DIHK

STELLUNGNAHME

Berlin, 5. April 2012

Deutscher Industrie- und Handelskammertag

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 endg

Registriernummer des DIHK im Register der Europäischen Kommission: 22400601191-42

Der Deutsche Industrie- und Handelskammertag (DIHK) ist die Dachorganisation der 80 Industrie- und Handelskammern (IHKs), die 3,6 Millionen Unternehmen als Mitglied haben. Der DIHK vertritt die Interessen der deutschen Wirtschaft gegenüber der Bundespolitik und den europäischen Institutionen und betreut und koordiniert darüber hinaus das Netzwerk der Deutschen Auslandshandelskammern (AHKs) mit 120 Standorten in 80 Ländern weltweit.

A. Vorbemerkungen

In unserer Stellungnahme zur Strategie zur Überarbeitung der Datenschutzrichtlinie 95/46/EG hatten wir folgende Punkte als wesentlich aus Sicht der Wirtschaft benannt:

- Datenschutz zu einem internationalen Thema machen
- Recht auf Vergessen angemessen regeln
- Einwilligung als zulässige Grundlage für Datenverarbeitung erhalten
- Verbesserung des Datentransfers in Drittländer.

Die nun vorgelegte Verordnung behandelt die genannten Themen nach unserer Auffassung nur in einigen Punkten wirtschaftsnah:

- **Datenschutz zu einem internationalen Thema machen**

Positiv ist der Ansatz der VO, den Datenschutz als ein internationales Thema zu definieren. Unternehmen wie facebook, Google u. a. zeigen, dass Daten global verarbeitet werden. Daher ist auch grundsätzlich der Vorschlag zu begrüßen, für Unternehmen die VO gelten zu lassen, wenn sie keinen Sitz in der EU haben, aber Daten von EU-Bürgern verarbeiten. Hier stellt sich dann allerdings die Frage der Rechtsdurchsetzung bei Verstößen. Wird dann jedoch an eine solche Verarbeitung die Voraussetzung geknüpft, dass dieses Unternehmen einen Vertreter in der EU nachweisen muss, geht dies weit über datenschutzrechtliche Anforderungen hinaus und stellt ein unzulässiges Hemmnis für Dienstleistungen und Handel dar. Denn dann darf ein Nicht-EU-Unternehmen seine Waren und Dienstleistungen per Internet in der EU nicht anbieten, ohne einen Vertreter mit Sitz in der EU zu benennen (Art. 25 Abs. 3).

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

- **Recht auf Vergessen angemessen regeln**

Diesen Punkt unterstützen wir vom Ansatz her. Allerdings darf seine Regelung nicht dazu führen, dass berechtigte Interessen der Unternehmen, aber auch z. B. öffentlicher Einrichtungen, unberücksichtigt bleiben. Es gibt eine Vielzahl von Gründen, warum Daten, die z. B. ein Verbraucher freiwillig der verantwortlichen Stelle übermittelt hat, nicht unter das Recht auf Vergessen fallen können. Hierzu gehören steuerrechtliche, handelsrechtliche und sonstige gesetzliche Vorgaben zu einer längeren Aufbewahrung. So gilt in Deutschland für die Verjährung z. B. von deliktischen Schadensersatzansprüchen eine Frist von 30 Jahren. Auch bei gewerblichen Schutzrechten ist eine sehr langfristige Aufbewahrung von Daten, die durchaus Personenbezug haben können, notwendig. Gerade das Steuerrecht verlangt eine manipulations- und revisionssichere Aufbewahrung und Archivierung, so dass die Datensätze oder Teile von ihnen auch nicht anonymisiert werden dürfen. Es wäre also falsch, den Bürgern/Verbrauchern zu suggerieren, dass ihre Daten auf Anforderung komplett gelöscht würden. Für die Unternehmen ergäben sich daraus zusätzliche Informationspflichten, um die Verbraucher über die unterschiedliche Behandlung ihrer Daten aufzuklären.

- **Einwilligung als zulässige Grundlage für Datenverarbeitung erhalten**

Die Einwilligung ist neben Rechtsvorschriften die einzige Rechtfertigung für Datenverarbeitung. Sie ist Ausfluss des Selbstbestimmungsrechts des Einzelnen. Eine Einschränkung bedeutet damit grundsätzlich immer eine Entmündigung des Betroffenen.

- **Verbesserung des Datentransfers in Drittländer**

Die Überlegung eines One-Stop-Shops für die Zulässigkeitsprüfung z. B. von binding corporate rules halten wir für sehr sinnvoll. Es entspricht der Forderung insbesondere derjenigen Unternehmen, die in mehreren EU-Mitgliedstaaten tätig sind. Damit werden unterschiedliche rechtliche Einschätzungen der jeweiligen Aufsichtsbehörden vermieden und eine stärkere Einheitlichkeit in der Rechtsauffassung erzielt. Für die Unternehmen ergibt sich daraus eine höhere Rechtssicherheit. Es sollte geprüft werden, ob das Prinzip des One-Stop-Shops nicht nur für Niederlassungen sondern auch für Tochtergesellschaften gelten sollte. Vielfach wird die Organisationsform der Niederlassung oder der Tochtergesellschaft durch steuer- oder aufsichtsrechtliche Rahmenbedingungen in dem betreffenden Land bestimmt, was sich bei der datenschutzrechtlichen Betrachtung nicht auswirken sollte.

Allerdings gibt es darüber hinaus noch Unternehmensorganisationsformen, die von dieser Erleichterung nicht profitieren. Hierzu zählen insbesondere Konzerne bzw. verbundene Unternehmen. Weltweit tätige Unternehmensverbünde, verteilte Vertriebssysteme und Konzerne haben häufig ihre Datenverarbeitung bei einem verbundenen Unternehmen/einer Konzerntochter konzentriert. Sie können jetzt zwar von den binding corporate rules insofern profitieren, als damit ein einheitliches Konzerndatenschutzniveau hergestellt werden kann. Allein für die Datenübermittlung bieten sie keine Rechtsgrundlage.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

- **Wahl des Rechtsinstruments**

Ein Aspekt ist auch die – richtige – Analyse, dass der Datenschutz in der EU sehr unterschiedlich umgesetzt und angewendet wird und sich daraus für grenzüberschreitend tätige Untenehmen erhebliche Schwierigkeiten ergeben. Die Umsetzung der EU-Regeln zum Datenschutz in einer Verordnung halten wir nicht für zwingend; eine Richtlinie mit der Anwendung entsprechender Sanktionen (Vertragsverletzungsverfahren) wäre ebenfalls eine Option gewesen. Denn eine Verordnung ist keine Garantie dafür, dass in den einzelnen Mitgliedstaaten der Datenschutz entsprechend einheitlich umgesetzt wird. Das Ziel, den Datenschutz in Europa mit der VO auf ein einheitliches Niveau zu bringen, ist recht ehrgeizig.

Gegen eine Verordnung sprechen bereits formale Gründe:
Es fehlt an einer tragfähigen Begründung, warum statt einer Richtlinie eine Verordnung vorgesehen wird. Da eine VO nicht der Rechtsakt mit der geringsten Eingriffstiefe in mitgliedstaatliche Autonomien ist, verstößt eine VO solange gegen das Subsidiaritätsprinzip, als anders die Angleichung der mitgliedstaatlichen Rechtsvorschriften nicht erreicht werden kann, dafür fehlt aber jeder Anhaltspunkt.

Eine EU-VO verhindert zwar sog. gold plating, also die Normierung noch höherer Anforderungen z. B. an die Unternehmen. Allerdings verhindert sie auch eine kohärente Anpassung an das nationale Recht, vorliegend u. a. im Bereich der strafrechtlichen Konsequenzen, die nicht in die Kompetenz der EU fallen. Nach dem Urteil des EuGH vom 24.11.2011 (Rechtssachen C-468/10 und C-469/10) ist es zudem ohnehin den EU-Mitgliedstaaten verwehrt, über das Maß der Regelung in der Datenschutzrichtlinie 95/46/EG hinauszugehen. Auch dies ist ein weiteres Argument für Regelungen im Rahmen einer Richtlinie.

Dennoch ist zuzugeben, dass insbesondere größere Unternehmen, die grenzüberschreitend in Europa tätig sind, sich von einer Verordnung mehr Rechtssicherheit und -klarheit versprechen. Die nunmehr eindeutig geregelten Zuständigkeiten der Aufsichtsbehörden für solche grenzüberschreitenden Datenverarbeitungen kommen diesen Unternehmen entgegen.

- **allgemeine Anmerkungen**

Grundsätzlich ist es notwendig und zu begrüßen, wenn bestehende Regelungen an die aktuelle technische Entwicklung und wirtschaftliche Globalisierung angepasst werden, der internationale Datentransfer erleichtert, die Anwendbarkeit des EU-Rechts auf grenzüberschreitende Sachverhalte klargestellt und ein europäischer Mindeststandard festgelegt wird. Dies muss jedoch mit Maß und Ziel geschehen und darf die Unternehmen nicht mit noch mehr Informationspflichten, Bürokratie und Mehrkosten belasten. Die Verordnung bringt eine Regelungstiefe mit sich, die mit 91 Artikeln notgedrungen sehr weit in Einzelheiten geht. Hinzu kommen die umfangreichen Ermächtigungsnormen für delegierte Rechtsakte bzw. Standardvorlagen, -verfahren oder Formulare, die sich die EU-Kommission vorbehält. Damit verhindert die EU eine Anpassung an mitgliedstaatliche Gegebenheiten und Traditionen, die es im Datenschutz gibt.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Schließlich müssen das Informationsgrundrecht (Art. 11 Grundrechtecharta) und das Recht auf unternehmerische Freiheit (Art. 16 Grundrechtecharta) berücksichtigt werden. Dies ist nach unserer Auffassung nicht durchgängig der Fall. Das Recht auf informationelle Selbstbestimmung sollte in der EU wie bereits in Deutschland anerkannt werden.

Positiv ist, dass die Verordnung technikneutral formuliert ist. So können auch weitere Entwicklungen z. B. im Internet aufgefangen werden, ohne dass die Rechtsgrundlage einem ständigen Änderungsbedarf unterliegt.

In dem Vorschlag der VO fehlen materielle Regelungen zu Berufsgeheimnisträgern und deren Datenverarbeitung. Dies gilt auch für Datenverarbeiter, die sonstige berufliche Geheimhaltungspflichten treffen wie z. B. Berater und Betreuer im Gesundheits- und sozialen Bereich. Hier bedarf es dann auch Regelungen zur Zulässigkeit der Auftragsdatenverarbeitung, ohne dass sofort strafrechtliche Verstöße wie in Deutschland nach §§ 203 ff. StGB greifen dürfen. Bisher kann eine Auftragsdatenverarbeitung nur mit Einwilligung des Betroffenen erfolgen. Im Rahmen z. B. von e-health werden aber zukünftig andere Rechtfertigungsgründe greifen müssen, weil in vielen Fällen der Betroffene nicht (mehr) einwilligen kann.

Die VO sieht eine umfassende Ausweitung der Aufgaben und Zuständigkeiten der Aufsichtsbehörden vor. Diese sind nicht einmal in Deutschland ausreichend personell und sächlich dafür ausgestattet. Da die EU-Mitgliedstaaten in der momentanen finanziellen Situation kaum Möglichkeiten haben werden, diese notwendige Ausstattung zu finanzieren, besteht die Gefahr, dass die Aufsichtsbehörden sich über Gebühreneinnahmen selbst finanzieren müssen. Dies würde eine erhebliche Belastung für die Unternehmen mit sich bringen.

B. Zu den einzelnen Vorschriften

Art. 3

Abs. 2

Die Ausweitung des Anwendungsbereichs der VO auf Verarbeitung von Daten aus der EU, die aber nicht in der EU stattfinden, halten wir für sinnvoll. Dadurch wird eine unterschiedliche Wettbewerbssituation der Unternehmen vermieden.

Abs. 3

Aus der Formulierung ist nicht erkennbar, inwieweit europäisches Recht für verantwortliche Stellen in Drittstaaten gilt, die personenbezogene Daten ohne Bezug zu EU-Bürgern durch Dienstleister in Europa, z. B. IT-Hosting für Tochtergesellschaften aus Drittstaaten, verarbeiten lassen. Nach aktueller Rechtslage in Deutschland unterliegen sie bei einer Auftragsdatenverarbeitung in Deutschland nur den Anforderungen des ordre public, nicht aber den einzelnen Zulässigkeitstatbeständen und formellen Anforderungen des BDSG.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Art. 4

Abs. 1

Die Definition der betroffenen Person erweitert den Anwendungsbereich des Datenschutzes erheblich. Insbesondere die sehr weitgehende Formulierung „nach allgemeinem Ermessen aller Voraussicht nach“ gibt der verantwortlichen Stelle keine ausreichenden Prüfkriterien an die Hand, wann datenschutzrechtliche Normen zu beachten sind.

Abs. 3

Der Begriff „mit oder ohne Hilfe automatisierter Verfahren“ erklärt sich nicht aus sich selbst heraus. Bedeutet dies, in Verbindung mit Abs. 4, dass die Verordnung auch gilt, wenn es sich um jede strukturierte Verarbeitung von Daten handelt, die sowohl mit als auch ohne Hilfe automatisierter Verfahren ausgeführt wird?

Abs. 6

Zunehmend stellen sich Fragen bei dem Begriff der Auftragsdatenverarbeitung. Stellt jede „Übergabe“ von Daten an einen anderen eine Auftragsdatenverarbeitung dar? Vor dem Hintergrund zunehmenden Fremdhostings und auch der Diskussion um cloud computing sollte hier geprüft werden, ob in jedem Falle die umfassenden Regelungen zur Auftragsdatenverarbeitung greifen sollen. Häufig geht es nur um eine temporäre „Aufbewahrung“ der Daten, ohne dass damit tatsächlich eine Verarbeitung der Daten verbunden ist.

Abs. 8

Die Anforderung an eine Einwilligung wird durch den Begriff „explizit“ erhöht. Gleichzeitig reicht aber auch eine konkludende Handlung aus, was zu unterstützen ist. Es ist nicht erkennbar, warum dann aber an die Einwilligung höhere Anforderungen gestellt werden. Es muss weiterhin möglich sein, im Rahmen von AGB die Einwilligung einzuholen.

Art. 6

Es fehlt an einer Privilegierung von Daten aus öffentlichen Quellen und Verzeichnissen. Zwar handelt es sich dabei auch um personenbezogene Daten. Sie müssen jedoch dem umfangreichen Schutz, den die Verordnung gewährt, nicht unterliegen.

Art.7

Hier verweisen wir zunächst auf die Vorbemerkungen.
Die Einwilligung ist ein wichtiges Instrument, das in vielen Fällen eine sinnvolle Basis für eine Datenverwendung darstellt. Die Einholung der Einwilligung ist sehr aufwändig und kaum flächendeckend einsetzbar. Der Einwilligungsgrundsatz erscheint daher ungeeignet, als vorrangige Legitimation aller Datenverarbeitungsvorgänge zu dienen. Regelungen zur Einwilligung sollten klar formuliert sein und nicht zu hohe Anforderungen enthalten. Weiterhin muss das Recht der informationellen Selbstbestimmung im Vordergrund stehen. Der teilweise Ausschluss der Möglichkeit von Einwilligungen ist nicht akzeptabel.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Abs. 2
Der Begriff der Trennung ist nicht eindeutig. Reicht hier eine drucktechnische Hervorhebung aus oder bedarf es tatsächlich z. B. einer zweiten Klärung? Sollte letzteres der Fall sein, geben wir zu bedenken, dass auch häufig aus wettbewerbsrechtlichen Gründen eine Einwilligung eingeholt werden muss, die in wesentlichen Teilen deckungsgleich mit der für den Datenschutz ist. Der Verbraucher versteht es nicht, wenn er zwei Mal in die gleiche Fragestellung einwilligen muss.

Geregelt ist die schriftliche Einwilligung, nicht jedoch die elektronische, die mittlerweile weit mehr Bedeutung hat. Für sie gilt grundsätzlich dasselbe: Eine zweite Erklärung neben z. B. einer wettbewerbsrechtlichen bedeutet für den Verbraucher nicht mehr Datenschutz sondern eher Verwirrung.

Abs. 4
Das „erhebliche Ungleichgewicht“ ist ein sehr schillernder Begriff. Diese grundsätzliche Regelung beträfe wohl viele wirtschaftsrelevante Bereiche.

Das Vorliegen eines erheblichen Ungleichgewichts kann nicht von Einzelfallkonstellationen abhängen und damit zulasten der verantwortlichen Stelle gehen. Insbesondere vor dem Hintergrund der höchsten Geldbuße bis zu einer Mio. Euro oder drei Prozent des weltweiten Jahresumsatzes eines Unternehmens ist eine solche Unsicherheit nicht zu vertreten.

Auch im Arbeitsverhältnis mag ein Ungleichgewicht dort vorhanden sein, wo hohe Arbeitslosigkeit herrscht, nicht aber dort, wo Angebot von Arbeitskräften und die Nachfrage sich die Waage halten.
Es fehlt nun an einer klaren Regelung, ob für das Arbeitsverhältnis ein (strukturelles) Ungleichgewicht angenommen wird. Dies wird den einzelnen Mitgliedstaaten überlassen, so dass in diesem für die Wirtschaft wichtigen Bereich eine Rechtszersplitterung möglich ist, die aber nicht sinnvoll ist. Zudem lässt hier Erwägungsgrund 34 vermuten, dass die EU-Mitgliedstaaten gar keine echte Möglichkeit der Rechtsetzung haben.

Insgesamt fördert die Norm eher die Rechtsunsicherheit. Zudem würde gerade die Ausnahme für das Beschäftigungsverhältnis zu einer Rechtszersplitterung in der EU führen, so dass das Ziel der Verordnung auf dem wichtigen Gebiet der Arbeitsverhältnisse nicht umgesetzt würde. Wir schlagen daher vor, diesen Absatz zu streichen.

Sollte mit dem erheblichen Ungleichgewicht eher ein Kopplungsverbot gemeint sein, also die Vermischung verschiedener Zwecke der Datenverarbeitung, schlagen wir vor, die Regelung zum Kopplungsverbot aus dem deutschen Bundesdatenschutzgesetz, § 28 Abs. 3b, zu übernehmen (http://www.gesetze-im-internet.de/bdsg_1990/index.html).

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Art. 12 ff.
Eine Ausweitung von Benachrichtigungs- und Informationspflichten ist abzulehnen. Den Betroffenen ist mit einer Flut an Informationen und Benachrichtigungen nicht gedient. Die Inhalte werden ab einer gewissen Menge überhaupt nicht mehr wahrgenommen. Zu viel Information führt faktisch zu Desinformation.

Kreditinstituten, die aufgrund der häufig vielfältigen Geschäftsbeziehungen sowie der rechtlichen Vorgaben eine Vielzahl an verschiedenen Daten ihrer Kunden zu speichern haben, wird eine Umsetzung einer all diese Daten umfassenden „einfachen" Listenart unmöglich. Bereits jetzt ist die Beantwortung entsprechender Anfragen mit erheblichem Aufwand verbunden.

Art. 14 ff.
Bei der Geschäftsabwicklung, insbesondere im Onlinehandel, bei dem sich die Vertragspartner nicht kennen und nicht persönlich gegenübertreten, haben verlässliche Informationen über den potenziellen Vertragspartner einen hohen Stellenwert. Die Beteiligten müssen in der Lage sein, die Seriosität und Bonität der anderen Seite beurteilen zu können. Die vorgesehenen Regelungen schränken diese Möglichkeiten zu stark ein. Dies würde zu einer Gefährdung der Unternehmen, insbesondere der Internetwirtschaft, führen.

Art. 17
Hier verweisen wir zunächst auf die Vorbemerkungen.

Abs. 1
Eine Differenzierung des Rechts auf Vergessen findet nicht statt. So mag im Bereich von Social Media eine solche Regelung zutreffen, auch wenn neben europäischen dringend international einheitliche Standards geschaffen werden müssten. Die Verpflichtung allerdings auf alle sonstigen Bereiche der Wirtschaft auszudehnen, geht zu weit. Dadurch wären dann auch gängige Werbeinstrumente betroffen wie z. B. die Eintragung in Gästebücher und die Bewertungen von Produkten und Dienstleistungen im Internet.

Abs. 2
Es erscheint sehr fraglich, ob die ursprünglich verantwortliche Stelle überhaupt die rechtliche und auch technische Möglichkeit hat, nachzuvollziehen, wohin die Daten der betroffenen Personen übermittelt wurden. Insofern sehen wir hierin eine Überforderung der verantwortlichen Stelle. Ihr kann nur die Verantwortung für die Löschung der Daten auferlegt werden, die noch in ihrer Verfügungsgewalt und in ihrem Zugriff liegen.

Art. 18
Diese Vorschrift zielt wesentlich auf soziale Netzwerke ab. Dabei wird aber übersehen, dass „traditionelle" Unternehmen große Schwierigkeiten mit einer solchen Regelung hätten.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Das Recht auf Datenportabilität ermöglicht den Betroffenen, vom Daten verarbeitenden Unternehmen eine elektronische und strukturierte Kopie seiner Daten anzufordern. Diese Kopie haben die Unternehmen dem Betroffenen in einem gängigen und weiterverarbeitbaren Format anzubieten. Diese Pflicht ist mit einem erheblichen Aufwand für die Unternehmen verbunden, weil die verantwortliche Stelle z. B. den Anfragenden zuerst authentifizieren muss. Die Daten müssen auch sicher übertragen werden, wozu Hinweise fehlen.

Hinzu kommt, dass häufig die Daten zu einem Betroffenen in dem Unternehmen an sehr verschiednen Stellen verarbeitet werden. Diese müssten zuerst zusammengefasst werden, was zu neuen Datensammlungen führt und für die Unternehmen einen hohen Aufwand bedeutet. Die Übermittlung der Daten kann zudem zur Offenbarung von Geschäfts- und Betriebsgeheimnissen führen, denn es geht um die Weitergabe von Daten an direkte Konkurrenten. Darüber hinaus können von der Übermittlung auch Rechte Dritter betroffen sein, z. B. Daten der Beschäftigten, die die Daten bearbeitet haben, oder Berater z. B. im Rahmen der Inanspruchnahme von sozialen Diensten.

Es erscheint sehr fraglich, ob diese Regelung uneingeschränkt positiv für die Verbraucher ist. Denn es kann durchaus im Interesse des Verbrauchers liegen, dass nicht alle Daten von einem Dienstleister zum anderen transportiert werden. Hier ist z. B. an Krankendaten oder soziale Beratungsleistungen zu denken.

Ungeklärt ist für uns, wie der öffentliche Bereich mit dieser Regelung umgehen soll. Soll bei einem Umzug die Möglichkeit bestehen, sämtliche Daten zu der neu zuständigen Verwaltung transportieren zu lassen?

Generell ist nicht erkennbar, was der Begriff des Überführens bedeuten soll. Denn er ist nicht unter Art. 4 Abs. 3 als Schritt der Verarbeitung definiert. Notwendig ist aber, dass die überführende Stelle weiterhin bestimmte Daten behalten muss, weil es hierfür eventuell gesetzliche Vorgaben gibt.

Art. 22

Die Formulierung eines Datenschutzkonzepts halten wir für eine sinnvolle Maßnahme, um die rechtlichen, technischen und organisatorischen Maßnahmen, die bei der verantwortlichen Stelle ergriffen wurden, zu dokumentieren. Die Unternehmen müssen ohnehin bereits ein Verfahrensverzeichnis, ihre technisch-organisatorischen Maßnahmen und ihre Datenschutzziele formulieren, so dass ein Datenschutzkonzept im Wesentlichen vorhanden ist. Dies gilt insbesondere für IT-Dienstleister, die als Auftragsdatenverarbeiter tätig sind, und von denen im Rahmen einer Beauftragung ein solcher Nachweis verlangt wird.

Zur Entlastung von KMU ist es notwendig, nicht erst auf delegierte Rechtsakte nach Abs. 4 zu warten, sondern bereits in der Rechtsgrundlage eine Ausnahmeregelung für Kleinstunternehmen vorzusehen, z. B. anhand einer Beschäftigten- bzw. Personengrenze von z. B. 10 Personen.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Art. 23
Datenschutz durch Technik und entsprechende Voreinstellungen unterstützen wir. Wir sind davon überzeugt, dass sich aufgrund dieser Vorschriften neue Produkte entwickeln werden, die diesen Anforderungen entsprechen.

Art. 28 Abs. 4b
Für uns ist nicht erkennbar, um welche Unternehmen es sich hier handeln soll. Sollten dies Unternehmen sein, bei denen die Datenverarbeitung nur Mittel zum Zweck ist, bedeutete dies, dass alle anderen Unternehmen keinerlei Dokumentation über die Datenverarbeitung in ihren Unternehmen vornehmen müssen. Dann ist aber ein Widerspruch zu Art. 22 vorhanden, der eine solche Ausnahme von Unternehmen nicht vorsieht. Das würde bedeuten, dass ein Datenschutzkonzept von allen Unternehmen erstellt werden muss. Nur die Unternehmen, die weniger als 250 Beschäftigte haben, benötigen keine Dokumentation und müssen keinen Datenschutzbeauftragten benennen. Entscheidend ist nicht die Anzahl der Beschäftigten, sondern die Intensität der Datenverarbeitung und die Sensibilität der Daten, die verarbeitet werden. Somit sollte die Unterscheidung z. B. an Branchen (Datenverarbeitung zur geschäftsmäßigen Übermittlung an Dritte sowie Markt- und Meinungsforschungseinrichtungen) und an bestimmte Datenverarbeitungen z. B. besonders sensibler Daten geknüpft werden.

Wenn in Unternehmen aber kein entsprechendes Verfahrenverzeichnis nach Art. 28 vorhanden ist, ist nicht erkennbar, wie die Pflichten nach Art. 22 erfüllt werden können und sollen.

Art. 30

Abs. 3
Die Festlegung der technischen und organisatorischen Maßnahmen steht völlig im Belieben der EU-Kommission. Die Maßnahmen müssen aber sofort nach Inkrafttreten der VO von den Unternehmen ergriffen werden (siehe Datenschutzkonzept). Zudem sind sie von erheblicher Bedeutung für die Unternehmen, so dass über ihren Inhalt im Rahmen der Verordnung auch das Europäische Parlament entscheiden sollte.

Inhaltlich verweisen wir auf die Anlage zu § 9 BDSG, deren Maßnahmen sich in der Praxis bewährt haben.

Art. 31
Die Meldung von Verletzungen des Schutzes personenbezogener Daten geht hier eindeutig zu weit. Betroffen ist jede Verletzung, ohne Unterschied des Schweregrades. Somit kommt auch eine fahrlässige Verletzung in Frage, die die gesamten Benachrichtigungspflichten auslöst, wie z. B. eine fehlgeleitete E-Mail. Eine solche Konsequenz ist unverhältnismäßig. Sinnvoll ist mindestens eine Beschränkung auf schwerwiegende Beeinträchtigungen, wie es das BDSG in § 42a vorsieht.

Die Reihenfolge der zu Benachrichtigenden ist nicht sachgerecht: Zuerst muss der Betroffene informiert werden, danach die Aufsichtsbehörde.

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

Die Frist von 24 Stunden ist zu kurz bemessen, denn häufig muss die verantwortliche Stelle selbst erst einmal Untersuchungen durchführen, um die Verletzung lokalisieren zu können. Die Aufsichtsbehörden wären im Übrigen personell völlig überfordert, sollten sie diese Meldungen entgegennehmen und gar noch überprüfen. Sie hat zu einem solch frühen Zeitpunkt überhaupt noch keine Handlungsmöglichkeiten, weil im Zweifel der Sachverhalt nicht einmal aufgeklärt ist.

Die für einen Verstoß vorgesehenen Sanktionen sind ebenfalls – wegen der Undifferenziertheit des Verstoßes – völlig unangemessen und unverhältnismäßig (Art. 79 Abs. 6s).

Art. 32 Abs. 3
In dem letzten Satz wird eine Verschlüsselung gefordert. Diese technische Lösung stellt eine Überforderung der Software dar, weil sie – zumindest momentan – objektiv nicht geleistet werden kann.

Art. 33
Die Folgenabschätzung ersetzt die vormalige Vorabkontrolle.

Abs. 2
Die Regelung differenziert nicht nach dem Sinn und Zweck der Verarbeitungsvorgänge. So müssen z. B. Anwälte oder auch Detekteien Daten sammeln und aufbereiten, um bestimmte Sachverhalte zu beurteilen bzw. ihren Auftraggebern zur Bewertung vorzulegen. Für diese – bislang zulässigen – Datenverarbeitungen fehlt es an Ausnahmeregelungen.

Abs. 4
Daraus folgt auch, dass diese Regelung zur Offenbarung der Informationen gegenüber dem Betroffenen ebenfalls fehlgeht, weil keine Ausnahmetatbestände vorhanden sind.
Zudem stößt sie z. B. da an Grenzen, wo eine weiträumige Überwachung öffentlich zugänglicher Bereiche nach Abs. 2c stattfindet, bei der die Pflicht nach Abs. 4 zur Einholung der Meinung der betroffenen Personen faktisch nicht möglich ist.

Art. 34
Die Formulierung legt nahe, dass bei jeder Verarbeitung die Aufsichtsbehörde um eine Genehmigung zu ersuchen bzw. zu Rate zu ziehen ist. Dies widerspricht jeglicher praktischer Handhabung. Vor allem sind damit die Aufsichtsbehörden völlig überfordert, sowohl technisch als auch personell. Daher schlagen wir vor, die Einschaltung der Aufsichtsbehörde auf Fälle des besonderen Risikos zu beschränken (vgl. § 4d Abs. 5 BDSG). Ferner sollten Unternehmen von diesen Pflichten entbunden werden, wenn sie einen betrieblichen Datenschutzbeauftragten bestellt haben.

Art. 35

Abs. 1b
Die Grenze von 250 Beschäftigten basiert wohl auf der Definition der EU von KMU. Dennoch erschließt sie sich nicht. Sie hätte zur Konsequenz, dass ein Produktionsunternehmen mit 1.000 Beschäftigten, von denen 950 in der Produktion tätig sind und keine personenbezoge-

nen Daten verarbeiten, trotzdem unter das Gesetz fällt, während ein Unternehmen, das 240 Beschäftigte hat und nur personenbezogene Daten verarbeitet, nicht darunter fällt. Eine solche Konsequenz ist nicht logisch. Da es um den Schutz personenbezogener Daten geht, kann es nur um die Intensität der Datenverarbeitung durch ein Unternehmen gehen. Insofern kann als Abgrenzungskriterium nur eine Definition einer Grenze in Frage kommen, die die Verarbeitung personenbezogener Daten zum Gegenstand hat.

Eine so hohe Beschäftigtengrenze, die z. B. in Deutschland dazu führen würde, dass nur 0,3 % der Unternehmen einen Datenschutzbeauftragten bestellen müssten, vermittelt den anderen Unternehmen den – falschen – Eindruck, dass sie datenschutzrechtliche Regelungen nicht beachten müssen.

Wir schlagen daher vor, dass hier nur eine allgemeine Regelung aufgenommen wird, die besagt, dass der Datenschutz sicherzustellen ist. Die EU-Mitgliedstaaten sollten dann ermächtigt werden, dies mit eigenen Regelungen unter folgenden Vorgaben auszufüllen:

- Es sollte eine Grenze von 50 Personen vorgesehen werden für Unternehmen, in denen personenbezogene Daten automatisiert verarbeitet werden.
- Unter der Grenze von 50 Personen sollen alle Unternehmen einen betrieblichen Datenschutzbeauftragten bestellen, die der Datenschutzfolgenabschätzung unterliegen oder personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Meinungsforschung automatisiert verarbeiten (vgl. § 4f BDSG).

Abs. 7

Das Vorsehen einer Frist für die Benennung eines Datenschutzbeauftragten halten wir für schädlich, weil gerade nach zwei Jahren erst das ausreichende Know how vorhanden ist. Die Vorschrift soll wohl so verstanden werden, dass die Mindestdauer einen Schutz für den betrieblichen Datenschutzbeauftragten darstellen soll. Dann müsste aber anders formuliert werden: “Der für die Verarbeitung Verantwortliche oder der Auftragsdatenverarbeiter benennt einen Datenschutzbeauftragten. Die Mindestfrist für die Benennung beträgt zwei Jahre.“

Abs. 9

Die verantwortliche Stelle ist verpflichtet, der Aufsichtsbehörde den Namen des Datenschutzbeauftragten mitzuteilen. Ob diese Mitteilung tatsächlich notwendig ist, erscheint fraglich, da die Aufsichtsbehörde ohnehin eine jederzeitige Überprüfung von Unternehmen durchführen kann. Zumindest ist die Namensnennung gegenüber der Öffentlichkeit überflüssig, zumal in größeren Unternehmen häufig mit einer Sammelmail gearbeitet wird wie Unternehmensname.Datenschutzbeauftragter/Datenschutz@.... Dies halten wir für völlig ausreichend. Der betriebliche Datenschutzbeauftragte muss nicht in der Öffentlichkeit so exponiert herausgestellt werden, denn verantwortlich für den Datenschutz ist weiterhin die Unternehmensleitung.

Art. 38
Der Begriff „Verhaltensregeln“ erschließt sich aus der Vorschrift nicht umfassend. Grundsätzlich schätzen wir aber eine solche Möglichkeit branchenspezifischer Kodizes positiv ein. Sie sind Ausfluss der Selbstverantwortung der Wirtschaft für den Datenschutz.

Abs. 4, 5
Wir schlagen vor, dass die EU-Kommission die allgemeine Gültigkeit nur zuerkennen darf, wenn sie überprüft hat, ob grundsätzlich alle Branchenzugehörigen die dort formulierten Anforderungen erfüllen können. Damit soll verhindert werden, dass in den Kodizes Kriterien festgelegt werden, die sich Binnenmarkt hemmend auswirken können und KMU überfordern.

Art. 39
Über die Sinnhaftigkeit von Zertifizierungen, Gütesiegeln und -zeichen lässt sich trefflich streiten. Sollten sie jedoch eingeführt werden, ist es dringend erforderlich, einheitliche Standards für Siegel und Zertifikate festzulegen. Nur dann können sich Unternehmen, die z. B. entsprechend qualifizierte Auftragsdatenverarbeiter suchen, auf den Inhalt solcher Labels und Gütesiegel verlassen.

Art. 41
Das Verfahren der Feststellung eines angemessenen Datenschutzniveaus durch die EU-Kommission mag sinnvoll sein. Die Erfahrungen mit der Richtlinie 95/46/EG haben jedoch gezeigt, dass es ein langwieriges Verfahren ist, dessen Ergebnis nach 17 Jahren Gültigkeit nicht überzeugt. Daher ist nicht erkennbar, inwiefern eine Negativliste nach Art. 41 Abs. 6 Unternehmen behilflich ist.

Art. 42, 43
Hier verweisen wir zunächst auf die Vorbemerkungen.

Die Regelung zu den binding corporate rules und den Standardvertragsklauseln lassen einen erheblichen bürokratischen Aufwand im Rahmen des Kohärenzverfahrens befürchten. Insbesondere die zeitliche Abfolge von Stellungnahmen der zu beteiligenden Stellen wird zu einem langwierigen Verfahren führen, das keine Erleichterungen für das betroffene Unternehmen im Vergleich zum jetzigen Rechtsstand bringt. Zu befürchten ist, dass die Dauer des Koheränzverfahrens direkte Auswirkungen auf operative Vorgänge in den Unternehmen hat und diese aufgrund der möglichen Langwierigkeit zu erheblichen Störungen führen kann.

Ob die Regelung der Haftung bei der Verwendung von binding corporate rules dazu beiträgt, dieses Instrument intensiver zu nutzen, ist zweifelhaft.

Art. 42
Die Regelung sieht vor, dass angefragte Unternehmen ohne Wissen und Zustimmung der zuständigen Datenschutzaufsichtsbehörde auf Anfrage Justiz und Strafverfolgungsbehörden in Drittstaaten keine europäischen Daten übermitteln dürfen. Für global agierende Unternehmen ist hier eindeutig der Konflikt vorprogrammiert, weil US-Behörden diese Vorgabe als "blocking statute" einstufen

DIHK | Deutscher Industrie- und Handelskammertag e. V.
Breite Straße 29 | 10178 Berlin-Mitte | Telefon ++49-(0)30-20308-0 | Fax ++49-(0)30-20308-1000
E-Mail Berlin: infocenter@dihk.de | E-Mail Brüssel: dihk@bruessel.dihk.de | Internet: www.dihk.de

könnten. Daher sollte eine eindeutige rechtliche Aussage für die Unternehmen gemacht werden, um diesen Rechtsunsicherheit schaffenden Zustand aufzulösen.

Art. 45

Hier verweisen wir zunächst auf die Vorbemerkung.
In unserer Stellungnahme zum Grünbuch haben wir bereits darauf hingewiesen, dass aufgrund der Tatsache, dass der Datenschutz nicht an EU-Grenzen halt macht, eine intensivere internationale Zusammenarbeit bei diesem Thema erforderlich ist. Wir begrüßen daher ausdrücklich die Intention einer internationalen Zusammenarbeit.

Art. 47

Eine völlige Unabhängigkeit der Aufsichtsbehörden widerspricht dem Grundsatz zur demokratischen Legitimation von Verwaltungsbehörden. Da die Aufsichtsbehörden Teil der Exekutive sind, müssen sie zumindest einer Rechtsaufsicht unterliegen, um sie demokratisch zu legitimieren. Da die Aufsichtsbehörden zumindest in Deutschland Verwaltungstätigkeiten ausüben, z. B. Untersagung von Anwendungen, Erlass von Bußgeldbescheiden, sind sie „Behörden“ im Sinne des Verwaltungsverfahrensgesetzes.

Art. 58, 59 Kohärenzverfahen

Hier verweisen wir auf unsere Anmerkungen zu Art. 42, 43.
Bei der Stellungnahme der EU-Kommission gegenüber dem Europäischen Datenschutzausschuss stellt sich die Frage, ob hier die Unabhängigkeit des Ausschusses vor dem Hintergrund des Urteils des EuGH vom 9.3.2010 (Rechtssache C-518/07) ausreichend gewährleistet ist.

Art. 73 Abs. 2 und 3, Art. 76 Abs. 1

Datenschutz ist Ausfluss des Persönlichkeitsrechts. Dieses steht zuvörderst dem Einzelnen zu und sollte auch nur vom Betroffenen selbst durchgesetzt und eine Verletzung gerügt werden können. Im Datenschutz gibt es zudem die Aufsichtsbehörden, deren Zuständigkeit unter anderem auch die Verfolgung der Beschwerden betroffener Personen umfasst. Weitere Institutionen, die sich dieser Rechte annehmen, bedarf es daher nicht. Ein Beschwerde- und Klagerecht für Verbände lehnen wir ab.

Art. 74

Abs. 4

In dieser Regelung sehen wir eine Verletzung der Souveränität des jeweiligen EU-Mitgliedstaats.

Art. 79

Sowohl die Tatbestände als auch die Höhe der Bußgelder stehen nicht im Verhältnis zu den Verfehlungen. Sie sind völlig unangemessen. Die Regelung erweckt den Eindruck, als könne der Datenschutz nur mit härtesten Sanktionen durchgesetzt werden. Dies widerspricht z. B. dem Selbstver-

ständnis der Aufsichtsbehörden in Deutschland, die sich eher als Berater und Unterstützer, denn als Bestrafer sehen.

Zudem fehlen jegliche Verfahrensregeln. Das dann höchst unterschiedlich zur Anwendung kommende nationale Recht wird zu massiven Ungleichbehandlungen in identischen Fallgestaltungen führen.

Art 81 Abs. 1

Die Einschränkung der Zulässigkeit der Datenverarbeitung auf die Personen, die beruflichen Geheimhaltungspflichten unterliegen, bedeutet eine Behinderung z. B. für Sanitätshäuser, die für ihre Kunden individuelle Leistungen erbringen, für die sie jedoch eine genaue Kenntnis der Krankendaten benötigen. Diese müssen auch verarbeitet werden, um die Leistungen mit den Krankenkassen abrechnen zu können.

Ansprechpartnerin: Annette Karstedt-Meierrieks
E-Mail: karstedt-meierrieks.annette@dihk.de