Stellungnahme (Entwurf)

Zum Vorschlag der Datenschutz-Grundverordnung der EU-Kommission, KOM(2012) 11 endgültig

Die EU-Kommission hat im Januar 2012 eine „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" vorgelegt, sog. Datenschutz-Grundverordnung. Mit der neuen Verordnung soll die bestehende Datenschutz-Richtlinie 95/46/EG ersetzt werden. Ziel der EU-Kommission ist eine Modernisierung des europäischen Datenschutzrechts, die auch den technologischen Entwicklungen im Internet Rechnung trägt. Die Verordnung soll auf sämtliche Unternehmen Anwendung finden, die in der EU ansässig sind oder die personenbezogene Daten von EU-Bürgern verarbeiten.

I. Executive Summary

Der BDI begrüßt den Vorschlag der EU-Kommission, die Datenschutzregulierung innerhalb der Europäischen Union zu harmonisieren und für eine einheitliche Rechtsdurchsetzung einzutreten. Durch die unmittelbare Wirkung der gewählten Rechtsform einer Verordnung wird gegenüber der bestehenden Rechtslage mehr Rechtssicherheit geschaffen: Eine europaweit einheitliche Rechtslage und -durchsetzung können Akzeptanz und Vertrauen in den Datenschutz stärken und zur Etablierung einheitlicher Standards in Europa beitragen.

Der Entwurf enthält jedoch auch zahlreiche problematische Regelungen, die aus Sicht der Industrie einer Überarbeitung bedürfen. So ist eine Flexibilisierung der Rechtsgrundlage für die Datenverarbeitung unverzichtbar, um Datenverarbeitung innovationsoffen und wettbewerbsfähig zu gestalten. Darüber hinaus hält der BDI eine grundsätzliche Debatte über das Verbotsprinzip mit Erlaubnisvorbehalt, das auch dieser Verordnung zu Grunde liegt, für überfällig. Angesichts der Herausforderungen effizienter und datenintensiver Dienste kann ein grundsätzliches Verbot jeder Datennutzung kontraproduktiv auf das Ziel der Vermeidung kritischer und missbräuchlicher Datennutzung wirken und erscheint vor diesem Hintergrund nicht mehr zeitgemäß.

Im Bereich der Auftragsdatenverarbeitung, die eine wichtige Grundlage für das Cloud Computing darstellt, müssen die Regelungen für den Auftragnehmer praktikabler, d.h. deutlicher von den Pflichten des Auftraggebers abgegrenzt werden. In einer branchenübergreifenden Betrachtung unterliegen zudem die Regelungen über das Recht auf Vergessen (Art. 17. ff) sowie zur Portabilität von Daten (Art. 18) und der Profilbildung (Art. 15) erheblichen Bedenken und müssen überarbeitet

Bundesverband der Deutschen Industrie e .V.
Mitgliedsverband
BUSINESSEUROPE

Telekontakte
T: 030 2028-1419
F: 030 2028-2419

E-Mail
M.Littger@bdi.eu

Telekontakte
T: 030 2028-1461
F: 030 2028-2431

E-Mail
J.Sahl@bdi.eu

Internet
www.bdi.eu

werden.

Schließlich plädiert der BDI für eine Vereinfachung der gesellschaftsübergreifenden Datenübermittlung innerhalb eines Konzerns (Art. 41 ff.) sowie eine deutliche Herabsetzung des Sanktionsrahmens, der eine Geldbuße von bis zu zwei Prozent des weltweiten Jahresumsatzes vorsieht (Art. 79). Überarbeitungsbedarf sehen wir darüber hinaus bei den Regelungen zum Kohärenzverfahren sowie dem Umfang der delegierten Rechtsakte. Weitere Kritikpunkte betreffen zusätzliche Bürokratiepflichten, die Regelung zur Einführung eines Datenschutzbeauftragten sowie die geplante Einführung von Verbandsklagerechten.

II. Anmerkungen zu den wesentlichen Einzelpunkten

Der BDI nimmt im Folgenden Stellung zu zehn wesentlichen Regelungskomplexen des Verordnungsentwurfs, die aus der Sicht der deutschen Industrie dringend einer Überarbeitung bedürfen.

1. Grundlagen zukunftsoffen gestalten, Art. 4 ff. VO-E

Eine sichere und effiziente Verarbeitung personenbezogener Daten ist für die gesamte Industrie von zentraler Bedeutung. Denn über die Gestaltung effizienter, unternehmensinterner Prozesse hinaus ist Datenverarbeitung auch zur wichtigen Voraussetzung für neue Geschäftsmodelle geworden: Die intelligente Vernetzung (auch) personenbezogener Daten eröffnet beispielsweise in der Mobilität und Energieversorgung bis zur Gesundheitswirtschaft neue Chancen für die Informationsgesellschaft. Sie setzen innovative und sichere Verfahren der Datenverarbeitung voraus, für die ein modernes Datenschutzregime das notwendige Fundament schaffen muss.

Um im künftigen Datenschutzregime einen angemessenen Ausgleich zwischen dem Grundrecht auf Datenschutz und dem freien Verkehr personenbezogener Daten zu erreichen, halten wir Korrekturen im Entwurf bei den Rechtsgrundlagen (a), dem Anwendungsbereich (b), den Regelungen zur Einwilligung (c) sowie im Verhältnis zur E-Privacy Richtlinie (d) für unabdingbar.

a) Rechtsgrundlage flexibilisieren, Art. 5 f. VO-E

Der VO-Entwurf geht von einem grundsätzlichen Verbot sämtlicher Datennutzung aus, es sei denn, es liegt eine Erlaubnis vor („Verbotsprinzip“). Mit Blick auf die künftige Relevanz von Daten in allen Lebensbereichen halten wir eine Debatte über die Notwendigkeit dieses Verbotsprinzips für überfällig: Nach unserer Ansicht ist das Verbotsprinzip für die Vermeidung missbräuchlicher Datennutzung im privatwirtschaftlichen Umfeld nicht erforderlich und kann stattdessen eine legitime und intelligente Datenverarbeitung erschweren.

In jedem Fall bedürfen die im Entwurf vorgesehenen Erlaubnistatbestände einer wirksamen Flexibilisierung, um die gewollte Zukunftsoffenheit der Regulierung für die Informationsgesellschaft zu erzielen. Die strenge Zweckbindung der Datenverarbeitung in Art. 5 b)und c) hemmt innovative Weiterentwicklungen von Produkten und Verfahren und ist daher aufzugeben: Eine spätere Änderung des Zwecks muss möglich sein, soweit dies nicht den Interessen des Betroffenen widerspricht.

Die Datenverarbeitung wegen zulässiger Interessen *Dritter* darf entgegen der Regelung nach Art. 6 Abs. 1 f) VO-E nicht entfallen. Sie würde beispielsweise die Arbeit von Auskunfteien ohne Not erheblich erschweren. Zudem sollte die Öffnungsklausel für mitgliedsstaatliche Erlaubnistatbestände nicht auf „rein öffentliche“ Schutzzwecke beschränkt bleiben.

b) Anwendungsbereich präzisieren, Art. 4 VO-E

Der BDI spricht sich für eine Präzisierung des Personenbezugs im aktuellen Entwurf aus. Die umfassende Definition würde andernfalls dazu führen, dass nahezu sämtliche Daten unter den Anwendungsbereich der Verordnung fallen. So würden gemäß Art. 4 Abs. 1 und 2 bereits Produktionsnummern und IP-Adressen einen hinreichenden Personenbezug begründen, was erhebliche Folgeprobleme aufwirft.

Es sollte vielmehr eine Dynamisierung des Personenbezugs mit konkreten Anreizen zur Selbstbeschränkung erreicht werden. Die faktischen Zugriffsmöglichkeiten sowie die konkreten Vorkehrungen zum Datenschutz beim Verantwortlichen müssten berücksichtigt werden. Nach einer Pseudonymisierung oder Anonymisierung sollten Daten grundsätzlich vom Anwendungsbereich ausgenommen werden. Dies schafft zusätzliche Anreize für einen sparsamen Umgang mit personenbezogenen Daten und ist auch daher im Sinne der Betroffenen. Insoweit ist eine grundsätzliche Überarbeitung erforderlich.

c) Einwilligung praktikabel gestalten, Art. 7 VO-E

Die Möglichkeit zur Einwilligung in die Datenverarbeitung sollte möglichst einfach zu handhaben sein: Betroffene müssen ihre Einwilligung auch implizit oder mit Vornahme eines Anmeldeprozesses geben können, soweit ausreichende Transparenz gewährleistet wird. Die formalen Anforderungen an die Einwilligung sollten dabei insgesamt stärker am spezifischen Risiko des Betroffenen ausgerichtet werden.

Im Widerspruch dazu steht das strikte Gebot der Ausdrücklichkeit gemäß Art. 4 Abs. 8 VO-E. Dieses würde neuen technischen Entwicklungen für eine informierte und freiwillige Einwilligung entgegenwirken und ist daher zu flexibilisieren.

Nicht akzeptabel ist auch das generelle Verbot von Einwilligungen bei Vorlage eines „erheblichen Ungleichgewichts“, Art. 7 Abs. 4 VO-E. Hier muss entgegen den Vorgaben in Erwägungsgrund 34 klargestellt werden, dass eine Einwilligung in Beschäftigungsverhältnissen möglich bleibt sowie auch im Rahmen von (Massen-)Geschäften zwischen Betroffenen und Unternehmen. Dies gilt umso mehr,

als Verbraucher von intelligenten Datenverarbeitungsvorgängen in der Regel auch profitieren.

d) Verhältnis zur E-Privacy-Richtlinie klären, Art. 89 VO-E

Das Verhältnis der Verordnung zu den Bestimmungen in der E-Privacy-Richtlinie gemäß Art. 89 VO-E sollte klargestellt werden. Elektronische Datenverarbeitung ist heute ein branchenübergreifendes Anliegen für die Wettbewerbsfähigkeit von Unternehmen. Dadurch verliert eine sektorspezifische Regulierung zunehmend ihre Rechtfertigung, was im Verhältnis beider Regulierungsakte berücksichtigt werden sollte.

2. Auftragsdatenverarbeitung vereinfachen, Clouddienste stärken, Art. 22 VO-E

Eine effiziente und sichere Datenverarbeitung erfolgt in der Industrie schon heute oftmals über professionelle Drittanbieter. Dieser Trend wird durch die Verbreitung von Clouddiensten massiv beschleunigt. Neben klassischen Unternehmensprozessen übernehmen Clouddienste das Datenmanagement auch für neue, datenintensive Geschäftsmodelle und schaffen damit neues Wachstum und Wohlstand in der Informationsgesellschaft.

a) Verantwortlichkeiten trennen, Selbstverpflichtung stärken

Um die Entwicklung der Auftragsdatenverarbeitung und Clouddienste in Europa zu stärken, ist eine strikte Trennung der Verantwortlichkeiten zwischen dem Verantwortlichen („Controller“) und dem Verarbeiter („Processor“) gemäß Erwägungsgrund 62 VO-E unverzichtbar. In zahlreichen Regelungen des VO-E unterliegen beide Parteien gleichen Vorgaben, wodurch innovative Entwicklungen sowie Geschäftschancen beim Datenverarbeiter bzw. Cloudanbieter gehemmt würden. Stattdessen sollten mehr Anreize zur Selbstverpflichtung und Zertifizierung geschaffen werden, die Differenzierungsmerkmale am Markt als Wettbewerbsvorteil ermöglichen.

Erfolgt eine Datenverarbeitung auf Weisung des Verantwortlichen, sollte beim Verarbeiter entgegen Art. 27 VO-E vom Vorbehalt einer Rechtsprüfung abgesehen werden und stattdessen eine reine Hinweispflicht genügen. Andernfalls könnten konfligierende Rechtsauslegungen zu zusätzlichen Komplikationen im Auftragsverhältnis führen. Auch auf die Ausweitung der Dokumentationspflicht des Verantwortlichen auf den Verarbeiter nach Art. 26 und 28 ist zu verzichten.[1]

b) Vereinfachte Compliance-Prüfung

Nach Art. 26 ist der Auftraggeber dafür verantwortlich, dass der Datenverarbeiter die Datenschutzregelungen einhält. Unklar bleibt, wann diese Verpflichtung als erfüllt

[1] Vgl. dazu auch unten III. 4) Bürokratie vermeiden.

anzusehen ist. Für KMU begründet die Prüfung zudem oft unverhältnismäßigen Aufwand, wenn z.B. die Lohnbuchhaltung auf Dritte übertragen werden soll. Hier sollte genügen, dass der Verarbeiter eine entsprechende Bestätigung über die Einhaltung der Datenschutzverordnung erteilt. Andernfalls drohen Rechtsunsicherheiten, vergleichbar der deutschen Regelung nach § 11 BDSG.

Ferner sollte in Art. 3 VO-E klargestellt werden, dass die Anwendung der Datenschutzverordnung für alle Anbieter gilt, die Auftragsdatenverarbeitung in der Europäischen Union anbieten - unabhängig vom Ort ihrer Niederlassung.

3. Praktikabilität branchenübergreifend betrachten, Art. 17 ff. VO-E

Der BDI sieht Anpassungsbedarf bei solchen Regelungen im Entwurf, die auf konkrete Geschäftsmodelle im Onlinebereich ausgerichtet sind, in ihrer Anwendung durch andere Unternehmen jedoch zu erheblichen Probleme führen können.

a) Datenübertragbarkeit überdenken, Art 18

Die Verpflichtung aller Unternehmen gemäß Art. 18 VO-E, personenbezogene Daten sowie weitere Informationen von betroffenen Personen in einem gängigen Format zur Verfügung zu stellen, sollte grundsätzlich überdacht bzw. beschränkt werden.

Zwar ist der Grundgedanke einer Datenübertragung – im Rahmen Sozialer Netzwerke und anderer Dienstleistungen des Web 2.0 – grundsätzlich nachvollziehbar. Ein Recht auf Datenübertragbarkeit kann die Hürde für einen Anbieterwechsel senken und dadurch den Wettbewerb befördern.
Fraglich ist aber bereits, ob Datenübertragbarkeit als wettbewerbspolitisches Instrument in einer Datenschutzverordnung an der gesetzessystematisch richtigen Stelle verortet ist. Problematisch erscheint außerdem, ob die Zusammenführung personenbezogener Daten aus unterschiedlichen Systemen dem Datenschutz wirklich dient – oder diesem nicht eher schadet. Kritisch beurteilt die Industrie vor allem, dass – über personenbezogenen Daten hinaus – sonstige Informationen über die Kundenbeziehung offengelegt und Wettbewerbern zugänglich gemacht werden könnten. Für Industrieunternehmen könnten dadurch erhebliche Nachteile entstehen, wenn sie Wettbewerbern entsprechende Kundenakten jederzeit offen zu legen hätten, ohne dass überdies eine Rechtfertigung unter Datenschutzaspekten ersichtlich ist.

b) Recht auf Vergessen und Löschung präzisieren, Art. 17

Die Regelungen zum Recht auf Vergessen bzw. Löschen müssen zu einem ausgewogenen Verhältnis zwischen den Interesse des Datenschutzes und legitimer Datenverarbeitung führen. Die Dispositionsbefugnis des Betroffenen nach Art. 17 VO-E könnte das vertragliche Verhältnis dagegen in ein Ungleichgewicht führen., beispielsweise dann, wenn die Einwilligung auf Seiten des Verantwortlichen eine Voraussetzung für das Zustandekommen war, nachträglich aber wieder entzogen wird. Als Lösung sollte im Entwurf eine stärkere und rechtsklare Flexibilisierung des Löschungsanspruchs im Sinne einer Interessenabwägung eingefügt werden.

Die Regelungen zum Recht auf Vergessen laufen weitgehend parallel zum Recht auf Löschen und sollten aus Gründen der Rechtsklarheit daher begrifflich zusammengefasst werden.

c) Profilbildung nicht stigmatisieren, Art. 20

Die Bildung von Profilen über Personen ist eine wichtige Voraussetzung für zahlreiche Geschäftsmodelle – innerhalb und außerhalb des Internets. Der BDI regt an, die bislang erlaubten Sachverhalte nicht weiter zu verengen. Dies sollte im Entwurf klargestellt werden, soweit der Wortlaut Zweifel daran begründet, beispielsweise mit Blick auf das Wort „maßgeblich“ in Art. 20 Abs. 1 VO-E. Profilbildungen aufgrund von Interessenabwägungen sowie anonymisierter Datenlage sollten zudem ausdrücklich als zulässig benannt werden.

4. Datenübertragung im Konzern vereinfachen, Art. 40 ff VO-E

Für global tätige Unternehmen ist der einfache, grenzüberschreitende Austausch personenbezogener Daten innerhalb des Konzern unverzichtbar. Insoweit sieht der VO-E zwar begrüßenswerte Vereinfachungen vor, enthält aber keine hinreichende Regelung zum konzerninternen Datentransfer:

- Nach Artikel 43 VO-E kann die Aufsichtsbehörde Unternehmensvorschriften als notwendige Garantie bei der Datenübermittlung in Drittstaaten verbindlich genehmigen; dies soll nach Art. 43, 58 VO-E allerdings nur in Zusammenwirken mit EU-Kommission und Europäischem Datenschutzausschuss geschehen. Der BDI regt an, von dieser Voraussetzung des Zusammenwirkens abzusehen, da sonst eine unverhältnismäßige Komplexität sowie zeitliche Verzögerungen im Genehmigungsverfahren drohen.

- Wir regen an, von einer Ermächtigung der EU-Kommission zum Erlass von Kriterien und Anforderungen im Rahmen des Genehmigungsverfahrens nach Art. 51 DS-GVO-E abzusehen. Andernfalls könnte die Entscheidungskompetenz der Aufsichtsbehörde für ihr Hoheitsgebiet beeinträchtigt werden – zum Nachteil der Planungssicherheit von Unternehmen für den konzerninternen Datentransfer.

- Grundsätzlich begrüßen wir die Regelungen nach Art. 44 Abs. 1 VO-E zur Übermittlung von Daten aufgrund eines berechtigten Interesses; jedoch wird die Zulässigkeit daran geknüpft, dass die Übermittlung nicht als häufig oder massiv bezeichnet werden kann. Bei der konzerninternen Bündelung von Aufgaben ist ein häufiger Datenaustausch jedoch eher der Regelfall. Daher sollte auf diese Einschränkung als Voraussetzung für den Datenaustausch zwischen Konzernunternehmen in einem Drittland verzichtet werden.

Erforderlich ist ferner eine Klärung im Verhältnis zum Safe Harbor Abkommen, das den internationalen Datentransfer in die USA regelt.

5. Aufsichtsbehörden und Datenschutzausschuss stärken, Art. 51 ff. VO-E

Der BDI begrüßt das Prinzip der einheitlichen Zuständigkeit von Datenschutzaufsichtsbehörden in der EU („One-Stop-Shop“) sowie der Entscheidungsbefugnis durch den EU-Datenschutzausschuss im Rahmen des Kohärenzverfahrens gemäß Art. 57 VO-E als wichtigen Beitrag für mehr Rechts- und Planungssicherheit in Europa. Für das gemeinsame Ziel einer konsistenten Rechtsdurchsetzung bedürfen die Regelungen aus unserer Sicht jedoch folgender Anpassungen:

- Die Einrichtung eines EU-Datenschutzausschusses nach Art. 58 VO-E, der zu Entscheidungen der Datenschutzbehörden rechtsverbindlich Stellung nimmt, ist ein richtiger Schritt zur einheitlichen Auslegung und Durchsetzung des EU-Datenschutzes. Nicht akzeptabel hingegen ist der mangelnde Rechtsschutz gegen die Ausschussentscheidungen; hier ist ein transparenter sowie rechtsstaatlicher Kontrollmechanismus notwendig. Zudem ist das Ausschussverfahren durch Anhörungs- und Mitwirkungsrechte der Wirtschaft zu ergänzen.

- Die Rolle der führenden Aufsichtsbehörde sollte gestärkt werden. Es muss sichergestellt werden, dass die Befugnis der lokalen Aufsichtsbehörde zu vorläufigen Maßnahmen gemäß Art. 55 Abs. 8 VO-E nicht die Entscheidungskompetenz der führenden Behörde unterminieren kann. Im Falle geplanter Ermittlungen und Sanktionierungen durch lokale Aufsichtsbehörden sollte der Kohärenzmechanismus zum Tragen kommen. Lokale Aufsichtsbehörden sollten zudem eindeutig als Bindeglied zwischen der verantwortlichen Stelle und Betroffen agieren sowie dafür Sorge tragen, dass Beschwerden an die führende Aufsichtsbehörde geleitet werden.

- Für die zentrale Zuständigkeit der Aufsichtsbehörde ist eine Klarstellung erforderlich, wer innerhalb eines Konzernverbundes – mit lokal selbständigen Landesgesellschaften – Verantwortlicher im Sinne der Verordnung ist: Sinnvollerweise müsste dabei auf die Obergesellschaft oder die größte Landesgesellschaft innerhalb der EU abgestellt werden. Um Rechtsunsicherheit zu vermeiden, sollte zudem die Hauptniederlassung im Sinne des Art. 51 Abs. 2 für Verantwortlichen und Auftragsdatenverarbeiter gleichermaßen definiert werden.

6. Sanktionsrahmen angemessen gestalten, Art. 79 VO-E

Die Regelungen zur Sanktionierung sind gerechtfertigt, soweit sie Verstöße gegen die Datenschutzvorschriften wirksam ahnden und damit auch zu ihrer effektiven Einhaltung beitragen. Erforderlich ist jedoch, den Sanktionsrahmen verhältnismäßig auszugestalten, um ungewollte Nachteile und Schäden bei den Unternehmen zu vermeiden.

- Nicht akzeptabel ist aus Sicht der Industrie die mangelnde Differenzierung der Sanktionsvorschriften zwischen Unternehmen, deren Geschäftsmodell in der Verwendung von Daten besteht und solchen, die eine Datenverarbeitung lediglich für die üblichen Unternehmensprozesse verwenden. Letztere sollten schon im Grundsatz einem deutlich modifizierten, abgeschwächten Sanktionsmechanismus unterliegen. Eine mögliche Sanktionierung von bis zu zwei Prozent des Jahresumsatzes, Art. 79 Abs. 6, würde ein völlig unverhältnismäßiges Risiko für die Wirtschaft begründen.

- Aber auch für Unternehmen, deren Geschäftsmodell innovative Datenverarbeitung umfasst, begründet die Regelungen im Entwurf eine kritische Ausgangslage. Für die Erprobung neuer Geschäftsmodelle würden geplante Sanktionsdrohungen von bis zu zwei Prozent des Jahresumsatzes erhebliche Planungsunsicherheit verursachen. Dieser Sanktionsrahmen könnte von der EU-Kommission sogar im Rahmen delegierter Rechtsakte einseitig erhöht werden.[2] Insoweit sind die Sanktionsregelungen bereits nach der Höhe ihrer Bußgeldandrohung hin zu überdenken.

  Erschwerend wirken sich die teilweise drastischen Sanktionsdrohungen angesichts der teilweisen unklaren Tatbestandsvoraussetzungen sowie der unzureichenden Differenzierung zwischen vorsätzlichen und fahrlässigen Regelverstößen bzw. absichtlichen Schädigungshandlungen aus. Auch hier sind Änderungen dringend erforderlich, um dauerhafte Hemmnisse für innovative Entwicklungen in den Datenverarbeitungsprozessen zu vermeiden.

7. Delegierte Rechtsakte reduzieren, Selbstregulierung fördern

Der BDI appelliert an den europäischen Gesetzgeber, die Verweise auf delegierte Rechtsakte der EU-Kommission nach Art. 290 AEUV – an 26 Stellen im Entwurf – kritisch zu überdenken und ihre Anzahl deutlich zu reduzieren. Vergleichbar zu „Rechtsverordnungen“ im deutschen Recht dürfen delegierte Rechtsakte nur „nicht wesentliche“ Aspekte des Gesetzes betreffen.

Derartige Delegationen können gerechtfertigt sein, um Regelungen zu einem späteren Zeitpunkt zu konkretisieren und aktuellen Entwicklungen anzupassen. Dem steht aber das Risiko gegenüber, dass die Rechts- und Planungssicherheit beeinträchtigt wird. Auch könnte sich die alleinige Entscheidungsbefugnis der EU-Kommission teilweise als problematisch erweisen. Wir regen daher an, die delegierten Rechtsakte im Entwurf unter folgender Maßgabe zu überprüfen:

- Soweit wie möglich sollten delegierte Rechtsakte in der Verordnung durch verbindliche Konkretisierungen ersetzt werden[3]; denkbar sind auch Verweise auf bestehende nationale Regelungen, soweit dies nicht der erwünschten

[2] Vgl. dazu weiter unten III 1) Delegierte Rechtsakte reduzieren.

Einheitlichkeit im Datenschutz entgegensteht.

- Soweit delegierte Rechtsakte technische Fragen der Standardisierung, Zertifizierungsverfahren oder Ähnliches betreffen, sollten Mechanismen der Selbstregulierung berücksichtigt werden. Dadurch könnte die Akzeptanz der Betroffenen sowie auch der Praxisbezug gestärkt stellen.

- Soweit delegierte Rechtsakte beibehalten werden, sollte der Wirtschaft im Verfahren der Entscheidungsfindung unbedingt eine beratende Funktion zugedacht werden.

8. Datenschutzbeauftragten stärken, Art. 35 VO-E

Der BDI unterstützt die verbindliche Einführung eines betrieblichen Datenschutzbeauftragten in Art. 35 DS-GVO-E und spricht sich für eine Stärkung seiner Kompetenzen aus. Seine Existenz hat sich in Deutschland insgesamt bewährt.

- Der pauschale Schwellenwert von 250 Mitarbeitern als Kriterium für die Benennung eines Datenschutzbeauftragten ist zu fragwürdig. Würde dieser Schwellenwert für Deutschland gelten, wären nur noch etwa 0,3 Prozent der Unternehmen zur Bestellung eines Datenschutzbeauftragten verpflichtet. Bei kleinen Unternehmen könnte zudem der unzutreffende Eindruck entstehen, Datenschutz werde erst ab einer Größe von 250 Mitarbeiter relevant.

- Wir begrüßen den Ansatz, dass die Einführung des Datenschutzbeauftragten gemäß Art. 35 Abs. 1 c) VO-E auch anhand des Kriteriums über die Art und Intensität der Datenverarbeitung in einem Unternehmen erfolgen kann. Diese Regelung sollte – vergleichbar zum deutschen Recht – um eine Vorgabe ergänzt werden, die auf die Anzahl derjenigen Mitarbeiter abstellt, die automatisiert personenbezogene Daten verarbeiten. Wir halten hier eine Grenze von 50 betroffenen Mitarbeitern für konsensfähig.

- Daneben sollte die betriebliche Selbstkontrolle und Selbstregulierung auch in der Form gestärkt werden, dass Unternehmen, die über einen betrieblichen Datenschutzbeauftragten verfügen, von Melde- und Informationspflichten gegenüber der Aufsichtsbehörde befreit werden. Dadurch würden zusätzliche Anreize auch für kleine Unternehmen zur Einführung eines Datenschutzbeauftragten geschaffen.

  Insgesamt regen wir an, dem betrieblichen Datenschutzbeauftragten mehr Verantwortung zu übergeben und damit auch die betriebliche Selbstkontrolle zu stärken. Ein solches Vorgehen könnte eine zusätzliche Akzeptanz des

[3] Die geplante Ermächtigung der EU-Kommission, die Sanktionshöhe beim Regelverstoß anzupassen, nach Art. 79 Abs. 5 VO-E haben wir bereits kommentiert und sollte gestrichen werden, vgl. oben II 6.

betrieblichen Datenschutzbeauftragten innerhalb der europäischen Wirtschaft schaffen sowie die Aufsichtsbehörden finanziell und personell entlasten.

9. Kein Klagerecht für Organisationen, Art. 73 ff. VO-E

Der Entwurf sieht vor, neben den betroffenen Personen künftig auch selbständigen Einrichtungen eine Beschwerde im Namen der betroffenen Person gegenüber Aufsichtsbehörden zu ermöglichen und deren Entscheidungen gerichtlich überprüfen zu lassen. Der BDI lehnt eine derartige Ausweitung der Beschwerde- und Klagerechte auf Organisationen und Verbände gemäß Art 73 ff. VO-E nachdrücklich ab.

Die Industrie begrüßt zwar die unterstützende Funktion der Aufsichtsbehörden für betroffene Personen zur Einhaltung der Schutzvorschriften. Eine darüber hinaus gehende Verankerung von gerichtlichen Klage- und Beschwerderechte durch Dritte ist aber schon unter Datenschutzaspekten nicht erforderlich.

Denn Datenschutz ist der Ausdruck des individuellen Persönlichkeitsrechts, als dessen Ausfluss das Prinzip des individuellen Rechtsschutzes steht. In Übereinstimmung mit diesem Prinzip wird mehreren Beteiligten einer Klage – nach der deutschen Zivilprozessordnung – bereits heute durch die Streitgenossenschaft oder Prozessverbindung ausreichend Rechnung getragen.

Die Ausweitung des Klagerechts im Sinne des VO-E würde auf die Einführung von Sammelklagen hinauslaufen und damit auch für Unternehmen unkalkulierbare, neue ökonomische Risiken begründen. Erhebliche Friktionen im kontinentaleuropäischen Rechtssystem wären die Folge. Sowohl aus ökonomischen als auch aus rechtssystematischen Gründen ist daher am Prinzip des individuellen Rechtsschutzes festzuhalten.

10. Vermeidung von Bürokratie, Art. 12, 22, 28 ff. VO-E

Die Industrie regt eine umfassende Überprüfung der geplanten Dokumentationspflichten im Entwurf an. Zahlreiche Pflichten erscheinen weder im Sinne des Datenschutzes zwingend erforderlich, noch stehen sie in einem vertretbaren Verhältnis zum Aufwand der betroffenen Unternehmen. Daraus ergibt sich aus unserer Sicht insbesondere bei folgenden Regelungen ein Korrekturbedarf:

- Die gesetzliche Benachrichtigungspflicht der Unternehmen nach Art. 12, 14 VO-E geht über das Ziel einer bloßen Eingangsinformation weit hinaus. Der umfängliche Informationskatalog droht den Betroffenen zudem zu überfordern mit dem Risiko, dass er die Informationen vollständig überliest.

  Statt überbordender Informationspflichten schlagen wir daher ein Stufenverhältnis vor, das dem Betroffenen die Möglichkeit vertiefender

Informationen einräumt. Die Eingangsinformation nach Art. 14 VO-E würde dann nur die wesentlichen Daten enthalten und im Einzelfall auch durch einfache Hinweispflichten erfolgen können.

- Im Bereich der Datenverarbeitung bzw. des Cloud Computing ist eine deutlichere Abgrenzung der Dokumentationspflichten erforderlich nach Art. 28 VO-E. Andernfalls drohen bis zu drei parallele Dokumentationsstellen für identische Abläufe mit dem Risiko widersprüchlicher Ergebnisse sowie der Vervielfachung sensibler Datensammlungen. Darüber hinaus sollte die Dokumentationspflichten nach Art. 22 auf die wirklich wesentlichen Vorgänge beschränkt werden, vorschlagsweise am Maßstab des BDSG.

- Die Regelungen zur Datenschutz-Folgenabschätzung erscheinen problematisch, soweit Kriterien für Genehmigungen bzw. die Zurateziehung der Aufsichtsbehörden gemäß Art. 34 Abs. 1 bzw. 2 VO-E nicht eindeutig definiert sind bzw. durch delegierte Rechtsakte erlassen werden sollen. Insbesondere muss sichergestellt werden, dass in der entsprechenden Kommunikation kürzeste Reaktionszeiten der Behörden vorliegen, um die Einführung innovativer Datenverarbeitungstools nicht ohne Not zu verzögern und zu beeinträchtigen.