die Ausgestaltung des Einwilligungserfordernisses muss auch berücksichtigt werden, dass **das Erfordernis** einer expliziten Einwilligung grundsätzlich diejenigen Unternehme begünstigt, deren Geschäftsmodell ohnehin auf einem Log-In-Modell aufgebaut ist, wie etwa große, international tätige soziale Netzwerke oder E-Mail-Anbieter.

c) Auswirkungen auf E-Privacy-Richtlinie. Die Forderung nach einer expliziten Einwilligung wirft zudem die Frage auf, ob dies eventuell Auswirkungen auf die Möglichkeit hat, die im Rahmen der E-Privacy-Richtlinie erforderliche Einwilligung unter bestimmten Voraussetzungen durch Browser-Einstellungen auszudrücken (Erwägungsgrund 66 der Richtlinie 136/2009). In diesem Zusammenhang sollte berücksichtigt werden, dass auch vordergründig nur geringfügige Änderungen des geltenden Rechtsrahmens erhebliche Konsequenzen haben können. Etwaige Verschärfungen des geltenden Rechtsrahmens dürfen nicht dazu führen, dass das Nutzerlebnis beeinträchtigt und die Funktionalität des Internets insgesamt gefährdet wird.

d) Keine Einwilligung bei erheblichem Ungleichgewicht. Unklar ist außerdem, wann ein erhebliches Ungleichgewicht zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen besteht, was nach Art. 7 Abs. 4 die Einwilligung als Rechtsgrundlage für die Datenverarbeitung ausschließt. In Erwägungsgrund 34 wird diesbezüglich lediglich ausgeführt, dass dies vor allem der Fall sei, wenn sich die betroffene Person in einem Abhängigkeitsverhältnis von dem für die Verarbeitung Verantwortlichen befindet. Auch diese Erläuterung vermag jedoch keine hinreichende Klarheit über alle in Betracht kommenden Anwendungsfälle zu geben und führt für Unternehmen zu erheblicher Rechtsunsicherheit.

3. Definition von „Kind“ (Art. 4 Nr. 18). Als Kind im Sinne der Verordnung gilt gem. Art. 4 Nr. 18 jede Person unter 18 Jahren. Dies wirft verschiedene Fragen auf.

a) Definition überhaupt notwendig? Die generelle Einordnung jeder Person unter 18 Jahren als Kind erscheint angesichts der unterschiedlichen Entwicklungsstufen und Erfahrungshorizonte von Kindern, Jugendlichen und jungen Erwachsenen nicht angemessen. Auch der von der Kommission herangezogene Verweis auf die UN-Kinderrechtskonvention vermag dies nicht zu rechtfertigen. Die Konvention enthält wesentliche Standards zum Schutz von Kindern, soll jedoch nicht dazu dienen, eine allgemeingültige Definition von „Kindern“ festzulegen. Die Frage, warum die Grenze von 18 Jahren gewählt wurde, stellt sich aber insbesondere angesichts des Umstandes, dass eine Einwilligung der Eltern bzw. des Vormunds gemäß Art. 8 Abs. 1 nur für die Verarbeitung personenbezogener Daten von Kindern *unter 13 Jahren,* denen direkt Dienste der Informationsgesellschaft angeboten werden*,* erforderlich sein soll.

b) Altersverifikation erforderlich? Die Verordnung nimmt darüber hinaus an verschiedenen Stellen auf Kinder und damit auf die Altersgrenze von 18 Jahren Bezug, so etwa bei den Informationspflichten (Art. 11, Erwägungsgrund 46), dem Recht auf Vergessenwerden (Art. 17, Erwägungsgrund 53) oder dem Profiling (Erwägungsgrund 58). Dies wirft die Frage der Rechtssicherheit für Unternehmen auf. Insbesondere bei Angeboten, die auf erwachsene Nutzer ausgerichtet sind, muss sichergestellt werden, dass die Vorschriften nicht zu einer

unangemessenen Belastung für Unternehmen gerade in Bezug auf digitale Geschäftsmodelle führen, indem diese feststellen müssen, ob entsprechende Dienste auch von einem Kind angesehen bzw. abgefragt werden. Es würde eine erhebliche Belastung der Unternehmen und zahlreicher Geschäftsmodelle bedeuten, wenn vor jedem Kontakt etwa eine Altersverifikation erforderlich wäre. Dies gilt insbesondere auch deshalb, weil anerkannte und praktikable Altersverifikationssysteme für Telemediendienste aktuell noch fehlen.

c) Abwägungsmöglichkeit fraglich. Anders als bei Kategorien von Daten sonstiger Personen ist angesichts des Wortlauts des Art. 6 Abs. 1 f) fraglich, ob bei Daten von Kindern überhaupt eine Abwägung zwischen berechtigten Interessen des Datenverarbeitenden und ggf. widerstreitenden Interessen des Kindes erfolgen kann oder ob das Ermessen hier generell auf null reduziert ist. Diese Konsequenz wäre jedoch angesichts der unterschiedslos geltenden Altersgrenze sowie der unterschiedlichen, unter die Vorschrift fallenden Datenverarbeitungsvorgänge, auch aus Kinderschutzgesichtspunkten weder angemessen noch sachgerecht.

4. Bedingungen für die zulässige Datenverarbeitung (Art. 6). Der Entwurf legt in Art. 6 Abs. 1 genau fest, unter welchen Voraussetzungen die Verarbeitung personenbezogener Daten zulässig ist. Eine der in der Vorschrift enthaltenen sechs Alternativen muss hierzu erfüllt sind. Die Einwilligung ist dabei *eine* Möglichkeit, aber nicht die einzige. Das ist auch sachgerecht, denn dadurch wird dem Umstand Rechnung getragen, dass es viele unterschiedliche Situationen gibt, in denen Daten verarbeitet werden müssen.

a) Sachgerechtes Direktmarketing für Presse essentiell. Die freie und unabhängige Presse sowie die Medienvielfalt hängen in hohem Maße von der Möglichkeit ab, effektiv für Zeitschriften und Zeitungen zu werben. Es ist daher insbesondere unabdingbar, dass die Datenverarbeitung für zentrale Bereiche des Direktmarketings weiterhin ohne Einwilligung, aber mit Information und Widerspruchsmöglichkeit, möglich bleibt. Dies ist für die Presse wie für viele andere Branchen eine wichtige, und teilweise sogar die einzige, Möglichkeit, mit ihren Kunden in Kontakt zu treten oder neue Kunden zu gewinnen. Das gilt besonders für kleine und mittelständische Unternehmen, die sich keine Postwurfsendungen oder Werbung in den Massenmedien leisten können.

In Deutschland hängen bis zu 20% der Abonnementauflage vieler Zeitungen und Zeitschriften von adressiertem Direktmarketing ohne vorherige Einwilligung an Fremdadressen ab. Für das Segment lokaler und regionaler Zeitungen haben aktuelle Befragungen sogar ergeben, dass Werbebriefe an Fremdadressen bis zu 50 % der befristeten Abonnements und bis zu 20 % der neugewonnenen unbefristeten Abonnements generieren. Dieses Bild wird auch durch die Erfahrungen aus anderen europäischen Ländern bestätigt, in denen der entsprechende Anteil der Auflage sogar teilweise über 40 % ausmacht.

Die Leserwerbung dient dabei primär dem Erhalt der Auflage durch Ausgleich der normalen Fluktuation. Zwischen 10 und 30 % der Abonnenten gehen jährlich verloren und müssen also neu beworben werden, um die Abo-Auflage nur zu halten.

Bei der Fachpresse macht der Abo-Anteil regelmäßig nur einen kleinen Teil der Auflage aus. Der größte Teil der Auflage (teilweise bis ca. 90 %) wird kostenlos im sog. Frei- und Wech-

selversand auf der Basis spezieller Adresslisten an die jeweils relevante Zielgruppe (zum Beispiel Maschinenbauer, Bäcker oder Architekten) versandt.

Weder auf die Werbebriefe der Publikumspresse noch auf die Zusendung der Fachzeitschriften gibt es relevante Beschwerden. Das negative Feedback kann in beiden Bereichen mit ca. 1 – 10 von 100.000 Adressaten angegeben werden. Dem stehen bei der Abonnementwerbung der Publikumspresse bis zu 2.000 Adressaten gegenüber, die regelmäßige Presseleser werden. Und bei der Fachpresse alle anderen Empfänger, für die diese Zeitschriften einen Beitrag zu ihrer beruflichen und gewerblichen Information und Bildung leisten.

b) Kommissionsentwurf garantiert nicht, dass sachgerechtes Direktmarketing auch künftig möglich bleibt. In der auch für das Direktmarketing maßgeblichen Vorschrift des Art. 6 Abs. 1 f) ist zwar wie auch in der bisherigen Vorschrift des Art. 7 f) festgelegt, dass die Datenverarbeitung zur Wahrung *berechtigter Interessen des für die Verarbeitung Verantwortlichen* zulässig ist, sofern nicht die Interessen oder Rechte des Einzelnen überwiegen. Es fehlt jedoch, anders als in der bisherigen Regelung des Art. 7 f), die Zulässigkeit der Datenverarbeitung *auch für legitime Interessen Dritter*. Gerade diese ist jedoch in vielen Fällen Voraussetzung, um überhaupt sachgerecht Direktmarketing durchführen zu können. Denn nur so wird etwa die Weitergabe von Adresslisten, der Kauf oder die Miete von Adressen von Adressbrokern oder die Durchführung von Marketingmaßnahmen durch spezialisierte Dienstleister ermöglicht. Diese Alternative muss daher wieder eingeführt werden.

c) Regelung zur Zweckänderung muss alle möglichen Formen der Datenverarbeitung berücksichtigen. Eine Datenverarbeitung zu anderen Zwecken als zu denen, zu denen die Daten ursprünglich erhoben wurden, kann aus verschiedenen Gründen erforderlich und sogar im Interesse des Kunden sein. In Betracht kommt etwa die Information einer relevanten Zielgruppe über die Einführung einer Fachzeitschrift als Reaktion auf den Erfolg eines bestimmten Themas im Rahmen einer Fachmesse. Diese muss zulässig sein, wenn die Voraussetzungen für die Datenverarbeitung ohne vorherige Einwilligung im Sinne von Art. 6 Abs. 1 vorliegen. Bislang ist dies in Art. 6 Abs.4 lediglich für die Alternativen des Art. 6 Abs. 1 a) – e) vorgesehen. Für eine solche Begrenzung gibt es jedoch keinen Grund. Eine solche würde vielmehr zu dem seltsam anmutenden Ergebnis führen, dass für solche Daten, die bereits einmal zulässigerweise erhoben bzw. genutzt wurden und in deren Nutzung evtl. sogar eine Einwilligung erteilt wurde, strengere Regeln gelten würden als für solche, die noch nie genutzt wurden. Diese Begrenzung sollte daher aufgehoben und generell auf die Vorschrift des Art. 6 Abs. 1 verwiesen werden.

d) Information und Widerspruchsmöglichkeit garantieren Selbstbestimmungsrecht des Verbrauchers. Wichtig ist, was auf Englisch mit „Information and Control“ beschrieben wird: Die Information über die Datenverarbeitung und die Möglichkeit, dieser zu widersprechen. Dies ist auch so in dem Verordnungsentwurf verankert: Festgelegt wird, dass der Einzelne über die Verarbeitung informiert werden muss (Art. 14) und ihr widersprechen kann (Art. 19 Abs. 1). Speziell für den Bereich des Direktmarketing wurde eingeführt, dass die betroffene Person nicht nur das Recht hat, der Verarbeitung ihrer personenbezogenen Daten zu Direktmarketingzwecken zu widersprechen, sondern auch ausdrücklich auf dieses Recht hingewiesen werden muss (Art. 19 Abs. 2).

e) Forderung nach genereller Einwilligung bevorteilt große, international tätige Unternehmen. Es muss zudem darauf geachtet werden, dass keine Vorgaben eingeführt werden, die zwar von großen, global tätigen Unternehmen relativ einfach erfüllt werden können, nicht jedoch von der Mehrzahl der kleinen und mittelständischen Unternehmen in Europa.

Das gilt besonders für die im Rahmen der Diskussion teilweise erhobene Forderung nach einer generellen Einwilligung für alle Datenverarbeitungsprozesse. Eine solche generelle vorherige Einwilligung würde grundsätzlich diejenigen Unternehmen begünstigen, deren Geschäftsmodell ohnehin auf einem Log-In-Modell aufgebaut ist. Das gilt etwa für große international tätige E-Mail-Anbieter oder soziale Netzwerke, die vor der Nutzung ihrer Dienste eine Anmeldung erfordern. Diese können wesentlich einfacher und von einer Vielzahl von Nutzern eine solche Einwilligung erhalten als andere, insbesondere national, regional oder sogar lokal gebundene Unternehmen, die einen freien Zugang zu ihren Angeboten ermöglichen (siehe bereits oben, Ziffer II. 2. b).

Es ist zum Beispiel regelmäßig nicht erforderlich, sich vorab anzumelden, um die Online-Angebote von Zeitschriften und Zeitungen zu nutzen. Jeder direkte Kontakt mit dem Kunden zur Einholung einer Einwilligung (wie etwa entsprechende Pop-Up-Fenster auf Internetseiten) birgt daher die Gefahr, von diesen als Störung und damit als negativer Aspekt des Angebotes wahrgenommen zu werden.

Darüber hinaus besteht bei einer derartigen Pflicht die erhebliche Gefahr, dass Verbraucher großen global agierenden Unternehmen, die ihnen bekannt sind und bei denen sie evtl. bereits sogar ein umfassendes Profil angelegt haben, eher eine Einwilligung erteilen, als evtl. nur national agierenden, nicht in der Öffentlichkeit stehenden kleineren Unternehmen. Für letzte würde dies zu einem erheblichen Wettbewerbsnachteil führen.

Hinzu kommen die ganz praktischen Bedenken, dass die weite Definition personenbezogener Daten zu einer Inflation von Einwilligungsanfragen an den Nutzer führen und zu einem enormen Datenvolumen in den Datenbanken der Unternehmen führen würde.

f) Problematik belästigender Werbung und unerbetener Nachrichten. Gerade bei der Diskussion über das Direktmarketing darf nicht vergessen werden, dass es in der Verordnung darum geht, einen Rechtsrahmen für die Verarbeitung personenbezogener Daten zu schaffen. Die Problematik belästigender Werbung oder unerbetener Nachrichten werden dagegen in der Richtlinie über unlautere Geschäftspraktiken 2005/29/EG (insbesondere Art. 6, 7, 8 und 9) und der E-Privacy-Richtlinie 2002/58/EG (siehe insbesondere Art. 13) ausreichend geregelt.

5. Informationspflichten (Art. 14). Die geltenden Informationspflichten wurden erheblich erweitert und zielen in vielen Bereichen offensichtlich auf den Online-Bereich ab. Es kann jedoch nicht sein, dass dadurch in der Konsequenz traditionelle und bewährte Marketingwege nicht mehr genutzt werden können, weil sich bei diesen die Fülle an geforderten Informationen einfach nicht angemessen verwirklichen lässt. Hinzu kommt, dass die Informationspflichten den Nutzungsvorgängen im stationären und mobilen Internet nicht gerecht werden. Um auch weiterhin einen sachgerechten Pressevertrieb zu ermöglichen, muss es daher möglich sein, dass die Information generalisierend erfolgen und dem übermittelnden Medium entsprechend angepasst werden kann.

a) Information über die Zweckbestimmung (Art. 14 Abs. 1 b). Um auch weiterhin einen sachgerechten Pressevertrieb zu ermöglichen, muss es möglich sein, dass die Information über die Zweckbestimmung generalisierend, insbesondere durch die Nennung von Kategorien – vergleichbar zu Kategorien von Daten und Empfängern (vgl. Art. 14 Abs. 1 f) – erfolgen kann.

Die Verpflichtung, dass diese Information unter bestimmten Voraussetzungen auch die Geschäfts- und allgemeinen Vertragsbedingungen umfassen muss, ist insbesondere für Direktmarketingmaßnahmen, die nicht online erfolgen, nicht praktikabel. Regelmäßig wird es sich bei diesen Bedingungen um solche handeln, die sich auf den Verkauf des konkreten Produkts bzw. auf die Erbringung der entsprechenden Dienstleistung beziehen (wie z. B. AGBs). Ein datenschutzrechtlicher Mehrwert wird durch diese Information in diesen Fällen regelmäßig nicht erzielt. Die Bereitstellung dieser Informationen ist jedoch z. B. im Rahmen einer Bestellkarte, wie sie für Abonnements verwendet wird, regelmäßig unmöglich.

b) Dauer der Datenspeicherung (Art. 14 Abs. 1 c). Die Dauer der Datenspeicherung lässt sich in vielen Fällen im Vorhinein noch nicht feststellen bzw. ist häufig an einen noch nicht absehbaren Faktor geknüpft (z. B. Länge einer Vertragsbeziehung, Dauer der Nutzung durch den Kunden, gesetzliche Pflicht zur Speicherung). Bei Abschluss eines unbefristeten Abonnements ist z. B. regelmäßig nicht ersichtlich, wie lange das Abonnement laufen und damit die personenbezogenen Daten gespeichert werden. Auch nach Beendigung der Vertragsbeziehung kann unter Umständen ein berechtigtes Bedürfnis zur weiteren Nutzung der entsprechenden Daten bestehen.

c) Kontaktdaten der Aufsichtsbehörde (Art. 14 Abs. 1 e). Die Pflicht zur Angabe der Kontaktdaten der Aufsichtsbehörde (Art. 14 Abs. 1 e) verbunden mit der Haftung für evtl. Falschinformationen führen zu einem erheblichen Aufwand für den Unternehmer, da dieser in regelmäßigen Abständen überprüfe muss, ob die entsprechenden Kontaktinformationen noch aktuell sind.

d) Information über Übermittlung in Drittland (Art. 14 Abs. 1 g). Eine Information über die Absicht des für die Verarbeitung Verantwortlichen, die Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das dort geltende Datenschutzniveau unter Bezugnahme auf einen Angemessenheitsbeschluss der Kommission, lässt sich wohl kaum praktikabel verwirklichen. Die Informationspflicht soll zudem bereits beim bloßen Vorhandensein einer Absicht einer Datenübermittlung bestehen.
Nicht berücksichtigt wird zudem der spezielle Fall der Auftragsdatenverarbeitung. Bedient sich ein Auftraggeber der Leistung eines Auftragsverarbeiters im Sinne von Art. 4 Abs. 6, bleibt der Auftraggeber bei einer Datenverarbeitung im Europäischen Wirtschaftsraum für die Datenverarbeitung verantwortliche Stelle iSv. Art. 4 Abs. 5. Der Auftragsverarbeiter ist dann grds. nicht verantwortliche Stelle. Das ergibt sich insbesondere aus dem Wortlaut von Art. 4 Abs. 6, Art. 24, und Art. 26 Abs. 4. Ein Informationsinteresse bezüglich der Identität des Auftragsverarbeiters besteht daher nicht, so dass insoweit eine Differenzierung erfolgen sollte. Eine pauschale Informationspflicht bzgl. des Empfängers der Daten ist vor diesem Hintergrund nicht notwendig.

Schließlich ist zu berücksichtigten, dass diese Pflicht auch bereits dann greift, wenn nur Teile der Datenverarbeitung, wie z. B. die Rechnungsdatenverarbeitung oder die Materialwirtschaft, im Drittland erfolgen. Insbesondere der Hinweis auf das im jeweiligen Drittstaat geltende Datenschutzniveau lässt sich gerade im Rahmen traditioneller Marketingwege (z. B. Postkarte, Brief) regelmäßig nicht sachgerecht erfüllen.

e) Sonstige Informationen (Art. 14 Abs. 1 h). Die bereits erheblichen Informationspflichten werden zudem noch generalklauselartig erweitert. Aufgeführt werden sollen auch sonstige Informationen, die unter Berücksichtigung der besonderen Umstände, unter denen die personenbezogenen Daten erhoben werden, notwendig sind, um gegenüber der betroffenen Person eine Verarbeitung nach Treu und Glauben zu gewährleisten. Für das einzelne Unternehmen lässt sich damit nicht mehr rechtssicher ersehen, welche Informationen im Einzelfall damit tatsächlich zur Verfügung gestellt werden müssen. Zudem führt eine solche Ausweitung der Informationspflichten zu einer Form von „Über-Information" und damit einer erheblichen Minderung des Nutzwertes für den Betroffenen.

f) Qualität der Datenabfrage und Folgen der Weigerung (Art. 14 Abs. 2). Die Information der betroffenen Person darüber, ob die Bereitstellung der Daten obligatorisch oder fakultativ ist und welche möglichen Folgen die Verweigerung der Daten hätte, erweitert nicht nur die Menge der aufzuführenden Informationen. Sie ist in vielen Fällen zudem auch überflüssig, da sie sich bereits aus dem Zusammenhang ergibt. So ist z. B. die Angabe einer Lieferadresse für die Lieferung eines Abonnements erforderlich. Ohne Angabe dieser Adresse kann das entsprechende Presseprodukt nicht geliefert werden. Mindestens sollte es jedoch möglich sein, mithilfe von im Einzelfall geeigneten Darstellungen die notwendigen Informationen zu erteilen.

g) Herkunft der personenbezogenen Daten (Art. 14 Abs. 3). Wenn Daten nicht bei der betroffenen Person erhoben werden, so muss dieser gem. Art. 14 Abs. 3 auch die Herkunft der personenbezogenen Daten mitgeteilt werden. Diese generelle Pflicht ist insbesondere dann zu weitgehend, wenn die entsprechenden Daten aus allgemein zugänglichen Quellen stammen.

h) Zeitpunkt der Information (Art. 14 Abs. 4). Die Vorgaben zum Zeitpunkt der Information berücksichtigen nicht, dass Zeitpunkt der Erhebung gerade im Bereich des traditionellen Pressevertriebs das Ausfüllen des Bestellscheins o. ä. ist. Die Pflicht zur Angabe dieser Menge an Informationen würde diesen Vertriebsweg schlicht nicht mehr praktikabel machen.

i) Bußgeldbedrohung. Hinzu kommt, dass der Tatbestand „nicht hinreichend transparenter" Informationserteilung zu unbestimmt ist, als das das einzelne Unternehmen ersehen könnte, wann dieser konkret erfüllt ist. Die führt neben der Fülle von Informationen, die in der Menge und Komplexität für Unternehmen schlicht nicht beherrschbar sind, gekoppelt mit einer Bußgeldbedrohung in Höhe von 1 % des weltweiten Jahresumsatzes des Unternehmens für nicht oder nicht vollständig oder in nicht hinreichend transparenter Weise erteilte Informationen (Art. 79 Abs. 5 a) zu einem erheblichen Risiko für Unternehmen.

6. Auskunftsrecht (Art. 15). Auch die erweiterten Vorschriften zum Auskunftsrecht bergen die Gefahr weiterer Belastungen für Verlage.

a) Praktikabilität fraglich. In vielen Fällen wird sich die entsprechende Auskunftsverpflichtung kaum praktikabel verwirklichen lassen. Verschiedene Verlage nutzen z. B. zur Darstellung bestimmter interner Transaktionen keine Klardaten, sondern bestimmte Variablen (bspw. bestimmte Ziffern für bestimmte Produkte oder Vorgänge). Abgesehen davon, dass eine Auskunft über die entsprechenden Daten möglichweise Geschäftsgeheimnisse des jeweiligen Unternehmens betreffen könnte, dürfte der Erkenntnisgewinn für Verbraucher in diesen Fällen regelmäßig gering sein.

b) Auskunft auf elektronischem Weg verpflichtend? Nicht überschaubare Risiken für Unternehmen birgt auch die in Art. 15 Abs. 2 enthaltene Pflicht, wonach die betroffene Person, sofern sie den Auskunftsantrag in elektronischer Form gestellt hat, grundsätzlich auch auf elektronischem Weg zu unterrichten ist. Für den Unternehmer ist es bei einer Antragstellung auf elektronischem Weg regelmäßig nicht ohne Weiteres nachprüfbar, ob die Person, über die Auskunft begehrt wird, auch tatsächlich mit der anfragenden Person übereinstimmt. Eine derartige Pflicht birgt daher die erhebliche Gefahr der Verpflichtung zu unzulässiger Datenweitergabe an Unberechtigte. Eine Auskunft auf elektronischem Weg sollte daher lediglich als Alternative, nicht jedoch als Pflicht festgelegt werden. Außerdem sollte festgelegt werden, welchen Anforderungen das jeweilige Unternehmen genügen muss, um festzustellen, ob es sich bei der anfragenden Person tatsächlich um diejenige Person handelt, über die Auskunft begeht wird.

c) Ausschluss einer Auskunftspflicht. Das Auskunftsrecht besteht, um dem Betroffenen die Möglichkeit zu geben, nachvollziehen zu können, wer welche personenbezogenen Daten über ihn gespeichert hat. Damit wird dem Umstand Rechnung getragen, dass die betroffenen Personen häufig keinen eigenen Zugang zu dem personenbezogenen Datenbestand haben. Das Informationsinteresse überwiegt jedoch in bestimmten Fällen nicht mehr. So fehlt das Informationsinteresse, wenn die betroffene Person bereits über die Informationen verfügt (Art. 14 Abs. 5 a). Gleiches muss jedoch auch gelten, wenn die Person jederzeit Zugriff auf die gespeicherten personenbezogenen Daten haben kann (z.B. über einen entsprechenden Zugang zu einem Kundenprofil im Internet). Ein Informationsinteresse besteht schließlich auch dann nicht, wenn die verarbeiteten personenbezogenen Daten allgemein zugänglich sind.

7. Recht auf Vergessenwerden und auf Löschung (Art. 17). Das in Art. 17 festgelegte Recht auf Vergessenwerden verbunden mit dem Recht auf Löschung wäre für Leserbeiträge im Rahmen journalistischer Angebote (sog. user-generierter Inhalte, z. B. Kommentare, Beiträge in Meinungsforen, Produktbewertungen, etc.) äußerst problematisch. Es kann zudem nicht ausgeschlossen werden, dass diese Vorgaben auch andere Formen der Datenverarbeitung, etwa im Rahmen der Verarbeitung des Widerspruches, betreffen.

a) Weite Auslegung möglich. Art. 17 ist derart weit gefasst ist, dass er nicht nur die Löschung eigener Beiträge ermöglicht, sondern auch die Löschung fremder Beiträge, indem er der betroffenen Person das Recht gibt, die Löschung *sie betreffender* personenbezogener Daten zu verlangen.

b) Gefahr der Unverständlichkeit von Meinungsäußerungen. Eine Pflicht zur Löschung hätte erheblich nachteilige Folgen im Rahmen von Leserbeiträgen in journalistischen Angeboten. Denn Meinungsäußerungen in der Abfolge digitaler Kommentarketten und Foren sind regelmäßig erst im Kontext der anderen Äußerungen verständlich.

c) Praktikabilität fraglich. Eine solche Pflicht führt zudem zu einem erheblichen und teilweise praktisch überhaupt nicht umsetzbaren Aufwand für Internetseitenbetreiber, aber auch für Unternehmen, die die entsprechenden Daten auf klassischem Wege verarbeiten. Dies gilt ebenso für die in Abs. 2 enthaltene Pflicht, auch Dritte über die gewünschte Löschung zu informieren.

Abgesehen davon findet teilweise eine Zuordnung user-generierter Inhalte zum Kundenkonto überhaupt nicht statt. Dies ist regelmäßig auch nicht nötig. Denn z. B. sind Produktbewertungen als solche wichtig, um Kundenbedürfnisse künftig sachgerecht zu decken. Unerheblich ist in der Regel jedoch, von welchem individuellen Kunden diese abgegeben wurden. Die Pflicht zur Löschung könnte daher die auch aus Datenschutzgesichtspunkten seltsam anmutende Folge haben, dass der Nutzer aufgrund der fehlenden Zuordnung dem Unternehmen mitteilen müsste, welche Inhalte von ihm stammen.

d) Ausnahme ausreichend? Ob die in Art. 17 Abs. 3 a) enthaltene Ausnahme für die freie Meinungsäußerung im Sinne des Art. 80 ausreicht, um die o. g. Konstellationen abzudecken, ist fraglich. Durch die weite Definition journalistischer Tätigkeit (Erwägungsgrund 121 a. E.) dürfte diese Ausnahme zwar einen weiteren Anwendungsbereich haben, unklar ist jedoch, ob es im weiteren Verlauf des Gesetzgebungsverfahrens bei dieser weiten Definition bleiben wird.

e) Löschung der Daten überhaupt sachgerecht? Zum Beispiel beim Direktmarketing stellt sich das Problem, dass der Einzelne untechnisch eine Löschung der Daten begehrt, obwohl er tatsächlich nur künftiger Werbung widersprechen möchte. Doch gerade in diesem Fall darf die Adresse nicht gelöscht, sondern lediglich gesperrt werden, um für zukünftige Werbemaßnahmen eine Nutzung dieser Adresse ausschließen zu können. Die in Art. 17 Abs. 4 genannten Fälle, in denen statt einer Löschung der Daten auch eine Beschränkung der Datenverarbeitung in Betracht kommen kann, dürften nicht alle relevanten Fälle abdecken. Die Kommission weist in der Begründung zu ihrem Verordnungsvorschlag unter Ziffer 3.4.3.3. zwar darauf hin, dass der mehrdeutige Ausdruck der „Sperrung“ vermieden werden soll. Sichergestellt werden muss jedoch zumindest, dass Konstellationen wie die oben geschilderte ebenfalls als eine entsprechende Ausnahme angesehen werden.

8. Recht auf Datenübertragbarkeit (Art. 18). Das Recht auf Datenübertragbarkeit und insbesondere die Pflicht, der betroffenen Person die Möglichkeit einzuräumen, ihre gespeicherten personenbezogenen Daten sowie etwaige sonstige von ihr zur Verfügung gestellte Informationen in einem gängigen elektronischen Format in ein anderes System zu überführen, lässt sich in vielen Fällen praktisch kaum verwirklichen.

Zahlreiche Verlage speichern die entsprechenden Daten nicht in einem gängigen elektronischen Format, sondern nutzen spezielle, an ihre spezifischen Bedürfnisse angepasste Formate. Eine

entsprechende Überführung wäre jedoch in vielen Fällen nicht nur technisch problematisch, sondern auch ohne relevanten Informationswert für die betroffene Person, da die entsprechenden Daten in vielen Fällen nicht als Klardaten dargestellt, sondern für bestimmte Transaktionsdaten Variablen (z.B. bestimmte Ziffern für bestimmte Produkte oder Vorgänge) genutzt werden.Der entsprechende Informationswert dürfte in vielen Fällen auch selbst fehlen, wenn die Daten digital in einem entsprechenden die Datenportierung ermöglichenden Format zur Verfügung stünden,

Zudem dürfen die berechtigten Interessen der verantwortlichen Stellen nicht unberücksichtigt bleiben. Aus Erwägungsgrund 59 wird nämlich deutlich, dass das neue Recht zu Datenübertragbarkeit neben den Rechten zur Datenlöschung, Unterrichtung, Auskunft, Berichtigung und dem Widerspruch steht. Es geht also gerade nicht darum, eine zusätzlich Funktionalität zu schaffen, die Daten von einer verantwortlichen Stelle an eine andere zu übermitteln. Vielmehr soll der Nutzer die Verfügungsgewalt über diejenigen personenbezogenen Daten haben, die auch Gegenstand eines Auskunftsrechts etc. wären. Deshalb bedarf es einer Klarstellung, dass die Überführung in ein anderes System nach Art. 18 Abs. 2 nicht bedeutet, dass der Bestand an personenbezogenen Daten an andere Anbieter übermittelt werden muss. Dies würde über das Interesse der betroffenen Personen hinausgehen und die verantwortlichen Stellen unangemessen benachteiligen.

9. Widerspruchsrecht (Art. 19). Die neue Formulierung des Widerspruchsrechts in Art. 19 wirft verschiedene Fragen auf.

a) Verständlichkeit der Widerrufsbelehrung. Unklar ist zunächst, wann die Widerrufsbelehrung als „verständlich“ im Sinne des Abs. 2 angesehen werden kann. Dies führt für Unternehmen zu erheblicher Rechtsunsicherheit, die erhebliche Konsequenzen haben kann: Denn gem. Art. 79 Abs. 6 c) ist eine Verletzung dieser Pflicht mit einer Geldbuße bis zu einer Höhe von 2 % des weltweiten Jahresumsatzes bedroht.

b) Speicherung des Widerspruchs überhaupt zulässig? Darüber hinaus stellt sich die Frage, ob es nicht bereits eine nach Art. 19 Abs. 3 verbotene weitere Nutzung oder anderweitige Verarbeitung im Sinne des Art. 4 Abs. 3 ist, wenn das datenverarbeitende Unternehmen den Widerspruch der betroffenen Person zu deren personenbezogenen Daten vermerkt. Dies ist jedoch wohl regelmäßig notwendig, um der entsprechenden Pflicht nachzukommen.

10. Profiling (Art. 20). Die mit Art. 20 neu eingeführte Vorschrift zum Profiling geht teilweise deutlich über die bisherige Vorschrift zu automatisierten Einzelentscheidungen (Art. 15 der Richtlinie 95/46/EG) hinaus. Aufgrund ihrer sehr weiten Formulierung birgt diese Vorschrift die Gefahr, traditionelle und bewährte Geschäftsmodelle deutlich zu belasten bzw. sogar unmöglich zu machen.

a) Anwendungsbereich unklar. Aufgrund der generalklauselartigen Formulierung des Art. 20 lässt sich nicht abschließend absehen, welche Datenverarbeitungsmaßnahmen konkret darunter fallen.

Nicht definiert wird i, wann eine Datenverarbeitung *rechtliche Wirkung entfaltet* und wann eine *Beeinträchtigung in maßgeblicher Weise* vorliegt. Unklar ist außerdem, unter welchen Voraussetzungen von einer auf einer *rein automatisierten Verarbeitung von Daten* basierenden

Maßnahme ausgegangen werden muss. Dies gilt insbesondere für die Fälle, in denen die entsprechende Datenverarbeitung zwar automatisiert, aber auf der Basis zuvor durch eine Person festgelegter Kriterien erfolgt.

Hinzu kommt, dass der Anwendungsbereich im Gegensatz zur bislang in diesem Zusammenhang maßgeblichen Vorschrift des Art. 15 der Richtlinie 95/46/EG auf solche Maßnahmen erweitert wurde, deren Zweck *in der Analyse beziehungsweise Voraussage der genannten Merkmale* besteht.

Die Kommission weist in der Begründung zu ihrem Verordnungsvorschlag unter Ziffer 3.4.3.4. darauf hin, dass sie auch die Empfehlung des Europarates zum Profiling (Empfehlung CM/Rec(2010)13 des Ministerkomitees an die Mitgliedstaaten über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit Profiling vom 23. November 2010) berücksichtigt habe. Im Anhang dieser Empfehlung ist in Ziffer 1 e) Profiling definiert als ein Verfahren der automatisierten Verarbeitung von Daten, das darin besteht, einer natürlichen Person ein „Profil" zuzuordnen, um insbesondere Entscheidungen in Bezug auf ihre Person zu treffen oder um ihre persönlichen Vorlieben, Verhaltensweisen und Einstellungen zu analysieren oder vorherzusagen. Diese Definition trägt ebenfalls nicht zu Eingrenzung bei, da sie praktisch jegliches Anreichern und Ergänzen von Daten erfasst, unabhängig von Inhalt und Qualität.

Es lässt sich daher nicht ausschließen, dass darunter auch zahlreiche Datenverarbeitungsprozesse fallen, die für Verlage wichtig sind, wie etwa Maßnahmen im Rahmen des sog. Customer Relationship Managements (etwa der Kundengewinnung oder -bindung) oder bestimmter Formen von interessenbasierter Werbung, die als eine wichtige Werbeform im Online-Bereich zur Finanzierung digitaler Verlagsangebote relevant sein können.

b) Anwendung auf nicht identifizierende Daten möglich. Diese Vorschriften könnten aufgrund der weiteren Formulierung sogar für Datenverarbeitungsprozesse gelten, bei denen keine Identifizierung einer bestimmten Person erfolgt, wie die Erstellung pseudonymisierter oder anonymisierter Nutzungsprofile. Berücksichtigt wird zudem nicht, dass es in nationalem Recht bereits detaillierte Regeln gibt, die für verschiedene Datenverarbeitungsvorgänge ähnlicher Art detaillierte Regeln vorsehen. So stellt etwa das in § 15 Abs. 3 des Telemediengesetzes vorgesehene und mit einer Bußgeldandrohung versehene Zusammenführungsverbot von pseudonymisierten Nutzungsprofilen mit dem Träger des Profils in Verbindung mit einem Widerspruchsrecht des Betroffenen den erforderlichen Schutz der Verbraucher sicher. Nicht ersichtlich ist außerdem, wie eine anonyme Profilbildung die Interessen einer der verantwortlichen Stelle unbekannten Person betreffen soll.

c) Rechtsfolge angesichts weiten Anwendungsbereichs unverhältnismäßig. Sofern bestimmte Maßnahmen als Profiling im Sinne der Vorschrift angesehen werden, gelten für sie die strengen Voraussetzungen des Art. 20 Abs. 2, d. h. grds. Vorbehalt der Einwilligung des Betroffenen, wenn das Profiling nicht im Rahmen von Vertragsabschluss oder -erfüllung erfolgt oder nach EU- oder mitgliedstaatl. Recht gestattet ist. Angesichts des möglichen weiten Anwendungsbereiches der Vorschrift, birgt dies die erhebliche Gefahr weiterer Einschränkungen bewährter und der Behinderung neuer Geschäftsmodelle. Zudem bevorteilt auch diese Vorschrift insbesondere große, international tätige Unternehmen, deren Geschäftsmodell ohnehin auf einem Log-In-Modell aufgebaut ist, wie etwa große, international tätige sozi-

ale Netzwerke oder E-Mail-Anbieter und führt daher zu einem erheblichen Wettbewerbsnachteil für kleine und mittelständige Unternehmen in Europa. Nicht nachvollziehbar ist vor diesem Hintergrund auch, warum hier, anders als in anderen Vorschriften, keine Abwägungsklausel enthalten ist.

11. Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 23). Die Vorgaben zur Verwirklichung von Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen könnten die Belastungen für Unternehmen erheblich erhöhen.

a) Stand der Technik und Implementierungskosten. Verlangt wird in diesem Zusammenhang von den Unternehmen eine Abwägung bezüglich Stand der Technik und Implementierungskosten. Eine solche setzt jedoch erhebliche Technik- und Marktkenntnisse voraus und wird von den betroffenen Unternehmen, gerade wenn es sich um kleinere und mittlere Unternehmen handelt, regelmäßig kaum zu leisten sein.

b) Verbraucherleitbild? Zudem stellt sich die Frage, wie sich derartige Vorgaben mit dem Leitbild eines mündigen Verbrauchers, der in der Lage ist, eine informierte Entscheidung zu treffen, vertragen. Die Anwendung dieses Konzeptes würde in vielen Fällen letztendlich dazu führen, Nutzern eine subjektive Auffassung darüber, wie Datenschutzeinstellungen auszusehen haben, aufzuerlegen.

c) Individuelle Einstellungen. Die Gefahr besteht zudem, dass eine derart generelle Festlegung keinen Raum mehr für den individuellen Bedürfnissen angepassten Datenschutzeinstellungen lässt, die im Einzelfalls strenger, weniger weitgehend oder schlicht differenzierter sein können. Ein Beispiel hierfür sind etwa moderne Browser-Einstellungen, die den Nutzern bereits heute die Wahl lassen, ob sie Cookies generell, nur für die jeweilige Browser-Sitzung oder nur im Einzelfall akzeptieren möchten.

12. Bürokratische Belastungen für Unternehmen müssen reduziert werden. Der Abbau bürokratischer Belastungen, der mit dem neuen Rechtsrahmen auch beabsichtigt ist, wird nur gefördert werden, wenn im Gegenzug nicht neue Hürden, wie etwa extensive Informations- (z. B. Art. 14, 15), Dokumentations- (Art. 28), Notifikations- (Art. 31, 32) und Konsultationspflichten (Art. 33, 34) eingeführt bzw. ausgeweitet werden.

13. Zertifizierung (Art. 39). Die in Art. 39 geforderte Förderung der Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -zeichen durch die Kommission birgt die Gefahr, dass derartige Zertifizierungen leicht zu einer faktischen Zertifizierungspflicht für Unternehmen führen können.

Das gilt insbesondere dann, wenn durch solche Zertifizierungen in der Öffentlichkeit der Eindruck entsteht, nur derart zertifizierte Verfahren, Technologien, Produkte oder Dienste seien datenschutzrechtlich unbedenklich. Ferner gilt hier in besonderem Maße, dass Zertifizierungsanforderungen nicht zum Konkurrenzschutz großer und finanzkräftiger Unternehmen gegenüber kleinen und mittelständischen Unternehmen werden dürfen, die sich aufwändige Zertifizierungen nicht leisten können.

14. Verbandsklage und –beschwerdebefugnisse (Art. 73, 76). Verbände der Zivilgesellschaft haben nach Artikel 73 Abs. 3 ein eigenes, vom Betroffenen unabhängiges Beschwerderecht. Das Klagerecht (Artikel 76 Abs. 1) wird ihnen zwar nicht unmittelbar eingeräumt. Indirekt führt aber eventuell Artikel 73 Abs. 3 möglicherweise doch zu einem Klagerecht.

a) Datenschutzrecht als verbraucherschützende Norm oder Marktverhaltensregeln? Dadurch, dass der Verband ein eigenes umfassendes Recht erhält, könnte man zumindest die Frage stellen, ob die Regelungen des Datenschutzrechts als verbraucherschützender Norm im Sinne § 2 Abs. 1 des Gesetzes über Unterlassungsklagen bei Verbraucherrechts- und anderen Verstößen (UKlaG) anzusehen sind.

Die umfassende Rechtseinräumung als eigenes Recht hat möglicherweise auch Konsequenzen für § 4 Nr. 11 des Gesetzes gegen den unlauteren Wettbewerb (UWG). Es lässt sich nicht ausschließen, dass dies so interpretiert werden könnte, dass es sich bei den datenschutzrechtlichen Regelungen insgesamt um Marktverhaltensregeln handelt.

Damit würde indirekt über UKlaG und UWG eine Klagemöglichkeit bestehen. Problematisch wäre dabei zunächst, dass die Voraussetzungen für ein solches Klagerecht dann über Artikel 73 Abs. 2 denkbar gering wäre. Dies würde europaweit einem Abmahn*un*wesen Tür und Tor öffnen, das man bereits aus anderen Rechtsbereichen kennt und das auch aus Verbraucherschutzgesichtspunkten nicht dienlich wäre.

b) Nebeneinander von Position. Die zeitgleiche Klagebefugnis von Aufsichtsbehörden und Verbänden der Zivilgesellschaft würde zudem zu einem unübersichtlichen Nebeneinander von Positionen führen: Verbraucherschutzverbände nutzen ihre Klagebefugnisse erfahrungsgemäß mehr zur Rechtsfortbildung denn zur Rechtsdurchsetzung. So haben die Verbraucherschutzverbände zum Beispiel im Rahmen ihrer in Deutschland auf Einwilligungsklauseln beschränkten Klagebefugnisse versucht, Rechtspositionen durchzusetzen, die von Datenschutzbehörden nicht getragen werden. Ein Nebeneinander von Klagemöglichkeiten durch unabhängige Datenschutzaufsichtsbehörden und Verbraucherschutzverbänden würde demnach zu weiteren Rechtsunsicherheiten führen**.**

15. Strafen und Bußgelder bei Verstößen gegen das Datenschutzrecht (Art. 79). Die bei Verstößen gegen das Datenschutzrecht möglichen Bußgelder wurden erheblich erhöht. Zum Vergleich: nach dem deutschen Bundesdatenschutzgesetz sind gem. § 43 Abs. 3 i. V. m. Abs. 1 und 2 Geldbußen bis zu dreihunderttausend Euro möglich. Diese können nur überschritten werden, wenn dieser Betrag den wirtschaftlichen Vorteil des Täters nicht übersteigen würde. In dem Kommissionsentwurf werden generell Bußgelder in Höhe von 0,5%, 1 % oder 2 % des Jahresumsatzes des jeweiligen Unternehmens vorgesehen.

Diese Erhöhung ist gerade mit Hinblick auf die teilweise mit Bußgeld bedrohten Tatbestände (z. B. nicht ausreichende Erfüllung der extensiven Informationspflichten, Art. 79 Abs. 5 a) nicht nachvollziehbar. Die Pflichten ergeben sich zudem nunmehr vielfach aus Generalklauseln bzw. aus weiten Formulierungen, so dass die Pflichten für die einzelnen Unternehmen nicht mehr rechtssicher überschaubar sind. Dies führt zu einem erheblichen Risiko für Unternehmen.

16. Ausnahme für die journalistische Datenverarbeitung (Art. 80). Der Entwurf sieht in Art. 80 vor, dass die Mitgliedstaaten für die Datenverarbeitung zu journalistischen Zwecken Abweichungen und Ausnahmen von bestimmten Kapiteln der Verordnung vorsehen sollen.

a) Direkte Anwendung der Ausnahme erforderlich. Die Möglichkeit der Mitgliedstaaten, entsprechende Ausnahmen vorzusehen, reicht nicht aus, um den geltenden Schutzstandard zu wahren. Die Ausnahmen müssen vielmehr unmittelbar und ohne Relativierung gelten**.** Anders als bisher soll das europäische Datenschutzrecht nun in einer Verordnung geregelt werden. Das bedeutet, dass auch alle Beschränkungen direkt Anwendung finden.

Eine Umsetzung auf nationaler Ebene birgt zudem die Gefahr unterschiedlicher Schutzstandards. Der jetzige Wortlaut fördert dies, indem er nur vorgibt, dass *Abweichungen und Ausnahmen* von bestimmten Kapiteln erlassen werden sollen. Wie diese im Einzelnen aussehen, bleibt den Mitgliedstaaten überlassen. Es lässt sich zudem nicht ausschließen, dass insbesondere der Begriff der *Abweichung* so interpretiert wird, dass er einen weiten Ermessensspielraum begründet.

Hinzu kommt, dass in der jetzigen Formulierung der Vorschrift die Titel der einzelnen Kapitel vor der jeweiligen Kapitelnummer aufgezählt werden. Es lässt sich nicht ausschließen, dass diese Titel lediglich als Beschreibungen von Teilbereichen interpretiert werden könnten. Dadurch könnte der Eindruck entstehen, dass nicht die Kapitel insgesamt, sondern nur einzelne Teile derselben ausgenommen werden sollen (so z. B. lediglich die allgemeinen Grundsätze des Kapitels II, welches den Titel „die allgemeinen Grundsätze“ trägt).

b) Umfassende Ausnahme wichtig. Neben den genannten Kapiteln sollten auch die Artikel 73, 74, 76 und 79 des Kapitels VIII (Rechtsbehelfe, Haftung und Sanktionen) ebenfalls von der Ausnahme umfasst sein. Dabei handelt es sich um neue Sanktionen bzw. Beschwerdemechanismen etc., die teilweise weit über das hinausgehen, was in der geltenden Datenschutzrichtlinie vorgesehen ist, und auf die journalistische Aktivität nicht passen bzw. für diese gefährlich sein könnten.

c) Unmittelbare Geltung der Ausnahme wird auch Postulat der Subsidiarität gerecht. Denn eine direkte Anwendung der Ausnahmen bedeutet nicht, dass die entsprechenden journalistischen Aktivitäten in einem rechtfreien Raum stattfinden. Diese können vielmehr weiterhin durch das jeweilige nationale Medien-, Äußerungs- und Persönlichkeitsrecht geregelt werden.

d) Weite Definition journalistischer Tätigkeit. Die Kommission geht von einem weiten Begriff der journalistischen Tätigkeit aus. Sie versteht darunter alle Aktivitäten, die dem Ziel der Veröffentlichung von Informationen, Meinungen oder Ideen gegenüber der Öffentlichkeit dienen. Das soll unabhängig vom gewählten Medium gelten und nicht auf Medienunternehmen beschränkt sein (Erwägungsgrund 121 am Ende). Nach der deutschen Fassung könnte sich die Ausnahme sogar eventuell auch auf sog. Aggregatoren erstrecken. Anstatt auf „disclosure“ wie in der englischen Fassung, wird dort auf die „Weitergabe“ der entsprechenden Informationen Bezug genommen.

Dieser weite Anwendungsbereich darf jedoch nicht dazu führen, dass im Rahmen des weiteren Gesetzgebungsprozesses der Anwendungsbereich der Ausnahme weiter eingeschränkt wird.

17. Verhältnis zur E-Privacy-Richtlinie. In Art. 89 wird nun klargestellt, dass die E-Privacy-Richtlinie für die von ihr geregelten Konstellationen Vorrang gegenüber der Datenschutzverordnung hat. Die Klarstellung, dass die Datenschutzverordnung keine weiteren Pflichten, als die in der E-Privacy Richtlinie vorgesehen einführt, wird begrüßt. Allerdings darf diese Formulierung nicht dazu führen, dass die in der Verordnung als Rechte der betroffenen Personen formulierten Vorschriften (z.B. Art. 15, 17 und 20) zu einer Aushöhlung dieser Vorschrift führt. Darüber hinaus dürften auch nicht alle für digitale Geschäftsmodelle relevanten Datenverarbeitungsprozesse unter die E-Privacy-Richtlinie fallen, so dass für diese die Datenschutzverordnung gelten würde. Es lässt sich daher nicht ausschließen, dass dadurch weitere Beschränkungen eingeführt werden.

18. Delegierte Rechtsakte. Delegierte Rechtsakte sind kein sachgerechtes Instrument, um das Datenschutzrecht zu regeln bzw. zu spezifizieren. Insbesondere kann der neu zu gründende Europäische Datenschutzausschuss den demokratischen Prozess nicht ersetzen. Das Datenschutzrecht hat die in Einzelfällen schwierige Balance zwischen dem legitimen Interessen des Einzelnen und den Kommunikationsnotwendigkeiten einer modernen Wirtschaft zu erzielen. Das Ergebnis dieses Abwägungsprozesses kann weitreichende Auswirkungen auf Verbraucher und Unternehmen haben und darf daher nicht einer einzigen Institution vorbehalten bleiben.

Hinzu kommt, dass es aufgrund der Nutzung zahlreicher Generalklauseln sowie des Vorbehalts des Erlasses delegierter Rechtsakte an verschiedenen Stellen der Verordnung für Unternehmen überhaupt noch nicht absehbar ist, welche Verpflichtungen tatsächlich eingeführt werden. Dies birgt nicht nur die Gefahr weiterer Einschränkungen, sondern führt auch zu erheblicher Rechtsunsicherheit für Unternehmen.

Ansprechpartner:

VDZ
Dr. Christoph Fiedler
Geschäftsführer Europa- und Medienpolitik
Tel.: 0049 30 72 62 98 120
c.fiedler@vdz.de

Dr. Karina Lott
Referentin Europa- und Medienpolitik
Tel.: 0032 2 536 06 03
k.lott@vdzv.de

BDZV
Helmut Verdenhalven
Geschäftsführer Medienpolitik
Tel.: 0049 30 72 62 98 203
verdenhalven@bdzv.de

Carolin Wehrhahn
Referentin Europapolitik
Tel.: 0032 2 551 01 94
wehrhahn@bdzv.de