Bundesrat **Drucksache** **4/1/09**

03.02.09

Empfehlungen
der Ausschüsse

In - A - Fz - R - Wi

zu **Punkt ...** der 854. Sitzung des Bundesrates am 13. Februar 2009

Entwurf eines Gesetzes zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften

Der federführende **Ausschuss für Innere Angelegenheiten** (In),

der **Agrarausschuss** (A),

der **Finanzausschuss** (Fz),

der **Rechtsausschuss** (R) und

der **Wirtschaftsausschuss** (Wi)

empfehlen dem Bundesrat, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

Zu Artikel 1 - DSAG allgemein

In
Fz

1. Der in Artikel 1 vorgesehene Entwurf eines Datenschutzauditgesetzes bedarf einer grundlegenden Überarbeitung. Denn das im Gesetzentwurf vorgesehene Verfahren für ein Datenschutzaudit ist bürokratisch, kostenträchtig und nicht transparent.

...

Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln
Telefon: (02 21) 97 66 83 40, Telefax: (02 21) 97 66 83 44
ISSN 0720-2946

In Fz*

2. a) Der Gesetzentwurf bringt eine überbordende, überflüssige Bürokratie mit sich. Es sollen private Kontrollstellen eingerichtet werden, die erst vom Bundesbeauftragten für den Datenschutz zugelassen und dann durch die Datenschutzaufsichtsbehörden der Länder überwacht werden. Diese müssen wiederum beim Bundesbeauftragten für den Datenschutz gegebenenfalls die Entziehung der Zulassung anregen. Zusätzlich sieht der Gesetzentwurf auch noch einen Datenschutzauditausschuss und für ihn eine „Aufsichtsbehörde“ vor.

b) Das vorgesehene Verfahren der Zulassung und Überwachung der Stellen, die zukünftig die Befugnis erhalten sollen, bei datenverarbeitenden Stellen im nicht-öffentlichen Bereich Datenschutzkonzepte und informationstechnische Einrichtungen zu kontrollieren, führt zu einem unverhältnismäßig hohen Verwaltungsaufwand bei den Datenschutzaufsichtsbehörden der Länder. Während der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit nach § 2 Absatz 2 des Gesetzentwurfs für die Zulassung der Kontrollstellen, die Entziehung der Zulassung und die Vergabe der Kennnummern an die Kontrollstellen zuständig sein soll, obliegt die Durchführung des Gesetzes und der auf Grund dieses Gesetzes erlassenen Rechtsverordnungen grundsätzlich den nach Landesrecht zuständigen Behörden. Diese sollen die nach § 7 Absatz 1 Satz 1 des Gesetzentwurfs vom Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zugelassenen Kontrollstellen überwachen und bei Bedarf Überprüfungen dieser Stellen veranlassen. Es ist abzusehen, dass der mit der Wahrnehmung dieser Überwachungsaufgabe verbundene Aufwand außer Verhältnis zu dem zu erwartenden Nutzen steht. Vor allem aber werden hierdurch in nicht unerheblichem Maße personelle und sachliche Ressourcen gebunden, die den Datenschutzaufsichtsbehörden bei der Erfüllung ihrer eigentlichen Aufgabe, die Betroffenen bei der Wahrung ihrer Datenschutzrechte zu unterstützen, nicht mehr zur Verfügung stehen werden.

* Fz als Begründung zu Ziffer 1

In

3. c) Das Verhältnis dieser privaten Kontrollstellen zur Selbstkontrolle durch betriebliche Datenschutzbeauftragte und zur Fremdkontrolle durch die Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich ist unklar.

Der Gesetzentwurf sieht vor, dass Unternehmen, Betriebe und sonstige private Stellen ihr Datenschutzkonzept und ihre informationstechnischen Einrichtungen durch eine weitere Kontrollstelle überprüfen lassen können. Hierdurch kann sowohl die Stellung des jeweiligen betrieblichen Datenschutzbeauftragten als auch die Stellung der zuständigen Datenschutzaufsichtsbehörde nachhaltig beeinträchtigt werden. Dies gilt insbesondere dann, wenn bei der Beurteilung von Datenschutzfragen Meinungsverschiedenheiten zwischen der privaten Kontrollstelle und den für die Datenschutzkontrolle zuständigen Aufsichtsbehörden auftreten.

In
Wi

d) Jedenfalls sollte auf das vorgesehene Instrument eines Datenschutzauditausschusses im Hinblick auf den hohen bürokratischen Aufwand verzichtet werden.

In

e) Die Nomenklatur des Gesetzentwurfs ist in sich widersprüchlich und würde in der Praxis zur Verwirrung führen.

aa) Der Begriff „Kontrollstelle“ wird in Artikel 28 EG-Datenschutzrichtlinie für die staatlichen Behörden verwendet, die in den Mitgliedstaaten den Datenschutz im öffentlichen wie im nicht-öffentlichen Bereich kontrollieren. Konsequent redet § 38 BDSG davon, dass die Aufsichtsbehörden die Ausführung dieses Gesetzes sowie anderer Vorschriften über den Datenschutz kontrollieren.

In dem Gesetzentwurf wird der Begriff „Kontrollstelle“ aber für nicht-öffentliche Stellen (also Private) verwendet, die wiederum nicht-öffentliche Stellen (also Private) kontrollieren sollen (§ 3 Satz 1, § 1 Satz 2 Nummer 4).

bb) Der Begriff „Aufsichtsbehörde“ wird vom geltenden Bundesdatenschutzgesetz seit 1978 für die Datenschutzaufsichts-behörden für den nicht-öffentlichen Bereich (§ 38 BDSG) verwendet. Der Gesetzentwurf benutzt den Begriff aber inkonsequent für das Bundesministerium des Innern, das als Rechtsaufsichtsbehörde für den Datenschutzauditausschuss fungieren soll.

Begründung:

Wi Zu Ziffer 3 Buchstabe d:

Die vorgesehene Bildung eines Datenschutzauditausschusses, der Richtlinien zur Verbesserung des Datenschutzes und der Datensicherheit erlassen soll, seine vorgesehene Berichtspflicht sowie seine Zusammensetzung sind zu aufwändig und unpraktikabel. Auf Grund der sich ständig weiter entwickelnden Technik in den verschiedenen Anwendungsbereichen müssten einheitliche Richtlinien ständig angepasst werden.

R 4. Zu Artikel 1 (§ 4 Absatz 1 Satz 1 Nummer 4 DSAG)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens zu prüfen, ob § 4 Absatz 1 Satz 1 Nummer 4 DSAG-E mit Artikel 9 Absatz 1 Buchstabe a und Artikel 10 Absatz 2 Buchstabe a in Verbindung mit Absatz 1 der Richtlinie 2006/123/EG des Europäischen Parlaments und des Rates vom 12. Dezember 2006 über Dienstleistungen im Binnenmarkt (EU-Dienstleistungsrichtlinie - ABl. L 376 vom 27.12.2006, S. 36) vereinbar ist.

Begründung:

An der Vereinbarkeit der Regelung mit den oben genannten Bestimmungen der EU-Dienstleistungsrichtlinie bestehen Zweifel. Nach Artikel 9 Absatz 1 der EU-Dienstleistungsrichtlinie dürfen Genehmigungsregelungen nicht diskriminierend sein. Die Kriterien, auf denen sie beruhen, dürfen nach Artikel 10 Absatz 1 und 2 der EU-Dienstleistungsrichtlinie ebenfalls nicht diskriminierend sein.

Die Kontrollstelle nach den §§ 3 ff. DSAG-E ist grundsätzlich nicht hoheitlich tätig, sondern übt ihre Tätigkeit aufgrund eines privatrechtlichen Vertrages mit der nichtöffentlichen Stelle aus. Zwar sieht § 16 Absatz 1 Satz 1 Nummer 1 DSAG-E die Ermächtigung der Landesregierungen zur Beleihung zugelassener Kontrollstellen durch Rechtsverordnung vor. Zwingend ist eine Beleihung je-

doch nicht. Es kann also nicht davon ausgegangen werden, dass Kontrollstellen in jedem Fall hoheitliche Tätigkeit ausüben und damit dem Anwendungsbereich der EU-Dienstleistungsrichtlinie nach deren Artikel 2 Absatz 2 Buchstabe i entzogen sind.

Damit erscheint fraglich, ob das Erfordernis eines inländischen Sitzes oder einer inländischen Niederlassung nach § 4 Absatz 1 Satz 1 Nummer 4 DSAG-E der Anforderung der Artikel 9 und 10 der EU-Dienstleistungsrichtlinie an eine diskriminierungsfreie Genehmigung entspricht.

R
In

5. Zu Artikel 1 (§ 9 Absatz 1 Satz 1 DSAG)

Der Bundesrat bittet, im weiteren Verlauf des Gesetzgebungsverfahrens zu prüfen, ob es angesichts der Bedeutung des Datenschutzes sachgerecht ist, dass das Datenschutzauditsiegel (ähnlich wie beim Gütesiegel im ökologischen Landbau) bereits vor einer ersten Prüfung durch die Kontrollstelle verwendet werden darf, oder ob es erforderlich ist zu bestimmen, dass das Siegel erst nach der erfolgten Überprüfung genutzt werden darf.

Begründung:

Nach dem Gesetzentwurf können Firmen bereits ab der Mitteilung der beabsichtigten Verwendung mit dem Datenschutzsiegel werben, das heißt bevor die Konzepte, Programme oder technischen Anlagen tatsächlich überprüft wurden. Die Kontrolle soll erst erfolgen, "sobald" die Arbeit der Kontrollstelle "es ermöglicht" (§ 3 Satz 4 DSAG-E).

Dies birgt die Gefahr, dass Daten verarbeitende Stellen im Vertrauen auf das Datenschutzauditsiegel erhebliche Summen in ungeprüfte Programme oder technische Anlagen investieren oder beispielsweise Verträge mit einem Callcenter abschließen und später die Kontrollstelle feststellt, dass die Anforderungen des Audit-Gesetzes nicht erfüllt oder möglicherweise sogar datenschutzrechtliche Vorschriften nicht eingehalten werden.

In dieser Zeit kann jedoch bereits eine Vielzahl von personenbezogenen Daten verarbeitet worden sein, mit den entsprechenden Konsequenzen für die Betroffenen. Investitionsentscheidungen von Unternehmen oder öffentlichen Stellen müssen gegebenenfalls in Frage gestellt werden, was mit erheblichen Kosten verbunden sein kann.

Vor diesem Hintergrund ist es angezeigt, die vorgesehene Regelung noch einmal zu überprüfen.

In 6. Zu Artikel 2 Nummer 1a - neu - (§ 4 Absatz 3 Satz 1 BDSG)

Nach Nummer 1 ist folgende Nummer einzufügen:

'1a. § 4 Absatz 3 Satz 1 wird wie folgt gefasst:

„Werden personenbezogene Daten beim Betroffenen erhoben, so ist er von der verantwortlichen Stelle über

a) die Identität der verantwortlichen Stelle,

b) die Zweckbestimmung der Erhebung, Verarbeitung oder Nutzung und

c) den Empfänger

zu unterrichten." '

Begründung:

Die bisherigen Einschränkungen haben aufgrund der ungenauen Regelungen über die Informationspflicht des Betroffenen durch die verantwortliche Stelle über die Erhebung seiner Daten dazu beigetragen, dass die ausdrückliche Informationspflicht der Ausnahmefall gewesen ist. Die ausdrückliche Informations- und Dokumentationspflicht der verantwortlichen Stelle dient der Rechtsklarheit.

In 7. Zu Artikel 2 Nummer 2 (§ 4f Absatz 2 Satz 1 und 2 BDSG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob und gegebenenfalls wie die Anforderungen an die Fachkunde der Beauftragten für den Datenschutz konkretisiert werden können.

Begründung:

Der Gesetzentwurf sieht eine Stärkung der Stellung der Beauftragten für den Datenschutz vor. Dies ist zu begrüßen.

Ebenso wichtig ist jedoch, die Anforderungen an die Fachkunde der Beauftragten für den Datenschutz zu konkretisieren. § 4f Absatz 2 Satz 1 BDSG bestimmt bisher lediglich, dass die Beauftragten die zur Erfüllung ihrer Aufgabe erforderliche Fachkunde besitzen müssen und sich das Maß der erforderlichen Fachkunde insbesondere nach dem Umfang der Datenver-arbeitung der verantwortlichen Stelle bestimmt.

In der Praxis ist zunehmend festzustellen, dass Beauftragte für den Datenschutz nicht über die zur Erfüllung ihrer Aufgaben erforderlichen Mindestkenntnisse, namentlich des Datenschutzrechts, verfügen. In nichtöffentlichen Stellen, die solche Personen zu Beauftragten für den Datenschutz bestellen, ist eine effektive Selbstkontrolle der Einhaltung datenschutzrechtlicher Vorschriften damit oftmals nicht gewährleistet. Eine funktionierende Selbstkontrolle ist jedoch zur Verhinderung von Datenschutzverstößen und zur Unterstützung der nur über begrenzte Ressourcen verfügenden Aufsichtsbehörden unabdingbar.

Es sollte daher geprüft werden, ob und gegebenenfalls wie die Anforderungen an die Fachkunde des Beauftragten für den Datenschutz konkretisiert werden können. Denkbar wäre, in einem ersten Schritt eine gesetzliche Ermächtigung dafür zu schaffen, durch Rechtsverordnung nähere Regelungen über die Anforderungen an die Fachkunde zu treffen, zumindest jedoch Mindestkenntnisse vorzuschreiben. Geregelt werden sollte auch der Nachweis der erforderlichen Fachkunde bzw. Mindestkenntnisse, durch Bescheinigungen über den Besuch geeigneter Aus- und Fortbildungsveranstaltungen und das Ablegen einer Prüfung.

In

8. Zu Artikel 2 (§ 9 und Anlage zu § 9 Satz 1 BDSG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob § 9 BDSG und insbesondere die Anlage zu § 9 Satz 1 BDSG dergestalt verändert werden kann, dass nicht mehr ein Katalog von Einzelmaßnahmen zur Gewährleistung der Datensicherheit vorgegeben wird, sondern stattdessen nach dem Muster mehrerer Landesdatenschutzgesetze die Sicherheitsziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz vorgegeben werden.

Begründung:

Durch die Vorgabe von Sicherheitszielen würde das Gesetz in diesem Punkt technologieunabhängig formuliert und insoweit Anforderungen der modernen, sich ständig fortentwickelnden Technik besser angepasst sein. Zugleich würde eine inhaltliche und begriffliche Angleichung an für die Sicherheit in der Informationstechnik (IT-Sicherheit) bestehende Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit) erreicht. Wird den Sicherheitszielen in einer Weise entsprochen, dass getroffene Maßnahmen in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen, kann einerseits präventiv dem unbefugten Zu- und Umgang mit personenbezogenen Daten entgegengewirkt werden, andererseits lässt sich gegebenenfalls anhand von Protokollierungen usw. im Nachhinein feststellen, wer für den unbefugten Umgang mit personenbezogenen Daten verantwortlich ist.

In 9. Zu Artikel 2 (§ 11 Absatz 2 Satz 2 BDSG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob § 11 Absatz 2 Satz 2 BDSG so gefasst werden kann, dass die der Norm unterworfenen nichtöffentlichen Stellen die gesetzlichen Anforderungen besser erkennen können.

Begründung:

Anlass für das vorliegende Gesetzgebungsverfahren hat vor allem der rechtswidrige Umgang von Call-Center-Mitarbeitern mit personenbezogenen Daten gegeben. Call-Center verarbeiten personenbezogene Daten regelmäßig im Auftrag (§ 11 BDSG). Es stellt sich daher die Frage, ob die aktuellen Ereignisse Anlass geben, die Vorschriften über die Datenverarbeitung im Auftrag zu verbessern.

In der Praxis ist festzustellen, dass insbesondere § 11 Absatz 2 Satz 2 BDSG häufig nicht beachtet wird. So wird in vielen Fällen der Auftrag nicht schriftlich erteilt bzw. der schriftliche Auftrag enthält keine schriftlichen Regelungen hinsichtlich der Datenerhebung, -verarbeitung oder -nutzung, der technischen und organisatorischen Maßnahmen oder etwaiger Unterauftragsverhältnisse. Häufig beschränken sich die „Festlegungen“ auch auf den Satz, die Vorschriften des Bundesdatenschutzgesetzes seien vom Auftragnehmer zu beachten bzw. auf eine Wiedergabe der gesetzlichen Regelungen. Mitunter wird vertraglich vereinbart, nähere Festlegungen erfolgten mündlich, was jedoch regelmäßig nicht geschieht. Schriftliche Regelungen zur Löschung der Daten bzw. deren Rückgabe nach Erledigung des Auftrags werden nur selten getroffen.

Festzustellen ist auch, dass insbesondere Call-Center häufig von (mitunter vor Jahren erteilten) angeblichen Einwilligungen Betroffener in die Verarbeitung und Nutzung ihrer Daten Gebrauch machen, ohne dass sich Auftraggeber oder Call-Center davon überzeugt haben, dass im Einklang mit gesetzlichen Vorschriften zustande gekommene Einwilligungen tatsächlich vorliegen. Hinzu kommt, dass in vielen Fällen weder Auftraggeber noch Call-Center auf Verlangen der Betroffenen oder der Aufsichtsbehörde einen Nachweis darüber vorlegen können, dass der Betroffene in die Verarbeitung seiner Daten eingewilligt hat. Diesbezügliche schriftliche Festlegungen fehlen durchweg.

Vor diesem Hintergrund ist es zu begrüßen, dass der Gesetzentwurf die Möglichkeit eröffnet, Verstöße gegen § 11 Absatz 2 Satz 2 BDSG mit einem Bußgeld zu ahnden.

Dies greift jedoch zu kurz. Gespräche von Datenschutzaufsichtsbehörden mit nichtöffentlichen Stellen haben ergeben, dass diese die Vorschrift oftmals nicht absichtlich missachten, sondern nicht erkennen, was von ihnen verlangt wird. Es erscheint daher notwendig, § 11 Absatz 2 Satz 2 so zu präzisieren, dass die der Norm unterworfenen nichtöffentlichen Stellen die gesetzlichen Anforde-

rungen besser erkennen können. So sollte deutlicher werden, dass auch die Festlegungen hinsichtlich der Datenverarbeitung und -nutzung, der technischen und organisatorischen Maßnahmen und etwaiger Unterauftragsverhältnisse schriftlich zu treffen sind und konkrete generelle Weisungen bezogen auf den Einzelfall und die einzelnen Verarbeitungsschritte, namentlich die Löschung der Daten bzw. deren Rückgabe an den Auftraggeber, die Datensicherung und die Vergabe von Unteraufträgen zu erteilen sind. Ein Hinweis auf die gesetzlichen Bestimmungen oder deren Wiedergabe genügt nicht. Hilfreich wäre, wenn einige besonders wichtige Bestandteile einer solchen Festlegung im Gesetz beispielhaft („insbesondere“) aufgeführt würden.

In R

10. Zu Artikel 2 Nummer 3a -neu- (§ 11 Absatz 2 Satz 4 BDSG)

Der Bundesrat bittet im Hinblick darauf, dass unzureichende Kontrollen der als Auftragnehmer bei der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eingeschalteten Unternehmen (insbesondere Callcentern) zu schwerwiegenden Datenschutzverletzungen beigetragen haben, im weiteren Verlauf des Gesetzgebungsverfahrens zu prüfen, ob Häufigkeit, Tiefe und Dokumentation der vom Auftraggeber vorzunehmenden Kontrollen in § 11 Absatz 2 Satz 4 BDSG näher geregelt werden sollten.

Begründung:

Wenn unterschiedlichste personenbezogene Daten unterschiedlicher Herkunft bei einem Unternehmen vorhanden sind - dies gilt insbesondere für Callcenter - besteht eine hohe Missbrauchsgefahr durch die unberechtigte Verknüpfung dieser Datenbestände. Es ist jedoch zu besorgen, dass die Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmungen gerade in diesem Bereich hinter dem Gebotenen zurückbleibt, weil die die Erhebung, Verarbeitung oder Nutzung von Daten vornehmende Stelle selbst nicht die datenschutzrechtliche Verantwortung trägt. Umgekehrt wird sich der gemäß § 11 Absatz 1 BDSG in der datenschutzrechtlichen Verantwortung bleibende Auftraggeber ohne entsprechende gesetzliche Verpflichtung nur in sehr zurückhaltender Weise von der Ordnungsmäßigkeit der Geschäftstätigkeit des Vertragspartners überzeugen. Die jüngsten Vorfälle geben Anlass zu der Überlegung, ob die stärkere Inpflichtnahme der Auftraggeber durch Vorgabe konkreter Kontrollmaßnahmen vorgesehen werden sollte. Deren Häufigkeit und Dokumentation ist geboten, um sicherzustellen, dass die selbst für die Wahrung der Datenschutzanforderungen nicht verantwortlichen Auftragnehmer die Einhaltung der gesetzlichen Vorgaben gewährleisten.

In 11. Zu Artikel 2 (§ 11 Absatz 4 BDSG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob der Katalog der nach § 11 Absatz 4 BDSG für Auftragsdatenverarbeiter geltenden Vorschriften des Bundesdatenschutzgesetzes um § 42a ergänzt werden muss.

Begründung:

In den vergangenen Monaten festgestellte Fälle der unrechtmäßigen Kenntniserlangung personenbezogener Daten durch Dritte waren mehrfach von Auftragsdatenverarbeitern oder deren Mitarbeitern zu verantworten. In solchen Fällen, insbesondere wenn die unrechtmäßige Kenntniserlangung personenbezogener Daten durch Dritte auf unzureichende Datensicherungsvorkehrungen des Auftragnehmers oder die unzulässige Verknüpfung von Datenbeständen mehrerer Auftraggeber beim Auftragnehmer zurückzuführen ist, erscheint eine originäre Pflicht des Auftragnehmers zu Informationen im Sinne des § 42a BDSG angeraten.

Soweit der Auftraggeber zu Informationen nach § 42a BDSG verpflichtet ist, könnte zudem - unbeschadet vertraglicher Verpflichtungen - gesetzlich festgelegt werden, dass der Auftragnehmer dem Auftraggeber alle erforderlichen Informationen zur Verfügung zu stellen hat.

In 12. Zu Artikel 2 Nummer 5 Buchstabe b (§ 28 Absatz 1 Satz 1 Nummer 1 BDSG)

Artikel 2 Nummer 5 Buchstabe b ist wie folgt zu fassen:

’b) Absatz 1 Satz 1 Nummer 1 wird wie folgt gefasst:

„1. wenn es zur Durchführung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,“ ’

Begründung:

Über die im Gesetzentwurf vorgesehene Ersetzung der Begriffe „Vertragsverhältnisses“ bzw. „vertragähnlichen Vertrauensverhältnisses“ durch die mit der Schuldrechtsnovelle 2002 eingeführten Begriffe „rechts-geschäftlichen Schuldverhältnisses“ und „rechtsgeschäftähnlichen Schuldverhältnisses“ hinaus soll deutlich gemacht werden, dass nur die für die Abwicklung des Rechtsgeschäftes erforderlichen Daten erhoben und verarbeitet werden dürfen und keine weiteren „überschießenden Daten“. Die aufgrund des sog. Datenschutzgipfels am 04.09.2008 in Berlin eingesetzte Länder-Arbeitsgruppe hat seinerzeit festgestellt, dass die Erhebung und Verarbeitung der sog. „überschießenden Daten“ eine der Ursachen für die bekannt gewordenen Datenschutzverstöße gewesen sind.

In 13. Zu Artikel 2 Nummer 5 Buchstabe b (§ 28 Absatz 1 Satz 1 Nummer 1 BDSG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob mit der neu vorgesehenen Terminologie „rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis“ in § 28 BDSG anstelle der bisherigen Begriffe „Vertragsverhältnis“ und „vertragsähnliches Vertrauensverhältnis“ wie bisher auch Vereine, Verbände, Parteien, Gewerkschaften u. ä. Organisationen erfasst bleiben.

Begründung:

Mit dem vorliegenden Gesetzentwurf sollen in § 28 BDSG die Begriffe „Vertragsverhältnis“ und „vertragsähnliches Vertrauensverhältnis“ durch die Begriffe „rechtsgeschäftliches oder rechtsgeschäftsähnliches Schuldverhältnis“ ersetzt werden. Begründet wird die Änderung mit der Anpassung der Begriffe an die durch die Schuldrechtsnovelle des Jahres 2002 eingeführte Terminologie. Zumindest klärungsbedürftig ist, ob die nunmehr vorgesehene Terminologie auch Vereine, Verbände, Parteien, Gewerkschaften u. ä. Organisationen erfasst. Bisher konnten solche nicht-kommerziell tätigen nichtöffentlichen Stellen zumindest unter den Begriff des „vertragsähnlichen Vertrauensverhältnisses“ subsumiert werden. Wäre dies aufgrund einer geänderten Terminologie künftig nicht mehr möglich, entfiele für diese Stellen die zentrale gesetzliche Grundlage für den Umgang mit personenbezogenen Daten. Dies kann mit einer bloßen Anpassung der Terminologie offensichtlich nicht gewollt sein.

Wi 14. Zu Artikel 2 Nummer 5 Buchstabe d (§ 28 Absatz 3 allgemein BDSG)

Der Bundesrat bittet im weiteren Gesetzgebungsverfahren zu prüfen, ob die grundsätzliche Abschaffung des so genannten Listenprivilegs in § 28 Absatz 3 Satz 1 Nummer 3 BDSG sachgerecht ist und nicht eine Verbesserung des Widerspruchsrechts gegen eine Übermittlung oder Nutzung für Werbezwecke die bessere Lösung darstellt.

Eine solche Verbesserung des Widerspruchsrechts kann darin bestehen, dass der Bundesgesetzgeber die zweite Alternative des Artikels 14 Absatz 1 Buchstabe b der EG-Datenschutzrichtlinie übernimmt: Der Betroffene ist vor der ersten Weitergabe personenbezogener Daten an Dritte oder vor der erstmaligen Nutzung im Auftrage Dritter zu Zwecken der Direktwerbung zu informieren und ihm die Möglichkeit zu geben, gegen eine solche Weitergabe oder Nutzung Widerspruch einzulegen. Diese Lösung wird dem Recht auf informationelle Selbstbestimmung gerecht, ohne gleich zur stärksten Maßnahme, der Einwilligungsvoraussetzung, zu greifen.

Der vorliegende Gesetzentwurf, der (bis auf wenige Ausnahmen wie für die Spendenwerbung gemeinnütziger Organisationen) die Einwilligung verlangt, würde das Direkt-Marketing und damit die Neukundengewinnung wesentlich erschweren und damit weite Bereiche der Wirtschaft teilweise existentiell treffen. Zu den betroffenen Wirtschaftsbereichen gehören neben der Marketingbranche selbst insbesondere der Versandhandel und das Verlagswesen.

Daneben gehen auch Markt- und Meinungsforschungsunternehmen davon aus, dass bei Umsetzung des Gesetzentwurfs eine Vielzahl von bislang üblichen Verbraucher- und Bürgerbefragungen, darunter auch solche, die von staatlichen Stellen in Auftrag gegeben werden, nicht mehr durchgeführt werden können. Dies wird auch diese Branche wirtschaftlich treffen und zu erheblichen Arbeitsplatzverlusten führen.

Im Vorblatt zu dem Gesetzentwurf wird unter "Problem und Ziel" auf die in der jüngeren Vergangenheit zunehmend bekanntgewordenen Fälle des rechtswidrigen Handelns Bezug genommen. Hierzu ist festzuhalten, dass die aufgetretenen Datenschutzskandale nicht durch das Listenprivileg verursacht wurden und durch die Abschaffung des so genannten Listenprivi-

legs solche Skandale auch für die Zukunft nicht verhindert werden können. Das Listenprivileg umfasst insbesondere keine Kontonummern.

Weiterhin heißt es im Vorblatt zu dem Gesetzentwurf, der Erlaubnistatbestand des § 28 Absatz 3 Satz 1 Nummer 3 BDSG habe sich für die Herstellung der notwendigen Transparenz als besonders nachteilig erwiesen. Die notwendige Transparenz könnte durch die oben erwähnte zweite Alternative des Artikels 14 Absatz 1 Buchstabe b der EG-Datenschutzrichtlinie herbeigeführt werden, ohne dem Direktmarketing und der Marktforschung den Boden zu entziehen.

A 15. Zu Artikel 2 Nummer 5 Buchstabe d (§ 28 Absatz 3 Satz 4, Satz 5 BDSG)

In Artikel 2 Nummer 5 Buchstabe d ist § 28 Absatz 3 wie folgt zu ändern:

a) Satz 4 ist zu streichen.

b) Im bisherigen Satz 5 sind die Wörter "nach den Sätzen 2 bis 4" durch die Wörter "nach den Sätzen 2 und 3" zu ersetzen.

Begründung:

Die im Gesetzentwurf vorgesehene Regelung für so genannte "Beipackwerbung" enthält eine aus Verbraucherschutzsicht nicht akzeptable Ausnahme von dem Grundsatz, dass die gezielte Ansprache zum Zwecke der Werbung oder Markt- und Meinungsforschung nur nach vorheriger Einwilligung der Betroffenen zulässig sein soll. Nach der Ausnahmeregelung sollen bereits im Geschäftskontakt mit Verbraucherinnen und Verbrauchern stehende Unternehmen berechtigt sein, unaufgefordert nicht nur Werbung sowie Markt- oder Meinungsforschung für eigene, sondern auch für Produkte fremder Unternehmen zuzusenden.

Wie der Gesetzentwurf in der Begründung selbst ausführt, wird die gezielte Ansprache zu Werbezwecken sowie zur Markt- und Meinungsforschung von Bürgerinnen und Bürgern zunehmend als Belastung empfunden und ist mit dem Wunsch nach mehr Selbstbestimmung verbunden. Jede Einschränkung dieses Grundsatzes bedarf daher einer überzeugenden Begründung, die auch dem gesetzlich intendierten Schutz der Betroffenen Rechnung trägt. Insbesondere bei der Übersendung von Fremdwerbung kann aber - anders als in den Fällen von unternehmerischer Eigenwerbung im Rahmen bestehender Kundenbeziehungen - von einem verringerten Schutzbedürfnis der Betroffenen nicht ausgegangen werden. Denn Betroffene müssen gerade nicht damit rechnen, dass der Kauf eines Produktes bei einem bestimmten Unternehmen und die da-

bei erfolgte Preisgabe von persönlichen Daten zum Anlass genommen wird, in der Folge auch uneingeschränkt mit Werbung anderer Unternehmen belästigt zu werden. Auch ist es für die eintretende Belästigungswirkung ohne Belang, ob Werbematerialien allein oder zusammen mit Unterlagen eines bereits bekannten Unternehmens übersandt werden. Aus Sicht der betroffenen Verbraucher besteht daher kein sachlicher Grund, diese Form der Werbung gesetzlich zu privilegieren.

Zur Rechtfertigung einer solchen Ausnahmeregelung reicht es nicht aus, die Verbraucher auf ihr Widerspruchsrecht gegenüber dem verantwortlichen Unternehmen nach § 28 Absatz 4 Satz 1 BDSG-E zu verweisen. Gerade wenn unternehmerische Eigenwerbung mit Fremdwerbung verknüpft wird, ist für betroffene Verbraucher schwer erkennbar, wer die Übersendung veranlasst und aus datenschutzrechtlicher Sicht zu verantworten hat. Solange der Gesetzgeber auf die Einführung einer gesetzlichen Kennzeichnungspflicht von Daten verzichtet, erscheint es sachlich nicht gerechtfertigt, diese Verknüpfung von Werbeaktivitäten verschiedener Unternehmen gesetzlich zuzulassen.

Die vorgesehene Zulässigkeit der "Beipackwerbung" birgt auch die Gefahr, dass in nicht unerheblichem Umfang das grundsätzliche Einwilligungserfordernis nach § 28 Absatz 3 Satz 1 BDSG-E durch eine entsprechende Vereinbarung von Unternehmen über eine Bündelung von Werbemaßnahmen umgangen wird und Dritte ohne Einwilligung der Betroffenen zu Werbezwecken Zugriff auf personenbezogene Daten erhalten. Ein Verzicht auf die Einwilligung des Betroffenen erscheint jedoch angesichts der in den vergangenen Monaten bekannt gewordenen Fälle von Datenmissbrauch nur dann gerechtfertigt, wenn die beabsichtigte Datennutzung im Rahmen eigener geschäftlicher Zwecke der verantwortlichen Stelle erfolgt. Die in § 28 Absatz 3 Satz 4 BDSG-E vorgesehene Regelung ist daher zu streichen.

In

16. Zu Artikel 2 Nummer 5 Buchstabe d (§ 28 Absatz 3 Satz 6 BDSG)

In Artikel 2 Nummer 5 Buchstabe d sind in § 28 Absatz 3 Satz 6 die Wörter „Nach den Sätzen 1 bis 3 übermittelte Daten dürfen“ durch die Wörter „Sind nach den Sätzen 1 bis 3 Daten übermittelt worden, dürfen sie nur“ zu ersetzen.

Begründung:

Klarstellung des Gewollten, weil in Fällen der Sätze 2 und 3 keine Übermittlungen vorliegen müssen.

...

A 17. Zu Artikel 2 Nummer 5 Buchstabe d (§ 28 Absatz 3 Satz 7 - neu - BDSG)

In Artikel 2 Nummer 5 Buchstabe d ist dem § 28 Absatz 3 folgender Satz anzufügen:

"Der Betroffene kann im Falle des Satzes 1 verlangen, dass ihm das Vorliegen einer wirksamen Einwilligung nachgewiesen wird."

Begründung:

Der Gesetzentwurf verzichtet darauf, die Gültigkeit der Einwilligung in die Datennutzung zeitlich zu beschränken und die von der Rechtsprechung zu § 4a BDSG entwickelten Anforderungen an die Zweckbindung der Einwilligung für den Adresshandel näher zu präzisieren. Damit werden sich die Betroffenen auch weiterhin häufig im Ungewissen darüber befinden, von wem und zu welchen Zwecken im Einzelnen ihre Daten genutzt werden. Auch werden die Betroffenen vielfach nicht sicher beurteilen können, ob der Datennutzung eine wirksame, möglicherweise schon mehrere Jahre zuvor erklärte Einwilligung zu Grunde liegt.

Gerade im Bereich des Direktmarketings nutzen Unternehmen nicht selten diesen Umstand aus und berufen sich auf eine Einwilligung des Betroffenen, deren Existenz jedoch nicht nachgewiesen wird. Um den Betroffenen, denen möglicherweise erst durch unerwünschte Werbeanrufe oder ähnliche Belästigungen der Umfang der zunächst gebilligten Datennutzung deutlich wird, eine effektive Durchsetzung ihrer Rechte zu ermöglichen, ist es erforderlich, in § 28 Absatz 3 BDSG-E einen Anspruch auf Nachweis der Einwilligung gesetzlich zu verankern. Nur so wird der Betroffene in die Lage versetzt, beispielsweise sein Recht auf Widerruf der Einwilligung auszuüben. Die Nachweispflicht unterstützt außerdem die Maßnahmen zur Bekämpfung der nach § 7 Absatz 2 UWG unzulässigen unerbetenen Telefonwerbung und ergänzt die Auskunftsansprüche des § 34 BDSG.

A 18. Zu Artikel 2 Nummer 5 Buchstabe e (§ 28 Absatz 3a Satz 1,

Satz 2 - neu - BDSG)

In Artikel 2 Nummer 5 Buchstabe e ist § 28 Absatz 3a Satz 1 durch folgende Sätze zu ersetzen:

"Die Einwilligung bedarf der Schriftform. Sie kann auch elektronisch erklärt werden, wenn die verantwortliche Stelle sicherstellt, dass die Einwilligung protokolliert wird und der Betroffene deren Inhalt jederzeit abrufen und die Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen kann."

Begründung:

Mit der Streichung des so genannten "Listenprivilegs" soll nach dem Gesetzentwurf die Verwendung personenbezogener Daten für Zwecke des Adresshandels, der Werbung oder Markt- und Meinungsforschung grundsätzlich nur zulässig sein, wenn der Betroffene darin eingewilligt hat. Der Einwilligungsvorbehalt entfaltet seine Schutzwirkung zu Gunsten von Verbraucherinnen und Verbrauchern aber nur dann, wenn für die Wirksamkeit der Einwilligung die Einhaltung der Schriftform gesetzlich vorgeschrieben wird. Das Schriftformerfordernis dient nicht nur der Rechtssicherheit, indem etwaige Grenzen der Einwilligung unmissverständlich dokumentiert werden. Es ist auch mit einer aus Verbraucherschutzsicht zu begrüßenden Warnfunktion verbunden. Soll sich die erteilte Einverständniserklärung beispielsweise auf die Weitergabe der Daten an Dritte erstrecken, wird der Betroffene durch die geforderte Abgabe der Einwilligung in Schriftform davor geschützt, voreilig dem dann nur noch schwer kontrollierbaren Datenhandel zuzustimmen.

Demgegenüber lässt es der Gesetzentwurf in der vorgesehen Fassung zu, dass unter den Voraussetzungen des § 4a Absatz 1 Satz 3 BDSG von der Schriftform abgewichen werden kann. Damit sind beispielsweise auch telefonisch abgegebene Einwilligungserklärungen denkbar. Zum Schutz von Verbraucherinnen und Verbrauchern sieht der Gesetzentwurf lediglich vor, dass der Inhalt der abgegebenen Einwilligungserklärung vom Unternehmer später schriftlich zu bestätigen ist. Dies kann nicht überzeugen. Es ist zu befürchten, dass Verbraucherinnen und Verbraucher die rechtliche Relevanz einer später zugesandten Bestätigungserklärung - die ggf. auch mit weiteren Werbematerialien verbunden ist - nicht immer erkennen. Auch werden sich Verbraucherinnen und Verbraucher vielfach an den genauen Inhalt telefonisch abgegebener Erklärungen, denen ggf. ein Werbeanruf vorangegangen ist, später nicht genau erinnern. Sollten Unternehmen diese Unsicherheit zu ihren Gunsten ausnutzen, ist es nicht gerechtfertigt, Verbraucherinnen und Verbraucher auf die Ausübung ihres Widerrufsrechtes nach § 28 Absatz 4 Satz 1 BDSG-E zu verweisen.

Den Interessen der Wirtschaft wird hinreichend Rechnung getragen, indem ausnahmsweise auch die in elektronischer Form abgegebene Erklärung zugelassen wird.

In
A
R

19. Zu Artikel 2 Nummer 5 Buchstabe e (§ 28 Absatz 3b BDSG)

In Artikel 2 Nummer 5 Buchstabe e § 28 Absatz 3b sind die Wörter ", wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist" zu streichen.

...

Begründung:

A Die Einführung eines Koppelungsverbotes in den Gesetzentwurf ist zu begrüßen. Die Einschränkung des Verbotes auf Unternehmen mit marktbeherrschender Stellung greift aber zu kurz. Wünschenswert wäre ein umfassendes Kopplungsverbot unabhängig von der Marktmacht eines Unternehmens.

In R Abweichend vom Gesetzentwurf wird das Verbot, den Abschluss eines Vertrags von der Einwilligung des Betroffenen abhängig zu machen ("Koppelungsverbot"), ohne Einschränkung auf alle Unternehmen ausgedehnt. Auf diese Weise wird die Freiwilligkeit der Einwilligung nach § 28 Absatz 3 Satz 1 BDSG-E über § 4a Absatz 1 Satz 1 BDSG hinaus abgesichert, indem jeder Versuch, die gesetzlich nicht legitimierte Datenverarbeitung mit der Drohung, den Vertrag anderenfalls nicht abzuschließen, zu erzwingen, zur Unwirksamkeit der Einwilligung führt.

Die im Gesetzentwurf vorgesehene Einschränkung, dass dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist, lehnt sich an die bisherigen bereichsspezifischen Koppelungsverbote in § 95 Absatz 5 des Telekommunikationsgesetzes (TKG) und § 12 Absatz 3 des Telemediengesetzes an und verallgemeinert diese. Ziel dieser eingeschränkten Koppelungsverbote ist es zu verhindern, dass Anbieter von Dienstleistungen im Telekommunikations- und Multimediasektor eine eventuelle Monopolstellung ausnutzen (vgl. die Einzelbegründung zu § 93 TKG-E, BT-Drs. 15/2316, S. 89). Anders als bei Leistungen der zivilisatorischen Grundversorgung wie Telekommunikations- und Multimediadienstleistungen sind Monopol-stellungen jedoch im normalen Geschäftsverkehr der Ausnahmefall. Die im Gesetzentwurf vorgesehene Regelung würde daher kaum praktische Relevanz entfalten.

A Nach der im Gesetzentwurf vorgesehenen Regelung darf die verantwortliche Stelle den Abschluss eines Vertrages nicht von der Einwilligung des Betroffenen abhängig machen, "wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht in zumutbarer Weise möglich ist". Die Erfahrungen mit der entsprechenden Regelung des Telemediengesetzes zeigen, dass hierdurch den Interessen der Verbraucherinnen und Verbraucher auf Marktzugang nicht hinreichend Rechnung getragen werden kann. Im Übrigen wirft die Formulierung auf Grund ihrer Unbestimmtheit Auslegungsschwierigkeiten auf. Es besteht Unklarheit, in welchen Fällen Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist.

In R Ein (eingeschränktes) Koppelungsverbot für marktbeherrschende Unternehmen ergibt sich zudem bereits nach geltendem Recht aus § 4a Absatz 1 Satz 1 BDSG. Danach ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht, also "ohne Zwang" erfolgt (vgl. die Einzelbegründung zu § 4a BDSG-E, BT-Drs. 14/4329, S. 34 unter Hinweis auf Artikel 2 Buchstabe h der EG-Datenschutzrichtlinie). Die Einwilligung wird als Verwendungsregulativ nur so lange akzeptiert, wie sich die Betroffenen nicht in einer Situation befinden, die sie faktisch dazu zwingt, sich mit dem Zugriff auf ihre jeweils verlangten Daten einverstanden zu erklären. Daran fehlt es re-

gelmäßig bei der Inanspruchnahme von Leistungen, auf welche die Betroffenen existentiell angewiesen sind und die ihnen unter Ausnutzung einer wirtschaftlichen Machtposition "abgepresst" werden. § 4a Absatz 1 Satz 1 BDSG möchte in diesen Situationen jeden Versuch der verantwortlichen Stelle unterbinden, ihre Leistungen an die Bereitschaft der Betroffenen zu knüpfen, in die Verwendung bestimmter sie betreffender Daten einzuwilligen; die verantwortliche Stelle bleibt zwar unverändert berechtigt, die jeweils erforderlichen Daten zu verarbeiten (§ 28 Absatz 1 Satz 1 Nummer 1 BDSG-E), darf aber nicht ihre Leistung mit dem Zugriff auf weitere konkret nicht benötigte Angaben verknüpfen. Bei richtiger Auslegung generalisiert mithin § 4a Absatz 1 Satz 1 BDSG das im Telekommunikations- und Multimediarecht ausdrücklich vorgesehene Koppelungsverbot (vgl. Simitis-Simitis, BDSG, 6. Auflage 2006, § 4a RNummer 62 f.; Gola/Schomerus, BDSG, 8. Auflage 2005, § 4a RNummer 6). Die im Gesetzentwurf vorgesehene Regelung würde angesichts dessen nicht nur kein Mehr an Verbraucherdatenschutz bringen, sondern könnte darüber hinaus zu Auslegungsschwierigkeiten hinsichtlich § 4a Absatz 1 Satz 1 BDSG führen, indem sie dessen Regelungsgehalt infrage stellt.

In

20. Zu Artikel 2 Nummer 5 (§§ 28 bis 30 BDSG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Tätigkeit der Markt- und Meinungsforschungsinstitute durch klarstellende Regelungen insbesondere in den §§ 28 bis 30 BDSG besser abgesichert werden kann.

Begründung:

Die Markt- und Meinungsforschung nimmt eine wichtige gesellschaftliche Aufgabe wahr. Sie stellt für öffentliche und private Auftraggeber mittels wissenschaftlicher Methoden und Techniken notwendige Informationen als empirische Grundlage und zur Unterstützung wirtschaftlicher, gesellschaftlicher und politischer Entscheidungen bereit und schafft damit eine wichtige Voraussetzung für die nachhaltige demokratische und wirtschaftliche Entwicklung der Bundesrepublik Deutschland.

Gleichwohl wird die Markt- und Meinungsforschung im BDSG in den §§ 28 und 29 BDSG mehrfach mit der Werbung, dem Adresshandel und der Tätigkeit von Auskunfteien gleichgestellt. Dabei hat die Markt- und Meinungsforschung im Gegensatz zur Werbung, zum Adresshandel und zur Tätigkeit der Auskunfteien nicht Aussagen über konkrete Einzelpersonen zum Gegenstand, sondern zieht personenbezogene Daten lediglich heran, um daraus von der Einzelperson unabhängige, verallgemeinerungsfähige Aussagen zu gewinnen. Die von der Markt- und Meinungsforschung erhobenen Daten werden dem Auftraggeber dementsprechend nur in anonymisierter Form übermittelt.

Die Einschränkung des Listenprivilegs im Hinblick auf Markt- und Meinungsforschungsinstitute durch Artikel 2 Nummer 5 Buchstabe d des Gesetzentwurfs (Markt- und Meinungsforschung nur noch zu eigenen Zwecken bzw. gegenüber Freiberuflern und Gewerbetreibenden) könnte die Tätigkeit der Markt- und Meinungsforschungsinstitute über Gebühr behindern. Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu Zwecken der Markt- und Meinungsforschung sollte daher in den §§ 28 und 30 BDSG klargestellt werden.

Auch im Vorblatt und in der Begründung zum Gesetzentwurf sollten die Unterschiede zwischen der Werbung, dem Adresshandel und der Tätigkeit der Auskunfteien einerseits und der Markt- und Meinungsforschung andererseits stärker zum Ausdruck gebracht werden.

A 21. Zu Artikel 2 Nummer 7a - neu - (§ 35 Absatz 5 BDSG)

In Artikel 2 ist nach Nummer 7 folgende Nummer 7a einzufügen:

'7a. § 35 Absatz 5 wird wie folgt gefasst:

"(5) Personenbezogene Daten dürfen nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien erhoben, verarbeitet oder genutzt werden, soweit der Betroffene dieser bei der verantwortlichen Stelle widerspricht. Dies gilt nicht, wenn eine Interessenabwägung ergibt, dass das Interesse der verantwortlichen Stelle das Interesse des Betroffenen erheblich überwiegt oder wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung der Daten verpflichtet." '

Begründung:

Der Bundesrat nimmt Bezug auf seine Stellungnahme zum Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (BR-Drs. 548/08 - Beschluss -, Ziffer 12).

Die Bundesregierung hatte in ihrer Gegenäußerung zur Stellungnahme des Bundesrates (BT-Drs. 16/10581) dem Vorschlag des Bundesrates nicht zugestimmt. Allerdings wurde seitens der Bundesregierung angekündigt, dass im Rahmen des von ihr angekündigten gesonderten Gesetzentwurfes ein Vorschlag gemacht werde. Dem vorliegenden Gesetzentwurf ist eine entsprechende Passage jedoch nicht zu entnehmen.

Nach aktueller Rechtslage dürfen grundsätzlich personenbezogene Daten für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien dann nicht erhoben, verarbeitet oder genutzt werden, wenn der Betroffene widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen das Interesse der verantwortlichen Stelle überwiegt. Die in

§ 35 Absatz 5 Satz 1 BDSG geregelte Interessenabwägung zwischen Betroffenem und verantwortlicher Stelle schränkt das Widerspruchsrecht des Betroffenen wesentlich ein. Die verantwortliche Stelle kann sich regelmäßig darauf berufen, dass ihr Interesse an einer Datenerhebung, Verarbeitung oder Nutzung das Interesse des Verbrauchers überwiegt. Daher soll der Verbraucher grundsätzlich ein umfassendes Widerspruchsrecht eingeräumt bekommen.

Ausnahmsweise sollen trotz Widerspruch des Verbrauchers personenbezogene Daten durch die verantwortliche Stelle erhoben, verarbeitet oder genutzt werden, soweit eine Interessenabwägung ergibt, dass das Interesse der verantwortlichen Stelle an einer Erhebung, Verarbeitung oder Nutzung der Daten das Interesse des Verbrauchers erheblich überwiegt oder wenn eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung der Daten verpflichtet.

Durch diese Regelung wird die Kontrollmöglichkeit der Verbraucher über die Verwendung ihrer personenbezogenen Daten verbessert und die Verbraucher werden damit besser geschützt.

In 22. Zu Artikel 2 (§ 38 Absatz 5 BDSG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Eingriffsbefugnisse der Datenschutzaufsichtsbehörden dahingehend erweitert werden können, dass diese über § 38 Absatz 5 BDSG hinaus generell Anordnungen und Untersagungsverfügungen in Bezug auf materiell rechtswidrige Datenverarbeitungen oder sonstige Verstöße gegen datenschutzrechtliche Vorschriften erlassen können.

Begründung:

Eingriffsbefugnisse der Aufsichtsbehörden in Bezug auf konkrete Datenverarbeitungen sind in § 38 Absatz 5 BDSG geregelt. Danach kann die Aufsichtsbehörde lediglich Anordnungen treffen und Verfahren untersagen, wenn technische und organisatorische Mängel festgestellt wurden. Die Regelung erfasst nicht materiell unzulässige Verarbeitungen und sonstige Verstöße gegen datenschutzrechtliche Vorschriften. In diesen Fällen ist es der Aufsichtsbehörde nicht möglich, ihre Rechtsauffassung durchzusetzen, wenn die nichtöffentliche Stelle diese nicht teilt. Auch durch Erlass eines Bußgeldbescheids – sofern ein solcher rechtlich möglich ist – kann keine verbindliche Klärung der Rechtslage herbeigeführt werden, ganz abgesehen davon, dass dies hierfür nicht der richtige Weg ist. Diese Rechtslage wirkt sich auf den Vollzug des BDSG nachteilig aus. Angesichts der bekannt gewordenen Datenschutzverstöße aber auch mit Blick auf die Erfahrungen der Aufsichtsbehörden beim Gesetzesvollzug ist eine Ausweitung der Handlungsmöglichkeiten dringend erforderlich.

Dadurch würde es den Aufsichtsbehörden auch möglich, wirksam präventiv tätig zu werden und letztlich den Einsatz einzelner Verarbeitungen zu untersagen, wenn diese materiell rechtswidrig sind.

Für die Schaffung von Anordnungsbefugnissen für die Aufsichtsbehörden auch in Bezug auf materiell rechtswidrige Datenverarbeitungen bzw. Verstöße gegen datenschutzrechtliche Vorschriften spricht Artikel 28 Absatz 3, 2. Spiegelstrich der EG-Datenschutzrichtlinie, wonach die Kontrollstellen über wirksame Eingriffsbefugnisse verfügen“ müssen. Hierzu gehört beispielsweise die Möglichkeit, das vorläufige oder endgültige Verbot einer Verarbeitung anzuordnen.

Darüber hinaus erscheint es widersprüchlich, dass die zuständigen Stellen, mutmaßlich die Aufsichtsbehörden nach § 38 BDSG, im Zusammenhang mit ihren Aufgaben nach dem Datenschutzauditgesetz über Anordnungs- bzw. Untersagungsbefugnisse bzgl. einer rechtswidrigen Verwendung des Siegels verfügen sollen, den Datenschutzaufsichtsbehörden im Anwendungsbereich des BDSG jedoch eine solche Befugnis nicht zugestanden wird.

A 23. Zu Artikel 2 Nummer 7b - neu - (§ 38 Absatz 5a - neu - BDSG)*

In Artikel 2 ist nach Nummer 7 folgende Nummer 7a einzufügen:

'7b. In § 38 wird nach Absatz 5 folgender Absatz 5a eingefügt:

"(5a) Die Aufsichtsbehörde kann den rechtswidrigen Umgang mit personenbezogenen Daten untersagen, soweit mit ihm eine besondere Gefährdung des Persönlichkeitsrechts verbunden wäre. Die Untersagung kann mit Mitteln des Verwaltungszwangs durchgesetzt werden." '

Begründung:

Eingriffsbefugnisse der Aufsichtsbehörden in Bezug auf konkrete Datenverarbeitungen sind bislang in § 38 Absatz 5 BDSG geregelt. Danach kann die Aufsichtsbehörde jedoch lediglich vorhandene Verfahren untersagen, wenn technische und organisatorische Mängel festgestellt wurden. Ein materiell unzulässiger Umgang mit personenbezogenen Daten kann nicht untersagt werden.

Diese Rechtslage wirkt sich auf den Vollzug des BDSG sehr nachteilig aus. Die Aufsichtsbehörde kann einen künftigen rechtswidrigen Umgang mit personenbezogenen Daten selbst dann nicht untersagen und mit Mitteln des Verwaltungszwangs unterbinden, wenn schwerste Schädigungen des Persönlichkeitsrechts drohen. Die Aufsichtsbehörden sind nach geltender Rechtslage gezwungen, schwerwiegende Datenschutzverstöße zunächst sehenden Auges hinzunehmen, um sie erst anschließend mit Bußgeldern zu sanktionieren.

* Ist bei Annahme von Ziffer 21 redaktionell anzupassen.

Dies läuft dem Zweck des BDSG zuwider, den Einzelnen effektiv vor unzulässigen Beeinträchtigungen seines Persönlichkeitsrechts durch den Umgang mit seinen personenbezogenen Daten zu schützen, vgl. § 1 Absatz 1 BDSG.

Mit dem Änderungsvorschlag werden die Aufsichtsbehörden befähigt, den künftigen Umgang mit personenbezogenen Daten zu untersagen, die materiell rechtswidrig sind.

Die Befugnis zur Untersagung ist auf drohende erhebliche Beeinträchtigungen des Persönlichkeitsrechts beschränkt, um das Verhältnismäßigkeitsprinzip zu wahren.

Das BDSG kommt mit dem Änderungsvorschlag zugleich der Forderung des Artikels 28 Absatz 3 zweiter Spiegelstrich der EG-Datenschutzrichtlinie 95/46/EG nach, die Aufsichtsbehörden mit "wirksamen Einwirkungsbefugnissen" auszustatten.

A 24. Zu Artikel 2 Nummer 8 (§ 42a Satz 1 BDSG)

In Artikel 2 Nummer 8 sind in § 42a Satz 1 die Wörter "und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen" zu streichen.

Begründung:

Die neu geschaffene und aus Verbraucherschutzsicht sehr zu begrüßende Informationspflicht bei Datenpannen ist gemäß § 42a Satz 1 Nummer 1 bis 4 BDSG-E auf besonders sensible personenbezogene Daten begrenzt. Soweit diese personenbezogenen Daten einem Dritten unrechtmäßig zur Kenntnis gelangt sind, bergen diese - wie beispielsweise personenbezogene Daten zu Bankkonten - bereits ihrer Art nach eine besondere Missbrauchsgefahr, die eine Informationspflicht der verantwortlichen Stelle rechtfertigt. Eine weitergehende Einschränkung der Informationspflicht ist sachlich nicht geboten.

Die Formulierung wirft auch Auslegungsschwierigkeiten auf. Sie lässt offen, welche Erwägungen von der verantwortlichen Stelle bei der Prüfung einer Informationspflicht im konkreten Fall herangezogen werden dürfen. Soll sich beispielsweise eine verantwortliche Stelle bei massenhaftem Verlust von Kontonummern verschiedenster Personen pauschal darauf berufen dürfen, eine schwerwiegende Gefahr eines materiellen Schadens habe nicht bestanden, weil unberechtigte Abbuchungen im Lastschriftenverfahren widerrufen werden können? Ein solches Ergebnis wäre aus Verbraucherschutzsicht nicht akzeptabel, da die neu eingeführte Informationspflicht die Betroffenen in die Lage versetzen soll, sich die erhöhte Missbrauchsgefahr zu vergegenwärtigen und ggf. weitere Vorsorgemaßnahmen zu treffen.

Es ist zu begrüßen, dass nach der vorliegenden Fassung des Gesetzentwurfs ein Verstoß gegen die Informationspflichten bei Datenpannen gemäß § 43 Absatz 1 Nummer 7 BDSG-E als Ordnungswidrigkeit mit einem Bußgeld geahn-

det werden kann. Wegen des drohenden Imageverlustes bedarf es einer abschreckenden Sanktionierung, wenn von den verantwortlichen Stellen gegen die Informationspflicht verstoßen wird. Damit der neu geschaffene Ordnungswidrigkeitstatbestand auch dem Bestimmtheitsgebot entspricht, muss der Gesetzgeber dafür Sorge tragen, dass die Voraussetzungen eines Verstoßes eindeutig normiert werden. Auch aus diesem Grund erscheint daher eine Streichung dieser Formulierung geboten.

In 25. Zu Artikel 2 Nummer 8 (§ 42a Satz 5 BDSG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Anforderung des § 42a Satz 5 BDSG nach mindestens halbseitiger Veröffentlichung in zwei bundesweit erscheinenden Tageszeitungen abgemildert werden kann, insbesondere wenn das die Veröffentlichungspflicht auslösende Ereignis nur regionale Bedeutung hat.

Begründung:

Eine Pflicht zu mindestens halbseitigen Veröffentlichungen in zwei bundesweit erscheinenden Tageszeitungen erscheint unverhältnismäßig, wenn das mit der Veröffentlichung beabsichtigte Ziel der Information der Betroffenen auch auf andere geeignete, aber weniger kostenträchtige Weise erreicht werden kann.

R 26. Zu Artikel 2 Nummer 9 Buchstabe a Doppelbuchstabe aa (§ 43 Absatz 1 Nummer 2b BDSG)

In Artikel 2 Nummer 9 Buchstabe a Doppelbuchstabe aa § 43 Absatz 1 Nummer 2b ist nach dem Wort "Auftrag" das Wort "nicht," zu streichen.

Begründung:

Entsprechend der Begründung des Gesetzentwurfs soll sich nach § 43 Absatz 1 Nummer 2b BDSG-E ordnungswidrig verhalten, wer einen anderen mit der Erhebung, Verarbeitung oder Nutzung von Daten beauftragt, ohne die Vorgaben des § 11 Absatz 2 Satz 2 BDSG zu beachten (vgl. BR-Drs. 4/09, S. 53).

Durch die bisherige Formulierung verhält sich aber auch derjenige ordnungswidrig, der dem Dritten überhaupt keinen Auftrag erteilt. In einem solchen Fall könnte dem Betroffenen jedoch lediglich vorgeworfen werden, seine Daten nicht ausreichend gesichert oder sie unbefugt weitergegeben zu haben. Es kann ihm jedoch - etwa in dem Fall einer Entwendung der Daten - nicht vorgeworfen werden, keinen Auftrag erteilt zu haben. Sofern ein Auftrag zur Datenverarbeitung nicht erteilt wurde, dürfte § 11 BDSG schon nicht einschlägig sein.

In 27. Zu Artikel 2 Nummer 9 Buchstabe b (§ 43 Absatz 2 Nummer 1 BDSG)

In Artikel 2 Nummer 9 Buchstabe b ist Doppelbuchstabe aa folgender Doppelbuchstabe voranzustellen:

'aa0) In Nummer 1 werden die Wörter „erhebt oder verarbeitet" durch die Wörter „erhebt, verarbeitet oder nutzt" ersetzt.'

Begründung:

Eine wesentliche Lücke innerhalb der Bußgeldvorschriften besteht darin, dass die rechtswidrige Nutzung personenbezogener Daten nicht von den Tatbeständen des § 43 BDSG erfasst ist.

Eine unzulässige Nutzung personenbezogener Daten kann in gleich schwerwiegender Weise in die Rechte der Betroffenen eingreifen, wie die rechtswidrige Datenerhebung oder Datenverarbeitung. Dies betrifft beispielsweise die Nutzung von personenbezogenen Daten, denen keine Erhebung vorangegangen ist, sondern wo diese Daten z.B. mittels einer CD „zugespielt" wurden.

Daher sollte die derzeitige Beschränkung auf die rechtswidrige Datenerhebung und Datenverarbeitung entfallen und jedweder rechtswidrige Umgang mit personenbezogenen Daten als Ordnungswidrigkeit geahndet werden.

In 28. Zu Artikel 2 Nummer 9 (§ 43 BDSG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob für Verstöße gegen § 4 Absatz 3 Satz 1 bis 3, § 11 Absatz 2 Satz 4, § 35 Absatz 3 und 4 BDSG und für die unbefugte Nutzung einer Telefon- oder Telefaxnummer oder einer Email-Adresse in § 43 BDSG Bußgeldtatbestände geschaffen werden können.

Begründung:

Mit dem Antrag wird die Aufnahme einiger weiterer Bußgeldtatbestände in § 43 des Bundesdatenschutzgesetzes angestrebt. In der Praxis hat sich nämlich gezeigt, dass nichtöffentliche Stellen datenschutzrechtlichen Vorschriften, deren Verletzung nicht bußgeldbewehrt ist, wenig Beachtung schenken. Da die Aufsichtsbehörden derzeit keine Möglichkeit haben, ihre Rechtsauffassung im Wege einer verbindlichen Anordnung durchzusetzen, können sie nur durch die Androhung oder den Erlass eines Bußgeldbescheids Druck auf eine nichtöffentliche Stelle ausüben, das geltende Recht einzuhalten.

Den Unterrichtungs- und Hinweispflichten des § 4 Absatz 3 Satz 1 bis 3 BDSG wird in der Praxis häufig nicht oder nur unzureichend Rechnung getragen. Da § 4 Absatz 3 BDSG eine zentrale Bestimmung ist, um dem informationellen Selbstbestimmungsrecht der Betroffenen Rechnung zu tragen, müssen zumindest erhebliche, beharrliche oder wiederholte Zuwiderhandlungen gegen diese Vorschrift mit einem Bußgeld geahndet werden können. Da strittig ist, ob und gegebenenfalls in welchen Fällen ein Verstoß gegen § 4 Absatz 3 BDSG die Datenerhebung als solche unzulässig macht und damit als unbefugte Datenerhebung im Sinne des § 43 Absatz 2 Nummer 1 BDSG anzusehen ist, soll hierfür ein eigener Bußgeldtatbestand geschaffen werden.

Der Gesetzentwurf sieht bereits einen neuen Bußgeldtatbestand für Verstöße gegen § 11 Absatz 2 Satz 2 BDSG vor. Dies ist zu begrüßen. Es sollten jedoch auch Verstöße eines Auftraggebers gegen die in § 11 Absatz 2 Satz 4 BDSG statuierte Pflicht, sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen, bußgeldrechtlich geahndet werden können. Nach den Feststellungen von Aufsichtsbehörden kommen nur wenige Auftraggeber ihrer gesetzlichen Verpflichtung nach. Bei den Auftraggebern von Call-Centern sind solche Verstöße besonders häufig zu beobachten.

Bislang kann gegen eine nichtöffentliche Stelle, die eine erforderliche Sperrung personenbezogener Daten nach § 35 Absatz 3 oder 4 BDSG nicht vornimmt, bußgeldrechtlich erst vorgegangen werden, wenn die Daten unbefugt übermittelt oder genutzt werden. Es sollte daher die Möglichkeit geschaffen werden, ein Bußgeld schon dann zu verhängen, wenn eine nichtöffentliche Stelle die erforderliche Sperrung nicht vornimmt. Solche Fälle sind in der Praxis häufig. Mitunter werden umfangreiche Datenbestände entgegen den gesetzlichen Bestimmungen nicht gesperrt.

Viele Bürger wenden sich an die Aufsichtsbehörden, weil eine nichtöffentliche Stelle ihre Telefon- oder Telefaxnummer oder E-Mail-Adresse ohne die dafür erforderliche Einwilligung für Zwecke der Telefon-, Telefax- oder E-Mail-Werbung genutzt hat. Stellt die Aufsichtsbehörde einen Datenschutzverstoß fest, kann sie bislang lediglich eine Beanstandung gegenüber der nichtöffentlichen Stelle aussprechen, nicht jedoch ein Bußgeld verhängen. Dies ist insbesondere bei wiederholten Verstößen einer nichtöffentlichen Stelle misslich und für die Beschwerdeführer unverständlich.

Zu Artikel 2 Nummer 9 (§ 43 BDSG)

In 29. Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob in den Bußgeldkatalog des § 43 BDSG eine Regelung aufgenommen werden kann, wonach ordnungswidrig handelt, wer entgegen § 9 BDSG unzureichende technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit trifft und dadurch ermöglicht, dass Unbefugte personenbezogene Daten zur Kenntnis nehmen können.

Begründung:

Beim Vollzug des BDSG stellen die Aufsichtsbehörde immer wieder fest, dass von vielen Unternehmen Vorschriften nur befolgt werden, wenn deren Nichtbeachtung mit einer Sanktion verbunden ist. Insoweit ist es für die Aufsichtsbehörden äußerst problematisch auf die Einhaltung der Vorschriften des BDSG hinzuwirken, wenn nicht letztlich eine Sanktionsmöglichkeit besteht.

Die Datenschutzverstöße des Jahres 2008 belegen, dass mangelhafte technische und organisatorische Maßnahmen in den Unternehmen (mit-)ursächlich für die Missbrauchsfälle waren. Beispielsweise war u. a. nicht nachvollziehbar, wer auf welche Daten zugegriffen hat; ganze Datenbestände konnten offenbar kopiert werden. Dies ließe sich durch angemessene technische und/oder organisatorische Maßnahmen vermeiden, zumindest jedoch erheblich erschweren. Eine Sanktionsmöglichkeit würde den Druck auf die Unternehmen erhöhen, die zum Schutz der Rechte der Betroffenen notwendigen Maßnahmen zu treffen. Hierdurch würden in einigen Unternehmen eine deutliche Verbesserung des Datenschutzniveaus erzielt und zukünftig Missbrauchsfälle erheblich eingedämmt werden können.

In

30. Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob in den Bußgeldkatalog des § 43 BDSG eine Regelung aufgenommen werden kann, wonach ordnungswidrig handelt, wer entgegen § 28 Absatz 3b den Abschluss eines Vertrages von einer Einwilligung des Betroffenen nach Absatz 3 Satz 1 abhängig macht.

Eine entsprechende Bußgeldregelung sollte auch im TMG erhalten und im TKG aufgenommen werden.

Begründung

Das Koppelungsverbot ist bereits in § 12 Absatz 3 TMG und § 95 Absatz5 TKG verankert und bislang bereits in § 16 Absatz 2 Nummer 2 TMG bußgeldbewehrt. Die Bußgeldregelung im TMG soll nach dem Entwurf aufgehoben werden.

Die Aufsichtsbehörden stellen indessen immer wieder fest, dass Vorschriften des Datenschutzgesetzes nicht eingehalten werden, wenn die Verstöße nicht sanktioniert werden können. Der Betroffene selbst kann den Abschluss eines Vertrages, der entgegen § 28 Absatz 3b des Entwurfs von seiner Einwilligung abhängig gemacht wird, nicht erzwingen.

Zur wirksamen Durchsetzung des Koppelungsverbots sind Bußgeldregelungen notwendig, weil andernfalls ein Verstoß gegen das Verbot sanktionslos bliebe.

In 31*. Zu Artikel 2 Nummer 9a - neu - (§ 44 Absatz 2 - neu -)

In Artikel 2 ist nach Nummer 9 folgende Nummer einzufügen:

'9a. In § 44 Absatz 2 Satz 1 werden nach dem Wort „verfolgt“ die Wörter „, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält“ eingefügt.'

Begründung:

Straftaten nach § 44 Absatz 1 BDSG werden bislang nur auf Antrag verfolgt.

Antragsberechtigt sind zum einen der Betroffene, auf dessen Daten sich die Straftat bezieht und zum anderen die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit sowie die Aufsichtsbehörde.

Die Ausgestaltung der Strafvorschrift als absolutes Antragsdelikt wird dem Allgemeininteresse am Schutz personenbezogener Daten nicht gerecht. Der unbefugte Umgang mit personenbezogenen Daten, soweit er durch § 44 Absatz 1 BDSG in Verbindung mit § 43 Absatz 2 BDSG unter Strafe gestellt wird, ist geeignet, den Rechtsfrieden über den Lebenskreis des Betroffenen hinaus zu stören. Die Strafverfolgung wird insbesondere dann ein Anliegen der Allgemeinheit sein, wenn die Straftat nach § 44 Absatz 1 BDSG in Verbindung mit § 43 Absatz 2 BDSG personenbezogene Daten in großen Mengen betrifft.

Mit diesem Antrag wird die bereits in Ziffer 14 der Stellungnahme des Bundesrates vom 19.09.2008 zum Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (BR-Drs. 548/08 (Beschluss)) geäußerte Forderung wiederholt.

A 32. Zu Artikel 2 Nummer 9a - neu - (§ 44 Absatz 2 Satz 2 BDSG)

In Artikel 2 ist nach Nummer 9 folgende Nummer 9a einzufügen:

'9a. In § 44 Absatz 2 Satz 2 werden die Wörter "und die Aufsichtsbehörde" durch die Wörter ", die Aufsichtsbehörde und anerkannte Verbraucherverbände" ersetzt.'

* Ziffern 31 und 32 sind bei Annahme redaktionell zusammenzuführen.

Begründung:

§ 44 Absatz 2 des Bundesdatenschutzgesetzes sieht vor, dass eine Straftat nach dem Bundesdatenschutzgesetz nur auf Antrag verfolgt wird.

Antragsberechtigt sind der Betroffene, die verantwortliche Stelle, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit und die Aufsichtsbehörde.

Zur effektiven Wahrnehmung der Interessen der Verbraucherinnen und Verbraucher ist es geboten, auch anerkannten Verbraucherverbänden eine Strafantragsbefugnis einzuräumen.

Zukünftig sollten der "Verbraucherzentrale Bundesverband" und die Verbraucherzentralen der Länder berechtigt sein, einen Strafantrag zu stellen.

In 33. Zu Artikel 2 Nummer 10 (§ 47 BDSG)

In Artikel 2 Nummer 10 sind in § 47 nach dem Wort „erhobener“ die Wörter „oder gespeicherter“ einzufügen.

Begründung:

Die Übergangsregelung muss auch für solche Daten gelten, die ohne vorherige Datenerhebung gespeichert worden sind.

A 34. Zu Artikel 2 Nummer 10 (§ 47 BDSG)

In Artikel 2 Nummer 10 ist in § 47 die Angabe "1. Juli 2012" durch die Angabe "1. Juli 2010" zu ersetzen.

Begründung:

Das Bedürfnis der Wirtschaft, sich auf die neuen Datenschutzbestimmungen einzustellen, ist anzuerkennen. Eine dreijährige Übergangsfrist erscheint aber aus Sicht der Verbraucher zu lang.

Verbraucher haben ein Interesse daran, dass die Bestimmungen möglichst früh in Kraft treten, damit ein Missbrauch ihrer personenbezogenen Daten effektiv unterbunden werden kann. Ziel muss es sein, dass die Verbraucher möglichst früh von den neuen Vorschriften profitieren können, wobei der Wirtschaft ausreichend Zeit gelassen werden sollte, sich auf die neuen Bestimmungen einzustellen. Eine einjährige Übergangsfrist erscheint für die Wirtschaft ausreichend, um sich an die neuen Rahmenbedingungen anzupassen.

In 35. Zu Artikel 3 Nummer 3 (§ 15a TMG)

Zu Artikel 4 Nummer 1 (§ 93 Absatz 3 TKG)

a) In Artikel 3 Nummer 3 ist in § 15a nach dem Wort „Dritten“ das Wort „unrechtmäßig“ einzufügen.

b) In Artikel 4 Nummer 1 ist in § 93 Absatz 3 nach dem Wort „Dritten“ das Wort „unrechtmäßig“ einzufügen.

Begründung:

Klarstellung des Gewollten und redaktionelle Angleichung an die in Artikel 1 Nummer 8 gewählte Formulierung des § 42a Absatz 1 Satz 1 BDSG.

In 36. Zu Artikel 4 Nummer 2 (§ 95 Absatz 5 TKG)

Artikel 4 Nummer 2 ist wie folgt zu fassen:

’2. In § 95 Absatz 5 werden nach den Wörtern „wenn dem Teilnehmer ein anderer Zugang zu diesen Telekommunikationsdiensten“ die Wörter „ohne die Einwilligung“ eingefügt.’

Begründung

Die Entwurfsfassung ist missverständlich, weil das Wort „Telekommunikationsdiensten“ in § 95 Absatz 5 zweimal verwendet wird. Die Ergänzung bezieht sich allein auf den zweiten Halbsatz.

Zum Gesetzentwurf allgemein

Wi 37. Der Bundesrat anerkennt die Zielsetzung des Gesetzentwurfs, ein hohes Niveau beim Datenschutz im nicht-öffentlichen Bereich zu gewährleisten und dafür effektive Instrumente - vom freiwilligen Datenschutzaudit für Unternehmen bis hin zu geeigneten Kontrollverfahren - zur Verfügung zu stellen. Die Datenmissbrauchsfälle in der Vergangenheit haben gezeigt, dass die Befürchtungen von Verbrauchern und Medien hinsichtlich des rechtswidrigen Handels mit personenbezogenen Daten ernst zu nehmen

sind. Illegaler Datenhandel muss deshalb mit allen zur Verfügung stehenden Mitteln unterbunden werden, ebenso wie Kontrolldefizite hinsichtlich der Einhaltung der Datenschutzregelungen und gesetzliche Schutzlücken ausgeräumt werden müssen.

R 38. Der Bundesrat bittet die Bundesregierung, einen Diskussionsentwurf für ein grundsätzlich überarbeitetes Datenschutzrecht vorzulegen, der die allgemeinen Regelungen im Bundesdatenschutzgesetz mit den bereichsspezifischen Vorschriften zusammenführt und systematisiert sowie das Datenschutzrecht angesichts neuer Formen und Techniken der Verarbeitung personenbezogener Daten risikoadäquat fortentwickelt.

Begründung:

Datenschutz ist Grundrechtsschutz und Funktionsbedingung eines demokratischen Gemeinwesens. Er ist notwendiger Bestandteil einer freiheitlichen Kommunikationsordnung. Teilhabe und Teilnahme an demokratischer Willensbildung und einem freien Wirtschaftsverkehr sind nur zu erwarten, wenn jeder Teilnehmer sein Handeln auf freier Willensbildung gründen kann. Diese ist nur möglich, wenn die Erhebung und Verwendung von Daten über ihn seiner freien Selbstbestimmung unterliegt (vgl. BVerfG, Urteil vom 15. Dezember 1983 - 1 BvR 209/83 u.a. -, BVerfGE 65, 1 - "Volkszählungsurteil"). Datenschutz ist zudem ein wichtiger Akzeptanzfaktor in der Informationsgesellschaft. Seine rechtliche Gestaltung beeinflusst die Entwicklung einer modernen Wirtschaft. Er ist der entscheidende Vertrauensfaktor, der es ermöglicht, in der Informationsgesellschaft personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen.

Diesen Grundsätzen trägt das derzeitige Datenschutzrecht in Deutschland nur noch bedingt Rechnung. Es ist immer noch zu sehr auf das Konzept der räumlich abgegrenzten Datenverarbeitung fixiert, nimmt neue Formen personenbezogener Daten und deren Verarbeitung nur ungenügend auf und berücksichtigt unzureichend die Gefahren und Chancen neuer Techniken der Datenverarbeitung. Darüber hinaus ist es in seinen Formulierungen häufig widersprüchlich und durch seine Normierung in hunderten von speziellen Gesetzen unübersichtlich und schwer zu handhaben.

Es gilt daher, zum einen die Konsistenz der gesetzlichen Regelung und damit deren Glaubwürdigkeit zurückzugewinnen. Das Volkszählungsurteil verlangt vollzugsgeeignete Regelungen, deren effektive Kontrolle sichergestellt ist. Voraussetzungen und Umfang der Beschränkungen des informationellen Selbstbestimmungsrechts müssen klar und für den Betroffenen erkennbar geregelt werden. Dies verlangt eine gezielte Reduktion der bereichsspezifischen

Datenschutzvorschriften und deren sorgfältige Abstimmung mit den allgemeinen Datenschutzgesetzen. Darüber hinaus müssen die Transparenz der Datenverarbeitung und die Selbstbestimmung der Betroffenen gestärkt sowie die Selbstregulierung und Selbstkontrolle der Datenverarbeiter ermöglicht und verbessert werden.

Zum anderen zwingt die Entwicklung der Kommunikationstechnologie dazu, das Datenschutzrecht fortzuentwickeln. Ein modernes Datenschutzrecht kann sich nicht mehr auf rein normative Vorgaben verlassen. Die Verarbeitungstechnologie muss anders als bisher nicht nur Regelungsgegenstand, sondern ebenso Regelungsmittel sein. Regelungen, die das Recht auf informationelle Selbstbestimmung einschränken, müssen Vorgaben für die Entwicklung und verbindliche Nutzung technischer Vorkehrungen enthalten, die einen datenschutzkonformen Ablauf des Verarbeitungsprozesses sichern. Vor allem im nicht-öffentlichen Bereich müssen zudem Konzepte des Selbstdatenschutzes und des Systemdatenschutzes umgesetzt werden.

Als Grundlage für eine Überarbeitung des Datenschutzrechts können die Ergebnisse des Gutachtens "Modernisierung des Datenschutzrechts" herangezogen werden, das Alexander Roßnagel, Andreas Pfitzmann und Hansjürgen Garstka 2001 im Auftrag des Bundesministerium des Innern erstellt haben.

Ausgehend hiervon sollte insbesondere geprüft werden, ob die bisherige Normenflut und Rechtszersplitterung verringert und Widersprüche vermieden werden können, indem das Vorrangverhältnis zwischen Bundesdatenschutzgesetz und bereichsspezifischen Regelungen umgedreht wird. Ein allgemeines Gesetz könnte anstelle von offenen Abwägungsklauseln grundsätzliche und präzise Regelungen der Verarbeitung personenbezogener Daten festlegen. Darüber hinaus könnte das Gesetz allgemeine Regelungen zur Technikgestaltung, zur Datensicherung, zur Datenschutzorganisation, zur Datenschutzkontrolle und zur Selbstregulierung enthalten. Spezialregelungen in bereichspezifischen Gesetzen könnten sich dann auf Ausnahmen von den allgemeinen Regelungen beschränken und nur für bestimmte riskante Datenverarbeitungen die Anforderungen verschärfen oder bei unterdurchschnittlich riskanten Datenverarbeitungen Erleichterungen bieten. Zudem sollte geprüft werden, ob die datenschutzrechtlichen Vorschriften des Telekommunikations- und Multimediarechts in das Bundesdatenschutzgesetz integriert werden können. Dadurch könnten Wertungswidersprüche und Überschneidungen der Anwendungsbereiche beseitigt sowie eine Vereinheitlichung auf hohem Niveau erreicht werden.

A 39.a) Der Bundesrat hält es für notwendig, das Bundesdatenschutzgesetz als Verbraucherschutzgesetz im Sinne des § 2 des Unterlassungsklagengesetzes (UKlaG) anzuerkennen. Durch eine entsprechende Klarstellung im UKlaG würden Verbraucherzentralen und ähnliche Organisationen in die Lage versetzt werden, einen entsprechenden Unterlassungsanspruch geltend zu machen.

b) Der Bundesrat sieht eine Kennzeichnung der Herkunft personenbezogener Daten sowie die Protokollierung ihrer Weitergabe als eine wichtige Voraussetzung dafür an, Datenmissbräuche effektiv verfolgen zu können. Die Bundesregierung wird gebeten, einen Bericht über mögliche Verfahren zur Kennzeichnung der Herkunft von Daten und zur Dokumentation der Datenweitergabe vorzulegen und Vorschläge zu unterbreiten, wie diese etabliert werden können.

Begründung (nur gegenüber dem Plenum):

Zu Buchstabe a:

In der Rechtsprechung werden einzelne Vorschriften des Bundesdatenschutzgesetzes bislang nicht als Verbraucherschutzgesetze im Sinne des § 2 UKlaG anerkannt. Aus diesem Grund sind Verbraucherverbände und ähnliche Organisationen nicht berechtigt, wegen Verstoßes gegen datenschutzrechtliche Vorschriften Ansprüche auf Unterlassung nach § 2 UKlaG zu stellen.

Eine entsprechende Klarstellung, dass auch datenschutzrechtliche Vorschriften als Verbraucherschutzgesetze anerkannt werden, könnte dazu beitragen, dass die Rechtsvertretung der Verbraucher im Kollektiv auch im Bereich des Datenschutzrechts gestärkt wird. Auf diese Weise werden nicht nur die Rechtsschutzmöglichkeiten des einzelnen Verbrauchers, sondern vor allem der kollektive Schutz der Verbraucherinteressen verbessert.

Zu Buchstabe b:

Nach den geltendem § 34 des Bundesdatenschutzgesetzes sind die verantwortlichen Stellen derzeit nicht verpflichtet, Auskunft über die originäre Herkunft der Daten, soweit diese nicht von den Unternehmen gespeichert werden, zu erteilen. Eine Kennzeichnung der Herkunft personenbezogener Daten sowie die Protokollierung ihrer Weitergabe stellt eine wichtige Voraussetzung dar, um Datenmissbräuche effektiv verfolgen zu können und eine Überprüfung durch die Aufsichtsbehörden zu erleichtern. Die Bundesregierung wird gebeten zu berichten, welche Möglichkeiten bestehen, eine entsprechende Herkunftskennzeichnung und Protokollierungspflicht einzuführen.