Deutscher Bundestag **Drucksache 17/12319**

17. Wahlperiode 04. 01. 2013

Unterrichtung

durch die Bundesregierung

Bericht über die Auswirkungen der §§ 30a und 42a des Bundesdatenschutzgesetzes

Inhaltsverzeichnis

A. Auftrag

Die sogenannte BDSG-Novelle II (Bundestagsdrucksache 16/12011 mit den Änderungen der Bundestagsdrucksache 16/13657; in Kraft getreten am 1. September 2009) enthält in dem neu eingefügten § 48 den Auftrag an die Bundesregierung, über die Auswirkungen der §§ 30a und 42a des Bundesdatenschutzgesetzes (BDSG) bis zum 31. Dezember 2012 zu berichten.

Dieser Berichtspflicht kommt die Bundesregierung im Folgenden nach.

B. Bericht

I. § 30a BDSG

1. Ziel der Regelung

Die Regelung soll – entsprechend einer Prüfbitte des Bundesrates – den Besonderheiten der geschäftsmäßigen Markt- und Meinungsforschung gegenüber der Werbung Rechnung tragen. Die geschäftsmäßige Markt- und Meinungsforschung 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.

2. Auswirkungen in der Praxis

Erfahrungen mit den Regelungen des § 30a BDSG liegen außerhalb der Markt- und Meinungsforschungsinstitute nicht bzw. kaum vor. In anderen Wirtschaftsbranchen sowie für die Tätigkeit der Aufsichtsbehörden hatte die Vorschrift seit ihrem Inkrafttreten keine Relevanz.

Für die Markt- und Meinungsforschungsinstitute haben sich die folgenden Verbände der Markt- und Sozialforschung in Deutschland in einer gemeinsamen Stellungnahme zu den Auswirkungen der gesetzlichen Vorschriften des § 30a BDSG auf die Praxis der Markt-, Meinungs- und Sozialforschung geäußert:

– Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute (ADM)

– Arbeitsgemeinschaft Sozialwissenschaftlicher Institute e.V. (ASI)

– Berufsverband Deutscher Markt- und Sozialforscher e.V. (BVM)

– Deutsche Gesellschaft für Online-Forschung e.V. (DGOF)

Die Verbände begrüßen insbesondere, dass mit § 30a BDSG die sachlich nicht zutreffende Gleichsetzung mit der Werbung, der Tätigkeit von Auskunfteien und mit dem Adresshandel im Datenschutzrecht aufgehoben wurde und die bewährten grundlegenden berufsständischen Verhaltensregeln der geschäftsmäßigen Markt-, Meinungs- und Sozialforschung Gesetzesrang erhalten haben.

Redaktionell wird angemerkt, dass zu einem besseren Verständnis der Norm die Sätze 1 und 2 in § 30a Absatz 2 BDSG getauscht werden sollten.

Die Aufsichtsbehörden haben in keinem Falle von gravierenden Problemen bei der Auslegung bzw. der Anwendung der Normen berichtet.

Unterschiedlich diskutiert wird teilweise die Abgrenzung zwischen der Eigen-Marktforschung durch Unternehmen

Zugeleitet mit Schreiben des Bundesministeriums des Innern vom 31. Dezember 2012 gemäß § 48 Absatz 1 Satz 1 des Bundesdatenschutzgesetzes

nach § 28 BDSG, der geschäftsmäßigen Markt- und Meinungsforschung im Sinne von § 30a BDSG sowie der wissenschaftlichen Forschung nach § 40 BDSG.

3. Stellungnahme der Bundesregierung

§ 30a Absatz 2 BDSG regelt die Zweckbindung der im Rahmen des § 30a erhobenen Daten. Satz 1 enthält die allgemeine Regel, Satz 2 eine Sonderregelung für Daten, die nicht aus allgemein zugänglichen Quellen entnommen worden sind und die die verantwortliche Stelle auch nicht veröffentlichen darf. Satz 3 regelt sodann die Verwendung von Daten für andere als die in den Sätzen 1 und 2 genannten Zwecke. Angesichts dieser Abfolge sieht die Bundesregierung einen Änderungsbedarf nicht.

Die zum Teil diskutierten Abgrenzungsprobleme zwischen der Eigen-Marktforschung durch Unternehmen nach § 28 BDSG, der geschäftsmäßigen Markt- und Meinungsforschung im Sinne von § 30a BDSG und der wissenschaftlichen Forschung nach § 40 BDSG sind nach Auffassung der Bundesregierung Fragestellungen, die typischerweise mit der Anwendung der abstrakten Norm in der Praxis einhergehen. Da durch diese Auslegungsfragen bislang keine gravierenden praktischen Probleme aufgetreten sind, sieht die Bundesregierung keinen Handlungsbedarf.

II. § 42a BDSG

1. Ziel der Regelung

Die Vorschrift enthält eine Informationspflicht für nichtöffentliche Stellen und diesen gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen in den Fällen, in denen bestimmte besonders sensible personenbezogene Daten unrechtmäßig übermittelt oder Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Die Vorschrift knüpft an einen Vorschlag der Kommission der Europäischen Gemeinschaften zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (KOM(2007) 698 endg.) sowie Regelungen im Recht der Vereinigten Staaten von Amerika mit dem Grundgedanken der „security breach notification“ an. Die Informationspflicht ist nach Satz 1 Nummer 1 bis 4 auf besonders sensible personenbezogene Daten aus dem Verfügungsbereich der verantwortlichen Stelle begrenzt.

Voraussetzung ist, dass die verantwortliche Stelle anhand von tatsächlichen Anhaltspunkten feststellt, dass bei ihr gespeicherte personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen. Letzteres bestimmt sich unter anderem nach der Art der Daten und den potenziellen Auswirkungen der unrechtmäßigen Kenntniserlangung durch Dritte auf die Betroffenen. Die verantwortliche Stelle hat in diesem Fall sowohl die zuständige Datenschutzaufsichtsbehörde als auch die Betroffenen zu informieren.

Während die Benachrichtigung der Aufsichtsbehörden aufgrund ihrer Verschwiegenheitspflicht auch vor der Beseitigung von Datensicherheitslücken und im Falle laufender Strafverfolgungsmaßnahmen erfolgen muss, stellt Satz 2 für die Benachrichtigung der Betroffenen klar, dass ein schuldhaftes Zögern insbesondere dann nicht gegeben ist, soweit die Datensicherungspflichten des § 9 BDSG oder Interessen der Strafverfolgung einer Veröffentlichung der Datenschutzverletzung vorläufig noch entgegenstehen. Im ersteren Fall zielt die Regelung darauf ab, dem Verpflichteten die Möglichkeit zu geben, etwaige technische Sicherheitslücken, unter deren Ausnutzung die Datenschutzverletzung erfolgte, zu analysieren und so weit wie möglich zu beheben, bevor breitere Kreise von der Lücke Kenntnis erhalten. Dies entspricht dem in Fachkreisen mit „Responsible Disclosure“ („Verantwortungsvolle Offenlegung“) bezeichneten Vorgehen.

Die Vorschrift dient damit zum einen der Eindämmung von Schäden, die durch die Datenschutzverletzung insbesondere beim Betroffenen entstanden sind. Als Reflex soll sie zum anderen zu verstärkten Anstrengungen der Unternehmen zur Sicherung dieser Daten führen.

2. Auswirkungen in der Praxis

Die Auswirkungen der neu geschaffenen Norm können vor allem anhand der Feststellungen der Aufsichtsbehörden dargestellt und ausgewertet werden, zumal, da ihnen gegenüber eine Meldepflicht besteht. Aufgrund ihrer Unabhängigkeit steht es den Aufsichtsbehörden frei, dem Bund über ihre Erfahrungen zu berichten. Gleichwohl haben die Länder und der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die Anzahl der nach § 42a BDSG abgegebenen Meldungen mitgeteilt. Von den insgesamt 305 gemeldeten Fällen wurde nach den vorliegenden Unterlagen in 177 Fällen das Vorliegen der Tatbestandsvoraussetzungen des § 42a BDSG bejaht.

Soweit der Hintergrund der Meldungen geschildert wurde, lassen sich folgende typische Fälle feststellen:

- Verlust (Diebstahl, Abhandenkommen) von Hardware (USB-Stick/Laptop/Notebook)
- Falscher Versand/Verlust von Dokumenten mit personenbezogenen Daten (z. B. Bankunterlagen wie Kontoauszüge etc.)
- Unberechtigter Zugriff auf Webserver/Erschleichen von Daten

Der Schwerpunkt der Meldungen nach § 42a BDSG liegt erwartungsgemäß in solchen Ländern, die über eine hohe Dichte von Unternehmen verfügen, die personenbezogene Daten verarbeiten.

Im Einzelnen liegen folgende Meldungen (Stand 13. Dezember 2012) vor:

Aufsichtsbehörde	Meldungen insgesamt	§ 42a bejaht
Baden-Württemberg 03.2011 bis 15.10.2012	22	14
Bayern bis 12.2012	49	29
Berlin 03.2011 bis 08.2012	40	22
Brandenburg 01.2012 bis 01.10.2012	2	1
Bremen 03.2011 bis 09.10.2012	4	4
Hamburg 03.2011 bis 12.2012	41	14
Hessen bis 02.2012	24	21
Mecklenburg-Vorpommern bis 03.2012	0	0
Niedersachsen 03.2011 bis 12.2012	19	7
Nordrhein-Westfalen 20.11.2009 bis 06.12.2012	64	45
Rheinland-Pfalz bis 02.2012	12	2
Saarland 28.02.2011 bis 17.04.2011	1	0
Sachsen bis 02.2012	7	5
Sachsen-Anhalt bis 03.2012	0	0
Schleswig-Holstein bis 03.2012	10	5
Thüringen 09.12.2011 bis 03.04.2012	4	4
Bund bis 02.2012	6	4

Zum Verständnis der Tabelle muss darauf hingewiesen werden, dass die Aufsichtsbehörden aufgrund EU-Rechts und der entsprechenden deutschen Vorschriften völlig unabhängig sind und im Rahmen dieser Unabhängigkeit eigenständig beurteilen, ob ein Fall des § 42a BDSG vorliegt.

3. Stellungnahmen der Aufsichtsbehörden für den Datenschutz

Einige Aufsichtsbehörden für den Datenschutz haben kritische Anmerkungen zu der Norm übermittelt:

a. Der Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI) Nordrhein-Westfalen (NRW), (für den letzten Spiegelstrich schließt sich der Berliner Beauftragte für Datenschutz und Informationsfreiheit an) weist darauf hin, dass es

   – unterschiedliche Interpretationen zwischen Aufsichtsbehörde und Unternehmen hinsichtlich der Voraussetzungen für die Anwendbarkeit des § 42a BDSG, wann eine schwerwiegende Rechts- und Interessenbeeinträchtigung droht, gebe. Es fehlten Richtlinien für die Gefahrenprognose, um in der Praxis eine einheitliche Entscheidungsfindung herbeiführen zu können

   – zweifelhaft sei, ob auch ein Dritter, stellvertretend für den Benachrichtigungspflichtigen, der Informationspflicht nachkommen könne (z. B. Versicherung stellvertretend für selbständige Makler)

   – ein Spannungsverhältnis zwischen der Notwendigkeit der Benachrichtigung und dem Vorbehalt für die Ermittlungstätigkeit bestehe

   – unterschiedliche Voraussetzungen bzw. eine Kollision zwischen § 42a BDSG und § 15a Telemediengesetz (TMG)/§ 93 Telekommunikationsgesetz (TKG) bestünden: Beim TMG reiche es schon aus, wenn „nur“ Bestandsdaten betroffen seien.

   Die Bundesregierung sieht keinen Änderungsbedarf.

   Die hier geschilderten Abgrenzungs- und Interpretationsdifferenzen zwischen den Aufsichtsbehörden und den Unternehmen sind nach Auffassung der Bundesregierung Fragestellungen, die typischerweise mit der abstrakten Norm in der Praxis einhergehen. Da durch diese Auslegungsfragen bislang keine gravierenden praktischen Probleme aufgetreten sind, sieht die Bundesregierung keinen Handlungsbedarf.

   Nicht erkennbar ist, warum bei den in § 42a BDSG erforderlichen Meldungen die Stellvertretungsregelungen nicht gelten sollten.

   Die Bundesregierung sieht das Spannungsverhältnis zwischen der Notwendigkeit der Benachrichtigung und dem Vorrang der Ermittlungstätigkeit, das § 42a Satz 2 BDSG in sich birgt. Da insbesondere von Hacker-Angriffen in aller Regel eine erhebliche Wiederholungsgefahr ausgeht, sollte nach Auffassung der Bundesregierung im gesamtgesellschaftlichen Interesse daran festgehalten werden, dass der Strafverfolgung zunächst Vorrang vor der Schadensminderung im Einzelfall eingeräumt wird. Vor allem bei drohenden schwerwiegenden Rechts- und Interessenbeeinträchtigungen des Betroffenen sollte die verantwortliche Stelle aber Kontakt mit den Strafverfolgungsbehörden aufnehmen, um in Erfahrung zu bringen, wie und ob den Interessen des Betroffenen Rechnung getragen werden kann.

Im Hinblick auf die Regelungen des § 15a des Telemediengesetzes (TMG) und § 93 Absatz 3 des Telekommunikationsgesetzes (TKG) wird auf die Begründung im Gesetzentwurf der Bundesregierung hingewiesen. Danach zielten die entsprechenden Gesetzesänderungen darauf ab, die Vorschrift des § 42a BDSG bereichsspezifisch auch für Bestands- und Nutzungsdaten des Telemediengesetzes sowie für Bestands- und Verkehrsdaten des Telekommunikationsgesetzes zur Anwendung zu bringen (vgl. Bundestagsdrucksache 16/12011, S. 36). Wegen des Erfordernisses, dass schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers drohen müssen, sieht die Bundesregierung keinen Wertungswiderspruch.

§ 93 Absatz 3 TKG wurde durch Artikel 1 des Gesetzes zur Änderung telekommunikationsrechtlicher Regelungen vom 3. Mai 2012 (BGBl. I, S.958) geändert. In Umsetzung des geänderten Artikel 4 der Datenschutzrichtlinie 2002/58/EG (vgl. RL 2009/136/EG v. 25. November 2009, Abl. L 337 v. 18. Dezember 2009, S. 30) sind die Rechte und Pflichten für den Fall der Verletzung personenbezogener Daten durch Anbieter öffentlich zugänglicher Telekommunikationsdienste nunmehr im neuen § 109a TKG ausführlich geregelt. Daneben kommt nur noch § 42a Satz 6 BDSG entsprechend zur Anwendung (vgl. § 109a Absatz 1 TKG).

b. Dem Landesbeauftragten für Datenschutz und Informationsfreiheit Bremen und dem Bayerischen Landesamt für Datenschutzaufsicht (denen sich der Berliner Beauftragte für Datenschutz und Informationsfreiheit anschließt) zufolge sollte § 42a Satz 1, 2. Alt. BDSG in der Weise klar gestellt werden, dass es genügt, wenn die verantwortliche Stelle feststellt, dass die Daten Dritten unrechtmäßig zur Kenntnis gelangt sein können. Das Abstellen auf die Tatbestandsvoraussetzung, dass die speichernde Stelle feststellt, dass die Daten Dritten zur Kenntnis gelangt sind, sei zu eng und führe in der Praxis zu Diskussionen.

   Die Bundesregierung sieht keinen Änderungsbedarf.

   In der Literatur wird die Regelung richtigerweise so interpretiert, dass eine Meldepflicht nur besteht, wenn eine Kenntniserlangung mit hoher Wahrscheinlichkeit vorliegt (z. B. Dix, in: Simitis, BDSG, § 42a Rdnr. 8). Anderenfalls müsste jede folgenlose Unachtsamkeit gemeldet werden. Dies würde verkennen, dass die Norm keine umfassende Pflicht zur Selbstanzeige oder eine Bestrafung für Unachtsamkeit zum Ziel hat, sondern Schaden vom Betroffenen abwenden und die Verantwortlichen zu einer stärkeren Wahrnehmung ihrer Verantwortung veranlassen will.

c. Die Landesbeauftragte für Datenschutz und Informationsfreiheit Bremen, (der sich der Berliner Beauftragte für Datenschutz und Informationsfreiheit anschließt) kritisiert, dass neben der Tatsache des Abhandenkommens von Daten auch noch gefordert werde, dass aus dem Abhandenkommen Beeinträchtigungen drohen und diese schwerwiegender Art sein müssen. Sie empfiehlt, diese Voraussetzungen zu streichen.

   Die Bundesregierung sieht keinen Änderungsbedarf.

   § 42a BDSG beinhaltet durch die Pflicht zur Selbstoffenbarung und Selbstanzeige einen nicht unerheblichen Eingriff in die Grundrechte der verantwortlichen Stelle. Dieser ist nur zu rechtfertigen, wenn auf der Seite des Betroffenen ebenfalls ein erheblicher Eingriff droht oder stattgefunden hat, selbst wenn eine solche Beeinträchtigung bei sensiblen Daten besonders wahrscheinlich ist.

d. Der Landesbeauftragte für den Datenschutz Niedersachsen (LfD Niedersachsen) ist der Auffassung, dass die Neuregelung nicht zu einer Verbesserung des technisch-organisatorischen Datenschutzes geführt hat.

   Die Bundesregierung sieht keinen Änderungsbedarf.

   Aus den vorliegenden Stellungnahmen, soweit auf diesen Punkt eingegangen wird, kann geschlossen werden, dass von der Norm eine positive Wirkung auf die Umsetzung von technischen und organisatorischen Maßnahmen in Unternehmen ausgeht. Es wird daher davon ausgegangen, dass die aus dem April 2012 stammende Beobachtung der Aufsichtsbehörde noch vorläufig und der Tatsache geschuldet ist, dass die durch das Inkrafttreten der Norm eingeleitete positive Entwicklung in der Zukunft auch im Bereich dieser Aufsichtsbehörde noch deutlicher hervortritt.

4. Stellungnahme der Verbände

a. Die angeschriebenen Verbände haben, soweit überhaupt Antworten vorliegen, übergreifend bestätigt, dass die Regelung positive Folgen zeitigt und sie die Sensibilität für den Datenschutz und infolgedessen die Aufmerksamkeit für die Datensicherheit in der Praxis erhöht hat. Vereinzelt wird von Interpretationsproblemen in dem schon bei den Aufsichtsbehörden erwähnten Rahmen berichtet. Hierzu wurde oben bereits Stellung genommen. Ebenfalls vereinzelt wird darauf hingewiesen, dass die Norm überflüssig sei, da die Unternehmen schon im Eigeninteresse, um Schadenersatz zu entgehen, die Betroffenen über Datenpannen unterrichten würden.

b. Seitens der IT-Wirtschaft (BITKOM) wird ein überaus positives Fazit gezogen. Die Neuregelung sei ein praxistaugliches Instrument für den Fall von Datenpannen. Unternehmen hätten ihre Prozesse im Hinblick auf Datensicherheit weiter optimiert und technisch-organisatorische Maßnahmen (Datenverschlüsselung) zur Vorbeugung unternommen. Neue Prozesse würden etabliert, um im Fall einer Datenpanne die notwendigen Schritte schnell unternehmen zu können. Unternehmen seien nicht unverhältnismäßig belastet, da die Maßnahmen mit der vorhandenen Technik umgesetzt werden könnten. Die Vorschrift gewähre durch den Katalog Rechtssicherheit. Das Merkmal der „drohenden schwerwiegenden Beeinträchtigung“ wahre die Verhältnismäßigkeit des Aufwandes für die verantwortlichen Stellen. Der Schutz des § 42a Satz 6 BDSG (Verwertungsverbot) sei für die Effektivität sinnvoll. Der Verband regt an, die Vorschrift in der geltenden

Fassung beizubehalten und als Vorbild für die Regelung entsprechender Mitteilungspflichten auf EU- bzw. Bundesebene zu nehmen.

c. Von Seiten der Banken wird kritisiert, dass die verantwortliche Stelle in Fällen des § 42a BDSG selbst Opfer eines Datenmissbrauchs sei und deshalb Folgenbeseitigung und Schadensbegrenzung im Interesse der verantwortlichen Stelle und der Betroffenen im Vordergrund stehen müssten. Die Schwelle für Meldungen müsse hoch sein, um eine Meldeflut zu verhindern und die Wahrnehmungsbereitschaft bei den Betroffenen zu erhalten (Erfahrungen aus den USA). Wenn die verantwortliche Stelle durch Gegenmaßnahmen die Missbrauchsgefahr abhanden gekommener Daten weitgehend beseitige, solle das Verfahren nach § 42a BDSG grundsätzlich seine Erledigung finden.

   Das strafrechtliche Verwertungsverbot sollte auf die in dem Unternehmen tätigen Personen ausgedehnt werden, da sonst ggf. Mitarbeiter keine Meldung machen, um sich nicht selbst zu belasten.

   Die Bundesregierung sieht keinen Änderungsbedarf.

   In bestimmten Fällen (Hacking) können sich Banken – auch – in der Rolle des Opfers einer Straftat befinden. Die Informationspflicht des § 42a BDSG dient aber nicht dazu, ein Fehlverhalten der verantwortlichen Stelle zu ahnden, sondern Schaden zu mindern. Wenn die übrigen Anforderungen erfüllt sind (Drohen schwerwiegender Beeinträchtigungen s. o.), ist es insofern sachgerecht, dass die Banken diesen Offenbarungspflichten gleichermaßen unterliegen. Da das Abhandenkommen von Konto- und anderen Bankdaten für die Betroffenen eine erhebliche Schadensgefahr bedeuten kann, tragen die Banken nicht nur besondere Verantwortung bei der Absicherung der Daten, sondern auch bei der Schadensminderung mittels der Mitteilungen nach § 42a BDSG.

   Das strafrechtliche Verwertungsverbot in § 42a Satz 6 BDSG dient der verfassungskonformen Auflösung des Spannungsverhältnisses, das darin besteht, dass der Benachrichtigungspflichtige sich entweder selbst bezichtigt oder nach § 43 Absatz 2 Nummer 7 BDSG ordnungswidrig verhält (vgl. Bundestagsdrucksache 16/12011, S. 35). Benachrichtigungspflichtig sind nach § 42a BDSG nicht-öffentliche Stellen im Sinne des § 2 Absatz 4 BDSG und diesen gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen nach § 27 Absatz 1 Satz 1 Nummer 2 BDSG. Das Verwendungsverbot in Satz 6 ist damit auf natürliche und juristische Personen sowie deren vertretungsberechtigte Organe und die von diesen mit der eigenverantwortlichen Aufgabenwahrnehmung beauftragten Personen anwendbar. Für eine Ausdehnung auf alle in einem Unternehmen tätigen Mitarbeiter besteht kein Bedarf, da diese nicht taugliche Täter von Datenschutzverstößen sind und gleichzeitig der Informationspflicht unterliegen.

C. Ergebnisse/Vorschläge

Sowohl § 30a BDSG als auch § 42a BDSG finden erst seit kurzer Zeit praktische Anwendung. Dem vorstehenden Bericht gem. § 48 BDSG zufolge haben sie sich bislang bewährt. Änderungen an den Vorschriften werden von Seiten der Bundesregierung derzeit nicht empfohlen.

Insbesondere im Hinblick auf die Informationspflicht bei Datenschutzverletzungen zeigt die Zahl der Meldungen nach § 42a BDSG, dass die Regelung trotz aller Diskussion um die richtige Interpretation, die eine solche fundamentale Neuregelung mit sich bringt, in der Praxis angenommen wird und zu mehr Transparenz führt. Die damit verbundene Öffentlichkeitswirksamkeit trägt zudem dazu bei, das Datenschutz-Bewusstsein in den Unternehmen weiter zu stärken. Vor diesem Hintergrund hält die Bundesregierung eine solche Informationspflicht auch auf europäischer Ebene für sinnvoll. Entsprechende Vorschläge der EU-Kommission im Entwurf für eine Datenschutz-Grundverordnung sind derzeit Gegenstand der Diskussion innerhalb der Bundesregierung und auf europäischer Ebene.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333