19. September 2012

Stellungnahme der Bundesregierung zu Kapitel III und Artikel 22 bis 27 von Kapitel IV des Vorschlags der Kommission für eine Datenschutz-Grundverordnung (KOM(2012) 11 endg.)

Mit Schreiben vom 5. September 2012 lädt die Präsidentschaft die Mitgliedstaaten ein, vor dem 20. September 2012 Änderungsvorschläge und Anmerkungen, unabhängig von den in der Ratsarbeitsgruppe DAPIX bereits gemachten, zu Kapitel III und Artikel 22 bis 27 von Kapitel IV des Vorschlags der Kommission für eine Datenschutz-Grundverordnung zu übermitteln.

A. Vorbemerkung

Deutschland dankt der Präsidentschaft für die Gelegenheit zur Stellungnahme. Wie in der Vorbemerkung zur Stellungnahme vom 9. Mai 2012 ausgeführt, hat Deutschland zu dem Rechtsakt allgemeine Fragen, die noch einer vertieften Erörterung bedürfen. Wie andere Mitgliedstaaten spricht sich auch Deutschland vor dem Hintergrund der bisherigen Erörterungen in der Ratsarbeitsgruppe DAPIX weiterhin dafür aus, dass der Regelungsvorschlag möglichst klar zwischen der Datenverarbeitung im öffentlichen und privaten Bereich sowie stärker zwischen risikoarmen und risikoreichen Datenverarbeitungen differenziert und darüber hinaus einen angemessenen Ausgleich zwischen den Schutzinteressen der Betroffenen und dem bürokratischen Aufwand herstellt. Die hier vorgelegten Vorschläge sind nur als vorläufige und nicht abschließende Beiträge zur weiteren Erörterung des Rechtsaktes anzusehen. Deutschland behält sich weiteren Vortrag, auch zu grundsätzlichen, artikelübergreifenden Themen ausdrücklich vor. Redaktionelle Hinweise und Anmerkungen zur deutschen Sprachfassung werden zu einem späteren Zeitpunkt erfolgen. Zu den Erwägungsgründen wird gesondert Stellung genommen. Die weiteren von Deutschland in der Ratsarbeitsgruppe DAPIX vorgetragenen Anmerkungen werden vorsorglich auch zum Gegenstand der Stellungnahme gemacht und im Folgenden zum Teil erneut aufgeführt.

B. Anmerkungen zu den Artikeln 11 bis 27

I.

Allgemeine Prüfvorbehalte sowie Vorbehalte zu einzelnen Regelungen, wie sie in der Ratsarbeitsgruppe DAPIX und in der Stellungnahme zu den Artikeln 1 – 10 vorgetragen worden sind, bleiben bestehen.

II.

Kapitel III enthält entgegen seinem Titel nicht nur Rechte der betroffenen Person, sondern auch Pflichten des für die Verarbeitung Verantwortlichen, siehe etwa Artikel 11, 12, 13. Titel und Aufbau des Kapitels sollten auch mit Blick auf Kapitel IV überprüft werden.

1. zu Artikel 11:

Artikel 11 zur Transparenz sollte präzisiert werden. Deutschland ist wie eine Reihe anderer Mitgliedstaaten in der DAPIX besorgt über die mit der sehr allgemein gehaltenen Formulierung („Strategie“) in Artikel 11 gegebenenfalls verbundenen Bürokratiekosten und die fehlende risikobasierte Differenzierung. Deutschland hätte sich eine belastbare Berechnung der Bürokratiekosten seitens der Kommission gewünscht. Es sollte geprüft werden, ob für bestimmte, näher zu definierende Bereiche, Ausnahmen vorgesehen werden können. Aus Sicht von Deutschland bedürfen die Pflichten des für die Verarbeitung Verantwortlichen, u.a. die in Artikel 12 vorgesehenen, in den Fällen der Erörterung, in denen eine natürliche Person für die Verarbeitung Verantwortlicher ist, z.B. in den Fällen des Artikel 2 Absatz 2 Buchstabe d oder im Gesundheitsbereich bei elektronischen Patientenakten.

- Absatz 1 enthält gegenüber Absatz 2 und Artikel 12 keinen erkennbaren Mehrwert und könnte daher gestrichen werden.
- Absatz 2 sollte mit den Pflichten des für die Verarbeitung Verantwortlichen bei der Rechteausübung der betroffenen Person in Artikel 12 zusammengeführt werden. Es sollte klargestellt werden, wann mit dem „zur Verfügung stellen“ von Informationen und Mitteilungen eine Bringschuld des für die Verarbeitung Verantwortlichen und wann eine Holschuld der betroffenen Person verbunden ist.
- Deutschland unterstützt, wie mehrere andere Mitgliedstaaten in der DAPIX eine Information „ *in verständlicher Form unter Verwendung einer klaren, einfachen und altersgerechten Sprache*“.

2. zu Artikel 12:

- Absatz 1 Satz 2 sollte gestrichen werden. Der Begriff „erleichtern“ ist unbestimmt und das erforderlich Maß an „Erleichterung“ streitanfällig.
- Absatz 1 Satz 3 sollte auf die Fälle begrenzt werden, in denen der für die Verarbeitung Verantwortliche elektronisch kommuniziert. Eine automatisierte Verarbeitung personenbezogener Daten (z.B. an einem PC) bietet noch keine Gewähr, dass auch eine elektronische Kommunikation (z.B. eine E-Mail-Adresse) besteht.
- Absatz 2 Satz 1 ist in der deutschen Sprachfassung in mehfacher Hinsicht unklar und sollte dahin formuliert werden, dass der für die Verarbeitung Verantwortliche seinen Pflichten und den Rechten der betroffenen Person nach Kapitel III unverzüglich, d.h. ohne schuldhaftes Verzögern, nachkommt.
- Absatz 2 Satz 2 sollte an Satz 1 anschließen („Dabei …“) und Fälle benennen, die - abhängig von den Möglichkeiten des für die Verarbeitung Verantwortlichen - eine längere Bearbeitungsdauer rechtfertigen können, z.B. unter bestimmten Voraussetzungen die Häufung von Anträgen bei kleineren und mittleren Unternehmen oder bei komplexen Sachverhalten.
- Absatz 2 Satz 3 sollte dahin formuliert werden, dass der für die Verarbeitung Verantwortliche die betroffene Person auf Verlangen schriftlich unterrichtet, dass er seinen Pflichten nach Satz 1 nachgekommen ist.
- Absatz 2 Satz 4 sollte dahin formuliert werden, dass die Unterrichtung in elektronischer Form erfolgen soll, wenn die betroffene Person es wünscht und das erforderliche Schutzniveau zur elektronischen Übermittlung von personenbezogenen Daten einschließlich einer zuverlässigen Authentifizierung des Empfängers eingehalten wird (vergleiche Erwägungsgrund 52).
- In Absatz 4 Satz 1 sollte die Unentgeltlichkeit der Pflichten des für die Verarbeitung Verantwortlichen und der Rechte der betroffenen Person in Kapitel III durch Bezugnahme auf die konkreten Artikel oder das Kapitel erfolgen, nicht durch Verweis auf Artikel 12 Absatz 1. Für Auskünfte nach Artikel 15, die die betroffene Person gegenüber Dritten zu wirtschaftlichen Zwecken nutzen kann, sollte aufgenommen werden, dass einmal je Kalenderjahr eine unentgeltliche Auskunft in Textform und für jede weitere Auskunft ein angemessenes, nicht prohibitives Entgelt verlangt werden kann. Ein Entgelt darf nicht verlangt werden, wenn eine Unrichtigkeit oder Unzulässigkeit der Daten zu vermuten ist oder die

Auskunft dies ergibt. Die betroffene Person muss die Möglichkeit haben, sich unentgeltlich persönlich Kenntnis zu verschaffen.

- Im Falle offenkundig unverhältnismäßiger Anträge nach Absatz 4 Satz 2 sollte durch die Streichung der Worte „ein Entgelt für die Unterrichtung oder“ lediglich vorgesehen werden, dass die beantragte Maßnahme unterbleiben kann. Eine Regelung zu Entgelten erscheint unangemessen und insbesondere zwischen nicht-öffentlichen Stellen sehr streitanfällig. Zur „Häufung“ von Anträgen sollte klargestellt werden, dass es um Anträge einer Person geht. Eine Vielzahl von Anträgen an sich muss nicht offenkundig unverhältnismäßig sein, sondern ist gegebenenfalls nur Folge der Unternehmensgröße oder des Umfangs der Datenverarbeitung.
- Die Beweislastregelung in Absatz 4 Satz 3 kann nach deutschem Rechtsverständnis gestrichen werden. Grundsätzlich hat jede Seite die für sie günstigen Umstände zu beweisen, vorliegend also der für die Verarbeitung Verantwortliche den offenkundig unverhältnismäßigen Charakter eines Antrags, weswegen er von der beantragten Maßnahme absehen will.
- Die Ermächtigung der Kommission in Absatz 5 ist zu streichen. Die Kommission würde durch die Bestimmung, wann ein Betroffenenrecht offenkundig unverhältnismäßig ausgeübt wird, weitreichend in die Rechte der Betroffenen eingreifen. Es handelt sich zudem um eine eng umgrenzte Thematik, so dass eine Regelung in der Verordnung erfolgen und ansonsten der Aufsichts- und Gerichtspraxis überlassen bleiben sollte.
- Die Ermächtigung der Kommission in Absatz 6 ist zu streichen, da sie den laufenden Beratungen des Entwurfs einer Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vorgreift. Die Festlegung von Standardvorlagen und -verfahren für Mitteilungen in elektronischer Form greift sehr weitreichend in technische Standardisierungen auch im öffentlichen Bereich ein (z.B. gibt es in Deutschland mit De-Mail einen besonders gesicherten E-Mail-Verkehr mit Behörden). Maßnahmen, die auch KMU zu Gute kommen, sollten unmittelbar in der Verordnung geregelt werden und nicht einer künftigen, ungewissen Regelung überlassen bleiben.

3. zu Artikel 13:

- Eine Nachberichtspflicht gegenüber den Empfängern von Daten ist grundsätzlich zu begrüßen.
- Artikel 13 enthält keine Rechte gegenüber Empfängern. Die Überschrift sollte in „Benachrichtigungspflicht bei Berichtigungen und Löschungen“ geändert werden.
- Es sollte klargestellt werden, dass die Benachrichtigungspflicht nicht bei der Weitergabe innerhalb des für die Verarbeitung Verantwortlichen besteht.
- Die Benachrichtigungspflicht sollte - vorbehaltlich der weiteren Erörterung - auch die Mitteilung von Widersprüchen nach Artikel 19 Absatz 3 umfassen, sofern der Widerspruch zur Unzulässigkeit der weiteren Verarbeitung führt.
- Die Benachrichtigungspflicht sollte zusätzlich nur dann bestehen, wenn schutzwürdige Interessen des Betroffenen nicht entgegenstehen, z.B. also nicht, wenn der Empfänger erstmals Kenntnis von negativen Daten über die betroffene Person erhielte, an denen er kein berechtigtes Interesse hat. Entsprechende Beispiele sollten in einem Erwägungsgrund erläutert werden.

4. zu Artikel 14:

Wie andere Mitgliedstaaten in der DAPIX ist auch Deutschland der Auffassung, dass Artikel 14 insgesamt zu viele Informationen vorsieht.

Es fehlt in Artikel 14 eine risikobasierte Differenzierung. Artikel 14 legt – insoweit weniger flexibel als Artikel 10 und 11 der Richtlinie 95/46/EG – stets die Notwendigkeit einer Information zugrunde. Dies wird der Realität nicht gerecht, wie die in der DAPIX genannten Fälle der „Bäckerei um die Ecke“ und der telefonischen Reservierung eines Tisches im Restaurant gezeigt haben. Hier sollte geprüft werden, wie Ausnahmefälle definiert werden können, in denen die in Artikel 14 geregelte aktive Informationspflicht nicht besteht. Eine solche Ausnahme könnte nicht nur Bürokratiekosten gerade für kleine Betriebe vermeiden. Primäres Ziel der Informationen sollte es sein, dass der Nutzer die Folgen der Datenverarbeitung abschätzen kann.

Es sollte klarer zum Ausdruck gebracht werden, dass die Information der betroffenen Person nach Artikel 14 eine Bringschuld des für die Verarbeitung Verantwortlichen ist. Dabei sollte Artikel 14 allerdings zwischen Basisinformationen, die eine Einschätzung der Datenverarbeitung erlauben, z.B. wie in Artikel 10 und 11 der Richtlinie 95/46/EG die Informationen nach Absatz 1 Buchstabe a und b, und

weiterführenden Datenschutzinformationen unterscheiden. Die Basisinformationen sollten dem Betroffenen in geeigneter Weise direkt zur Verfügung gestellt werden, z.B. durch ein Pop-Up Fenster, am Telefon oder auf einer Postkarte, für weiterführende Datenschutzinformationen sollte der Betroffene auf einen leicht zugänglichen Ort verwiesen werden können, z.B. über eine Verlinkung oder durch Benennung einer Webseite. Dies trägt den unterschiedlichen Verarbeitungssituationen und praktischen Gegebenheiten Rechnung, z.B. im Fall einer Videoüberwachung oder telefonischen Ansprache, einem Bestellschein oder der Displaygröße eines Mobilfunkgerätes. Zu berücksichtigen ist, dass es sich bei der Information nach Artikel 14 regelmäßig nur um standardisierte und nicht individualisierte Informationen handeln kann, da Aufwand und Komplexität sonst zu sehr erhöht würden.

- Absatz 1 Buchstabe a: Die Worte „und des Datenschutzbeauftragten“ sind zu streichen. Die Angaben sind bereits nach Artikel 35 Absatz 9 zu veröffentlichen. Dort sollte zudem geprüft werden, ob eine namentliche Individualisierung tatsächlich notwendig ist oder ob die Angabe der Kontaktdaten ausreichend ist.
- In Absatz 1 Buchstabe b sollte auf die verpflichtende Angabe zu Geschäfts- und allgemeinen Vertragsbedingungen verzichtet werden, jedenfalls soweit diese nicht datenschutzrelevant sind und ihre Einbeziehung anderen (zivilrechtlichen) Vorgaben unterliegt. Zudem sind diese Informationen in aller Regel so lang, dass verschiedene Informationsformen und Wege ausgeschlossen wären bzw. die Information eine Länge erreichte, die vom Betroffenen nicht mehr wahrgenommen oder als reine Förmelei betrachtet wird. Die Angabe des „verfolgten berechtigten Interesses“ sollte gestrichen werden, da sie neben dem Verarbeitungszweck keinen praktischen Informationsmehrwert erzeugt und die Information unnötig verlängert.
- Zu Absatz 1 Buchstabe c haben eine Reihe von Staaten sich in der DAPIX für die Ergänzung der Worte „soweit bekannt“ ausgesprochen. Deutschland stimmt dem zu.
- Bei Absatz 1 Buchstabe d sollte der Begriff „or“ (englisch), in der deutschen Sprachfassung „beziehungsweise“, durch ein „and“ („und“) ersetzt werden, da er fälschlich suggeriert, das Widerspruchsrecht sei eine Alternative zu den übrigen Betroffenenrechten.
- Der Hinweis nach Absatz 1 Buchstabe e zum „Bestehen eines Beschwerderechts bei der Aufsichtsbehörde“ sollte dahin formuliert werden, dass der Betroffene sich entsprechend Artikel 73 Absatz 1 an jede Aufsichtsbehörde wenden kann. Die

weitergehende Information über die Kontaktdaten der jeweils zuständigen Aufsichtsbehörde sollte gestrichen werden.

- Die Information nach Absatz 1 Buchstabe f sollte um die Worte „soweit der Betroffene nach den Umständen des Einzelfalls nicht mit der Übermittlung an diese rechnen muss“ ergänzt werden.
- In Absatz 1 Buchstabe g sollte redaktionell klargestellt werden, dass es um die Übermittlung von Daten an einen Empfänger in einem Drittland geht. Der zweite Satzteil ab dem Wort „sowie“ zum geltenden Datenschutzniveau im Drittland bedarf der weiteren Prüfung. Eine derartige Information kann von einem für die Verarbeitung Verantwortlichen nicht immer geleistet werden.
- Absatz 1 Buchstabe h sollte gestrichen werden. Die Vorschrift ist für eine unmittelbar anwendbare Verordnung zu unbestimmt.
- Über die Folgen der Verweigerung der Daten sollte bei Absatz 2 - vergleichbar Artikel 10 Buchstabe c der Richtlinie 95/46/EG - nur informiert werden, soweit dies nach den Umständen des Einzelfalles erforderlich ist oder der Betroffene dies verlangt. Im Privatrechtsverkehr ist die Information entbehrlich, weil die Folgen in aller Regel selbstverständlich sind, z.B. ein Vertrag kommt nicht zustande oder eine Belieferung ist nicht möglich.
- Die Information sollte nach Absatz 4 Buchstabe b „zum Zeitpunkt der Erhebung der personenbezogenen Daten oder unverzüglich nach der Erhebung“ erfolgen. Es bedarf einer Beschränkung der Information auf die *erstmalige* Verarbeitung. Andernfalls müsste z.B. bei einer Auskunftei die betroffene Person bei jeder Einmeldung und Beauskunftung erneut benachrichtigt werden. Zum Begriff des „Empfängers“ ist klarzustellen, dass Empfänger innerhalb der verantwortlichen Stelle nicht eingeschlossen sind (vergleiche Anmerkung zu Artikel 4).
- Bei Absatz 5 Buchstabe a sollte klargestellt werden, dass die Regelung bereits für die *jeweilige* Information zur Anwendung kommt und nicht nur dann, wenn der Betroffene über alle Informationen verfügt.
- In Absatz 5 Buchstabe b bis d sind die Worte „die Daten werden nicht bei der betroffenen Person erhoben und“ zu streichen. Die Ausnahmen greifen auch bei einer Erhebung beim Betroffenen.
- Es sollte klargestellt werden, dass Absatz 5 Buchstabe b greift, wenn die betroffene Person aufgrund der Verwendung eines Pseudonyms nicht bestimmbar ist („unmöglich“).

- Absatz 5 Buchstabe d sollte - entsprechend Artikel 13 der Richtlinie 95/46/EG - nicht auf Buchstabe f (die Rechte und Freiheiten anderer Personen) des Artikel 21 Absatz 1 beschränkt sein, da insbesondere im öffentlichen Bereich auch die öffentliche Sicherheit entgegenstehen kann.
- In einem Absatz 5 Buchstabe e-neu sollte die Pflicht zur Benachrichtigung ausgeschlossen werden, wenn die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen eines überwiegenden berechtigten Interesses eines Dritten, geheim gehalten werden müssen.
- Absatz 6 ist zu unbestimmt für eine unmittelbar anwendbare Verordnung.
- Zu Absatz 7 und 8 besteht ein Vorbehalt. Die der Kommission eingeräumte Ermächtigung ist sehr weitgehend, z.B. mit Blick auf die Ausgestaltung des Absatz 1 Buchstabe h für verschiedene Bereiche und Verarbeitungssituationen, aber auch umgekehrt mit Blick auf die Ausnahmen von der Information nach Absatz 5. Die Ermächtigung der Kommission in Absatz 8 ist zu streichen, da sie den laufenden Beratungen des Entwurfs einer Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vorgreift. Die Bemerkungen zu Art. 12 Abs. 6 gelten hier analog.

5. zu Artikel 15:

- Das Auskunftsrecht sollte in Absatz 1 „jederzeit“, jedoch „vorbehaltlich Artikel 12 Absatz 4 Satz 2“ verlangt werden können. Es sollte eine Regelung zur Mitwirkung des Betroffenen vorgesehen werden, die Auskunft zu ermöglichen, z.B. durch Angaben zu einer Vertragsbeziehung oder zu einem Kontakt mit der öffentlichen Stelle.
- In Absatz 1 Buchstabe c sollte das Wort „müssen“ gestrichen werden.
- In Absatz 1 Buchstabe d sollten die Worte „soweit bekannt“ ergänzt werden. Es kann vorkommen, dass die konkrete Dauer der Speicherung zum Zeitpunkt der Auskunft nicht oder noch nicht angegeben werden kann.
- Die Auskunft nach Absatz 1 Buchstabe f zum „Bestehen eines Beschwerderechts bei der Aufsichtsbehörde“ sollte dahin formuliert werden, dass der Betroffene sich entsprechend Artikel 73 Absatz 1 an jede Aufsichtsbehörde wenden kann. Die weitergehende Information über die Kontaktdaten der jeweils zuständigen Aufsichtsbehörde sollte gestrichen werden.
- Absatz 1 Buchstabe g: Es sollte klargestellt werden, dass die Herkunft der Daten nicht beauskunftet werden muss, wenn die Erhebung beim Betroffenen erfolgt ist.

- Absatz 1 lit. h: Die Begriffe „Tragweite der Verarbeitung“ und „angestrebten Auswirkungen“ sind unklar. Es sollte entsprechend der Richtlinie 95/46/EG und Erwägungsgrund 51 eine Auskunft zum „logischen Aufbau der Verarbeitung“ oder besser zu „Aufbau, Struktur und Ablauf der Datenverarbeitung“ erfolgen. Die Formulierung „zumindest im Fall der Maßnahmen gemäß Artikel 20“ sollte lauten „zumindest im Fall des Artikel 20“, um auch Fälle der Profilbildung zu erfassen.
- In Bezug auf „Scorewerte“ zur Zahlungsbereitschaft und -fähigkeit sollte ein gesondertes Auskunftsrecht bestehen. Dies sollte im Wesentlichen wie folgt gestaltet sein: Der Verwender des Scorewerts, z.B. eine Bank, sollte Auskunft über die Scorewerte der letzten sechs Monate, die zur Berechnung genutzten Datenarten, das Zustandekommen und die Bedeutung des Scorewertes einzelfallbezogen, nachvollziehbar und in allgemein verständlicher Form erteilen. Soweit der Scorewert oder ein Bestandteil von Dritten berechnet wurde, muss dieser die erforderlichen Angaben zuliefern. Hat der Dritte den Scorewert insgesamt berechnet, kann für die Auskunft an ihn verwiesen werden. Daneben sollte gegenüber dem Dritten ein vergleichbares eigenes Auskunftsrecht bestehen, dass die übermittelten Scorewerte und Empfänger der letzten zwölf Monate, einen aktuell berechneten Scorewert, die genutzte Datenarten, das Zustandekommen und die Bedeutung des Scorewertes umfasst.
- Es sollte entsprechend Erwägungsgrund 51 ergänzt werden, ob und in welchen Fällen die Herkunft der Daten nach Buchstabe g und die Empfänger nach Buchstabe c im Bereich der Wirtschaft ggf. nicht beauskunftet werden müssen, soweit im Einzelfall das Interesse an der Wahrung von Betriebs- oder Geschäftsgeheimnisses das Interesse des Betroffenen an der Information überwiegt. Es sollte – vorbehaltlich eines eigenen Abschnitts für öffentliche Stellen - ergänzt werden, dass eine Pflicht zur Auskunft nicht besteht, wenn
  - im öffentlichen und nicht-öffentlichen Bereich:
    - die Daten nur aufgrund gesetzlicher Aufbewahrungsvorschriften gespeichert sind und die Auskunft einen unverhältnismäßigen Aufwand bedeuten würden,
    - die Daten oder die Tatsache ihrer Speicherung nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen, z.B. bei Rechtsanwälten aufgrund einer Schweigepflicht zugunsten ihres Mandanten,
  - im nicht-öffentlichen Bereich:

- die zuständige öffentliche Stelle gegenüber dem für die Verarbeitung Verantwortlichen festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle eines Mitgliedsstaates Nachteile bereiten würde,
- die Auskunft die Geschäftszwecke des für die Verarbeitung Verantwortlichen erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt,
- die Verarbeitung für Zwecke der wissenschaftlichen Forschung erforderlich ist und die Auskunft einen unverhältnismäßigen Aufwand erfordern würde,
- die Daten aus allgemein zugänglichen Quellen entnommen sind und eine Auskunft wegen der Vielzahl der betroffenen Fälle einen unverhältnismäßigen Aufwand bedeuten würde,

• im öffentlichen Bereich:

- das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Mitgliedstaates Nachteile bereiten würde,
- die Auskunft die ordnungsgemäße Erfüllung der in der Zuständigkeit des für die Verarbeitung Verantwortlichen liegenden Aufgabe gefährden würde es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt.

Für den öffentlichen Bereich sollte ergänzt werden, dass die Ablehnung der Auskunftserteilung keiner Begründung darf, soweit dadurch der mit ihr verfolgte Zweck gefährdet würde. In diesem Fall ist der Betroffene darauf hinzuweisen, dass er sich an die Aufsichtsbehörde wenden kann. Der Aufsichtsbehörde ist die Auskunft auf Verlangen des Betroffenen zu erteilen, soweit nicht im Einzelfall festgestellt wird, dass dadurch die Sicherheit des Mitgliedstaates gefährdet würde. Die Mitteilung der Aufsichtsbehörde an den Betroffenen darf keine Rückschlüsse auf den Erkenntnisstand des für die Verarbeitung Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Mitteilung zustimmt.

- Absatz 2 sollte gestrichen werden. Satz 1 bietet keinen erkennbaren Mehrwert gegenüber Absatz 1 Buchstabe g. Satz 2 ist bereits in Artikel 12 Absatz 2 Satz 4 allgemein geregelt. Die o.a. Bemerkungen gelten hier analog.

- Absatz 3 sollte gestrichen werden. Die Ermächtigung bezieht sich nur auf Einzelheiten der Auskunft nach Absatz 1 Buchstabe g. Eine Regelung zu diesem umgrenzten Inhalt sollte bereits in der Verordnung erfolgen.
- Die Ermächtigung der Kommission in Absatz 4 ist zu streichen, da sie den laufenden Beratungen des Entwurfs einer Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt vorgreift Die Festlegung von Standardvorlagen und -verfahren für die Überprüfung der Identität der betroffenen Person greift sehr weitreichend in technische Standardisierungen auch im öffentlichen Bereich ein (z.B. gibt es in Deutschland etablierte Verfahren zur Identifizierung durch den neuen elektronischen Personalausweis). Auch ist die Frage der sektorspezifischen Regelungen im Rahmen der o.a. Beratungen noch offen. Die Bemerkungen zu Art. 12 Abs. 2 Satz 4 zu Mitteilungen auf elektronischem Wege gelten analog.

6. zu Artikel 16:

Satz 1 sollte mit Blick auf Artikel 5 Buchstabe d nicht von einem Verlangen der betroffenen Person abhängen und lauten:

„Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind.“

Ergänzt werden sollte, dass bestrittene Daten, deren Richtigkeit oder Unrichtigkeit sich nicht feststellen lässt, zu sperren sind. Ergänzt werden sollte auch, dass an die Stelle des Berichtigungsrechts ein Recht auf Gegendarstellung tritt, wenn die personenbezogenen Daten geschäftsmäßig verarbeitet werden, aus allgemein zugänglichen Quellen stammen und zu Dokumentationszwecken gespeichert sind, z.B. Datenbanken mit Presseauswertungen, die durch eine Berichtigung selbst unrichtig würden. Die Daten dürfen nur mit der Gegendarstellung übermittelt werden. Daten nach Artikel 9 sollten allerdings auch in diesen Fällen berichtigt werden.

Satz 2 bedarf weiterer Erörterung. Der Inhalt des Rechts auf Vervollständigung neben dem Berichtigungsrechts bleibt unklar, etwa im öffentlichen Bereich bei einer Verarbeitung auf Grundlage einer Rechtsvorschrift.

7. zu Artikel 17:

Die Ausgestaltung der Löschungspflichten gehört zu den zentralen Punkten des Verordnungsvorschlags. Deutschland unterstützt das Ziel einer Stärkung der Löschungsrechte. Dies gilt insbesondere für selbst ins Internet gestellte Inhalte.

Wie eine Reihe anderer Mitgliedstaaten in der DAPIX sieht auch Deutschland noch weiteren Erörterungsbedarf, inwieweit ein „Recht auf Vergessenwerden“ als Rechtsprinzip eingeführt werden sollte. Insbesondere stellt sich die Frage, welche rechtlichen und praktischen Folgen an den in der Überschrift gewählten Begriff des „Vergessenwerden“ geknüpft werden. Nach den Aussagen der Kommission in der DAPIX sollen nur begrenzte Fallgruppen, vor allem soziale Netzwerke, erfasst werden. Im Regelungstext sollte klar geregelt werden, welche Pflichten generell und welche nur für bestimmte Bereiche gelten sollen. Vor allem mit Blick auf Anwendungen im Internet ist zum Teil bereits unklar, wer nach dem Verordnungsvorschlag als für die Verarbeitung Verantwortlicher und damit als Normadressat gesehen wird, z.B. bei der Veröffentlichung von Daten in einem sozialen Netzwerk: (nur) die veröffentlichende Person oder (auch) der Betreiber des Portals bzw. bei Postings auf der Seite eines Dritten gegebenenfalls auch dieser? Ohne eine eindeutige Klarstellung des Adressaten der Löschungspflichten besteht die Gefahr, dass gerade die zentrale Vorschrift des Artikel 17 gegenüber den Marktteilnehmern, die man im Blick hat, ins Leere läuft.

Des weiteren ist unklar, was „vertretbare Schritte auch technischer Art“ sind. W as ist mit Querverweisen, Kopien und Replikationen, die nach der Information erstellt werden, was passiert, wenn der ursprünglich für die Verarbeitung Verantwortliche nicht mehr existiert, identifiziert oder kontaktiert werden kann? Es bestehen insgesamt Zweifel an der Praktikabilität, vor allem bei Daten, die bereits aus öffentlichen Quellen stammen oder bei denen der Erstveröffentlichende nicht bekannt ist. Unklar ist auch, inwieweit die Regelung für Veröffentlichungen außerhalb des Internets zur Anwendung kommen soll.

Die Systematik des Artikel 17 ist, wie eine Reihe von Mitgliedstaten in der DAPIX hervorgehoben hat, unklar: Absatz 1 enthält ein subjektives Recht des Betroffenen auf Löschung, z.B. in Buchstabe a, wenn die personenbezogenen Daten für den Zweck der Verarbeitung nicht mehr notwendig sind. Es fehlt jedoch eine entsprechende allgemeine Löschungspflicht des für die Verarbeitung Verantwortlichen. Absatz 3 enthält dagegen eine allgemeine Löschungspflicht, selbst wenn die personenbezogenen Daten für den Zweck der Verarbeitung notwendig sind, sofern nicht einer der Buchstaben a bis d greift. Auch das Verhältnis zu den allgemeinen Verarbeitungsgrundsätzen in Artikel 5 und 7 bleibt unklar.

Aus Sicht der Bundesregierung sollte Artikel 17 Absatz 1 und 3 des Verordnungsvorschlags im Ergebnis ersetzt werden durch eine allgemeine Löschungspflicht des für die Verarbeitung Verantwortlichen, unabhängig von einem Verlangen der betroffenen Person, wenn die Speicherung des personenbezogenen Datums unzulässig oder seine Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist. Dies sollte sich auch in der Überschrift widerspiegeln. Die derzeit in Artikel 17 Absatz 3 a bis d geregelten Ausnahmen sollten dabei inhaltlich sichergestellt sein.

Zu Absatz 1 und 3:

- Absatz 1 sieht ein Recht auf Löschung und auf Unterlassung der weiteren Verbreitung vor. Es bleibt unklar, wie eine solche Unterlassung der weiteren Verbreitung nach bzw. neben einer Löschung aussehen soll und weshalb das Unterlassen sich nur auf das Verbreiten und nicht die weitere Verarbeitung bezieht.

  Deutschland unterstützt Bemühungen um einen verstärkten Schutz für Kinder. Allerdings ist die Bezugnahme „speziell“ auf im Kindesalter öffentlich gemachte Daten unsystematisch. Besteht das Recht auf Löschung und Unterlassung der Verbreitung uneingeschränkt, kann dies systematisch nicht „speziell“ für im Kindesalter öffentlich gemachte Daten gelten. Sprachlich bedeutet dies eine graduelle Entwertung des Löschungsrechts in anderen Fällen und sollte daher gestrichen und an anderer Stelle, z.B. im Zusammenhang mit der Veröffentlichung, im Rahmen einer Interessenabwägung bei Artikel 19 oder in einem eigenen Absatz, geregelt werden.

- Buchstabe b 2. Alternative sieht indirekt vor, dass eine Einwilligung befristet erteilt werden kann. Dies wäre in Artikel 7 zu regeln. Die gewählte Formulierung („Ablauf der Speicherfrist der Einwilligung“) bringt die Befristungsmöglichkeit auch nur unzureichend zum Ausdruck. Der Widerruf erfolgt ex nunc und darf durch eine Löschung der personenbezogengen Daten keine Wirkung ex tunc erlangen. Dies stünde im Widerspruch zu Artikel 7 Absatz 3 Satz 2.

- Buchstabe c ist missverständlich formuliert, weil ein Löschungsanspruch nicht mit dem Einlegen eines Widerspruchs nach Artikel 19 einher geht, sondern nur, sofern dessen materiellen Tatbestandsvoraussetzungen zur Unzulässigkeit der Datenverarbeitung führen. Zudem darf die Möglichkeit einer Sperrung statt Löschung nicht ausgeschlossen werden. Ziel eines z.B. Werbewiderspruchs ist die Unterbindung der weiteren (Adress-)Datenverarbeitung. Um dies sicherzustellen, dürfen die Daten gerade nicht gelöscht, sondern müssen in

Bezug auf Werbezwecke gesperrt werden können (vergleiche Anmerkung zu Artikel 19 Absatz 3).

- Buchstabe d, die Unvereinbarkeit aus anderen Gründen, ist zu weitgehend. Wenn im Umkehrschluss zu Buchstaben a bis c die personenbezogenen Daten für den Verarbeitungszweck notwendig sind, eine Einwilligung oder anderweitige Rechtsgrundlage besteht und der Betroffene auch nicht widersprochen hat, können andere Gründe, z.B. ein Verstoß gegen formale Pflichten, nicht pauschal einen Löschungsanspruch begründen.

Zu Absatz 4 bis 6:

- Das Konzept des „Sperrens“ sollte in der Verordnung verankert werden. „Sperren“ sollte in Artikel 4 definiert werden, z.B. als „ *das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung einzuschränken*“. Der für die Verarbeitung Verantwortliche sollte bei Vorliegen der Voraussetzungen zur Sperrung verpflichtet sein, was nach der deutschen Sprachfassung nicht der Fall ist („kann“). Unklar ist, wie eine Beschränkung oder Sperrung bei bereits veröffentlichen Daten erfolgen soll.
- Bei Buchstabe a sollte berücksichtigt werden, dass die Richtigkeit oder Unrichtigkeit sich gegebenenfalls nicht feststellen lässt.
- Bei Buchstabe b sollte eine Sperrung erfolgen, wenn die Daten für den Zweck der Speicherung nicht mehr erforderlich sind, der Löschung aber gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen. Eine hierüber hinausgehende Speicherung zu bloßen Beweiszwecken würde mit Blick auf etwaige künftige Streitverfahren „auf Vorrat“ geschehen und sollte nicht möglich sein.
- Buchstabe c erscheint als ein seltener Spezialfall. Geregelt werden sollte allgemein eine Sperrpflicht, wenn Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden.
- Buchstabe d ist nicht immer ein Fall der Sperrung. Nicht immer wollen Nutzer einen Dienst vollständig wechseln. Wenn der Wechsel zur Sperrung führt, würde ein neues Wechselhindernis geschaffen, wenn ein Nutzer zunächst einmal einen neuen Dienst ausprobieren will oder zwei Dienste parallel nutzen möchte.
- Neu geregelt werden sollte, dass eine Sperrung erfolgt, wenn eine Löschung wegen der besonderen Art der Speicherung (z.B. WORM-Systeme, Papierakten) nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

- Eine Verarbeitung gesperrter Daten sollte ohne Einwilligung der betroffenen Person nach Absatz 5 nur zulässig sein, wenn es zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot oder aus sonstigen im überwiegenden Interesse des für die Verarbeitung Verantwortlichen oder eines Dritten liegenden Gründen unerlässlich ist und die Daten hierfür verarbeitet werden dürften, wenn sie nicht gesperrt wären. Es sollten zumindest die Anforderungen erfüllt sein, die an eine Verarbeitung gestellt worden wären, wenn die Daten nicht gesperrt gewesen wären.
- Absatz 6 setzt voraus, dass eine Aufhebung der Sperrung grundsätzlich möglich ist. Dies sollte in der Verordnung klargestellt, und es sollten zulässige Fälle benannt werden, z.B. wenn nach einer Unklarheit über die Richtigkeit der Daten deren Richtigkeit belegt ist.

Zu Absatz 7 bis 9:

- Absatz 7 wird unterstützt, ist jedoch eine Querschnittsregelung, die wie Artikel 5 des Rahmenbeschlusses 2008/977/JI für öffentliche Stellen als eigener Artikel gestaltet werden sollte.
- Absatz 8 sollte gestrichen werden. Nach der Löschung stehen die Daten für eine Verarbeitung in sonstiger Weise nicht mehr zur Verfügung, so dass die Regelung überflüssig erscheint. Ggf. könnte eine entsprechende Klarstellung auch in einem Erwägungsgrund erfolgen. Eine Definition des Löschens sollte aufgrund der unmittelbaren Anwendbarkeit der Verordnung in Artikel 4 vorgenommen werden, z.B. als „*das Unkenntlichmachen gespeicherter personenbezogener Daten*“.
- Zu Absatz 9 besteht ein Vorbehalt. Die Ermächtigung der Kommission ist sehr weitgehend und zudem unbestimmt formuliert. Regelungen zur Löschungspflicht oder Beschränkung der Verarbeitung wirken unmittelbar auf die Möglichkeiten einer zulässigen Datenverarbeitung ein. Eine Regelung sollte in der Verordnung getroffen oder den Mitgliedstaaten eingeräumt werden.

8. zu Artikel 18:

Wie eine Reihe anderer Mitgliedstaaten in der DAPIX sieht auch Deutschland bezüglich Anwendungsbereich und Umsetzbarkeit des Artikel 18 weiterhin starken Erörterungsbedarf. Es stellt sich die Frage, ob es sich beim Recht auf Datenübertragbarkeit um eine datenschutzrechtliche oder nicht vielmehr um eine wettbewerbs- oder urheberrechtliche Frage handelt. Die Vorschrift trifft eine sehr spezifische Regelung, die z.B. bei sozialen Netzwerken, Cloud- oder E-Mail-Diensten eine Berechtigung hat, als generelle Regelung jedoch unangemessen erscheint, z.B.

auch mit Blick auf die Anwendbarkeit im öffentlichen Bereich, im Gesundheitsbereich, im Forschungsbereich oder bei Privatpersonen. Im öffentlichen Bereich können hochrangige öffentliche Interessen bestehen, die einer Kopie über die verarbeiteten Daten entgegenstehen. Im Bereich der Wirtschaft kann die Vorschrift Probleme mit sich bringen, z.B. wenn der Betroffene mit seiner Einkaufshistorie zu einem konkurrierenden (Online-) Händler oder mit seinen Kundendaten zu einer konkurrierenden Bank wechselt und mit der Herausgabe einer Kopie des Datensatzes geschützte Unternehmenspositionen oder Betriebs- und Geschäftsgeheimnisse offen gelegt werden müssten. Gerade im Online-Handel könnte die Regelung sogar neue Gefahren für den Datenschutz schaffen, wenn Unternehmen bei Neukunden Anreize dafür schaffen würden, ihnen die Kundenhistorie aus anderen Geschäftsbeziehungen zur Verfügung zu stellen. Betroffen sein dürften oft auch die personenbezogenen Daten anderer Personen (z.B. Empfänger einer Überweisung oder E-Mail, Lieferant einer Ware, Freunde auf Facebook). Zusätzliche datenschutzrechtliche Risiken entstehen, wenn der Anbieter, zu dem die betroffene Person personenbezogene Daten auch anderer Personen überführt, niedrigeren datenschutzrechtlichen Vorschriften oder Anforderungen unterliegt, etwa in einem Drittland. Zusätzliche datenschutzrechtliche Risiken können auch dadurch hervorgerufen werden, dass der für die Verarbeitung Verantwortliche, um Artikel 18 nachzukommen, dezentral verarbeitete Daten an einer Stelle zusammenführen muss. Die Umsetzung der Vorschrift wäre technisch anspruchsvoll und birgt die Gefahr erheblicher neuer bürokratischer Belastungen.

- Unklar ist, was in Absatz 1 mit einer „elektronischen Verarbeitung“ in Abgrenzung zur „automatisierten Verarbeitung“ gemeint ist.

  Der Begriff des „strukturierten gängigen elektronischen Formats“ ist unklar. Es ist nicht erkennbar, warum ein „Recht“ des Betroffenen von einer rein technischen Gestaltung abhängig sein soll. Unklar ist, wer bestimmt, wann ein Format „gängig“ ist. Ein in bestimmten Bereichen „gängiges Format“ kann in anderen Bereichen oder Staaten nicht verbreitet sein. Im Gesundheitsbereich etwa sind gängige Formate häufig nicht für eine weitere Bearbeitung durch die betroffene Person geeignet und eine Umstrukturierung ist nicht immer möglich. Unklar ist auch das Kriterium „strukturiert“. Bezugspunkt sind hier eher die Daten als das Format.

  Unklar ist die Anforderung, dass die betroffene Person die Daten in einem „von ihr weiter verwendbaren … Format“ verlangen kann. Für den für die Verarbeitung Verantwortlichen ist nicht erkennbar, welches Format die betroffene Person weiter verwenden kann. Es bleibt auch offen, was „weiter verwenden“ bedeutet,

ob dies z.B. eine automatisierte Verarbeitung verlangt oder die Möglichkeit eines Ausdrucks und weiteren Verwendung im Papier-Format genügt. Generell hängt die weitere Verwendung von ungewissen Faktoren und Vorgaben anderer Stellen ab. Insofern sollte hier ein objektiver Maßstab angelegt werden, z.B. indem man auf ein „üblicherweise elektronisch weiter verwendbares Format“ abstellt.

- In Absatz 2 erscheint es mit Blick auf das Schutzziel nicht konsistent, ein solches Recht nur zu gewähren, wenn die Verarbeitung auf einer Einwilligung oder einem Vertrag basiert und die betroffene Person die Daten zur Verfügung gestellt hat. Was bedeutet letzteres z.B. mit Blick auf das soziale Netzwerke, Cloud- oder E-Mail-Dienste, wenn der Diensteanwender dem Diensteanbieter personenbezogene Daten zur Verfügung stellt, die (auch) andere Personen betreffen (Freunde, Kunden, Empfänger). Des weiteren sollte auf den Begriff „entzogen“ verzichtet werden, da dieser zum einen unklar ist und zum anderen die Übertragung auch möglich sein sollte, wenn die betroffene Person den alten und den neuen Dienst nutzen möchte, die Daten also gerade nicht entziehen will.

  Unklar sind die Rechtsfolgen, z.B. wenn der für die Verarbeitung Verantwortliche auch nach Geltendmachung des Rechts nach Absatz 2 aufgrund eines Erlaubnistatbestandes berechtigt ist, die personenbezogenen Daten zu verarbeiten. Die Ausübung des Rechts nach Absatz 2 darf i.V.m. Artikel 17 Absatz 4 Buchstabe d und Absatz 5 dem für die Verarbeitung Verantwortlichen die weitere Vertragserfüllung nicht unmöglich machen.

  Unklar ist, was mit „etwaigen sonstigen von ihr zur Verfügung gestellten Informationen“ gemeint ist. Sollten hiermit auch nicht personenbezogene Daten gemeint sein, bestünden Zweifel an der Reichweite des Artikel 16 AEUV.

  Unklar ist, inwieweit der für das Empfängersystem für die Verarbeitung Verantwortliche verpflichtet ist, an der Überführung der Daten mitzuwirken, und inwieweit der für die Verarbeitung Veranwortliche des Ausgangssystems den Entzug der Daten „behindert“, wenn er an der Überführung lediglich nicht mitwirkt, z.B. keine Export-Funktion vorsieht.

- Zu Absatz 3 besteht ein Vorbehalt. Der Regelungsgehalt ist wesentlich. Erst durch die delegierten Rechtsakte würden der Anwendungsbereich und die Umsetzung der in den Absätzen 1 und 2 aufgestellten Anforderungen für die betroffenen Rechtsanwender präzise bestimmt. Eine solche Regelung sollte soweit wie möglich in der Verordnung selbst erfolgen. Berührt wären auch technische Standards und Verfahren, die bestehende Formate und Infrastruktur in den Mitgliedstaaten berühren. Soweit die Kommission festlegen könnte, in

welchem Format ein für die Verarbeitung Verantwortlicher personenbezogene Daten vorhalten muss, wäre dies ein Eingriff in den Geschäftsbetrieb und grundrechtsrelevant.

9. zu Artikel 19:

Deutschland begrüßt die Aufnahme einer Regelung zum Widerspruchsrecht, hat jedoch einen Prüfvorbehalt zu der Formulierung der Regelung. Artikel 19 weist gegenüber Artikel 14 der Richtlinie 95/46/EG einige Änderungen auf:

- Die Formulierung der Abwägung in Absatz 1 weicht von der Formulierung der Abwägung in Artikel 6 Absatz 1 Buchstabe f ab, anders als in der Richtlinie 95/46/EG der Artikel 14 Buchstabe a von Artikel 7 Buchstabe f. Bislang muss der Betroffene „überwiegende, schutzwürdige, sich aus seiner besonderen Situation ergebende Gründe“ angeben, um eine rechtmäßige Datenverarbeitung mit seinem Widerspruch zu unterbinden. Künftig genügen „Gründe, die sich aus seiner besonderen Situation ergeben“, während die verarbeitende Stelle nun überwiegende, zwingende schutzwürdige Gründe für die Verarbeitung nachweisen muss.

  Beim Widerspruchsrecht ist auf eine Differenzierung zwischen dem nicht-öffentlichen und dem öffentlichen Bereich zu achten,

  Statt von „schutzwürdigen Gründen für die Verarbeitung“ zu sprechen, sollte - wie in Erwägungsgrund 56 und 38 - von „berechtigten Interessen für die Verarbeitung“ gesprochen werden.

  Unklar ist, welche zusätzlichen Anforderungen sich aus dem Begriff „zwingende“ Gründe ergeben, ob es also nicht genügt, dass die Gründe für die Verarbeitung überwiegen, sofern sie nicht auch „zwingend“ sind. Erwägungsgrund 56 nennt dieses Kriterium nicht. Das Wort „zwingende“ sollte daher gestrichen werden.

  Ein Widerspruchsrecht sollte im öffentlichen und nicht-öffentlichen Bereich dann nicht bestehen, wenn eine Rechtsvorschrift zur Verarbeitung verpflichet.

- Deutschland sieht Klärungsbedarf beim Verhältnis von Artikel 19 Absatz 2 zu Artikel 6 Absatz 1 Buchstabe f und Artikel 6 Absatz 4. Das Widerspruchsrecht lässt darauf schließen, dass Direktwerbung ohne Einwilligung auf Grundlage einer Interessenabwägung möglich ist. Dem steht entgegen, dass Artikel 6 Absatz 1 Buchstabe f die Interessen Dritter nicht mehr nennt und dass auch Artikel 6 Absatz 4 für zweckändernde Datenverarbeitungen nicht mehr auf Artikel 6 Absatz 1 Buchstabe f verweist. Klärungsbedarf besteht insoweit auch mit Blick

auf Online-Werbung und die Richtlinie 2002/58/EG bzw. Artikel 89 des Verordnungsvorschlags.

Die Unentgeltlichkeit des Widerspruchs in Absatz 2 Satz 1 ergibt sich aus der horizontalen Regelung in Artikel 12 Absatz 4 Satz 1 und kann hier gestrichen werden. Satz 2 kann mit Blick auf Artikel 11 Absatz 2 ebenfalls gestrichen werden.

Soweit in Satz 2 als neues Erfordernis gegenüber Artikel 14 der Richtlinie 95/46/EG eine Information über den Werbewiderspruch in „von anderen Informationen klar abgegrenzten Form“ verlangt wird, stößt dies aus Platzgründen (Bsp.: Postkarte) und aufgrund weiterer zivil- und verbraucherrechtlicher Informationen, die abgesetzt werden sollen, an gestalterische Grenzen.

Der Zeitpunkt der Information über den Werbewiderspruch ist – anders als in Richtlinie 95/46/EG – nicht mehr gesondert geregelt. Dem insoweit maßgeblichen Artikel 14 Absatz 4 Buchstabe b i.V.m. Absatz 1 Buchstabe d fehlt allerdings die zu ergänzende Möglichkeit nach Artikel 14 Buchstabe b der Richtlinie 95/46/EG, „vor der erstmaligen Nutzung im Auftrag Dritter zu Zwecken der Direktwerbung informiert zu werden“.

Der zugehörige Erwägungsgrund 57 bedarf der Anpassung, da dort nur von Direktwerbung für „nichtkommerzielle Zwecke“ die Rede ist.

– Absatz 3 ist mit Blick auf Artikel 17 Absatz 1 Buchstabe c und Absatz 4 Buchstabe c unklar, da dort bereits eine Löschung bzw. Sperrung vorgesehen ist.

  Absatz 3 ist auch missverständlich formuliert. Werden Daten zum Zweck einer Vertragserfüllung erhoben und zudem für Werbezwecke verwendet und widerspricht die betroffene Person dieser Verwendung, so wäre es nicht im Interesse des Widersprechenden, wenn seine Daten auch nicht mehr für die Vertragserfüllung verarbeitet werden könnten. Folge des Widerspruchs sollte nur sein, dass die Verarbeitung zum Zweck der Direktwerbung nicht mehr möglich ist. Es ist auch zu berücksichtigen, dass, um den Werbewiderspruch beachten zu können, die Daten des Widersprechenden in der Praxis weiter genutzt werden müssen, um sie aus Adressbeständen für Direktmarketingmaßnahmen herauszufiltern. Absatz 3 bedarf daher einer entsprechenen Klarstellung.

10. zu Artikel 20:

Die Bundesregierung unterstützt eine Regelung zum Profiling. Dabei müssen zwei Aspekte berücksichtigt werden, nämlich

- zum einen, ob und unter welchen Voraussetzungen ein Profil im Sinne einer Verknüpfung von Daten, die eine besondere Aussagekraft über die Persönlichkeit des Betroffenen erlaubt, gebildet und weiterverarbeitet werden darf und
- unter welchen Bedingungen eine hierauf basierende ausschließlich automatisierte Maßnahme, die einen besonderen Nachteil für den Betroffenen hat, zulässig ist.

Es erscheint sinnvoll, hierfür zwei unterschiedliche Regelungen vorzusehen. Artikel 20 erfasst in Fortführung der Regelung zur automatisierten Einzelentscheidung in Artikel 15 der Richtlinie 95/46/EG im Wesentlichen nur den zweiten Aspekt.

Die Bundesregierung wünscht insbesondere eine Profilbildungsregelung zu Verfahren zur Berechnung der Wahrscheinlichkeit eines bestimmten Verhaltens, wie sie etwa § 28b des Bundesdatenschutzgesetzes vorsieht. Dort wird insbesondere verlangt, dass ein wissenschaftlich anerkanntes mathematisch-statistisches Verfahren zugrunde liegt, das nachweisbar für die Wahrscheinlichkeit des bestimmten Verhaltens erheblich ist.

Der Begriff des Profils und der Profilbildung, gegebenenfalls auch mit Blick auf eine Differenzierung nach Datenkategorien (z.B. allgemein zugängliche Daten, sensible Daten), bedarf noch weiterer Klärung und Ausgestaltung. Daten nach Art. 9 sollten nur in sehr engen Grenzen zur Profilbildung verwendbar sein. Eine Definition in Artikel 4 könnte mehr Rechtssicherheit bringen. Dabei ist auch die Europaratsempfehlung CM/Rec(2010)13 vom 23. November 2010 einzubeziehen.

Es sollten privilegierende Regelungen zum Umgang mit pseudonymen Profilen getroffen werden, z.B. zur Erstellung von ausschließlich pseudonymen Nutzungsprofilen durch Telemedienanbieter für Zwecke der Werbung, der Marktforschung oder zur bedarfgerechten Gestaltung der Telemedien, sofern der Nutzer nicht widerspricht. Über das Widerspruchsrecht ist der Nutzer zu informieren.

– In Absatz 1 sollten die Worte „Eine natürliche Person“, wie bei den anderen Rechten der betroffenen Person in Artikel 15 bis 19, durch die Worte „Die betroffene Person“ ersetzt werden.

Es sollte klargestellt werden, dass die Vorschrift auf die automatisierte Verarbeitung von „personenbezogenen Daten“ beschränkt sein soll (vergleiche Artikel 4 Absatz 3 und Artikel 9 des Richtlinienvorschlags KOM(2012) 10 endg.).

Unklar bleibt, wann eine Maßnahme die betroffene Person „in maßgeblicher Weise beeinträchtigt“ (nach der Richtlinie 95/46/EG: erheblich beeinträchtigt). Um die Voraussetzung eines Nachteils bei der betroffenen Person deutlicher zum Ausdruck zu bringen, sollte Absatz 1 Maßnahmen erfassen, die gegenüber der betroffenen Person „nachteilige rechtliche Folgen“ entfalten (vergleiche Artikel 7 des Rahmenbeschlusses 2008/977/JI) oder die betroffene Person „in vergleichbarer Weise erheblich beeinträchtigen können“. In einem Erwägungsgrund sollten hierzu Beispiele benannt werden.

Die Worte „oder in der Analyse bzw. Voraussage“ sollten gestrichen werden, da sie dem Tatbestandsmerkmal der „Auswertung“ bzw. in der Übersetzung der Richtlinie 95/46/EG „Bewertung“ entsprechen. Klarzustellen ist beim Begriff „Aufenthaltsort“ die Ortsgenauigkeit, ob also bereits das Land als Aufenthaltsort genügt, was z.B. bei der Geolokalisation von IP-Adressen bedeutsam wäre.

Es sollte klargestellt werden, wann von einer „ausschließlich automatisierten Verarbeitung“ auszugehen ist, etwa durch die Formulierung: „… insbesondere dann, wenn keine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine natürliche Person stattgefunden hat“.

– Es ist unklar welche spezifischen Anforderungen sich aus dem Wort „ausdrücklich in Absatz 2 Buchstabe b für den Gesetzgeber ergeben. Nach nationalem und EU-Recht wird etwa von Banken und Versicherungen ein angemessenes Risikomanagement oder eine Prüfung der Kreditwürdigkeit von Verbrauchern verlangt (siehe etwa § 10 Kreditwesengesetz, Artikel 44 der Richtlinie 2009/138/EG „Solvency II“, Artikel 8 der Richtlinie 2008/48/EG „Verbraucherkreditrichtlinie“), ohne dass klar ist, ob damit eine Verarbeitung, wie sie in Artikel 20 Absatz 1 vorgesehen ist, „ausdrücklich“ gestattet wird.

  Bei Buchstabe c sind die Worte „und vorbehaltlich entsprechender Garantien“ zu streichen, da diese Formulierung Rechtsunsicherheiten begründet und sich die allgemeinen Pflichten z.B. zu Datensicherheit und Zweckbindung bereits aus anderen Vorschriften ergeben.

– Das Verbot der Profilbildung von „ausschließlich“ personenbezogenen Daten nach Artikel 9 in Absatz 3 erscheint nicht sinnvoll.

  Das Merkmal „ausschließlich“ kann leicht umgangen werden, indem neben den Daten nach Artikel 9 ein weiteres Datum in das Profil einfließt. Im Werbebereich

könnte dies z.B. eine Altersgruppe oder das Geschlecht der betroffenen Person sein. Auch die Verknüpfung mit dem Namen oder der Anschrift der betroffenen Person würde das Verbot nach Absatz 3 aufheben, obwohl das Gefahrenpotential eher zunähme.

Ausschließlich auf Daten nach Artikel 9 gestützte Profile sollten auch nicht in jedem Fall verboten sein. Derartige Profile können beispielsweise im Bereich der Forschung erforderlich sein. In Bezug auf öffentlich zugängliche Daten und etwa politische Meinungen sind gegenläufige Grundrechte (z.B. Meinungsfreiheit, Informationsfreiheit, Forschungsfreiheit, Religionsfreiheit) angemessen zu berücksichtigen. Allerdings sollten an die Einbeziehung von Daten nach Artikel 9 in ein Profil und auch an die Qualität der Auswerteverfahren, die Transparenz und die Regeln zur Verwendung der Ergebnisse spezifische Anforderungen gestellt werden.

Nach Erwägungsgrund 58 sollen Kinder von auf Profilbildung beruhenden Maßnahmen generell ausgeschlossen sein. Dies findet keine Entsprechung im Regelungstext des Artikel 20 und bleibt daher unklar. Es wirft zudem – wie an anderen Stellen, an denen spezifische Maßnahmen zum Schutz von Kindern vorgesehen sind – die Frage auf, wie eine Altersverifikation vorgenommen werden soll und welcher Aufwand hiermit verbunden ist (Bsp.: Suchmaschine, Webstatistiken).

- Bei Absatz 4 sollte - entsprechend den Ausführungen zu Artikel 14 - die Information über die Existenz einer profilbildenden Verarbeitung dem Betroffenen als Basisinformation in geeigneter Weise direkt zur Verfügung gestellt werden. Die Formulierung „die angestrebten Auswirkungen auf die betroffene Person“ sollte entsprechend der Regelung in Artikel 15 Absatz 1 Buchstabe h ersetzt werden. Dabei handelt es sich - entsprechend den Ausführungen zu Artikel 14 - um eine weiterführende Datenschutzinformation, bei der der Betroffene auf einen leicht zugänglichen Ort verwiesen werden kann.
- Zu Absatz 5 besteht ein Vorbehalt. Es handelt sich um eine wesentliche Regelung, die in der Verordnung selbst geregelt werden sollte. Absatz 2 Buchstabe a nennt ein Beispiel für geeignete Maßnahmen. Artikel 15 der Richtlinie nennt mit der Möglichkeit, seinen Standpunkt geltend zu machen, ein weiteres Beispiel. Bei Absatz 5 besteht zumindest die Gefahr der Kollision mit der in Beratung befindlichen Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt.

11. zu Artikel 21:

- Absatz 1 sollte nicht nur Beschränkungen von Rechten der betroffenen Personen zulassen, sondern auch deren Erweiterung. So verlangt etwa Artikel 20 Absatz 2 Buchstabe b von den Mitgliedstaaten „geeignete Maßnahmen zur Wahrung der berechtigten Interessen der betroffenen Person“, die etwa in Form erweiterter Auskunftsrechte, wie sie das deutsche Recht bei der Profilbildung zur Einschätzung der Kreditwürdigkeit (Scoring) vorsieht, über den Verordnungsvorschlag hinausgehen. Die Mitgliedstaaten benötigen auch mit Blick auf Artikel 6 Absatz 3 Spielräume, gerade im öffentlichen Bereich oder etwa im Gesundheitsbereich, zur näheren Konkretisierung und Ausgestaltung von Regelungen (insbesondere bei der Zweckbindung, der Art der Daten und der Empfänger) und zum Erlass strengerer Regelungen.

  Die Möglichkeit, auch die Prinzipien der Datenverarbeitung nach Artikel 5 Buchstabe a bis e einzuschränken, bedarf weiterer Erörterung. Unklar ist z.B., wie eine Einschränkung des Prinzips, Daten auf rechtmäßige Weise zu verarbeiten (Artikel 5 Buchstabe a), aussehen soll, zumal eine Einschränkung der Rechtmäßigkeit der Verarbeitung in Artikel 6 nicht vorgesehen ist. Unklar ist auch, weshalb Artikel 5 Buchstabe f von Einschränkungen ausgenommen ist.

  Es sollten in neuen Buchstaben, wie in Artikel 13 Absatz 1 der Richtlinie 95/46/EG die „Sicherheit des Staates“ und die „Landesverteidigung“ aufgenommen werden.

  Die in Buchstabe c geregelte Möglichkeit der Beschränkung von Rechten der betroffenen Personen „zum Schutz sonstiger öffentlicher Interessen der Union oder eines Mitgliedstaates“ ist in der Richtline 95/46/EG nicht vorgesehen. Vielmehr ist die vergleichbare Ausnahmeregelung in Art. 13 Abs. 1 Buchstabe e der Richtlinie 95/46/EG auf „ein wichtiges wirtschaftliches oder finanzielles Interesse eines Mitgliedstaats oder der Europäischen Union“ beschränkt. Hierzu hat Deutschland weiteren Prüfungsbedarf.

  Ein neuer Buchstabe oder eine Regelung in Artikel 10 sollte Einschränkungen auch bei der Verwendung pseudonymisierter Daten zulassen.

  Es sollte klargestellt werden, was bei Buchstabe f mit den Rechten und Freiheiten anderer Personen gemeint ist, z.B. der Schutz der Meinungsfreiheit, Geschäftsgeheimnisse oder Eigentumsrechte eines Dritten.

  Es sollte klargestellt werden, dass mitgliedstaatliche Regelungen nach Artikel 21, insbesondere nach Buchstabe f zum Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen mit Artikel 1 Absatz 3 vereinbar sind,

der Einschränkungen des freien Datenverkehrs aus Gründen des Schutzes natürlicher Personen gerade verbietet.

- In Absatz 2 sollte vom „Zweck der Verarbeitung“ gesprochen werden.

12. zu Artikel 22:

Artikel 22 gilt für alle für die Verarbeitung Verantwortlichen, seien es öffentliche Stellen, die „Bäckerei um die Ecke“ oder eine Privatperson, die nach Artikel 2 Absatz 2 Buchstabe d unter die Datenschutz-Grundverordnung fällt. Eine Differenzierung nach der Gefahrgeneigtheit der Datenverarbeitung oder nach Verantwortungsbereichen (z.B. im Verhältnis Anbieter und Nutzer) erfolgt nicht. Daher und aufgrund der Bußgeldbewehrung nach Artikel 79 Absatz 6 Buchstabe e sollte konkretisiert werden, was von den Normadressaten bei den „geeigneten Strategien und Maßnahmen“ erwartet wird, welche Anforderungen an den Nachweis gestellt werden, wem gegenüber und in welcher Form er zu erbringen ist. Etwa für den Gesundheitsbereich bedarf die Regelung im Hinblick auf besondere Verfahren ggf. der Anpassung (vgl. auch Stellungnahme zu Artikel 4)

- Der einleitende Satz von Absatz 2 sollte deutlicher machen, dass die Maßnahmen nach Buchstabe a bis e nur getroffen werden müssen, wenn die in dem jeweiligen Artikel vorgesehen Voraussetzungen erfüllt sind. So müssen z.B. die Maßnahmen nach Buchstabe a und e nicht durch KMU vorgenommen werden, sofern deren Tätigkeit nicht mit besonderen Gefahren in Bezug auf den Datenschutz verbunden sind.
- Es sollte zu Absatz 3 klargestellt werden, was „geeigneten Verfahren zur Überprüfung“ sind, z.B. mit Blick auf Absatz 2 Buchstabe e.

  Die Überprüfung der Wirksamkeit nach Satz 1 sollte angesichts der Breite der Normadressaten und der fehlenden Risikobasiertheit – wie in Satz 2 vorgesehen – nur verlangt werden, „wenn dies angemessen ist“. Es sollte auch konkretisiert werden, unter welchen Umständen eine Überprüfung „angemessen“ ist. Diese Einschränkung wäre allerdings entbehrlich, wenn der Anwendungsbereich auf besonders risikobehaftete Datenverarbeitungen oder auf das Verhältnis Anbieter-Nutzer beschränkt würde.

  Es bedarf der Klarstellung, was mit der „Unabhängigkeit“ der Prüfer gemeint ist, z.B. wenn diese gegen Entgelt tätig werden. Das Kriterium sollte die Einschaltung interner Stellen, wie der Revisions- oder Compliance-Abteilung, nicht ausschließen. Konkretisiert werden sollte auch das Verhältnis der

unabhängigen Prüfer zu den innerbehördlichen und -betrieblichen Datenschutzbeauftragten und deren Einbindung in die Überprüfung.

Es sollte klargestellt werden, dass der Prüfer nur eine Stellungnahme abgibt, die Entscheidung über die Maßnahme und deren Wirksamkeit aber dem für die Verarbeitung Verantwortlichen obliegt. Zudem sollte klargestellt werden, dass die für die Verarbeitung Verantwortlichen das Ergebnis der Überprüfung veröffentlichen können.

- Zu Absatz 4 besteht ein Vorbehalt. Es handelt sich um eine wesentliche Regelung, insbesondere soweit der Katalog der Maßnahmen nach Absatz 2 erweitert werden kann und soweit die Bedingungen für die Überprüfungs- und Auditverfahren festgelegt werden sollen.

13. zu Artikel 23:

Deutschland begrüßt die Aufnahme einer Regelung zum Datenschutz durch Technik (by design) und durch Voreinstellungen (by default), wünscht sich aber – im Bewußtsein der Notwendigkeit von Technologieneutralität, aber auch der Bußgeldbewehrung in Artikel 79 Absatz 6 Buchstabe e – genauere Vorgaben und Ziele für die Technikgestaltung und die Voreinstellungen in die Absätze 1 und 2 aufzunehmen. Z.B. sollte mit Blick auf Artikel 5 Buchstabe c der Grundsatz der Datensparsamkeit und -vermeidung sowie die Anonymisierung und Pseudonymisierung als zentrale Möglichkeit der Umsetzung aufgeführt werden. Die Notwendigkeit der Konkretisierung besteht auch, soweit Artikel 23 Anforderungen an den für die Verarbeitung Verantwortlichen stellt, die über die in Artikel 6 festgelegten Voraussetzungen einer rechtmäßigen Datenverarbeitung hinausgehen.

Zum Normadressaten der Absätze 1 und 2 sieht die Bundesregierung noch Erörterungsbedarf. Es sollten rechtliche Anreizen dafür geschaffen werden, dass auch die Technikentwickler und Hersteller ihre Produkte und Dienstleistungen datenschutzkonform gestalten.

- Bei Absatz 1 sollten – wie bei Artikel 30 – nur „angemessene“ Maßnahmen vorgesehen werden. Bezugspunkt der Angemessenheit sollte auch das mit der Datenverarbeitung verbundene Gefährdungspotential sein.

  Vor den Worten „und die Rechte der betroffenen Person gewahrt werden“ sollte das Wort „insbesondere“ eingefügt werden.

- Notwendig erscheinen auch bei Absatz 2 konkretere Anforderungen an die Voreinstellungen, z.B. ob zunächst die höchste Sicherheitseinstellung

einzustellen ist oder unter welchen Voraussetzungen die betroffene Person die Voreinstellungen ändern kann.

Unklar bleibt die Anwendung insbesondere des Satzes 2 auf natürliche Personen als für die Verarbeitung Verantwortliche nach Artikel 2 Absatz 2 Buchstabe d, z.B. bei der Gestaltung einer Webseite oder beim Bloggen.

In der deutschen Sprachfassung müssen in Absatz 2 Satz 1 und 2 die Wörter „durch Voreinstellung“ (in der englischen Fassung „by default“) ergänzt werden.

– Zu Absatz 3 und 4 besteht ein Vorbehalt. Es handelt es sich um wesentliche Regelungen, die Rückwirkungen auf in den Mitgliedstaaten bereits etablierte Verfahren der technischen Standardisierung und Zertifizierung, sowie in den Mitgliedstaaten etablierte Sicherheits-Infrastrukturen (elektronische Signaturen, neuer Personalausweis, De-Mail) haben können Die Bundesregierung wünscht sich zur Konkretisierung technischer Standards einen Ansatz, der nur ausnahmsweise „von oben“ (top-down), im Regelfall jedoch „von Unten“ (bottom-up“) erfolgt. Hierfür können die bewährten Strukturen etwa im Bereich der technischen Standardisierung (z.B. durch ISO-Normen) und Zertifizierung (einschließlich der gegenseitigen Anerkennung entsprechender Zertifikate im Sinne des „new approach“) genutzt werden. Auch das Vorgehen beim Privacy Impact Assessement für RFID-Anwendungen auf EU-Ebene könnte ein Vorbild sein. Erörterungsbedürftig ist darüber hinaus, inwieweit in der Verordnung notwendige Rahmenregelungen für Anreizsysteme etwa im Bereich des Datenschutzmanagements fehlen. Auch hierbei handelt es sich um wesentliche Regelungen, die durch die Verordnung selbst getroffen werden müssten. Bei Absatz 3 und 4 besteht zumindest die Gefahr der Kollision mit der in Beratung befindlichen Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. Hier muss eine klare Abgrenzung erfolgen.

14. zu Artikel 24:

Deutschland hält die Regelung, wie einige andere Mitgliedstaaten in der DAPIX, für noch nicht ausreichend klar. Durch die Vereinbarung darf nicht zum Nachteil des Betroffenen Verantwortung abgewälzt werden, z.B. auf für die Verarbeitung Verantwortliche in Drittstaaten. Klärungsbedürftig ist unter anderem, ob die Vorschrift auch die Datenverarbeitung im Konzern verbundener Unternehmen erfassen soll.

- Es sollte vorgesehen werden, dass ein Betroffener sich zur Ausübung seiner Rechte an jeden der gemeinsam für die Verarbeitung Verantwortlichen wenden kann, da Absprachen im Innenverhältnis nicht zu seinen Lasten gehen dürfen. Dabei sollte eindeutig zum Ausdruck gebracht werden, dass der Verantwortliche, an den sich der Betroffene wendet, nicht an den anderen verweisen darf.
- Es sollten – neben der Ermöglichung der Rechte betroffener Personen – weitere Inhalte benannt werden, die bei einer gemeinsamen Verantwortlichkeit zu regeln sind, z.B. wer Ansprechpartner der Aufsichtsbehörde ist.
- Es fehlen Verfahrens-, Streitbeilegungs- oder Zweifelsregeln, wie die Vereinbarung zustande kommen soll und wie zu verfahren ist, wenn eine Einigung nicht erfolgt.

15. zu Artikel 25:

Die Rechts- und Pflichtenstellung des Vertreters ist unklar. Nach Artikel 4 Absatz 14 und Erwägungsgrund 63 fungiert der Vertreter nur als „Ansprechpartner“ für Aufsichtsbehörden oder sonstigen Stellen in der Union. Artikel 53 Absatz 1 Buchstabe c legt dem Vertreter, korrespondierend mit seiner Nennung in Artikel 28 und 29, eine Pflicht zur Bereitstellung von Informationen auf. Ob Artikel 78 Absatz 2 hierauf begrenzt oder allgemein zu verstehen ist, bleibt unklar. Es sollte daher klargestellt werden, dass aufsichtsbehördliche oder gerichtliche Maßnahmen und Sanktionen gegenüber dem Vertreter rechtswirksam verhängt, zugestellt und durchgesetzt werden können.

Der Vertreter sollte nach Artikel 4 Absatz 14 ausdrücklich auch als Ansprechpartner von betroffenen Personen fungieren, wie dies Artikel 14 Absatz 1 Buchstabe a voraussetzt. Artikel 4 Absatz 14 ist entsprechend zu ergänzen.

- Mit Blick auf die Ausführungen in Erwägungsgrund 20 zu Artikel 3 Absatz 2, es sei „sicherzugehen, dass Personen nicht des Schutzes beraubt werden, auf den sie nach der Verordnung ein Anrecht haben“ und den Ausnahmen nach Absatz 2 besteht Erörterungsbedarf. Deutschland hat Zweifel, ob eine effektive

Durchsetzung des Artikel 3 Absatz 2 gewährleistet ist. Artikel 4 Absatz 2 der Richtlinie 95/46/EG sah keine Ausnahme von der Pflicht zur Benennung eines Vertreters vor.

Buchstabe a sollte gestrichen werden. Die Frage, ob in einem Drittland ein angemessenes Datenschutzniveau gewährleistet wird, sollte keine Rolle spielen, da im Falle des Artikel 3 Absatz 2 die Datenschutz-Grundverordnung und nicht das Recht des Drittstaates zur Anwendung kommen soll. Zudem gewährleisten die Angemessenheitsentscheidungen der Kommission keine gleichwertige Rechtsdurchsetzung von Betroffenenrechten und aufsichtsbehördlichen Maßnahmen wie in der EU.

Bei Buchstabe b bestehen Zweifel an der Eignung des Kriteriums. Die mit der Rechtsdurchsetzung verbundenen Probleme in Drittstaaten sind nicht abhängig von der Unternehmensgröße. Der Schwellenwert bedeutet, ginge man von der in der Folgenabschätzung für die EU genannten Unternehmenszusammensetzung aus, dass 99,8% aller Unternehmen in Drittländern von der Benennungspflicht entbunden sind. Für die Aufsichtsbehörde oder Dritte ist es zudem praktisch kaum feststellbar, wie viele Mitarbeiter ein Unternehmen in einem Drittland beschäftigt.

Bei Buchstabe d wird zu dem Wort „gelegentlich“ – trotz der Erläuterungen in Erwägungsgrund 64 – Klärungssbedarf gesehen.

- Absatz 3 führt bei Unternehmen, die Dienste im Internet regelmäßig EU-weit anbieten, zur freien Wahl, wo sie innerhalb der EU den Vertreter benennen. Die Regelung sollte mit der aufsichtsbehördlichen Zuständigkeitsbestimmung in den Fällen des Artikel 3 Absatz 2 einhergehen. Zuständig sollte jedenfalls auch die Aufsichtsbehörde des Mitgliedstaates sein, in dem der Vertreter benannt wird.

16. zu Artikel 26:

Die bislang in dem Verordnungsentwurf enthaltenen Vorschriften zur Auftragsdatenverarbeitung sind nur bedingt geeignet, neue technische Entwicklungen, insbesondere Cloud Computing-Dienste, praxisnah und rechtssicher zu erfassen. Das Cloud-Computing kann nicht mit klassischen Datenverarbeitungen im Auftrag, wie z.B. großen IT-Outsorcing-Projekten, verglichen werden. Der Nutzer eines Cloud Computing-Dienstes kann regelmäßig nicht als „Herr des Verfahrens“ und Verantwortlicher für die Datenverarbeitungsvorgänge in der Cloud angesehen werden. Einige Besonderheiten von Cloud Computing-Diensten im Zusammenhang mit den Regelungen zur Auftragsdatenverarbeitung können durch die nachfolgend

dargestellten Vorschläge berücksichtigt werden. Dies betrifft insbesondere differenzierte Regelungen für die Kontrolle des Auftragnehmers oder den Anforderungen an den Vertrag. Gegebenenfalls bedarf es weiterer noch zu bestimmender Regelungen.

Die Regelung bedarf weiterer Prüfung, inwieweit sie für bestehende und sich entwickelnde Verfahren und Dienstleistungen etwa im Gesundheitswesen anwendbar und sinnvoll sind, insbesondere die Verarbeitung pseudonymisierter oder verschlüsselter Daten und die Verwaltung medizinischer Aktensysteme unter Kontrolle des Patienten („google-health“, „health vault“) (vgl. Stellungnahme zu Artikel 4).

– Aus Sicht der Bundesregierung fehlt in Absatz 1, wie in Erwägungsgrund 62 gefordert, eine grundsätzliche Regelung zum Verhältnis zwischen dem für die Verarbeitung Verantwortlichen (Auftraggeber) und dem Auftragsverarbeiter (Auftragnehmer). Vorgesehen werden sollte einleitend:

  „Werden personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet, ist der für die Verarbeitung Verantwortliche für die Einhaltung der Vorschriften über den Datenschutz verantwortlich.“

  Hieraus folgend sollte in einem weiteren Satz klargestellt werden, dass die Rechte des Betroffenen sowie das Recht auf Schadensersatz gegenüber dem für die Verarbeitung Verantwortlichen geltend zu machen sind.

  Um die Zuteilung der Verantwortlichkeiten klarzustellen, sollten die Pflichten, die eigenständig an den Auftragsverarbeiter adressiert sind, vor allem die Gewährleistung der Datensicherheit (Artikel 30), in einem eigenen Absatz abschließend aufgeführt werden.

  Der letzte Halbsatz von Absatz 1 sollte ein eigener Satz werden und vorsehen, dass sich der Auftraggeber erstmals vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt. Es sollte dabei, vor allem auch mit Blick auf das Cloud Computing, klargestellt werden, dass es hierfür nicht erforderlich ist, dass der Auftraggeber vor Ort eine Kontrolle durchführt, was tatsächlich regelmäßig nicht zu leisten wäre, sondern dass ein geeignetes Testat eines unabhängigen, fachlich geeigneten Sachverständigen ausreicht. Auch durch eine Verschärfung der Haftung kann die dem Auftragnehmer obliegenden Gewährleistung der Datensicherheit verbessert und der Auftraggeber von deren Kontrolle entlastet werden.

- In Absatz 2 sollte am Anfang ein neuer Buchstabe zu den Essentialia des Auftrags aufgenommen werden, namentlich „Gegenstand und Dauer des Auftrags, Art und Zweck der Verarbeitung, Art der Daten und Kreis der Betroffenen“. Eine solche Festlegung im Auftrag erscheint notwendig, damit der Auftragsverarbeiter die Grenzen seines Auftrags vor Augen hat.
- Mit Blick auf das Cloud Computing sollten die Anforderungen an Inhalt und Form des Vertrages so modifiziert werden, dass der Vertragsinhalt vom Auftragnehmer den gesetzlichen Vorgaben entsprechend zu einem Großteil vorbereitet und über Webformular erfüllt werden kann. Damit kann der Praxis Rechnung getragen werden, wenn wie bei Cloud Computing üblich standardisierte Dienste angeboten werden.
- Es sollte in einem eigenen Satz geregelt werden, dass „ *der Auftragsverarbeiter die personenbezogenen Daten nur im Rahmen der Weisungen des für die Verarbeitung Verantwortlichen verarbeiten darf* “. Diese für die Auftragsverarbeitung zentrale Bestimmung sollte nicht nur indirekt über eine Vorgabe des Inhalts des Auftrags erfolgen. Buchstabe a sollte dann, diesen Satz aufgreifend, vorsehen, dass „die Weisungsbefugnisse, des für die Verarbeitung Verantwortlichen“ festzulegen sind. Klarzustellen ist, dass eine Weisung auch unmittelbar im Auftrag erfolgen kann. Die derzeitige Formulierung des Buchstaben a ist missverständlich. Das „insbesondere“ kann relativierend dahin verstanden werden, der Auftragsverarbeiter dürfe in bestimmten Fällen ohne Weisung handeln. Zudem wird der Anschein erweckt, der Auftragsverarbeiter solle unzulässige Datenübermittlungen nur auf Weisung des für die Verarbeitung Verantwortlichen vornehmen. Die Unzulässigkeit einer Datenverarbeitung wird durch eine Weisung aber nicht „geheilt“. Ergänzend sollte in einem neuen Satz vorgesehen werden, dass „ *der Auftragnehmer den Auftraggeber unverzüglich darauf hinzuweisen hat, wenn nach seiner Auffassung eine Weisung gegen datenschutzrechtliche Vorschriften verstößt*“.
- Die in Buchstabe b vorgesehene Verpflichtung auf das Datengeheimnis sollte nicht alle Mitarbeiter erfassen, sondern nur die mit der Datenverarbeitung beschäftigten und terminologisch („employ“) keine arbeitsrechtlichen Beschränkungen enthalten.
- Buchstabe c sollte vorsehen, dass im Auftrag konkret „ *die nach Artikel 30 zu treffenden technischen und organisatorischen Maßnahmen* “ festzulegen und nicht lediglich, dass Maßnahmen nach Artikel 30 zu treffen sind. Letzteres ergibt sich bereits aus Artikel 30. Die konkrete Festlegung im Auftrag erleichtert, sich, wie in Absatz 1 vorgesehen, von der Einhaltung der Maßnahmen zu überzeugen.

- Die unter Buchstabe d vorgesehene Verpflichtung auf eine vorherige Zustimmung ist in bestimmten Konstellationen nicht praktikabel, z.B. wenn ein Auftragsverarbeiter eine Vielzahl an Kunden hat und beim Wechsel eines technischen Dienstleisters mehrere tausend Zustimmungen einholen müsste. Vorgesehen werden sollte daher vor allem, dass im Auftrag „ *die etwaige Berechtigung zur Begründung von Auftragsverhältnissen*“ festzulegen ist, es aber den Parteien überlassen bleibt, ob und wie sie eine Zustimmungspflicht vorsehen wollen. Klargestellt werden sollte, dass die Zustimmung auch im Auftrag selbst erteilt werden kann.
- Bei Buchstabe e sollte vorgesehen werden, dass Auftraggeber und Auftragnehmer im Rahmen der Vertragsgestaltungsfreiheit für die konkrete Auftragsverarbeitung festzulegen haben, „ *ob und inwieweit der für die Verarbeitung Verantwortlichen bei der Erfüllung ihm obliegender Pflichten zu unterstützen ist* “. Dies betrifft neben der Erfüllung der Betroffenenrechte u.a. auch die unter Buchstabe f genannten Pflichten.
- Buchstabe f sollte nicht verbindlich festlegen, dass der Auftragsverarbeiter den für die Verarbeitung Verantwortlichen bei der Einhaltung der Artikel 30 bis 34 zu unterstützen hat. In verschiedenen Fällen kann der Auftragsverarbeiter eine solche Unterstützung tatsächlich nicht leisten, etwa weil der für die Verarbeitung Verantwortliche die Zwecke, Mittel und Bedingungen der Verarbeitung festlegt. Flexibler wäre, die zu Buchstabe e vorgeschlagene Formulierung.
- Zeitlicher Anknüpfungspunkt bei Buchstabe g sollte die Beendigung des Auftrags sein, nicht der Abschluss der Verarbeitung, da bei einer mitunter langjährigen Auftragsverarbeitung eine Vielzahl von Verarbeitungen durchgeführt und abgeschlossen wird. Unklar ist, was mit dem Aushändigen „sämtlicher Ergebnisse“ gemeint ist. Derzeit erlaubt Buchstabe g auch, dass die Daten personenbezogen beim Auftragsverarbeiter verbleiben. Vorgesehen werden sollte, dass der Auftragsverarbeiter „ *nach Beendigung des Auftrags die bei ihm zu dem Auftrag gespeicherten personenbezogenen Daten löscht und etwaige überlassene Daten und Datenträger zurückgibt*“.
- Die Pflicht zur Zusammenarbeit mit der Aufsichtsbehörde in Buchstabe h besteht entsprechend zu den Befugnissen der Aufsichtsbehörde in Artikel 53. Sie ist darüber hinaus in Artikel 29 geregelt und kann hier gestrichen werden. Mit Blick auf das Verhältnis zum für die Verarbeitung Verantwortlichen sollten im Auftrag allgemein „ *die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungsrechte des Auftragnehmers* “, z.B. Betretensrechte, periodische Berichtspflichten durch einen zertifizierten Prüfer, geregelt werden.

- Absatz 3 sollte keinen unnötigen Verwaltungsaufwand verursachen. Sofern eine Dokumentation bereits im Vertrag oder Rechtsakt nach Absatz 2 erfolgt, sollte dies auch für Absatz 3 genügen. Für die Dokumentation sollte Textform genügen, z.B. ein Webformular. Dies sollte, vor allem auch mit Blick auf das Cloud Computing, auch für den Vertrag nach Absatz 2 gelten.
- Absatz 4 sollte gestrichen werden. Verarbeitet der Auftragsverarbeiter personenbezogene Daten anders als vom für die Verarbeitung Verantwortlichen angewiesen, liegt ein Verstoß gegen den ihr Innenverhältnis regelnden Vertrag oder Rechtsakt vor, der hierfür Regelungen, z.B. Schadensersatz oder eine Vertragsstrafe, vorsehen sollte. Der Verweis auf Artikel 24 erscheint unnötig und auch ungeeignet, weil es unwahrscheinlich ist, dass die aufgrund des weisunsgwidrigen Handelns gegebenenfalls zerstrittenen Beteiligten sich über die Pflichtenverteilung einigen.
- Zu Absatz 5 hat Deutschland einen Vorbehalt. Deutschland erachtet die Regelung als wesentlich. Insbesondere die Frage, ob spezielle Regelungen für die Verarbeitung in Unternehmensgruppen getroffen werden sollen oder nicht, hat erhebliche Auswirkungen für Unternehmen wie für die Betroffenen, so dass entsprechende Regelungen in der Verordnung getroffen werden müssten.

17. zu Artikel 27:

Unklar ist, inwieweit sich durch die neue Überschrift der Regelungsgehalt der ansonsten mit Artikel 16 der Richtlinie 95/46/EG nahezu identischen Vorschrift geändert hat. Die Pflicht des Auftragsverarbeiters, nur auf Weisung des für die Verarbeitung Verantwortlichen zu handeln, folgt bereits aus Artikel 26. In Bezug auf dem Auftragsverarbeiter unterstellte Personen kann eine sich gegebenenfalls widersprechende Weisungslage durch den für die Verarbeitung Verantwortlichen und den Auftragsverarbeiter ergeben.

Aus Sicht Deutschlands enthält Artikel 27, wie bislang Artikel 16 der Richtlinie 95/46/EG die auch in Artikel 26 Absatz 2 Buchstabe b in Bezug genommene Verpflichtung, mit der Datenverarbeitung beschäftigte Personen persönlich auf einen rechtmäßigen Datenumgang zu verpflichten, um bei Verstößen z.B. arbeitsrechtliche Konsequenzen gegenüber der beschäftigten Person ziehen zu können.

Die persönliche Verpflichtung auf einen rechtmäßigen Datenumgang wird durch die Bezugnahme auf „Anweisungen“ allerdings nicht deutlich. Zudem ist unklar, weshalb auch der Auftragsverarbeiter selbst aufgeführt wird, der eine juristische Person sein kann und insoweit persönlich nicht verpflichtet werden kann.

Die Vorschrift sollte daher wie folgt formuliert werden:

> *„Mit der Datenverarbeitung beschäftigten Personen ist untersagt personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Hierauf sind sie bei Aufnahme ihrer Tätigkeit zu verpflichten. Die Pflicht wirkt nach Beendigung ihrer Tätigkeit fort.“*