

Stellungnahme des bvh
(Bundesverband des Deutschen Versandhandels e.V.)
zum Vorschlag der Europäischen Kommission
für eine europäische Datenschutz-Grundverordnung
(KOM(2012) 11/4 vom 25. Januar 2012)

Version 2.0

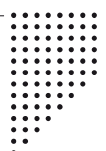
Berlin, 1. November 2012

Ansprechpartner:
RA Sebastian Schulz, Public Affairs | Datenschutz | Rechtspolitik

Der Ansatz der Europäischen Kommission (EU-KOM), die europäischen Regelungen zum Datenschutz zu modernisieren, verdient Unterstützung. Die innerhalb Europas eingetretene Rechtszersplitterung muss durch einen einheitlichen Rechtsrahmen ersetzt werden, der rechtsklare und praxisnahe Vorgaben für alle Beteiligten schafft. Oberstes Ziel der anstehenden Reform muss ein angemessener Ausgleich aller beteiligten Interessen sein. Zu Recht benennt deshalb der Entwurf die Wahrung des Verhältnismäßigkeitsprinzips als eine maßgebliche Orientierung für den Gesetzgeber.

Der Entwurf der EU-KOM wird dieser eigenen Maßgabe nicht gerecht. Das Regelwerk verfehlt die Zielsetzung einer dringend notwendigen Anpassung des Rechts an die veränderten Anforderungen der Informationsgesellschaft nahezu vollständig. Anstelle einer echten Reform des Datenschutzrechts, bewirkt die EU-KOM eine Verkomplizierung und zum Großteil widersprüchliche Verstetigung des fast 20 Jahre alten europäischen Rechtsrahmens. Durch die Verordnung werden europäische Unternehmen gegenüber nicht in Europa ansässigen Unternehmen benachteiligt. Verfassungsrechtlich garantierte Grundfreiheiten werden zu Lasten europäischer Unternehmen einseitig und unverhältnismäßig eingeschränkt. Wenn die Vorschläge der EU-KOM unverändert umgesetzt werden, werden etablierte Geschäftsmodelle im Online- und Versandhandel stark behindert bzw. gänzlich unmöglich.

Der bvh hat nachfolgend die aus der Perspektive der Online- und Versandhandelsbranche wichtigsten Bedenken zusammengefasst (I.) und unterbreitet Lösungsvorschläge für alternative Formulierungen (II.).



I. Unsere wichtigsten Bedenken

- Die Definitionen der Begriffe „personenbezogene Daten“ und „betroffene Person“ führen zu einem ausufernden Anwendungsbereich des Datenschutzrechts. Die erforderliche eindeutige Bestimmbarkeit, in welchen Fällen Daten als personenbezogen einzustufen sind, ist nicht gewährleistet. (Art. 4)
- Es existieren keine rechtsklaren Vorgaben für die Zulässigkeit von Datenverarbeitungen auf Grundlage der Einwilligung des Betroffenen. Durch überhöhte formale Anforderungen an die Wirksamkeit von Einwilligungen und die zu weitreichende Beschränkung der Einwilligungsmöglichkeit wird dieses zentrale Instrument im Verhältnis Unternehmen zu Verbraucher faktisch unbrauchbar. (Art. 7)
- Die Maßnahmen zur Beschränkung des Profilings sind unverhältnismäßig und verkennen die praktische Notwendigkeit solcher Verfahren. Kundenorientierte Ansprachen werden einem Verbot unterworfen, obwohl keine Gefahr für die informationelle Selbstbestimmung besteht. (Art. 20)
- Durch die fehlende Berücksichtigung von Drittinteressen im Rahmen von Abwägungen wird ganzen Wirtschaftszweigen die Geschäftsgrundlage entzogen. Nachgelagert wird dadurch auch die Versandhandelsbranche negativ beeinflusst. (Art. 6)
- Es fehlt ein Zulässigkeitstatbestand, der Datenverarbeitungen auch nach Zweckänderung weiterhin auf Grundlage einer Interessenabwägung zulässt. Datenverarbeitende Unternehmen werden dadurch auf umfangreiche Neuerhebungen von Daten verwiesen. (Art. 6)
- Informations- und Meldepflichten sind unangemessen ausgestaltet und gehen über das erforderliche Maß hinaus. Durch unklare Vorgaben und die fehlende Differenzierung, in welchen Fällen Informations- und Meldepflichten zu beachten sind, werden Unternehmen einem nicht akzeptablen Haftungsrisiko ausgesetzt. (Art. 11, 14, 31)
- Rechte des Betroffenen, namentlich das Recht, vergessen zu werden oder das Recht auf Datenübertragbarkeit, verfolgen ersichtlich das Ziel, im Internet angebotene Dienste regulieren zu wollen. Die teilweise gravierenden Folgen für

die übrige Realwirtschaft bleiben durch die EU-KOM gänzlich unberücksichtigt. Dem Recht des Betroffenen gegenüber Empfängern fehlt darüber hinaus jede in sachlicher und zeitlicher Hinsicht wirkende Beschränkung. (Art. 13, 17, 18)

- Die bewährte systematische Unterscheidung zwischen Datenübermittlungen und Datenverarbeitungen im Auftrag wird durch den Verordnungsentwurf teilweise aufgegeben. Die Anreizwirkung, durch Auslagerung von Datenverarbeitungsprozessen an spezialisierte Datenverarbeiter, Geschäftsprozesse zu optimieren, geht verloren. (Art. 26)
- Durch die Aufnahme von „Kollektivbeschwerderechten“ verursacht die EU-KOM Legitimations- und Repräsentationsprobleme, die im Datenschutzrecht systembedingt nicht überwunden werden können. (Art. 73)
- Die Verordnung unterscheidet nicht zwischen B2B- und B2C-Sachverhalten. Durch die fehlende Privilegierung von B2B-Ansprachen greift die Verordnung unnötig und unverhältnismäßig in die gewerbliche Kommunikation zwischen Unternehmen ein.
- Das Ziel der Harmonisierung wird durch übermäßige Eingriffsbefugnisse der EU-KOM stark gefährdet. Die Vielzahl an Befugnissen zum Erlass delegierter Rechtsakte bzw. von Durchführungsverordnungen ist nicht erforderlich und führt zu Verunsicherung bei Verbrauchern und Unternehmen.

II. Begründung und alternative Formulierungsvorschläge

1. Ausufernder Anwendungsbereich des Datenschutzrechts

In Artikel 4 Absätze 1 und 2 Entwurf für eine Datenschutz-Grundverordnung (DSGVO-E) werden die Begriffe „betroffene Person“ und „personenbezogene Daten“ definiert. Durch die Verordnung soll jede natürliche Person geschützt werden, die „direkt oder indirekt“ bestimmt werden kann. Die Mittel zur Bestimmung sollen dabei alle sein, die der Verantwortliche oder jeder sonstige Dritte „nach allgemeinem Ermessen aller Voraussicht nach“ einsetzen würde. Infolge der allgegenwärtigen Verfügbarkeit von Informationen im Internet und der Möglichkeit ihrer Verknüpfung wird nach dieser Definition faktisch jede Information im Online- und Offlinebereich dem Datenschutzrecht unterworfen.

Die in Artikel 4 Absätze 1 und 2 DSGVO-E vorgenommenen Definitionen sind zu unbestimmt und damit untauglich. Sie grenzen die Begriffe nicht in dem erforderlichen Maße ein. Eine randscharfe Bestimmung, in welchen Fällen das Datenschutzrecht gelten soll, ist für den Rechtsanwender auf dieser Grundlage nicht möglich. Die EU-KOM erkennt, dass bei Einsatz zahlreicher Technologien gar keine personenbezogenen Informationen erhoben und verarbeitet werden: Es werden selbst solche Informationen dem Datenschutzrecht unterworfen, die in der Praxis zu keinem Zeitpunkt zu einer Identifikation des Verbrauchers führen. In solchen Fällen besteht jedoch bereits kein Regelungsbedürfnis. Gerade im Bereich des Online-Marketings wird kaum auf andere Daten als Online-Kennungen oder sonstige endgerätebezogene Informationen zurückgegriffen, um den Verbraucher über Angebote bedarfsgerecht zu informieren. Allein der Umstand, dass solche Informationen theoretisch über mehrere Zwischenschritte und unter Zuhilfenahme von Sonderwissen eines Dritten auf eine natürliche Person zurückgeführt werden könnten, rechtfertigt nicht die Eröffnung des Anwendungsbereiches des Datenschutzrechts.

Bleibt es bei diesem undifferenzierten Anwendungsbereich sind Interaktive Händler für auf die Interessen des Kunden zugeschnittene Angebote künftig auf eine konkrete Einwilligung angewiesen, da die Abwägungsklausel in Artikel 6 Absatz 1 f) DSGVO-E aufgrund des unbestimmten Begriffes der „berechtigten Interessen eines für die Verarbeitung Verantwortlichen“ im Hinblick auf werbliche Ansprachen keine Rechtssicherheit bietet. Eine an den Interessen des Verbrauchers orientierte werbliche Ansprache wäre in Zukunft ausgeschlossen. Ein einwilligungsbasiertes Verfahren empfindet der Verbraucher jedoch nachweislich als ausgesprochen lästig. Die ihrer Begründung nach auf die Bedürfnisse des Verbrauchers abzielende Regelung erreicht damit in der Praxis genau das Gegenteil. Als Folge dessen würde das Werbevolumen durch nicht-personalisierte und damit nicht an den tatsächlichen Bedürfnissen des Verbrauchers ausgerichtete Werbung erheblich steigen. Hinzu kommt, dass der entstehende Aufwand und die Kosten für die ständige Einholung der Einwilligung für den Unternehmer administrativ und finanziell nicht mehr tragbar wären. Die über Artikel 5 Absatz 1 Satz 1 und Artikel 12 des Grundgesetzes geschützte Möglichkeit zur werblichen Ansprache wird in einem nicht zu rechtfertigenden Maße eingeschränkt.

Der bvh setzt sich für ein gestuftes Schutzkonzept des Datenschutzes ein, das für sensible Daten, bspw. Gesundheitsdaten, höhere Anforderungen vorsieht und für alltägliche Vorgänge wie im E-Commerce und in der Werbung ein angemessenes Schutzniveau schafft. Sensible personenbezogene Daten grundsätzlich genauso zu behandeln wie „bloße“ Adressdaten ist nicht sachgerecht.

Eine auf den jeweiligen Verwendungskontext bezogene Definition „alltäglicher Datenverarbeitung“ ist vorzunehmen. In diesem Zusammenhang müssen v.a. solche Informationen berücksichtigt werden, die Gegenstand von alltäglicher Kommunikation und Interaktion sind. Hiervon betroffen sind zuvorderst allgemein verfügbare Daten, soweit diese nicht ersichtlich gegen den Willen des Betroffenen allgemein verfügbar gemacht wurden. Allgemein verfügbare Informationen dem strengen Verbotsgrundsatz zu unterwerfen erscheint im Informationszeitalter als nicht mehr zielführend. Um jedoch auch solche personenbezogenen Daten für nicht gänzlich schutzlos zu erklären, wären hinreichende Transparenzpflichten in Form von Informationspflichten im Zeitpunkt der Ersterhebung sowie Auskunftspflichten für Fälle eines weitergehenden Transparenzinteresses des Betroffenen vorzusehen. Dem deutschen Recht vergleichbar sollte daneben in Artikel 4 DSGVO-E eine Bestimmung sensibler personenbezogener Daten erfolgen. Materielle Regelungen zum Umgang mit personenbezogenen Daten müssen dieses Stufenverhältnis in der Folge angemessen berücksichtigen.

Daneben sollte die Bestimmung des Personenbezuges allein aus der Perspektive des Informationsverarbeiters vorgenommen werden. Allein dadurch ist eine rechtsklare Bestimmung, in welchen Fällen ein Verarbeiter verantwortliche Stelle im Sinne des Datenschutzrechts ist, zu leisten. Nur wenn dem Verarbeiter mit eigenen Mitteln eine Identifikation des Betroffenen möglich ist, ist es gerechtfertigt, ihn mit datenschutzrechtlichen Vorgaben zu adressieren. Die widersprüchliche, regelbeispielhafte Aufzählung in Artikel 4 Absatz 1 DSGVO-E sollte aufgegeben werden. Sie ist redundant und sorgt in der praktischen Anwendung des Rechts eher für Auslegungsschwierigkeiten als dass diese hierdurch beseitigt würden.

Formulierungsvorschlag Artikel 4 Absatz 1 neu

„betroffene Person“ eine bestimmte natürliche Person oder eine natürliche Person, die direkt oder indirekt mit Mitteln bestimmt werden kann, die der für die Verarbeitung Verantwortliche ~~oder jede sonstige natürliche oder juristische~~

~~Person nach allgemeinem Ermessen aller Voraussicht nach einsetzen würde, etwa mittels Zuordnung zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck ihrer physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind;~~

2. Praktikable Rahmenbedingungen für Einwilligungen des Betroffenen schaffen

a) Das Zusammenspiel von Artikel 7 DSGVO-E und Erwägungsgrund 25 verlangt nach einer „explizit“ zu erklärenden Einwilligung. Eine stillschweigende Einwilligung „ohne Zutun der betroffenen Person“ genügt nicht. Auch umfangreiche Einwilligungen in mehrere, im Zeitpunkt der Einwilligung noch nicht feststehende Zwecke, werden dem Betroffenen versagt.

Die formalen Vorgaben für Einwilligungen sind zu starr und undifferenziert. Der Betroffene hat kein Interesse daran, für jeden Fall gesondert eine Einwilligung explizit erklären zu müssen. Die fehlende Gewichtung in Sinne einzelner Schutzstufen (vgl. oben II. 1.) führt auch bei den Vorgaben für die Zulässigkeit von Einwilligungen dazu, dass für die unterschiedlichsten Datenkategorien stets dieselben hohen Anforderungen an die Wirksamkeit von Einwilligungen gestellt werden. Es ist nicht zu verstehen, warum an Einwilligungen in alltägliche, dem Verbraucher dienliche Vorgänge, dieselben hohen Anforderungen gestellt werden, wie in Fällen der Verarbeitung von sensiblen personenbezogenen Daten.

Der bvh setzt sich für ein an der Schutzbedürftigkeit der Daten orientiertes Einwilligungskonzept ein. Einwilligungen in die Verarbeitung und Nutzung von sensiblen Daten müssen naturgemäß deutlich höheren Anforderungen genügen, als solche in Datenverarbeitungen des täglichen Lebens.

Auch das Rechtfertigungsinstrument der Einwilligung muss einem an unterschiedlichen Stufen orientierten Schutzkonzept folgen.

Konkludente Einwilligungen müssen im Informationszeitalter vor allem im Sinne des Verbrauchers möglich sein.

Formulierungsvorschlag Artikel 4 Absatz 8 neu:

"Einwilligung der betroffenen Person" jede ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgte explizite Willensbekundung in Form einer

Erklärung oder einer sonstigen eindeutigen Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Eine eindeutige Handlung kann auch in der Vornahme eines schlüssigen Verhaltens bestehen;

b) In Artikel 7 Absatz 4 DSGVO-E schränkt die EU-KOM die Möglichkeit, Datenverarbeitungen auf Grundlage einer Einwilligung des Betroffenen vorzunehmen, erheblich ein. Eine Einwilligung kann dann nicht als Rechtsgrundlage für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten dienen, wenn zwischen dem Betroffenen und der verantwortlichen Stelle ein „erhebliches Ungleichgewicht“ besteht. Eine Präzisierung, in welchen Fällen von einem solchen Ungleichgewicht auszugehen ist, erfolgt im Verordnungstext nicht.

Der Absatz ist zu unbestimmt und in der gewählten Form überflüssig. Erfolgen Einwilligungen im Kontext einer faktischen Übermacht des (Vertrags-)Partners, sind diese bereits nach allgemeinen Grundsätzen aufgrund der dann fehlenden Freiwilligkeit unwirksam. Die gewählte Formulierung erreicht in der Praxis allein eine nicht hinnehmbare Unsicherheit bei der Frage, ob personenbezogene Daten des Verbrauchers überhaupt auf Grundlage seiner Einwilligung erhoben, verarbeitet und genutzt werden dürfen. Zwar geht der bvh davon aus, dass diese Formulierung allein auf strukturelle Ungleichgewichte, wie etwa im arbeitsrechtlichen Über-Unterordnungsverhältnis (so auch Erwägungsgrund 34), Anwendung finden soll. Bei weiter Auslegung des Verordnungstextes wird darüber aber faktisch jede Situation erfasst, in denen ein Verbraucher einem Unternehmen gegenübertritt. Der Verweis auf gesetzliche Erlaubnistatbestände ist untauglich, da auch die in Artikel 6 Absatz 1 f) DSGVO-E normierte Abwägungslösung keine Rechtssicherheit schafft. Verbrauchern bleibt es so verwehrt, in die Datennutzung durch Unternehmen einwilligen zu können. Eine selbstbestimmte Teilnahme am Rechts- und Geschäftsverkehr ist damit gefährdet oder wird gänzlich ausgeschlossen.

Der bvh fordert eine Klarstellung in Artikel 7 Absatz 4 DSGVO-E, wonach die Datenerhebung, -verarbeitung und -nutzung von Verbraucherdaten durch Unternehmen nicht von der Beschränkung erfasst ist. Orientiert am aus dem deutschen Recht bekannten Kopplungsverbot dürfen allenfalls in Fällen einer eklatanten Vormachtstellung des Vertragspartners Zweifel an der „echten Wahl-

freiheit“, d.h. an der Freiwilligkeit der Einwilligung des Verbrauchers, bestehen.

Formulierungsvorschlag Artikel 7 Absatz 4 neu

~~Die Einwilligung bietet keine Rechtsgrundlage für die Verarbeitung, wenn zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht. Der für die Verarbeitung Verantwortliche darf den Abschluss eines Vertrages nicht von der Einwilligung des Betroffenen abhängig machen, wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist.~~

3. Beschränkung von Profiling-Maßnahmen mit Augenmaß

a) In Artikel 20 DSGVO-E reguliert die Verordnung Maßnahmen, die die Bildung von Profilen zum Gegenstand haben. Ausgehend von dem sehr weitgehenden Anwendungsbereich der Verordnung (vgl. oben II. 1.) wird die profilbasierte Abwicklung von Geschäftsbeziehungen auf wenige Ausnahmefälle beschränkt.

Artikel 20 ist bereits wegen systematischer Erwägungen unbrauchbar. Die durch die EU-KOM gewählte Formulierung vermengt Aspekte der sog. automatisierten Einzelentscheidung mit Maßnahmen des etwa zu Zwecken einer Bonitätsprüfung notwendigen Profilings in unzulässiger Weise. Die Regelung ist darüber hinaus zu undifferenziert und schadet damit Unternehmen und Verbrauchern gleichermaßen. Bei der Begrenzung von Profilingmaßnahmen muss Berücksichtigung finden, ob und inwieweit diese überhaupt negative Auswirkungen auf die Nutzer haben können. Eine solche Abstufung findet sich im Verordnungstext nicht. Automatisierte Entscheidungen sind jedoch Teil des Massenverkehrs. Gerade bei Profilingmaßnahmen im Werbebereich wird regelmäßig mit anonymisierten Daten und Pseudonymen gearbeitet, so dass auf den eigentlichen Nutzer keinerlei direkte Rückschlüsse gezogen werden. Es entstehen weder rechtliche Wirkungen noch sonstige Beeinträchtigungen. Vielmehr wird das Profiling genutzt, um die Angebote auf die Bedürfnisse des Kunden zuzuschneiden und entsprechend seiner Interessen zu verbessern. Durch diese Kundenorientierung werden eventuelle Belästigungen des Verbrauchers durch unerwünschte Angebote beschränkt. Über eigenverantwortlich vorzunehmende technische Maßnahmen, wie etwa durch die Begrenzung von Cookies in den Browsereinstellungen, kann der Verbraucher daneben auch einen

weitergehenden Ausschluss von Profilingmaßnahmen eigenverantwortlich erreichen.

Der bvh fordert, für pseudonymisierte und anonymisierte Profilingmaßnahmen eine Ausnahme nach dem Vorbild von § 15 Absatz 3 Telemediengesetz (TMG) vorzusehen, um hierdurch gezielt Anreize für eine Verminderung bzw. gänzliche Vermeidung des Personenbezugs zu schaffen.

Eine Privilegierung von Datenverarbeitungen unter Verwendung von Pseudonymen ist in einem gesonderten Artikel in Abschnitt 2 –Grundsätze– vorzusehen. Die Begriffsbestimmungen in Artikel 4 sind um die Definitionen der Anonymisierung und der Pseudonymisierung zu ergänzen.

b) Die Tragweite der vorgesehenen Ausnahmen in Artikel 20 Absatz 2 DSGVO-E ist zu unbestimmt und schafft keine Rechtssicherheit. Es ist unklar, ob hiervon auch „Profilingmaßnahmen“ erfasst sind, die im Rahmen der Begründung eines Vertrages vorgenommen werden, um die Bonität des Kunden sicherzustellen. Werden diese Verfahren beschränkt oder verboten, hat dies auf Seiten des Verbrauchers erhebliche nachteilige Folgen. In Deutschland würde dies dazu führen, dass bei Verbrauchern beliebte und durch diese bevorzugte Geschäftsmodelle wie der Kauf auf Rechnung oder Ratenkreditverträge durch die Unternehmen aufgrund des erhöhten Kreditausfallrisikos nicht mehr angeboten werden.

In Artikel 20 Absatz 2 DSGVO-E bedarf es der Klarstellung, dass Profilingmaßnahmen, die im Rahmen der Begründung von Verträgen erforderlich sind, von der Ausnahme erfasst bleiben.

*Formulierungsvorschlag Artikel 20 Absatz 2 lit. a)
im Rahmen **der Begründung** ~~des Abschlusses~~ oder der Erfüllung eines Vertrags vorgenommen wird und **die Begründung** ~~der Abschluss~~ oder die Erfüllung des Vertrags [...]*

*Formulierungsvorschlag Erwägungsgrund 58 neu
[...] Eine solche Maßnahme sollte allerdings erlaubt sein, wenn sie ausdrücklich per Gesetz genehmigt wurde, bei ~~Abschluss~~ **Begründung** oder in Erfüllung eines Vertrags, **insbesondere zur Bonitätsprüfung**, durchgeführt wird oder wenn [...]*

4. Berücksichtigung von Drittinteressen für die Zulässigkeit der Datenverarbeitung

Nach Artikel 6 Absatz 1 f) DSGVO-E soll die Verarbeitung von personenbezogenen Daten nur noch zur Wahrung berechtigter eigener Interessen des für die Verarbeitung Verantwortlichen zulässig sein. Gegenüber der bisherigen europäischen und deutschen Rechtslage ist damit die Zulässigkeit der Datenverarbeitung zur Wahrnehmung der berechtigten Interessen eines Dritten entfallen.

Die fehlende Möglichkeit der Berücksichtigung von Drittinteressen schränkt die geltende Rechtslage deutlich ein und wird die Online- und Versandhändler nachhaltig schädigen. Für einige Geschäftsmodelle wie z.B. den Kauf auf Rechnung ist unsere Branche auf die Zusammenarbeit mit geschäftsmäßigen Datenverarbeitern angewiesen. Hierunter fallen vor allem Auskunfteien. Diese Datenverarbeiter werden datenschutzrechtlich betrachtet nicht im eigenen Interesse, sondern stets im Interesse Dritter tätig. Bleibt es bei der in Artikel 6 Absatz 1 f) DSGVO-E vorgenommenen Einschränkung, wird solchen Datenverarbeitern die Geschäftsgrundlage entzogen. Bonitätsauskünfte können nicht mehr verlässlich erteilt werden.

Auch für den Verbraucher ist die vorgenommene Beschränkung in mehrfacher Hinsicht gravierend. Erstens: Sind Bonitätsprüfungen nicht mehr möglich, entfällt für Online- und Versandhändler das zentrale Mittel zur Minimierung des eigenen Kreditrisikos. Als Folge können die heute durch den Verbraucher bevorzugten Zahlungsarten wie der Kauf auf Rechnung oder Ratenlieferungsverträge nicht mehr angeboten werden. Zwangsläufig gehen damit ein ganz erheblicher Serviceverlust und die Reduzierung auf bei den Verbrauchern unbeliebte Zahlungsarten einher. Zweitens: Da Adressen Dritten nicht mehr für deren Werbezwecke übermittelt werden dürfen, wäre das sogenannte Listbroking, also die nach den bisherigen Datenschutzregelungen zulässige Weitergabe von zielgruppengerichteten Adresslisten zum Direktmarketing nicht mehr zulässig. Als Folge wird das nicht-personalisierte Werbevolumen enorm ansteigen. Verbraucher werden nicht bedarfsgerecht, sondern nach dem „Gießkannenprinzip“ mit Werbung überflutet.

Die EU-KOM darf in Artikel 6 Absatz 1 f) DSGVO-E nicht hinter geltendes Recht zurückfallen. Neben den Interessen des für die Verarbeitung Verantwortlichen müssen weiterhin auch Interessen Dritter die Rechtmäßigkeit der

Datenverarbeitung begründen können.

Formulierungsvorschlag Artikel 6 Absatz 1 f)

*Die Verarbeitung ist zur Wahrung der berechtigten Interessen des für die Verarbeitung Verantwortlichen **oder eines Dritten** erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Dieser gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.*

5. Abwäglungslösung auch bei Zweckänderung ermöglichen

Nach dem Entwurf bedarf es auch künftig für die Zulässigkeit der weiteren Nutzung von zuvor rechtmäßig erhobenen Daten in Fällen der Zweckänderung oder des Zweckfortfalls einer die Zweckänderung legitimierenden Erlaubnis. Anders als im geltenden Datenschutzrecht erfährt diese Vorgabe in Artikel 6 Absatz 4 DSGVO-E jedoch eine Einschränkung dergestalt, dass nunmehr künftig Zweckänderungen nicht mehr auf Grundlage einer Interessenabwägung möglich sein sollen.

Diese Einschränkung der Möglichkeit zur weiteren Nutzung ist systematisch verfehlt und sachlich nicht gerechtfertigt. Bleibt es bei dieser Beschränkung, sind Unternehmen auch in Fällen bislang gesetzlich anerkannter Konstellationen von Zweckänderungen, z.B. der werblichen Ansprache von Bestandskunden, auf umfangreiche Neuerhebungen angewiesen, obwohl aktuelle Datenbestände zur Verfügung stehen und schutzwürdige Interessen des Betroffenen hinreichend über Transparenz- und Widerspruchsrechte gesichert sind. Die hierdurch für die datenverarbeitenden Unternehmen entstehenden bürokratischen und kostenintensiven Mehrbelastungen stehen außer Verhältnis. In Fällen der Einwilligung würde auch der Verbraucher durch diese Regelung belastet: Obwohl dieser seine schutzwürdigen Interessen durch Widerrufs- und Widerspruchsmöglichkeiten umfassend berücksichtigt weiß, muss er bei jeder Zweckänderung erneut eine Einwilligung abgeben.

Der bvh setzt sich für eine Beibehaltung des geltenden Rechts ein. Danach müssen auch zukünftig Datennutzungen nach Zweckänderung oder Erreichung des ursprünglichen Zweckes auf Grundlage einer Interessenabwägung weiterhin möglich bleiben.

Formulierungsvorschlag Artikel 6 Absatz 4 neu
Ist der Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten erhoben wurden, nicht vereinbar, muss auf die Verarbeitung mindestens einer der in Absatz 1 ~~Buchstaben a bis e~~ genannten Gründe zutreffen. Dies gilt insbesondere bei Änderungen von Geschäfts- und allgemeinen Vertragsbedingungen.

6. Informations- und Auskunftspflichten angemessen ausgestalten

Durch Artikel 11, 14 und 15 DSGVO-E werden im Verhältnis zur geltenden Rechtslage weiterführende Informations- und Auskunftspflichten geschaffen. Nach Artikel 14 Absatz 4 a) DSGVO-E sind der betroffenen Person die geforderten Informationen bereits bei der Erhebung der Daten sämtlichst durch den für die Verarbeitung Verantwortlichen zu erteilen. In Artikel 15 DSGVO-E wird die verantwortliche Stelle dazu verpflichtet, bei jeder Anfrage des Betroffenen alle unter den Buchstaben a) bis h) genannten Daten, Entscheidungen und Auswirkungen mitzuteilen. Dies sogar als Prognoseentscheidung, da gemäß Buchstabe c) auch künftige Empfänger beaufkuntet werden müssen.

Die neuen Informationspflichten gehen weit über das Ziel einer transparenten Datenverarbeitung hinaus. Sie entsprechen weder den Bedürfnissen der Verbraucher nach einer konkreten Information über die tatsächlich relevanten Aspekte der Datenverarbeitung noch den praktischen Gegebenheiten der datenverarbeitenden Wirtschaft. Im Online- und Versandhandel werden sehr unterschiedliche Kommunikations- und Bestellmedien genutzt, so dass die Informationsmenge, die an den Kunden übermittelt wird, nicht immer gleich groß sein kann. Gerade bei telefonischen oder schriftlichen Bestellungen werden Händler vor eine unlösbare Aufgabe gestellt: Es ist schlicht nicht möglich, den Betroffenen auf kleineren Werbemedien, wie z.B. Postkarten, alle geforderten Informationen zur Verarbeitung seiner Daten zur Verfügung zu stellen. Die in Artikel 14 Absatz 5 DSGVO-E vorgesehene Ausnahme bei Unverhältnismäßigkeit ist aufgrund des weiten Auslegungsspielraumes nicht geeignet, Rechtssicherheit zu schaffen.

Andere Informations- und Auskunftspflichten sind nicht klar genug definiert und führen zu einer großen Unsicherheit bei ihrer konkreten Anwendung. Dies gilt etwa für die Verpflichtung zur Mitteilung sonstiger Informationen, die notwendig sind, um gegenüber dem Betroffenen eine Verarbeitung nach Treu

und Glauben zu gewährleisten, vgl. Artikel 14 Absatz 1 h) DSGVO-E. Ganz allgemein sind die in Artikel 14 DSGVO-E undifferenziert bei jeder Anfrage anzugebenden Informationen letztlich eine Verpflichtung zur Irrelevanz.

Informationspflichten müssen so ausgestaltet werden, dass sie praktisch umsetzbar sind. Auch angesichts der empfindlichen Bußgeldandrohungen in Artikel 79 Absatz 5 e) DSGVO-E, die ohne Abstufung nach der Schwere des Verstoßes bis zu 1 % des weltweiten Jahresumsatzes eines Unternehmens vorsehen, bedarf es einer rechtsklaren und praktisch realisierbaren Vorgabe. Als Vorbild sollte § 4 Absatz 3 BDSG dienen, der eine Verpflichtung zur Information über die Identität der verantwortlichen Stelle, über die Zweckbestimmung der Datenverwendung und ggf. über Kategorien von Empfängern vorsieht.

Formulierungsvorschlag Artikel 14 Absatz 1 neu

Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über

- 1. die Identität der verantwortlichen Stelle,*
- 2. die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und*
- 3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss, zu informieren.*

7. Meldepflichten bei Datenpannen auf relevante Fälle begrenzen

Die EU-KOM normiert in Artikel 31 DSGVO-E die Verpflichtung, bei einer Verletzung des Schutzes von personenbezogenen Daten ohne unangemessene Verzögerung, jedenfalls aber binnen einer Frist von 24 Stunden, die Aufsichtsbehörde zu informieren. Die Vorgabe macht keine Einschränkung hinsichtlich der Schwere der Verletzung und erfasst alle Arten personenbezogener Daten.

Die Regelung zur Meldepflicht bei Datenschutzverstößen ist zu undifferenziert und geht weit über das geltende Recht hinaus: Zunächst unterwirft die EU-KOM, anders als der nationale Gesetzgeber, ausnahmslos jedes bei der verantwortlichen Stelle gespeicherte Datum der Verpflichtung, in Fällen von Verletzungen der Vorgaben der Verordnung diese der Aufsichtsbehörde zu melden. Diese nicht differenzierende und daher sehr weitgehende Meldepflicht

erfährt auch im Folgenden keine Einschränkung durch eine etwa vorzunehmende Prognose, ob in Fällen faktischer Verletzungen des Rechts auch eine Beeinträchtigung des Betroffenen droht. Tatsächlich führt aber nicht jede Beeinträchtigung überhaupt zu einem messbaren Schaden auf Seiten des Betroffenen. Orientiert am Wortlaut des Artikels 31 Absatz 1 DSGVO-E, wonach die Meldepflicht „bei einer [d.h. jeder] Verletzung des Schutzes personenbezogener Daten“ greift, führt dies im Ergebnis zu einer unangemessen weitreichenden Verpflichtung der verantwortlichen Stelle. Auch Bagatellfälle, z.B. die unzulässige Kenntnisnahme von personenbezogenen Daten durch das Reinigungspersonal oder durch Mitarbeiter anderer Abteilungen innerhalb derselben Organisation, lösen in Zukunft die Meldepflicht aus.

Auch die in Artikel 31 Absatz 1 DSGVO-E vorgesehene 24-Stunden-Frist, binnen derer eine Meldung an die Aufsichtsbehörde zu erfolgen hat, stellt datenverarbeitende Stellen unnötig vor enorme Probleme. Unternehmen wird es verwehrt, zunächst eigene interne Ermittlungen anzustrengen und für Abhilfe zu sorgen. Andere Unternehmen, die Datenverarbeitungen in Auftrag vornehmen lassen, sind in Zukunft einem nicht vertretbaren Prozessrisiko ausgesetzt. Treten Verstöße in Fällen von Datenverarbeitungen im Auftrag, für die der Auftraggeber weiterhin vollumfänglich verantwortlich bleibt, auf, ist das Einhalten einer solchen Frist schlicht unmöglich. Der Auftraggeber ist in solchen Fällen stets auf eine umgehende Unterrichtung durch den Auftragnehmer angewiesen. Kommt der Auftragnehmer dieser Unterrichtungspflicht gegenüber dem Auftraggeber nicht nach, richtet sich die Bußgeldandrohung des Artikels 79 Absatz 6 s) DSGVO-E dennoch stets gegen den Auftraggeber als verantwortliche Stelle. Das als Standard genutzte Instrument der Auftragsdatenverarbeitung droht erheblich an Bedeutung zu verlieren.

Der bvh setzt sich für eine Meldepflicht ein, die sich an deutschem Recht orientiert. Bei der Frage der Fristbemessung soll allein auf die Kenntnis der verantwortlichen Stelle abgestellt werden. Flankierend ist in den Erwägungsgründen klarzustellen, dass im Falle andauernder eigener Ermittlungen nicht von einem schuldhaften Zögern auszugehen ist.

Formulierungsvorschlag Artikel 31 Absatz 1 neu

Stellt der für die Verarbeitung Verantwortliche fest, dass bei ihm gespeicherte

- 1. sensible personenbezogene Daten,*
- 2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,*

3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder

4. personenbezogene Daten zu Bank- oder Kreditkartenkonten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat er dies nach den Vorgaben des Absatzes 3 ohne schuldhaftes Zögern der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen.

8. Recht des Betroffenen, vergessen zu werden, Recht auf Datenübertragbarkeit und Rechte gegenüber Empfängern

a) Das in Artikel 17 Absatz 2 DSGVO-E normierte sog. Recht, vergessen zu werden führt neue Löschatbestände ein und zielt nachweislich auf eine Ausweitung der Betroffenenrechte im digitalen Raum ab. Die EU-KOM hat bereits im Rahmen der Konsultationsphase mehrfach deutlich gemacht, dass vor allem global agierende Internetkonzerne einer strengeren Regulierung unterworfen werden sollen. Die verantwortliche Stelle wird verpflichtet, alle zwischenzeitlich erfolgten Veröffentlichungen, die auf eine durch sie vorgenommene oder ermöglichte Erstveröffentlichung zurückzuführen sind, rückgängig zu machen. Nach dem Wortlaut werden hiervon sämtliche Veröffentlichungen im digitalen und nicht-digitalen Umfeld erfasst.

Die neue Regelung geht über die Verpflichtung zur Löschung rechtswidrig gespeicherter Daten deutlich hinaus. Die verantwortliche Stelle wird verpflichtet, „alle vertretbaren Schritte“ zu unternehmen, um eine vollständige Löschung der Information zu gewährleisten. Eine solche Verpflichtung ist außerhalb von Social-Media-Plattformen nicht gerechtfertigt und höhlt die Grundsätze der Datentrennung und Datensparsamkeit völlig aus: In der Praxis erfolgt in Fällen von durch den Betroffenen eigenverantwortlich auf interaktiven Plattformen vorgenommenen Veröffentlichungen, z.B. von Produktbewertungen, keine Verknüpfung mit etwa vorhandenen (Kunden-)Stammdaten. Um der Verpflichtung aus Artikel 17 Absatz 2 DSGVO-E nachkommen zu können, müssen künftig für eine zweifelsfreie Identifikation weitergehende Verknüpfungen mit vorhandenen Kundendaten erfolgen. Die verantwortliche Stelle ist darüber hinaus aufgefordert, sämtliche aus der Erstveröffentlichung hervorgehenden weiteren Veröffentlichungen nachzuverfolgen und zu dokumentieren, um diese

im Falle eines Löschbegehrens erfassen zu können. Die rechtskonforme Veröffentlichung von Daten sowie bereits das Bereitstellen von Plattformen zur eigenverantwortlichen Veröffentlichung durch die Betroffenen selbst sind künftig mit nicht mehr kalkulierbaren Risiken für die Unternehmen verbunden. Daneben fehlt es an einer Ausnahme für solche personenbezogenen Daten, die für den für die Verarbeitung Verantwortlichen selbst erforderlich sind, z.B. bei Veröffentlichung von Geschäftsinformationen oder Beschäftigtendaten.

b) Auch das in Artikel 18 DSGVO-E normierte Recht auf Datenübertragbarkeit zielt ersichtlich auf Betreiber von Social-Media-Plattformen ab, vgl. auch Erwägungsgrund 55. Die verantwortliche Stelle wird verpflichtet, sämtliche in einem strukturierten Verarbeitungssystem gespeicherten personenbezogenen Daten auf Verlangen dem Betroffenen in einem weiterverwendbaren strukturierten Format zur Verfügung zu stellen. Erreicht werden soll ein für den User erleichterter Wechsel zwischen einzelnen Plattformanbietern.

Durch die unbestimmte Formulierung des Vorschlages werden in der Praxis auch Sachverhalte erfasst, die von der EU-KOM schlechterdings nicht gemeint sein können. Die EU-KOM vergisst, dass heute jede moderne elektronische Datenverarbeitung in strukturierter Form erfolgt und damit auch jede Datenverarbeitung in den Anwendungsbereich von Artikel 18 DSGVO-E fällt. Das einschränkende normative Merkmal des „gängigen“ Formates ist schon wegen des stetigen technischen Wandels nicht hinreichend definierbar und damit als Korrektiv untauglich. Der undifferenzierte Wortlaut der Regelung erfasst damit auch Wirtschaftsbereiche, die von der EU-KOM nach eigenem Bekunden gar nicht erfasst werden sollen. So werden in (strukturierten) Kundendatenbanken neben Bestandsdaten auch Vermerke, Kaufhistorien oder Bonitätsdaten hinterlegt, die ausschließlich für die interne Verwendung in den Unternehmen bestimmt sind. Eine Verpflichtung zur Herausgabe solcher Informationen kommt einer Verpflichtung zur Weitergabe an einen Wettbewerber gleich und verletzt zahlreiche Grundrechte und -freiheiten der so adressierten Unternehmen in unverhältnismäßiger Weise. Schränkt die EU-KOM den Anwendungsbereich ihres Vorschlages nicht sachgerecht ein, führt dies zu einer nicht akzeptierbaren Offenbarungspflicht der Unternehmen hinsichtlich interner geschäftlicher Informationen.

Um ganz offensichtlich nicht gewünschte Rechtswirkungen zu vermeiden soll die EU-KOM sagen, was sie meint.

Der Anwendungsbereich von Artikel 17 Absatz 2 und Artikel 18 DSGVO-E ist auf Anbieter interaktiver Social-Media-Dienste zu beschränken. Jedenfalls sind vom Anwendungsbereich Geschäftsinformationen sowie solche Informationen auszunehmen, die in den Unternehmen ausschließlich der internen Verwendung dienen.

c) Artikel 13 DSGVO-E auferlegt der verantwortlichen Stelle neue Informationspflichten. Die verantwortliche Stelle wird verpflichtet, solchen Unternehmen, an die Daten des Betroffenen weitergegeben wurden, über Berichtigungen und Datenlöschungen zu informieren. Ausgehend von der nicht differenzierenden Definition der „Weitergabe“ in Artikel 4 Absatz 3 DSGVO-E werden sowohl Datenübermittlungen als auch die Weitergabe an Auftragsdatenverarbeiter erfasst.

Es handelt sich um eine neuartige Verpflichtung der verantwortlichen Stelle. Die fehlende sachliche und zeitliche Beschränkung des Anwendungsbereiches bewirkt auch an dieser Stelle einen ausufernden Anwendungsbereich. Verantwortliche Stellen werden in systemwidriger Weise verpflichtet, auch für die Datenverarbeitung von etwa daneben bestehenden weiteren verantwortlichen Stellen Sorge zu tragen. So ist es bspw. in Konzernverbünden nicht unüblich, dass für denselben Datensatz mehrere Gesellschaften datenschutzrechtlich verantwortlich zeichnen. Der Grundsatz, dass jede verantwortliche Stelle nur für die eigene Datenverarbeitung verantwortlich ist, wird über die neu eingeführte Informationspflicht durchbrochen. In der Praxis führt dies dazu, dass von einer verantwortlichen Stelle auf unbestimmte Dauer Dokumentationen aller berechtigten Datenweitergaben, sei es in Form einer Datenübermittlung oder in Form der Auftragsdatenverarbeitung, vorgehalten werden müssen. Dies gilt auch dann, wenn beim ursprünglichen Empfänger der Datenweitergabe die Daten zwischenzeitlich gelöscht wurden. Von dieser Datenlöschung erhält die weitergebende Stelle naturgemäß keine Kenntnis. Durch notwendig werdende Dokumentationen und Abgleiche sowohl bei der weitergebenden als auch bei der empfangenden Stelle entsteht ein nicht zu rechtfertigender bürokratischer Aufwand.

Der bvh setzt sich für eine Begrenzung der Mitteilungspflicht aus Artikel 13 DSGVO-E auf Datenweitergaben im Rahmen von Auftragsdatenverhältnissen ein. Eine solche Verpflichtung ergibt sich bereits aus dem

Auftragsverhältnis und bedarf insofern keiner gesonderten Erwähnung im Verordnungstext.

9. Eindeutige Trennung von Datenübermittlungen und Auftragsdatenverarbeitung

Der Verordnungsentwurf nimmt, anders als das geltende Europäische Recht, keine Definition des „Dritten“ vor. Eine eindeutige Abgrenzung hinsichtlich datenschutzrechtlicher Pflichten des für die Verarbeitung Verantwortlichen und des Auftragsdatenverarbeiters wird erst auf der Ebene des materiellen Rechts und auch hier nur teilweise vollzogen. Die Pflichten des Auftragsdatenverarbeiters werden an einigen Stellen deutlich ausgeweitet.

Bereits die Gesetzestechnik ist unbefriedigend. So trägt es nicht zur Rechtssicherheit bei, dass erst über einen Umkehrschluss aus Artikel 26 Absatz 4 DSGVO-E das Nebeneinander von Auftragsdatenverarbeiter einerseits und datenschutzrechtlich Verantwortlichem andererseits herausgelesen werden muss. Die erweiterten datenschutzrechtlichen Pflichten des Auftragsdatenverarbeiters sind systemwidrig und führen in der Praxis zu einem Bedeutungsverlust dieser Form der Datenübertragung. Es ist nicht einzusehen, warum neben den für die Verarbeitung Verantwortlichen auch den Auftragsdatenverarbeiter weitergehende datenschutzrechtliche Verpflichtungen treffen. Exemplarisch seien neue Dokumentationspflichten (Artikel 28 Absatz 1 DSGVO-E), die Pflicht zur Durchführung einer Datenschutzfolgenabschätzung auch durch den Auftragsdatenverarbeiter (Artikel 33 DSGVO-E) sowie die Klagemöglichkeit direkt gegen Auftragsdatenverarbeiter (Artikel 75 DSGVO-E) genannt. Die durch die EU-KOM vorgenommene Vermischung und Überlagerung von Verantwortlichkeiten lässt den Grundsatz außer Acht, dass für die Datenverarbeitung prinzipiell allein die verantwortliche Stelle verantwortlich zeichnet.

Der bvh setzt sich für eine Beibehaltung der strikten Zweiteilung in Datenübermittlung und Auftragsdatenverarbeitung ein. Datenschutzrechtliche Pflichten können auch zukünftig allein den für die Verarbeitung Verantwortlichen adressieren. Dieser hat, wie bereits im geltenden Recht, für die Einhaltung dieser Pflichten bei Auftragnehmer Sorge zu tragen.

In Artikel 26 DSGVO-E bedarf es der Klarstellung, dass eine Datenübertragung an Auftragsdatenverarbeiter auch in Zukunft außerhalb des Vorliegens eines Zulässigkeitstatbestands zur Datenübermittlung zulässig ist.

10. Kein Kollektivbeschwerderecht im Bereich des Datenschutzes

In Artikel 73 Absätze 2 und 3 DSGVO-E wird „Einrichtungen, Organisationen oder Verbänden, die sich den Schutz der Rechte und Interessen der betroffenen Person in Bezug auf den Schutz ihrer personenbezogenen Daten zum Ziel gesetzt haben“, ein abgeleitetes bzw. eigenes Beschwerderecht bei der zuständigen Aufsichtsbehörde eingeräumt. Dieses „Kollektivbeschwerderecht“ besteht bereits dann, wenn nach der Ansicht der jeweiligen Einrichtung, Organisation und des jeweiligen Verbandes Vorgaben der Verordnung verletzt wurden.

Die Wahrnehmung von Rechten aus der Verletzung des informationellen Selbstbestimmungsrechts durch ein Kollektivorgan ist systemwidrig und sollte gestrichen werden. Die damit einhergehende Kontrollfunktion privatrechtlich organisierter Institutionen ist aufgrund ihrer systematisch zweifelhaften Legitimation allenfalls kontraproduktiv. Der individualrechtliche Charakter des Rechts auf informationelle Selbstbestimmung und die Vielschichtigkeit der Interessenlagen auch und insbesondere der Betroffenen lässt keinen Raum für eine Rechtswahrnehmung durch Dritte, die ohnehin nur Partikularinteressen vertreten können. Die stets notwendige Repräsentation aller datenschutzrechtlich Betroffenen kann im Datenschutzrecht nämlich systembedingt nicht erreicht werden. Dieser Mangel würde noch verstärkt, wenn Forderungen nach einer Aufnahme auch von Verbraucherschutzverbänden in Artikel 73 Absätze 2 und 3 DSGVO-E berücksichtigt würden.

Der bvh setzt sich für eine ersatzlose Streichung des Artikels 73 Absätze 2 und 3 DSGVO-E ein.

11. Fehlende Unterscheidung zwischen B2B und B2C

Der Entwurf unterscheidet nicht zwischen B2B- und B2C-Sachverhalten. Im Zusammenspiel mit der fehlenden Beschränkung des Anwendungsbereiches der Verordnung (vgl. oben II. 1.) werden dadurch sämtliche Nutzungen von Unternehmensinformationen, die einer natürlichen Person zugeordnet werden können, einer datenschutzrechtlichen Regulierung unterworfen. Am Beispiel personalisierter Werbung stellt die EU-KOM die Privatadresse einer geschäftlichen Adresse ohne Ausnahme gleich. Die geschäftliche Praxis, Unternehmensdaten sowie Namen und Adressen von Funktionsträgern der jeweiligen Organisation zu nutzen, wird faktisch verboten.

Die Grundsätze des Verbraucherdatenschutzes ohne Einschränkung auch auf die Kommunikation zwischen Unternehmen auszudehnen ist unverhältnismäßig und schießt über das Ziel der EU-KOM, den Verbraucherdatenschutz stärken zu wollen, deutlich hinaus. Im Verhältnis zwischen Unternehmen besteht weder ein vergleichbarer Schutzbedarf noch der Wunsch nach strengeren Datenschutzregeln. Das Grundrecht des Unternehmers am eingerichteten und ausgeübten Gewerbebetrieb (Artikel 12 GG) wird durch die EU-KOM zwangsweise dem daneben bestehenden Recht der Unternehmer auf informationelle Selbstbestimmung untergeordnet. Die EU-KOM hat hier bereits keinen Schutzauftrag noch findet eine ausgewogene Abwägung der objektivrechtlichen Teilbereiche beider betroffenen Grundrechte statt.

Der bvh fordert eine bereichsspezifische Ausnahme im Verordnungstext für Datennutzungen im B2B-Verhältnis.

Im Abschnitt -Grundsätze- bedarf es einer Klarstellung, dass die Nutzung einer rein geschäftlichen Adresse für gewerbliche Zwecke weiter zulässig bleibt. Die Ausnahme muss sich auch auf relevante Funktionsträger erstrecken. Soweit personenbezogene Daten von gewerblich oder freiberuflich Tätigen im B2B-Verhältnis verarbeitet werden sollen, muss dies auch in Zukunft ohne Einwilligung der Betroffenen und außerhalb der allgemeinen Abwägungslösung möglich sein.

12. Übermäßige Eingriffsbefugnisse der EU-KOM

Der durch die EU-KOM gewählte Ansatz einer Vollharmonisierung im Wege der Verordnung soll zu verbindlichen einheitlichen Regelungen im gesamten europäischen Binnenmarkt führen. Wettbewerbsverzerrungen im Sinne eines „forum shoppings“ sollen vermieden werden. Auch das in Artikel 3 Absatz 2 DSGVO-E und in Erwägungsgrund 63 kodifizierte Marktlandprinzip, d.h. die angestrebte Erstreckung des Anwendungsbereiches der künftigen Verordnung auf nicht in der EU ansässige Datenverarbeiter, soll zu einer Aufwertung und Vereinheitlichung datenschutzrechtlicher Standards im internationalen Kontext führen.

Diesem selbstgesetzten Ziel einer Rechtsvereinheitlichung ohne Spielräume wird die EU-KOM nicht gerecht. Durch zahlreiche Befugnisse zu delegierten Rechtsakten bzw. zu Durchführungsverordnungen behält sich die EU-KOM ein aktives und unmittelbares Eingreifen vor, ohne dass dies erforderlich wäre. Solche

weitreichenden Befugnisse führen zu Unsicherheit, ob und wenn ja, wie und wann die EU-KOM entsprechende Rechtssetzungsakte vornimmt. Die datenverarbeitende Wirtschaft sowie Verbraucher und Aufsichtsbehörden sind jedoch auf einen klaren, verlässlichen Rechtsrahmen angewiesen. Wirtschaftswachstum und neue Geschäftsmodelle kann es nur in einem Umfeld geben, das Verlässlichkeit und Rechtssicherheit bietet.

Die EU-KOM muss den selbstgesetzten Maßstäben gerecht werden; die Kompetenz zur Setzung delegierter Rechtsakte bzw. von Durchführungsverordnungen darf allenfalls auf wenige Ausnahmefälle beschränkt bleiben. In Betracht kommen Bereiche, die einem permanenten technologischen Wandel unterworfen sind, z.B. der Bereich Datenschutz durch Technikgestaltung.

Über den bvh:

Dank E-Commerce und Internet ist der Versandhandel so vital wie nie. Der Bundesverband des Deutschen Versandhandels e.V. (bvh) ist die Branchenvereinigung der Interaktiven Händler (d.h. der Online- und Versandhändler). Dem bvh gehören derzeit mehr als 340 Unternehmen an. Darunter sind Versender mit gemeinsamem Katalog- und Internet-Angebot, reine Internet-Händler, Teleshopping-Unternehmen, Apothekenversender und eBay-Powerseller. Die Branche setzt aktuell jährlich im Privatkundengeschäft rund 36 Mrd. Euro um. Allein der Online-Handel mit Waren hat daran einen Anteil von rund 75 Prozent. Der jährliche Gesamtumsatz im Geschäft mit gewerblichen Kunden wird auf weitere 8 Mrd. Euro geschätzt.

Neben den Versendern sind dem bvh auch über 90 namenhafte Dienstleister angeschlossen.

Der bvh vertritt die Brancheninteressen aller Mitglieder gegenüber dem Gesetzgeber sowie Institutionen aus Politik und Wirtschaft. Darüber hinausgehören die Information der Mitglieder über aktuelle Entwicklungen und Trends, die Organisation des gegenseitigen Erfahrungsaustausches sowie fachliche Beratung zu den Aufgaben des Verbands.

Kontakt: sebastian.schulz@bvh.info; Tel: +49 30 206 1385-14