HDE
Handelsverband Deutschland
Der Einzelhandel

[Lobbyregister Nr.: 31200871765-41]

Stellungnahme zum Vorschlag der Europäischen Kommission für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)

(KOM(2012) 11/4 vom 25. Januar 2012

I. Einleitung

Der Handelsverband Deutschland (HDE) ist seit 90 Jahren die Spitzenorganisation des deutschen Einzelhandels für rund 400.000 selbstständige Unternehmen mit insgesamt 2,8 Millionen Beschäftigten und knapp 400 Milliarden Euro Jahresumsatz. Er vertritt die Belange und Interessen des gesamten Einzelhandels - aller Branchen, Standorte und Betriebsgrößen.

II. Allgemeine Anmerkungen

Der HDE begrüßt das mit dem Verordnungsvorschlag verfolgte Ziel, mit der Harmonisierung und Modernisierung des Europäischen Datenschutzrechts auf die Herausforderungen der zunehmenden Globalisierung und Digitalisierung der Wirtschaft zu reagieren. Einheitliche und angemessene Datenschutz-Standards in der EU können die Wettbewerbsfähigkeit der europäischen Wirtschaft erhöhen, indem bürokratischer Aufwand verringert, Kosten eingespart und Rechtssicherheit für Unternehmen und Verbraucher erhöht werden. Dies setzt jedoch voraus, dass Überregulierungen vermieden und der Datenschutzstandard sich nicht am höchsten Niveau der bisher bestehenden nationalen Regelungen orientiert.

Auch im Einzelhandel nimmt das Thema Datenschutz einen hohen Stellenwert ein. Unternehmen verarbeiten im täglichen Umgang mit Kunden, Mitarbeitern und Lieferanten auch deren personenbezogene Daten. Da Handelsunternehmen in fast allen Aktivitätsfeldern mit Datenschutzregelungen konfrontiert werden, sollte Datenschutz so praxisnah und unbürokratisch wie möglich reguliert werden.

1. Kompatible Regelungen für alle

Die Herausforderung liegt darin, allgemeingültige Vorschriften zu verfassen, die sowohl für die gesamte Wirtschaft als auch für die Verbraucher verhältnismäßig sind. In der Vergangenheit hat sich der Ansatz, allgemeingültige Datenschutzbestimmungen zu kodifizieren, die unter allen Umständen gewahrt werden müssen, als sehr erfolgreich erwiesen. Im Sinne dieser Erfahrung muss unbedingt vermieden werden Regeln aufzustellen, die vornehmlich auf bestimmte Internetdienste (z.B. Suchmaschinen oder Soziale Netzwerke) ausgerichtet sind. Aus unserer Sicht muss ein effektives europäisches Datenschutzrecht daher auf Regeln und Prinzipien basieren, die allgemeingültig sind. Es muss sowohl auf einen Handelsunternehmer, der zur Unterstützung seiner eigentlichen Geschäftstätigkeit eine Kundendatei führt, anzuwenden sein, als auch auf ein soziales Netzwerk, dessen Kerngeschäft darin liegt, Kundendaten werbewirksam weiterzuverarbeiten. Hierzu gehört nicht zuletzt auch die Notwendigkeit, wirtschaftliche Interessen an der Verarbeitung von Daten, an niedrigen Kosten und geringem Verwaltungsaufwand mit einem vernünftigen Verbraucherinteresse am Schutz personenbezogener Daten in ein Gleichgewicht zu setzen.

2. Erlaubnisvorbehalt zukunftsfähig?

Unternehmen sind zunehmend auf die Verarbeitung personenbezogener Daten angewiesen. Dies reicht von der Personalverwaltung (Gehältermanagement, Arbeitnehmergesundheit, soziale Zusatzleistungen (z.B. Betriebskindergarten) über

die Bürokommunikation bis hin zu Marketing und Logistik. Vor diesem Hintergrund ist grundsätzlich fraglich, ob ein Verbot der Verarbeitung personenbezogener Daten mit Erlaubnisvorbehalt noch zielführend ist und der Vielfalt an praktischen Konstellationen und den künftigen technischen Entwicklungen ausreichend Rechnung trägt. Es sollte daher ein Systemwechsel in Betracht gezogen werden, wonach die personenbezogene Datenverarbeitung grundsätzlich erlaubt und nur bei Vorliegen klar definierter Verbotstatbestände rechtswidrig ist. Generalklauseln mit der Verpflichtung zur Selbsteinschätzung sollten aber vermieden werden, weil dies zu einer unnötigen Rechtsunsicherheit und – aus Gründen der Risikoprävention – de facto zu einer unverhältnismäßigen Einschränkung der Handlungsfreiheit führen würde.

Sollte es aber bei dem System des Verbots mit Erlaubnistatbeständen bleiben, müsste aus unserer Sicht mindestens eine risikobasierte Beurteilung einer Datenverarbeitungssituation, unter Betracht der Interessen der betroffenen Person und der zu seinem Schutz ergriffenen Maßnahmen im Gesetz erfolgen.

In dieser Hinsicht wäre eine Aufnahme des sog. Listenprivilegs als Erlaubnistatbestand, also die Möglichkeit, bestimmte personenbezogene Daten (z.B. Name, Anschrift, Beruf) zu Werbezwecken und zu Zwecken der Markt- und Meinungsforschung auch ohne Einwilligung zu nutzen und unter bestimmten Vorgaben an Dritte weiterzugeben, wünschenswert. Die im deutschen Datenschutzrecht anerkannte Ausnahme böte ein ausgewogenes Vorbild, das ausreichenden Schutz für den Betroffenen vorsieht. So ist nach § 28 Absatz 3 BDSG die Datennutzung nicht erlaubt, wenn anzunehmen ist, dass diese gegen schutzwürdige Interessen des Betroffenen verstößt. Dies ist insbesondere dann der Fall, wenn der Betroffene einer Nutzung seiner Daten widersprochen hat (Opt-out). Außerdem muss die Stelle, die die Daten erstmalig erhoben hat, eindeutig aus der Werbung hervorgehen.

3. Flexibilität der Verordnung

Im Rahmen der bestehenden Datenschutzrichtlinie (95/46/EG) wurden sektorspezifische Regelungen in eigenständigen Richtlinien verfasst, die sich im Rahmen der Prinzipien der Datenschutzrichtlinie bewegten. So konnte auf technologische Entwicklungen reagiert werden, ohne die eigentliche Datenschutzrichtlinie regelmäßig überarbeiten zu müssen. Laut Verordnungsvorschlag soll diese Flexibilität zukünftig über delegierte Rechtsakte der Kommission sichergestellt werden. Mit Hilfe delegierter Rechtsakte würde die Kommission somit künftig bestimmen, wie die Datenschutzregeln auf gesamte Wirtschaftsbereiche anzuwenden sind.

Diese wichtigen Anpassungen dürfen aber keinesfalls unter Aushebelung des ordentlichen Gesetzgebungsverfahrens vorgenommen werden. Aus unserer Sicht muss die Flexibilität des Datenschutzrechts sichergestellt sein, ohne derart weitreichende Kompetenzen an die Kommission abzutreten, wie es im Vorschlag vorgesehen ist. Ungeachtet des schnellen technischen Fortschritts, sollte daher darauf hingewirkt werden, möglichst viele materielle Sachverhalte so konkret wie möglich in der Verordnung selbst zu regeln und die Befugnisübertragung auf technische Details zu beschränken, bei denen praktische Auswirkungen auf die materiellen Regelungen selbst ausgeschlossen sind. Alles andere würde zu Einschränkungen der Handlungsfreiheit und -sicherheit der Unternehmen ohne hinreichende

demokratische Legitimation führen und die Akzeptanz der gesamten europäischen Kodifikation in unerwünschter Weise gefährden.

III. Zur Datenschutz-Grundverordnung im Einzelnen

1. Anwendungsbereich (Art. 2, 3)

Es ist zu begrüßen, dass die Verordnung sowohl für die Datenverarbeitung von in der EU niedergelassenen Unternehmen, als auch von nicht in der EU ansässigen Datenverarbeitern erfasst, soweit Daten von in der EU ansässigen Betroffenen verarbeitet werden. Nur so lassen sich Rechtsumgehungen durch Sitzverlagerung und Wettbewerbsverzerrungen vermeiden. Allerdings stellt sich für uns die Frage, wie der Vollzug in der Praxis gewährleistet werden soll, z.B. im Fall von Unternehmen, die außerhalb der EU ansässig sind, ihre Waren aber über das Internet an Kunden innerhalb der EU vertreiben.

Im Übrigen ist nicht einzusehen, warum gem. Art. 2 Abs. 2 b) die Organe, Einrichtungen, Ämter und Agenturen der EU vom sachlichen Anwendungsbereich der Verordnung ausgenommen werden sollten. Es zählt zu den wesentlichen Charakteristiken eines Rechtsstaats, dass die staatlichen Organe auch an das geltende Recht und Gesetz gebunden sind. Wenn die EU-Kommission nun datenschutzrechtliche Regelungen erlassen will, deren Einhaltung sie selbst nicht gewährleisten kann oder will, dann sollte dies zum Anlass genommen werden, die geplanten Regulierungen auf ihre Praxistauglichkeit zu überprüfen und ggf. Deregulierung vorzunehmen.

2. Definitionen (Art. 4)

a) „Betroffene Person“ / „personenbezogene Daten“ (Abs. 1, 2)

Die Definition der „personenbezogenen Daten“ ist aus unserer Sicht zu weit gefasst. Die Ursache hierfür liegt in der Definition der „betroffenen Person“. Es ist dem für die Verarbeitung Verantwortlichen nicht möglich abzuschätzen, ob „jede sonstige natürliche oder juristische Person“ (z.B. eine Bank; die Post; Google) über die Mittel verfügt, um eine Person direkt oder indirekt zu bestimmen. Laut der Definition entscheidet sich aber hierdurch, ob Daten „personenbezogen“ sind, oder nicht. In der Konsequenz wären alle Daten, die zur Bestimmung einer Person verwendet werden *könnten*, völlig unabhängig von den Möglichkeiten, die dem für die Verarbeitung Verantwortlichen zur Verfügung stehen, grundsätzlich als personenbezogene Daten zu behandeln und dementsprechend zu schützen.

Diese Konstellation würde einer vollkommenen Abkehr vom risiko-basierten Ansatz gleichkommen. Diese Regel würde alle wirtschaftliche Aktivitäten, bei denen Daten verwendet werden, erschweren und unnötigen bürokratischen Aufwand verursachen, ohne dass der Schutz der Privatsphäre der betroffenen Personen verbessert würde. Die Definition sollte daher auf Personen beschränkt werden, die der für die Verarbeitung Verantwortliche mit den ihm aller Voraussicht nach zur Verfügung stehenden Mitteln bestimmen kann.

Die Begriffe „physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle und soziale Identität“ werden nicht näher erläutert und sorgen daher für weitere Rechtsunsicherheit. Da die Aufzählung nicht abschließend und indikativ

ist, sollte erwogen werden diesen Teil der Definition in die Erwägungsgründe zu verschieben.
Erhebliche Rechtsunsicherheit entsteht auch durch die unbestimmten Rechtsbegriffe „nach allgemeinem Ermessen aller Voraussicht nach“. Hier ist eine konkretere Erläuterung notwendig.

Entscheidende Einschränkungskriterien für die Prüfung des Vorliegens eines personenbezogenen Datums liefert ferner Erwägungsgrund (23). Wir halten eine Differenzierung zwischen Daten „bestimmter oder bestimmbarer“ Personen und anonymisierten Daten für sehr sinnvoll. Allerdings wären hier zusätzliche Erläuterungen zu den Grenzen der Anonymisierung hilfreich. Die Einschränkung in Erwägungsgrund (23), dass Grundsätze des Datenschutzes nicht für anonymisierte Daten gelten, sollte sich explizit aus der Verordnung ergeben. Eine Aufnahme einer Definition für „anonymisierte Daten“ in Art. 4 bietet sich an.

b) „Einwilligung der betroffenen Person“ (Abs. 8)
Hinsichtlich der Definition der Einwilligung ist insbesondere die „explizite“ Willensbekundung problematisch, da dies zur Folge hätte, dass Unternehmen viele einzelne Einwilligungen für jede spezifische Datenverarbeitung einholen müssten und dies für erheblichen Verwaltungs- und Kostenaufwand sorgen würde.

Hier wurde aus Transparenzgründen die Option eines „opt-in“ gewählt. Es stellt sich jedoch die Frage, ob nicht in diesem Zusammenhang auch ein „opt-out“ genügen könnte oder ob eine standardisierte Einwilligung über AGB möglich ist. In jedem Fall ist Praktikabilität zu gewährleisten.

Es stellt sich weiter die Frage, ob nicht auch konkludente Einwilligungen ausreichen. Unseres Erachtens ist Erwägungsgrund (25) dahingehend zu verstehen. Dies sollte unbedingt auch in der Definition von „Einwilligung“ in Art. 4 selbst klargestellt werden.

3. Rechtmäßigkeit der Verarbeitung (Art. 6)

a) Zweckbindung (Art. 6 Abs. 4)
Die strenge Zweckbindung als Grundvoraussetzung für die Datennutzung in Art. 5 b) und Art. 6 Abs. 4 ist insoweit problematisch, als sie zur Folge hätte, dass Daten, die einmal aufgrund eines Vertrages rechtmäßig erlangt wurden, nicht mehr für einen anderen Zweck, z.B. für den Adresshandel oder für Bonitätsprüfungen bzw. unternehmensinterne Sperrvermerke, sowie zielgerichtete Werbeaussteuerung, verwendet werden könnten. Dies hätte erhebliche finanzielle Auswirkungen und auch die Ansprache von Neukunden wäre nicht mehr möglich. Zu bedauern ist in diesem Zusammenhang, dass zwar Ausnahmen möglich sind – z.B. durch Einwilligung (Abs. 1 a) – das berechtigte Interesse des Unternehmens, welches die Daten erhoben hat (Art. 6 Abs. 1 f) jedoch gerade nicht dazu zählt und damit der Abwägungstatbestand des Art. 6 Abs. 1 f) letztlich in seiner Wirkung doch wieder eingeschränkt wird. Es sollte in Betracht gezogen werden, im Hinblick auf den Inhalt der Daten eine Differenzierung vorzunehmen, denn vom Inhalt und Umfang der Daten hängen im Ergebnis die Missbrauchsgefahr und das Risiko für den Betroffenen ab. Daher sollte mindestens nach dem Vorbild des § 28 Abs. 3 BDSG bei listenmäßig zusammengefassten Daten, die sich lediglich auf die Be-

rufs- Branchen- oder Geschäftsbeziehung, den Namen, Titel, akademischen Grad, Anschrift und Geburtsjahr beschränken, eine Ausnahme in Bezug auf die strenge Zweckbindung vorgesehen werden. Die derzeit vorgesehene Regelung ist dagegen nicht sachgerecht und daher abzulehnen. Hier ist ein genereller Verweis auf sämtliche Ausnahmeregelungen in Art. 6 Abs. 1 oder zumindest eine entsprechende Öffnungsklausel für mitgliedstaatliche Regelungen – z.B. durch Ausweitung des Art. 21 – wünschenswert.

Problematisch ist in diesem Zusammenhang auch die Befugnisübertragung an die EU-Kommission in Art. 6 Abs. 5, die die nähere Ausgestaltung der Anwendung des Abwägungstatbestands in delegierten Rechtsakten vorsieht. Derartig wesentliche Inhalte sollten unbedingt im Verordnungstext selbst und im ordentlichen Gesetzgebungsverfahren unter der vollen Beteiligung des EU-Parlaments geregelt werden.

b) Interessensabwägung (Art. 6 Abs. 1 (f))

In Artikel 6 Absatz 1 (f) wird im Vergleich zur Richtlinie 95/46/EG der Verweis auf das berechtigte Interesse Dritter gestrichen. Auch wenn dies auf den ersten Blick nicht ersichtlich ist, wird der Einzelhandel von dieser Änderung massiv beeinträchtigt, da die Änderung der Arbeit von Wirtschaftsauskunfteien die rechtliche Basis entzieht. Auskunfteien versorgen Handelsunternehmen mit Bonitätsauskünften über Kunden, so dass der Händler im Vorfeld eines Geschäfts das Risiko eines Zahlungsausfalls richtig einschätzen kann. Ohne diese Dienstleistung ist ein Verkauf auf Rechnung schlicht undenkbar, sowohl im B2C- als auch im B2B-Bereich und insbesondere im Online-Handel. Bei einer nur eingeschränkten Verfügbarkeit von Bonitätsprüfungen rechnen allein große Versandhändler mit Forderungsausfällen in einer Höhe von bis zu € 10 Mio. pro Jahr. Daher würden sich die Distanzhändler voraussichtlich auf die Bezahlmethoden der Vorkasse, Nachnahme und Kreditkartenzahlung beschränken und den in Deutschland bei den Verbrauchern sehr beliebten Kauf auf Rechnung nicht mehr anbieten. Die Nachteile dieser Entwicklung hätten vor allem die Verbraucher zu tragen, die entweder eine kostenpflichtige Kreditkarte vorhalten müssten und bei Vorkasse und Nachnahme erhöhten Betrugsrisiken unseriöser Anbieter ausgesetzt wären.

Auskunfteien erheben Daten über die Zahlungsmoral von Personen und Unternehmen. Auf Grundlage dieser Daten können sie dann auf Anfrage eines Unternehmens eine auf Tatsachen beruhende Vermutung über die Kreditwürdigkeit eines Unternehmens oder einer Person abgeben. Die Auskunftei erhebt und verarbeitet diese Daten aber nicht aus eigenem Interesse, sondern im Interesse der Unternehmen, die diese Dienstleistung schlussendlich in Anspruch nehmen.

Aus unserer Sicht ist es daher zwingend notwendig, im Art. 6 Absatz 1 (f) wieder auf das berechtigte Interesse dritter Parteien zu verweisen, um erheblichen wirtschaftlichen Schaden abzuwenden. Wir erinnern in dem Zusammenhang daran, dass eine Abwägung mit den „Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person“ stets erforderlich ist und daher angemessen geschützt werden.

c) Tarifverträge / Betriebsvereinbarungen

Die Liste der Erlaubnistatbestände für eine Datenverarbeitung sollte unbedingt dahingehend erweitert werden, dass auch Tarifverträge und Betriebsvereinbarungen eine rechtmäßige Rechtsgrundlage für die Datenverarbeitung darstellen (siehe auch Kommentar zu Art. 7 Abs 4), soweit das in der Verordnung oder in nationalen Rechtsvorschriften festgelegte Schutzniveau nicht unterschritten wird. Beide Instrumente werden im Detail zwischen legitimierten Arbeitgeber- und Arbeitnehmervertretern bzw. Betriebsräten ausgehandelt und sind somit den gesetzlichen Regelungen gleichzusetzen.

4. Einwilligungserfordernis (Art. 7) und Beschäftigtendatenschutz (Art. 82)

a) Beweislast (Art. 7 Abs. 1)

Hinsichtlich des Umfangs der Beweislast im Rahmen der Einwilligung ist aus Einzelhandelssicht dringend eine Klarstellung erforderlich. Muss allein das Vorliegen einer Einwilligung als solches dargelegt werden oder ist darüber hinaus die Identität der betroffenen Person nachzuweisen? Des Weiteren fehlt die notwendige Differenzierung zwischen der Einwilligung im Rahmen einer individuellen Vertragssituation und der anonymen Nutzung des Internets. Kann aus Art. 8 *a contrario* geschlossen werden, dass lediglich geringe Anforderungen an die Einwilligung in Art. 7 zu stellen sind? Eine einseitige Übertragung der Beweislast allein auf die Seite des Datenverarbeiters ist nicht akzeptabel. Dies wird dem Ziel einer ausgewogenen Risikoverteilung nicht gerecht.

b) Widerruf (Art. 7 Abs. 3)

Art. 7 Abs. 3 steht in gewissem Widerspruch zu Art. 17. Während nach Art. 7 Abs. 3 der Widerruf der Einwilligung die Rechtmäßigkeit der Datenverarbeitung nicht berührt, kann der Betroffene gem. Art. 17 Abs. 1 b) dennoch die Löschung und Sperrung der Daten verlangen. Dies ist aus unserer Sicht zu weitgehend, da die bisherige Datenverarbeitung rechtmäßig bleibt. In der Praxis wird ein Unternehmen ohnehin bei einem Widerruf der Einwilligung zunächst alle datenverarbeitenden Aktivitäten einstellen. Es muss jedoch möglich sein, dass die in der Vergangenheit erhobenen Daten nicht pauschal einer Löschungspflicht unterworfen werden. In Art. 7 Abs. 3 S. 1 sollte zur Klarstellung der Zusatz „mit Wirkung für die Zukunft“ nach „jederzeit“ und vor „zu widerrufen“ eingefügt werden.

c) Erhebliches Ungleichgewicht (Art. 7 Abs. 4)

Nach Art. 7 Absatz 4 bietet die Einwilligung der betroffenen Person keine Rechtsgrundlage für die Verarbeitung, wenn „zwischen der Position der betroffenen Person und des für die Verarbeitung Verantwortlichen ein erhebliches Ungleichgewicht besteht“. Diese Einschränkung des Erlaubnistatbestands der Einwilligung ist äußerst problematisch. Es existiert kaum eine Lebenssituation, in der sich die Vertragsparteien vollständig auf Augenhöhe gegenüberstehen. Der Vorbehalt könnte daher im Extremfall bei enger Auslegung durch die Aufsichtsbehörden dazu führen, dass de facto die Einwilligung in die Datenverarbeitung nicht mehr wirksam erfolgen kann. Dies ist auch mit dem Grundsatz der Autonomie in Bezug auf den Umgang mit den eigenen Daten nicht zu vereinbaren und daher sehr problematisch. Weiterhin bringt die Regelung eine erhebliche Rechtsunsicherheit mit sich, da nicht definiert wird, wie „Ungleichgewicht“ zu verstehen ist.

Da dies u.a. auch auf Beschäftigungsverhältnisse zutrifft (s. Erwägungsgrund 34), besteht hinsichtlich Art. 7 Abs. 4 erheblicher Nachbesserungsbedarf. Die Verordnung darf insbesondere keinen pauschalen Ausschluss der Einwilligung im Beschäftigungsverhältnis enthalten. Ansonsten droht eine Situation, in der Arbeitgeber ausschließlich Daten ihrer Arbeitnehmer verarbeiten können, wenn sie hierzu rechtlich verpflichtet sind.

Die Einschränkung der Möglichkeit, in die Verarbeitung eigener Daten einzuwilligen, sollte daher gestrichen oder doch wenigstens auf einzelne, enumerativ aufgezählte und eindeutig missbrauchsanfällige Tatbestände beschränkt werden.

Falls dies politisch nicht gewünscht wird, ist die Frage, ob tatsächlich ein „erhebliches Ungleichgewicht“ vorliegt, im Rahmen einer Einzelfallbetrachtung und –abwägung zu beurteilen. Andernfalls wäre künftig jegliche Erhebung und Verarbeitung von Arbeitnehmerdaten durch das Unternehmen, z.B. im Rahmen einer Impfaktion zum Grippeschutz der Angestellten, bei der Organisation eines Betriebskindergartens, für interne Angestelltenförderprogramme oder ähnlichen Zusatzleistungen, nicht mehr zulässig. Eine derartige Rechtsfolge ist jedoch unausgewogen und praxisfern und damit kaum akzeptabel. Unseres Erachtens sollte vielmehr danach differenziert werden, ob sich das Abhängigkeitsverhältnis auf die konkrete Einwilligung ausgewirkt hat bzw. ob dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich gewesen wäre. Nur in diesen Fällen sollte die Einwilligung keine Rechtsgrundlage für die Datenverarbeitung darstellen können.

d) Beschäftigtendatenschutz (Art. 82)

Zunächst ist anzumerken, dass grundsätzlich eine EU-weite einheitliche Regelung zum Beschäftigtendatenschutz als Teil dieser Verordnung zu begrüßen wäre. Dies gilt allerdings nur für den Fall, dass es gelingt, im Rahmen der Verordnung u.a. eine entsprechende Regelung zur Einwilligung im Beschäftigungsverhältnis durchzusetzen (siehe Ausführungen zu Art. 7 Abs. 4). Außerdem müsste sichergestellt werden, dass auch Kollektivvereinbarungen wie Tarifverträge und Betriebsvereinbarungen als Grundlage für eine Datenvereinbarung dienen können.

Sollte dies im Rahmen des Gesetzgebungsverfahrens nicht realisierbar sein, bedarf es einer Öffnungsklausel für das Arbeitsrecht, die es den nationalen Gesetzgebern ermöglicht, die Gegebenheiten des jeweiligen nationalen Arbeitsrechts ausreichend zu berücksichtigen und rechtliche Konflikte zwischen EU-Datenschutzrecht und nationalem Betriebsverfassungsrecht zu vermeiden. Die in dieser Hinsicht vorgeschlagene Öffnungsklausel des Art. 82 wird dieser Zielsetzung nicht in hinreichendem Maße gerecht. Insbesondere müsste darin die Einschränkung „in den Grenzen dieser Verordnung“ gestrichen bzw. klargestellt werden, dass auf nationaler Ebene bspw. abweichende Regelungen zur Einwilligung im Beschäftigungsverhältnis bzw. zu Kollektivvereinbarungen im Arbeitsrecht zulässig sind. Andernfalls ginge die Öffnungsklausel des Art. 82 ins Leere.

Problematisch ist in diesem Zusammenhang auch, dass gem. Art. 51 Abs. 2 künftig die Datenschutzbehörde des Unternehmenssitzes zuständig sein soll. Da gleichzeitig der Beschäftigtendatenschutz jedoch national geregelt und nicht harmonisiert wird (Art. 82) würde daraus folgen, dass eine nationale Datenschutzbehörde künftig für auch für die Überprüfung der Einhaltung der Arbeitnehmerdaten-

schutzregeln anderer Länder zuständig wäre. Dies dürfte in der praktischen Umsetzung für Kapazitäts- und Kompetenzprobleme sorgen.

5. Recht auf Vergessenwerden (Art. 17)

Aus unserer Sicht ist es wichtig, im Text der Verordnung klarzustellen, dass die Vorschriften in Art. 17 auch erfüllt werden, wenn der für die Verarbeitung Verantwortliche die personenbezogenen Daten anonymisiert oder verdichtet. Dies ist besonders wichtig für werbetreibende Handelsunternehmen. Im Anschluss an eine Werbekampagne, nach der die Speicherfrist, für die eine Einwilligung gegeben wurde, abgelaufen ist, muss es Unternehmen erlaubt sein, Informationen über den Erfolg der Kampagne und den Kundenzuspruch in anonymisierter Form weiter zu verarbeiten. Eine Löschpflicht würde die rechtmäßigen Interessen des Unternehmens übermäßig einschränken, ohne die Privatsphäre der betroffenen Person zu verbessern (anonyme Daten sind nicht personenbezogen).

6. Recht auf Datenportabilität (Art. 18)

Artikel 18 des Entwurfs verpflichtet Unternehmen, Kunden die sie betreffenden personenbezogenen Daten auszuhändigen. Diese Vorschriften sind aus unserer Sicht sehr einseitig auf bestimmte Dienstleistungen, wie z.B. soziale Netzwerke oder *Cloud Computing*, zugeschnitten. Offensichtlich sollen Verbraucher hiermit mehr Kontrolle über solche Daten erlangen, die sie selbst freiwillig im Internet eingestellt haben. Die hier vorgenommene Ausweitung des Auskunftsrechts (Art. 12 der Richtlinie 95/46/EG) geht deutlich über das angestrebte Ziel hinaus. Für Handelsunternehmen hätte die Aufnahme einer solchen Regel zur Datenportabilität in die Verordnung fatale Folgen. Daher sind differenzierte Regelungen notwendig, die den Bedürfnissen anderer Unternehmensmodelle, deren Schwerpunkt nicht auf der Datenverarbeitung liegt, ebenso Rechnung tragen.

In den verschiedenen Einzelhandelsformaten, sowohl im e-Commerce als auch im stationären Handel, werden Informationen über Kunden und deren Kaufverhalten gespeichert. Die rechtliche Grundlage bildet die Einwilligung der Person oder ein Vertrag. Ein geläufiges Beispiel sind Kundenkarten, die Handelsunternehmen zur Kundenbindung und zur besseren Kundenansprache nutzen. Diese vom Unternehmen über einen gewissen Zeitraum erhobenen Daten stellen einen erheblichen Mehrwert für die Unternehmen und damit ein wirtschaftliches Gut dar, da ein Unternehmen hier wichtige Erkenntnisse über die Präferenzen seiner Kunden gewinnen kann. Für den Einkauf des Sortiments, die Vorbereitung von Maßnahmen zur Kundenbindung (z.B. Preisnachlässe) sowie die Planung von Werbekampagnen sind diese Daten unerlässlich.
Die Verpflichtung für Unternehmen, diese Daten preiszugeben, geht aus unserer Sicht zu weit und ist auch nicht mit dem Schutz der Privatsphäre der betroffenen Personen zu rechtfertigen. Vollkommen inakzeptabel ist die Vorgabe, dass Unternehmen diese Daten „in einem gängigen elektronischen Format in ein anderes System […] überführen“ sollen. Abgesehen vom Wertverlust, der dem Unternehmen hieraus entsteht, droht ein beachtlicher Wettbewerbsnachteil, wenn die Daten an einen Wettbewerber weitergegeben werden könnten.

Um wirtschaftlichen Schaden in der oben beschriebenen Form zu vermeiden, sollte Artikel 18 auf diejenigen Dienste beschränkt werden, die Verbrauchern die Ver-

öffentlichung ihrer personenbezogenen Daten ermöglichen. In allen anderen Situationen wird das Recht der betroffenen Person auf Schutz der personenbezogenen Daten bereits durch die Einschränkungen der Rechtmäßigkeit der Verarbeitung (Art. 6), das Auskunftsrecht (Art. 15) und das Widerspruchsrecht (Art. 19) ausreichend gewahrt. Alternativ wäre eine Differenzierung im Hinblick auf die Art der Daten notwendig. So sollten lediglich freiwillig und auf eigene Initiative eingestellte Daten („user generated content“) unter das Recht auf Datenportabilität fallen, nicht jedoch vom Unternehmen systematisch ausgewertete operative Datensätze.

7. Bürokratischer Aufwand

Der Handel begrüßt ausdrücklich die Zielsetzung, den Bürokratieaufwand zu verringern. Obwohl im vorgelegten Verordnungsentwurf im Vergleich zur bestehenden Datenschutzrichtlinie einige Vorschriften gestrichen werden (vor allem die Meldepflicht in Art. 18 der RL 95/46/EG), werden zugleich in anderen Bereichen neue Vorschriften eingeführt, die im Endeffekt sogar zu einer Mehrbelastung der Unternehmen führen können.

Aus unserer Sicht verursachen insbesondere folgende Regelungen einen erhöhten bürokratischen Verwaltungs- und Kostenaufwand für die Unternehmen und sollten aus dem Grund überarbeitet werden:

a) Nachweispflicht (Art. 5 (f))

In Art. 5 f) ist aus Handelssicht die vorgesehene Nachweispflicht für die Einhaltung der Vorschriften der Verordnung problematisch, da sie einen erheblichen Bürokratieaufwand mit sich bringt. Im Gegensatz zur Haftung für die Auftragsverarbeitung oder zum Nachweis, dass die Sorgfaltspflicht ordnungsgemäß erfüllt wurde, erscheint eine pauschale Nachweispflicht nicht sachgerecht. In der vorliegenden Form ist eine Nachweispflicht praktisch kaum umsetzbar, da weder aufgeklärt wird, auf welche Art und Weise der Nachweis erfolgen soll, noch wem gegenüber der für die Verarbeitung Verantwortliche in der Pflicht steht.
Im Text sollten Redundanzen möglichst vermieden werden. Mit den Informationspflichten (Art. 14) und dem Auskunftsrecht (Art. 15) wir bereits durch detaillierte Vorschriften für ein zufriedenstellendes Maß an Transparenz und Rechenschaft gesorgt. Daher sollte die eher abstrakte Nachweispflicht in Artikel 5 (f) gestrichen werden.

b) Entwicklung einer Datenschutzstrategie (Art. 11)

Es bleibt unklar, was unter einer „Datenschutzstrategie“ zu verstehen ist. In Erwägungsgrund 61 ist von „internen Strategien“ die Rede; für Unternehmen stellt sich daher die Frage, ob sie zukünftig ihre interne Strategie „für jedermann leicht zugänglich“ machen müssen? Hier muss unbedingt klargestellt werden, dass keinesfalls IT-Sicherheitsaspekte oder Geschäftsgeheimnisse offengelegt werden müssen. Eine Möglichkeit wäre, zwischen öffentlichen und internen Verfahrensverzeichnissen zu unterscheiden. Eine entsprechende Differenzierung fehlt bislang.

Der Verordnungsvorschlag liefert leider keinen Vorschlag dafür, wie hochkomplexe Vorgänge der Datenverarbeitung in einer „klaren, einfachen und adressatengerechten Sprache“ dargestellt werden sollen. Für Unternehmen ergibt sich hier ganz konkret die Gefahr wettbewerbs- und verbraucherschutzrechtlich abgemahnt zu werden, für den Fall dass sie ihre Datenverarbeitungsvorgänge vereinfacht

(sprich: verbrauchergerecht) darstellen, hierbei aber nicht die gesamte Komplexität abbilden. Nicht hilfreich ist in dem Zusammenhang, dass laut Art. 11 Abs. 2 „alle Informationen und Mitteilungen zur Verarbeitung personenbezogener Daten“ zur Verfügung gestellt werden müssen. Dies widerspricht dem Ziel, die Informationen in klarer und adressatengerechter Sprache zu übermitteln. Hilfreicher wäre eine Auflistung der Elemente, die der betroffenen Person aus Transparenzgründen übermittelt werden sollen.

c) Informationspflicht (Art. 14)

Hinsichtlich der Pflicht zur Angabe der Dauer der Speicherung der personenbezogenen Daten gem. Art. 14 Abs. 1 c) sollte klar geregelt werden, dass dies nicht zwangsläufig durch Angabe eines Datums erfolgen kann. In der Praxis ist bei Beginn der Datenverarbeitung ein Ende der Vertragsbeziehung nicht immer klar definierbar. Bei dieser Regelung ist Flexibilität geboten, da eine weitgehende Beschränkung ungebührend in die internen Organisationsabläufe der Unternehmen eingreift.

Aus Vereinfachungserwägungen wäre eine Änderung des Wortlauts des Abs. 5 a) im Sinne eines Ersatzes von „gemäß den Absätzen 1, 2 oder 3“ durch den Wortlaut „Kenntnis von der Speicherung bzw. Übermittlung der Daten erlangt“ sinnvoll.

d) Auskunftsrecht (Art. 15)

Das in Art. 15 geregelte umfassende pauschale Auskunftsrecht ist aus unserer Sicht um eine Verhältnismäßigkeitsklausel zu ergänzen. Unseres Erachtens müsste eine zeitliche Beschränkung vorgesehen werden, die angibt, in welchen Abständen eine Auskunft eingeholt werden kann (z.B. einmal pro Kalenderjahr), um die Verhältnismäßigkeit zu wahren und Missbräuche zu verhindern.

Bedenklich ist außerdem Art. 15 Abs. 4, wonach die Kommission Standardvorlagen für die Auskunftserteilung festlegen kann. Dies würde nicht unerheblich in die jeweiligen Organisationsstrukturen der Unternehmen eingreifen.

8. Pflichten des für die Verarbeitung Verantwortlichen (Art. 22 ff)

a) Dokumentationspflichten (Art. 22 Abs. 1; Art. 28)

Die vorgesehene generelle Nachweispflicht des Art. 22 Abs. 1 ist zu pauschal und würde für erheblichen Bürokratie- und Kostenaufwand für die Unternehmen sorgen.

Auch die Dokumentationspflichten des Art. 28 sind zu weitgehend. Die nach dem deutschen Bundesdatenschutzgesetz vorgesehenen Dokumentationspflichten sind unseres Erachtens ausreichend (§ 4 g) Abs. 2 iVm. § 4 d) iVm. § 4e BDSG).
Zu Art. 28 Abs. 4 b ist generell anzumerken, das hier nicht auf die bloße Anzahl der Mitarbeiter per se abgestellt werden sollte, sondern vielmehr nur solche Mitarbeiter, die sich mit datenschutzrechtlichen Aspekten beschäftigen.

b) Meldung von Verletzungen des Datenschutzes (Art. 31,32)

Die vorgesehene Meldepflicht bei „Datenpannen“ ist zu pauschal und aus unserer Sicht in der Praxis kaum umsetzbar. Die Meldepflicht sollte auf schwerwiegende

Verstöße innerhalb eines begrenzten Zeitraums beschränkt werden (Vgl. § 42 a BDSG).

Der vorliegende Entwurf ist in zweifacher Hinsicht problematisch. Zum einen fehlt eine Beschränkung der Meldepflicht auf schwerwiegende Verstöße bzw. eine Differenzierung zwischen schweren (bei sensiblen Daten) und bagatellartigen Datenschutzverletzungen. Zum anderen ist die vorgesehene Meldepflicht innerhalb von 24 Stunden zu rigide. Zwar soll anscheinend durch den Wortlaut „nach Möglichkeit“ und Art. 31 Abs. 1 S. 2 eine gewisse Flexibilität geschaffen werden. Dies genügt aus unserer Sicht jedoch nicht, da „nach Möglichkeit“ denkbar ungenau ist und eine Abweichung von der 24 Stunden-Frist mit einer Begründungspflicht einhergeht. Insgesamt würde die vorgeschlagene Regelung bedeuten, dass Unternehmen auch Bagatellfälle innerhalb von 24 Stunden melden müssten, was einen immensen organisatorischen und finanziellen Aufwand darstellen würde. Vorzugswürdig wäre eine Streichung der 24 Stunden-Frist durch einen allgemeinen Begriff wie „in einem angemessenen Zeitraum“.

c) Pflicht zur vorherigen Genehmigung (Art. 34)

Die Verpflichtung gem. Art. 34, für jede Datenverarbeitung die vorherige Genehmigung bzw. den Rat der Aufsichtsbehörde einzuholen, bedarf der Klarstellung. So ist unklar, ob die Genehmigungspflicht gem. Art. 34 Abs. 1 bei allen Datenverarbeitungsvorgängen gilt oder sich lediglich auf die erwähnten Fälle (Vertragsklauseln gem. Art. 42 Abs. 2 d oder Mangel an Garantien gem. Art. 42 Abs. 5) bezieht. Nach unserem Verständnis ist letzteres der Fall, was jedoch bedauernswerter Weise nicht eindeutig aus dem Text hervorgeht. Hier sind zudem Inkonsistenzen der verschiedenen Sprachfassungen (englisch – deutsch) zu bemängeln. Eine zu pauschale Genehmigungspflicht hätte einen erheblichen bürokratischen Mehraufwand zur Folge und würde Datenverarbeitungsvorgänge erheblich verlängern. Dies würde die Wettbewerbsfähigkeit des von schnellen und unkomplizierten Abläufen gekennzeichneten Versand- und Onlinehandels stark einschränken.
Zudem tragen die unbestimmten Rechtsbegriffe in Art. 34 Abs. 2 a) und b) nicht zur Rechtssicherheit bei. So ist beispielsweise unklar, in welchem Fall Verarbeitungsvorgänge „hohe“ konkrete Risiken im Sinne von Abs. 2 a) bergen. Außerdem ist fraglich, ob 27 nationale Listen von Verarbeitungsvorgängen, wie in Art. 34 Abs. 2 b. i.V.m. Abs. 4 vorgesehen, hier Abhilfe schaffen könnten. Eine entsprechende Nachbesserung des Texts, die diesen Sachverhalt eindeutig darstellt, ist aus unserer Sicht dringend erforderlich. Aus unserer Sicht sollte die Meldepflicht gegenüber der Behörde entfallen, sobald ein Datenschutzbeauftragter bestellt wurde (vgl. § 4d) Abs. 2 BDSG).

d) Datenschutzbeauftragter (Art. 35)

Der Selbstregulierungsansatz der Benennung eines Datenschutzbeauftragten gem. Art. 35 wird begrüßt. Dieser ermöglicht, den im deutschen Recht bereits bewährten Datenschutzbeauftragten EU-weit auszudehnen. Grundsätzlich erscheint zweifelhaft, ob anhand der Anzahl der Mitarbeiter die potenziellen Datenschutzrisiken in einem Unternehmen beurteilt werden können. Sollte am Kriterium der Mitarbeiteranzahl festgehalten werden, sehen wir allerdings Verbesserungsbedarf bei der Definition von „Mitarbeiter“ und dem vorgesehenen Schwellenwert. Zum einen sollte klargestellt werden, in wie weit z.B. selbständige Mitarbeiter eines Unternehmens erfasst werden. Zum anderen sollten bei der Anzahl der angesprochenen Mitarbeiter nur solche berücksichtigt werden, deren Tätigkeit tatsächlich im

Bereich der Verarbeitung von Daten liegt. Nur so werden auch tatsächlich diejenigen Unternehmen erfasst, die in nicht nur unerheblichem Umfang Datenverarbeitung betreiben und ein effizienter Einsatz der Funktion eines Datenschutzbeauftragten erreicht.

9. Profiling (Art. 20)

Im Zusammenhang mit Art. 20 sollte ein größeres Maß an Rechtssicherheit hergestellt werden, indem der Begriff „Profiling“ in Artikel 4 definiert wird. Hierdurch könnten Missverständnisse in Bezug auf Profilbildung, die häufig auch als „Profiling“ bezeichnet wird, vorausschauend verhindert werden.

Äußerst problematisch ist aus Sicht des Handels Art. 20 Abs. 1 a.E. Damit wären interne Bonitätsprüfungen und Abschätzungen des Kreditausfallrisikos bei Rechnungs- und Ratenkauf („wirtschaftliche Situation“) künftig unmöglich. Dies hätte zur Folge, dass dem Kunden nur noch sichere Zahlungsmittel angeboten werden könnten. Sollten Bonitätsprüfungen künftig nur noch mit Einwilligung des Kunden möglich sein, rechnen große Versandhändler mit erheblichen monetären Auswirkungen von bis zu 10 Mio. € an Forderungsausfällen im Jahr.

Bedenklich ist aus unserer Sicht die Ermächtigung der Kommission in Art. 20 Abs. 5, im Wege delegierter Rechtsakte weitere Einschränkungen von Art. 20 Abs. 2 vorzunehmen, da hierdurch erhebliche rechtliche Unsicherheit geschaffen wird.

10. Videoüberwachung (Art. 33 Abs. 2 c)

Generell sind aus Sicht des Einzelhandels einseitige Regelungen im Bereich der Videoüberwachung zu vermeiden. So stellt die Videoüberwachung ein wichtiges Mittel dar, um die Sicherheit der Beschäftigten und das Eigentum der Unternehmen zu schützen sowie Straftaten zu verhindern. Dabei geht es ausschließlich um einen Einsatz zur Prävention, nicht um die Erhebung von Mitarbeiterdaten.

Im Hinblick auf die nach Art. 33 Abs. 2c) – unter der Bedingung einer durchgeführten Folgenabschätzung – zulässige Videoüberwachung sind folgende Gesichtspunkte aus unserer Sicht kritisch zu bewerten.
Zunächst bleibt undefiniert, was unter den Begriff der „öffentlich zugänglichen Bereiche“ fällt. Sollen hiervon nur öffentliche Plätze und Gebäude oder auch im Privateigentum stehende und für die Kundschaft geöffnete Geschäfte fallen?
In diesem Fall ist die in Art. 33 Abs. 4 vorgesehene Pflicht zur Konsultation der betroffenen Personen oder ihrer Vertreter vor Einsatz einer Videoüberwachung aus unserer Sicht problematisch. Es bleibt unklar, wer im Einzelfall die „Vertreter“ der betroffenen Personen sind. Im Übrigen wäre eine derartige pauschale Konsultationspflicht mit unverhältnismäßigem Aufwand verbunden, denn dies würde bedeuten, dass bei jeder Videoüberwachung zur Kriminalprävention eine Befragung unter Umständen jedes einzelnen Kunden durchgeführt werden müsste. Dies ist völlig impraktikabel. Die Aufsicht durch die Behörden und den betrieblichen Datenschutzbeauftragten, kombiniert mit der Folgenabschätzung, reicht in diesen Fällen vollständig aus, um die schützenswerten Rechte der betroffenen Personen zu wahren.

In Bezug auf das Arbeitsverhältnis ist eine Konsultation auch deshalb nicht erforderlich, da der Betriebsrat nach nationalen betriebsverfassungsrechtlichen Regelungen einer Videoüberwachung zustimmen muss. Es bleibt zu überlegen, ob es nicht sinnvoll wäre, an dieser Stelle für die arbeitnehmerschutzrechtlichen Konstellationen auf Artikel 82 des Verordnungsentwurfs zu verweisen (s. Anmerkungen oben).

11. Durchsetzung (Artikel 73 ff., v.a. Artikel 76)

Die in Art. 73 ff vorgesehene Möglichkeit der Verbandsklage ist unseres Erachtens überflüssig. Die Datenschutzbehörden sind verpflichtet, Beschwerden von betroffenen Personen anzunehmen und zu untersuchen. Sie verfügen bereits über ausreichend Korrekturmittel, da sie befugt sind, korrigierende Maßnahmen anzuordnen (Art. 53 Abs. 1) und bei Verstößen Klage zu erheben (Art. 53 Abs. 3). Probleme werden somit in der Regel bereits auf der Ebene der Datenschutzbehörde geklärt. Die Einführung eines zweiten, konkurrierenden Korrekturinstruments ist nicht sinnvoll.

Abgesehen davon fehlen Sicherungsmaßnahmen, um Missbrauchsfälle zu vermeiden. In diesem Sinne wäre insbesondere sowohl die Aufnahme einer Bagatellschwelle als auch eine klarere Eingrenzung bzw. Definition der klagebefugten Einrichtungen erforderlich.

12. Sanktionen (Art. 78 ff)

Die an den Jahresumsatz gekoppelten Sanktionen bzw. die vorgesehenen Bußgeldhöhen wären für margenschwache Branchen wie den Handel (in der Regel zwischen 0,5-2%) sowie für Firmen, deren Geschäftsmodell nicht auf der Datenverarbeitung basiert, existenzgefährdend und sind daher nicht akzeptabel.

Problematisch ist weiterhin, dass der Aufsichtsbehörde bei der Verhängung von Sanktionen kaum Ermessensspielraum eingeräumt wird, sondern gem. Art. 79 eine Pflicht der Sanktionsverhängung besteht, sobald einer der aufgeführten Tatbestände vorliegt. Vor diesem Hintergrund empfiehlt sich die Aufnahme einer Bagatellschwelle. Auch ist nicht nachvollziehbar, weshalb eine schriftliche Verwarnung nicht als „Sanktion“ gelten soll.

Alternativ könnte über einen Gewinnabschöpfungsanspruch nachgedacht werden, bei dem der Gewinn an Stelle des Umsatzes als maßgeblicher Wert zur Berechnung der Sanktionshöhe fungieren würde.

Ferner wird auch an dieser Stelle die Befugnisübertragung auf die EU-Kommission im Wege delegierter Rechtsakte zur Aktualisierung der Beträge der Geldbußen sehr kritisch gesehen.

13. Gesellschaftsübergreifende Datenübertragung

Im Zusammenhang mit der in Art. 43 angesprochenen gesellschaftsübergreifenden Datenübertragung in Drittländer und internationale Organisationen plädieren wir dafür, einen sog. „Konzernprivileg“, also eine Regelung, nach der die Datenweitergabe zwischen Tochterunternehmen innerhalb eines Konzerns ohne gesonderte vertragliche Vereinbarungen ermöglicht wird in die Verordnung aufzunehmen.

Die geltende Rechtslage, die eine Weitergabe von Personendaten im Konzern an Tochtergesellschaften wie eine Weitergabe an Dritte behandelt und komplexe Konzernrichtlinien und Auftragsdatenverarbeitungsverträge zwischen Tochtergesellschaften erforderlich macht, ist umständlich und praxisfern. Ein Konzern ist eine wirtschaftlich einheitliche Struktur, in dem – ungeachtet der Eigenständigkeit der Gesellschaften – eine gesellschaftsübergreifende Datenverarbeitung und andere zentral geregelte Sachverhalte unter Effizienzgesichtspunkten möglich und sinnvoll sind. Dies birgt insofern keine Risiken für die betroffene Person, als eine Gesamthaftung der gesellschaftlichen Strukturen weiterhin gegeben wäre.

Berlin / Brüssel, September 2012