Mauricio F. Paez (Attorney at Law; Jones Day New York), *Jörg Rehder* (Rechtsanwalt; Attorney at Law (Maryland und Minnesota) und Solicitor (England und Wales); Jones Day – Frankfurt/Main), *Gwendolynne Chen* (Attorney at Law; Jones Day New York) und *Joseph Bernasky* (Attorney at Law; Jones Day New York)*

Verschärfung des Bundesdatenschutzgesetzes; Einführung einer Informationspflicht bei Datenverstößen – Vergleich mit den Vereinigten Staaten

Im Juli 2009 hat der deutsche Gesetzgeber ein Gesetzgebungspaket zur Novellierung des Bundesdatenschutzgesetzes („BDSG" oder das „Gesetz") verabschiedet. Dieses Paket enthält drei BDSG-Novellen. Am 1. September 2009 ist die BDSG-Novelle II in Kraft getreten, die verschiedene umstrittene Änderungen des Datenschutzrechtes (die „Änderungen") enthält.[1] Obwohl die II.-Novelle nicht so umfassend war, wie viele anfangs gehofft oder gefürchtet hatten, werden einige der Änderungen zweifellos unmittelbare Auswirkungen auf in Deutschland tätige Unternehmen haben.

Die Änderungen erstrecken sich auf viele Felder im geschäftlichen Bereich, einschließlich der Nutzung von Datenlisten für Zwecke der Markt- und Meinungsforschung, der Verwaltung bzw. Benutzung von Arbeitnehmerdaten und Vertragsbestimmungen in Datenübermittlungsverträgen. Die II.-Novelle sieht außerdem eine Erhöhung der Bußgelder für Verstöße gegen das BDSG sowie erweiterte Befugnisse der Aufsichtsbehörden vor. Die bedeutsamste Änderung besteht jedoch in der neu eingeführten Informationspflicht bei Datenschutzverletzungen[2], die in ihrem Umfang verschiedenen bundesstaatlichen Bestimmungen der Vereinigten Staaten ähnelt[3].

I. Das BDSG

Das BDSG untersagt die Erhebung[4], Verarbeitung[5] und Nutzung[6] von „personenbezogenen Daten", sofern die betroffene Person (der „Betroffene") nicht ausdrücklich einwilligt oder das BDSG (bzw. eine andere Rechtsvorschrift) dies ausdrücklich erlaubt.[7] Im BDSG wird der Begriff „personenbezogene Daten" weit ausgelegt. Er umfasst sämtliche Angaben über persönliche und sachliche Verhältnisse einer natürlichen Person.[8] In diesem Zusammenhang ist die im BDSG für zulässig erklärte Ausnahme des „Listenprivilegs" am umstrittensten.

Gemäß dem bisherigen „Listenprivileg" können personenbezogene Daten, wie der Name, die Anschrift, die Berufsbezeichnung und das Geburtsjahr der Person, ohne die vorherige Einwilligung des Betroffenen für unternehmenseigene Zwecke der Werbung sowie der Markt- und Meinungsforschung verwendet werden und an Dritte (wie Direktmarketingunternehmen) für ähnliche Zwecke übermittelt werden, vorausgesetzt, dass diese Angaben listenmäßig für eine Personengruppe zusammengefasst wurden.[9] Die Betroffenen können einer Verbreitung oder Nutzung ihrer Daten widersprechen,[10] jedoch wird diese Möglichkeit aus praktischer Sicht selten wahrgenommen. Viele Datenschutzexperten sind der festen Überzeugung, dass diese Ausnahme ausschlaggebend dafür ist, dass eine große Menge personenbezogener Daten zu relativ niedrigen Preisen insbesondere über das Internet verkauft werden.[11] Dementsprechend sieht die II.-Novelle nun vor,

* Mauricio F. Paez, Gwendolynne Chen und Joseph Bernasky sind als Rechtsanwälte bei Jones Day New York, Jörg Rehder, Attorney at Law (Maryland und Minnesota) und Solicitor (England und Wales) ist als REchtsanwalt bei Jones Day Frankfurt/Main tätig.

1 Bundesdatenschutzgesetz vom 20.12.1990, BGBl. I 2954, in der jeweils gültigen Fassung.

2 Bei „Datenschutzverletzungen" handelt es sich um einen generischen Begriff, der alle Ereignisse umfasst, die die Gefährdung der Sicherheit oder der Integrität von personenbezogenen Daten zur Folge haben.

3 In den Vereinigten Staaten haben 45 Bundesstaaten, der District of Columbia, Puerto Rico und die Jungferninseln Gesetze erlassen, die Benachrichtigungen von Sicherheitsverstößen bei personenbezogenen Daten verlangen, wobei jedoch die Auslöser und Empfänger dieser Benachrichtigungen von Bundesstaat zu Bundesstaat unterschiedlich sind. Bundesstaaten ohne Gesetzgebung zur Benachrichtigung bei Datenschutzverletzungen sind Alabama, Kentucky, Mississippi, New Mexico und South Dakota. *State Security Breach Notification Laws, National Conference of State Legislature*, abrufbar unter http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotification-Laws/tabid/13489/Default.aspx (auf alle Websites wurde zuletzt am 20.10.2009 zugegriffen).

4 „Erhebung" bezeichnet das Beschaffen von Daten über den Betroffenen. § 3 Abs. 3 BDSG.

5 „Verarbeiten" bezeichnet das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. § 3 Abs. 4 BDSG.

6 „Nutzen" bezeichnet jede Verwendung personenbezogener Daten, soweit es sich nicht um eine Verarbeitung handelt. § 3 Abs. 5 BDSG.

7 § 4 Abs. 1 BDSG.

8 § 3 Abs. 1 BDSG. Demgegenüber legt Kalifornien, wie auch viele andere US-Bundesstaaten, „personenbezogene Daten" enger aus als eine vorgeschriebene Kombination von bestimmten Datenkategorien:
„personenbezogene Daten" bezeichnen den Vornamen oder Anfangsbuchstaben und den Nachnamen einer Person in Verbindung mit einem oder mehreren der folgenden Datenelemente, wenn entweder der Name oder die Datenelemente nicht verschlüsselt sind:
(1) Sozialversicherungsnummer.
(2) Führerscheinnummer oder Nummer des kalifornischen Ausweises.
(3) Kontonummer, Kredit- oder Bankkartennummer in Verbindung mit der jeweils erforderlichen Geheimzahl, dem Zugangscode oder Passwort, wodurch der Zugriff auf das Bankkonto der Person ermöglicht wird.
(4) Medizinische Informationen.
(5) Krankenversicherungsangaben.
California Computer Security Breach Notification Act, Cal. Civ. Code Ann. § 1798.82(e) (2009).

9 § 28 Abs. 3 BDSG (alte Fassung). Es ist zulässig, personenbezogene Daten für Zwecke der Markt- und Meinungsforschung und der Werbung zu übermitteln oder zu nutzen, wenn es sich um listenmäßige oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf:
- eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
- Berufs-, Branchen- oder Geschäftsbezeichnung,
- Name,
- Titel,
- akademische Grade,
- Anschrift,
- Geburtsjahr

beschränken und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung seiner Daten hat. Id.

10 §§ 6 Abs. 1 und 28 Abs. 4 BDSG.

11 *Schmitt*, Novellierung des BDSG: Datenschutz verbessert, April 2009, abrufbar unter http://www.dgrv.de/webde.nsf/.../$FILE/Novellierung_des_BDSG.pdf.

dass eine Person oder Stelle, die personenbezogene Daten erhebt, verarbeitet oder nutzt („verantwortliche Stelle"),[12] die Einwilligung von Betroffenen einholen muss. Gewisse zusammengefasste personenbezogene Daten, z. B. Datenlisten, dürfen jedoch auch ohne Einwilligung übermittelt werden, für (1) Zwecke der Werbung für eigene Angebote der verantwortlichen Stelle; (2) Zwecke der Werbung im Geschäftskontext, z. B. für die berufliche Tätigkeit; und (3) Zwecke der Werbung für Spenden. Die einwilligungsfreie Übermittlung ist ebenfalls zulässig, wenn (4) die Stelle, die die Daten erstmalig erhoben hat, aus der Werbung eindeutig hervorgeht und diese sowohl die Herkunft der Daten als auch den Empfänger der Daten für die Dauer von zwei Jahren speichert[13] und dem Betroffenen auf Verlangen Auskunft darüber erteilt.

In Deutschland ist die Anzahl an Datenschutzpannen, bei denen es um die fahrlässige Veröffentlichung bzw. den unerlaubten Handel mit Adresslisten und Bankkontoinformationen ging, in den letzten Jahren stark angestiegen.[14] Außerdem wurde einigen der größten deutschen Unternehmen in Schlüsselindustrien wie Verkehr, Finanzen, Automobil, Einzelhandel und Gesundheitswesen vorgeworfen, in das Grundrecht ihrer Mitarbeiter auf Privatsphäre[15] einzugreifen, z. B. durch Überwachung der personenbezogenen Daten und Tätigkeiten ihrer Mitarbeiter.[16] Die Berichterstattung in den Medien über diese Entwicklung stieß auf großes öffentliches Interesse bei Politikern, Gewerkschaften und Konsumenten am Missbrauch personenbezogener Daten.[17] Dementsprechend zielten etliche Gesetzesvorschläge Anfang des Jahres auf die vollständige Abschaffung des „Listenprivilegs" ab.

Angesichts der bevorstehenden Bundestagswahlen im September 2009 zögerten viele Beteiligte jedoch, wesentliche Gesetzesänderungen umzusetzen. Einige Interessensgruppen behaupteten außerdem, dass Datenschutzeinschränkungen im Direktmarketingbereich ganze Industriebranchen erheblich schädigen würden und den Anstieg der Arbeitslosenzahl zur Folge hätten, was politisch nicht vertretbar wäre. Als Kompromiss verabschiedete der Gesetzgeber die Novelle zur Einführung strikterer Beschränkungen der gewerblichen Nutzung von personenbezogenen Daten und behielt das „Listenprivileg" weitestgehend bei. Die größte Neuerung der Novelle ist die Einführung einer Informationspflicht bei Datenschutzverletzungen.

II. Informationspflicht bei Datenschutzverletzungen

Gemäß der II.-Novelle müssen die verantwortlichen Stellen die Betroffenen und die Aufsichtsbehörden benachrichtigen, wenn unberechtigt auf personenbezogene Daten zugegriffen wurde oder diese unrechtmäßig übermittelt wurden, falls durch dieses Ereignis „schwerwiegende Beeinträchtigungen" der Rechte und schutzwürdigen Interessen der Betroffenen drohen.[18] Das Gesetz liefert keine präzise Definition des Begriffs „schwerwiegende Beeinträchtigungen", wodurch Unternehmen ein gewisser Spielraum bei der Entscheidung eingeräumt wird, ob eine unberechtigte oder unrechtmäßige Handlung diese Schwelle überschreitet. Dennoch gilt, dass wenn „schwerwiegende Beeinträchtigungen" drohen, die Benachrichtigung „unverzüglich" erfolgen muss, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden sind und sichergestellt wurde, dass die Strafverfolgung nicht gefährdet wird.[19] Diese Informationspflicht beschränkt sich auf bestimmte Fälle des Missbrauchs von Daten oder Datenelementen, wie Bank- oder Kreditkarteninformationen, „besondere Arten personenbezogener Daten" oder Angaben, die dem Berufsgeheimnis oder anderen amtlichen Geheimhaltungspflichten unterliegen.[20] Das Gesetz definiert „besondere Arten personenbezogener Daten" als Angaben über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, Gesundheit oder das Sexualleben einer Person.[21] Im Gegensatz dazu wird in den Vereinigten Staaten eine Informationspflicht üblicherweise durch einen unberechtigten Zugriff ausgelöst oder durch die Nutzung des Namens des Betroffenen in Verbindung mit einem weiteren Erkennungsmerkmal, wie der vom Staat herausgegebenen Sozialversicherungsnummer, bestimmten Bankinformationen, persönlichen Informationen über den Gesundheitszustand oder anderen persönlichen Informationen, die zum Identitätsdiebstahl genutzt werden können.[22] Demzufolge ist gemäß der II.-Novelle ein einzelner Auslöser ausreichend, wohingegen nach den Gesetzen der meisten US-Bundesstaaten zwei Auslöser erforderlich sind.

In den Änderungen finden sich außerdem Vorgaben darüber, wie eine Benachrichtigung über eine Datenschutzverletzung zu erfolgen hat. In Fällen, in denen beispielsweise eine Vielzahl von Personen von dem Ereignis betroffen ist und eine persönliche Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde, hat die Benachrichtigung durch eine mindestens halbseitige Anzeige in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine gleichsam geeignete Maßnahme zu erfolgen.[23] Diese Pflicht ähnelt den ersatzweisen Informationspflichten, die in vielen US-Bundesstaatengesetzen verankert sind.[24] Unternehmen sollten sich selbstverständlich vorab über die Folgen für ihren Ruf im Falle einer solchen Benachrichtigung in einer Zeitung oder Ähnlichem im Klaren sein.

Obwohl die Offenlegung von Datenschutzverletzungen in Deutschland wahrscheinlich viele unzulässige Handlungen ans Licht bringen wird, die sonst unentdeckt bleiben würden, werden den Unternehmen, die in Deutschland tätig sind oder den deutschen Gesetzen unterliegende Daten verwalten, zusätzliche Kosten entstehen. Im Jahr 2008 beliefen sich die durchschnittlichen Kosten für Datenschutzverletzungen in Deutschland auf über € 2,41 Mio. pro Verstoß und € 112 pro betroffenen Datensatz[25] unter Einbezug der durchschnittlichen Kosten für die Be-

12 Ähnlich wie die EU-Datenschutzrichtlinie, siehe Randnr. 34, definiert das BDSG die „verantwortliche Stelle" sehr weit als jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. § 3 Abs. 7 BDSG.

13 § 28 Abs. 3, § 34 Abs. 1a BDSG.

14 Hintergrundpapier zur Novellierung des Bundesdatenschutzgesetzes von der Verbraucherzentrale, 09.12.2008, abrufbar unter http://www.vzbv.de/mediapics/hintergrundpapier_datenhandel.pdf.

15 Grundgesetz, Artikel 1 und 2. Artikel 1 und 2 des Grundgesetzes sehen die Achtung der „Würde des Menschen" und die „freie Entfaltung seiner Persönlichkeit" vor, was in der Auslegung der deutschen Gerichte das Recht auf ein überwachungsfreies Arbeitsumfeld umfasst, es sei denn, dies ist ausdrücklich im Arbeitsvertrag festgeschrieben.

16 *Medick/Wittrock*, Spiegel v. 21.4.2009, abrufbar unter http://www.spiegel.de/politik/deutschland/0,1518,620332,00.html.

17 http://de.statista.org/statistik/daten/studie/1758/umfrage/aussagen-zum-thema-datenschutz-indeutschland/.

18 § 42a BDSG.

19 Id.

20 Id.

21 § 3 Abs. 9 BDSG.

22 Siehe z. B. California Computer Security Breach Notification Act, Endnote 8.

23 § 42a BDSG.

24 Siehe z. B. California Computer Security Breach Notification Act, Cal. Civ. Code Ann. §§ 1789.29(g)(3), 1798.82(g)(3) (2009).

25 Heinzmann, Oktober 2009 abrufbar unter http://www.it-sa.de/fileadmin/itsa_files/Handouts/2009/AU_Di_13_00_Heinzmann.pdf?PHPSESSID=onmousedown%3Dreturn.

nachrichtigungen in Höhe von € 80.000 pro Verstoß oder € 4 pro Datensatz.[26] Diese Zahlen sind verglichen mit den Kosten für Datenschutzverletzungen in den Vereinigten Staaten niedrig, da das bisherige BDSG die Benachrichtigung der Betroffenen oder die Veröffentlichung von Datenschutzverletzungen nicht vorsah.[27] In den Vereinigten Staaten, wo die Mehrheit der Bundesstaaten auf verschiedene Weise die Benachrichtigung über Datenschutzverletzungen verlangt,[28] beliefen sich die durchschnittlichen Kosten einer Datenschutzverletzung im Jahr 2008 auf mehr als ca. € 4,5 Mio. pro Verstoß und ca. € 137 pro betroffenen Datensatz.[29] Es wird davon ausgegangen, dass diese Kosten in den nächsten Jahren steigen werden, insbesondere in Verbindung mit dem voraussichtlichen Anstieg von Rechtsstreitigkeiten im Bereich Datenschutz und Privatsphäre.[30]

Generell hat sich herausgestellt, dass die gesetzlichen Verpflichtungen in den USA und die bewährten datenschutzbezogenen Praktiken der Wirtschaft – z. B. Benachrichtigung von Betroffenen und Aufsichtsbehörden, Eindämmung von Rechts- und Reputationsrisiken, Beseitigung von technischen Mängeln – für die Unternehmen kostspieliger sind als andere von der US-Gesetzgebung vorgeschriebene Vorkehrungen zur Sicherung der Privatsphäre und Datenschutzmaßnahmen.[31] Diese Unterschiede zwischen den beiden Ländern lassen darauf schließen, dass die mit Datenschutzverletzungen verbundenen Kosten in Deutschland, zumindest diejenigen, die sich auf die Informationspflicht beziehen, im Rahmen des neuen BDSG wahrscheinlich steigen werden.

Darüber hinaus sollte die Möglichkeit eines Dominoeffekts beachtet werden, den die Informationspflicht über Datenschutzverletzungen in Deutschland auf die Europäische Union und ihre Mitgliedstaaten haben könnte. Die Geschichte der Informationspflicht über Datenschutzverletzungen in den Vereinigten Staaten begann im Jahr 2003, als Kalifornien als erster Bundesstaat ein Gesetz über die Informationspflicht bei Datenschutzverletzungen erließ.[32] Diesem Vorbild ist seitdem die Mehrheit aller US-Bundesstaaten gefolgt[33] und der US-Kongress erwägt derzeit eine landesweite Gesetzgebung zum Datenschutz.[34]

Während die Umsetzung der Europäischen Datenschutzrichtlinie[35] in den einzelnen Mitgliedstaaten dazu beigetragen hat, dass die Europäische Union in Bezug auf den Schutz personenbezogener Daten eine der am strengsten regulierten Gerichtsbarkeiten der Welt ist, verfügt die Europäische Union immer noch nicht über eine allgemeine Informationspflicht über Datenschutzverletzungen. Es gibt jedoch Anhaltspunkte dafür, dass sich die Datenschutzpraxis in Europa auf dem Weg der Änderung befindet. Der Europäische Rat ist gerade dabei, seine Telekommunikationsrichtlinien zu ändern, um darin eine branchenspezifische Informationspflicht für Kommunikationsdienstleister über Datenschutzverletzungen aufzunehmen.[36] Einige EU-Nachbarstaaten wie z.B. Norwegen verfügen bereits über Gesetze, die die Benachrichtigung von Aufsichtsbehörden über Datenschutzverletzungen vorschreiben.[37] Das Vereinigte Königreich verfügt praktisch durch die Empfehlung der unabhängigen britischen Datenschutzbehörde, dass diese durch die Unternehmen über sämtliche „schwerwiegende" Verletzungen zu informieren ist,[38] bereits über eine Art Benachrichtigungsgesetz. Dies erklärt vielleicht, warum eine anhaltende Debatte darüber geführt wird, ob derartige Gesetze verabschiedet werden sollen.[39] Das Parlament des Vereinigten Königreichs hat diese Gesetze im Jahr 2007 geprüft und damals beschlossen, darauf zu verzichten.[40] Diese Umstände in Verbindung mit den jüngsten Änderungen des BDSG lassen vermuten, dass sich die EU-Mitgliedstaaten, oder die Europäische Union insgesamt, möglicherweise auf dem Weg zu einem umfassenderen Informationssystem bei Datenschutzverletzungen befinden.

III. Weiter Änderungen

Weitere Änderungen des BDSG umfassen:

Arbeitnehmerdatenschutz. Eine Verarbeitung von Arbeitnehmerdaten ist nur zulässig, wenn die Verarbeitung für die Verwaltung, d. h. die Begründung, Durchführung und Beendigung des Arbeitsverhältnisses, erforderlich ist.[41] Zur Aufdeckung von Straftaten des Arbeitnehmers dürfen dessen personenbezogene Daten nur dann erhoben werden, wenn (1) die Daten den Verdacht begründen, dass der Arbeitnehmer im Beschäftigungsverhältnis eine Straftat begangen hat, (2) die Erhebung, Verarbeitung oder Nutzung der Daten zur Aufdeckung erforderlich ist und (3) Art und Ausmaß der Erhebung, Verarbeitung und Nutzung der Daten im Hinblick auf die schutzwürdigen Interessen des Arbeitnehmers und die Umstände der Aufdeckung nicht unverhältnismäßig sind.[42]

26 Id.
27 Hanloser; MMR 2009, 594 (598).
28 Siehe Endnote 3.
29 Siehe Cost of Data Breach, United States 2008 Annual Study, Ponemon Institute, abrufbar unter http://www.encryptionreports.com/costofdatabreach.html.
30 Seit dem Jahr 2005 sind die Kosten für eine Datenschutzverletzung um fast 40 Prozent oder mehr als $ 64 pro Datensatz gestiegen. Id.
31 Siehe Cost of Data Breach, United States 2008 Annual Study, Ponemon Institute, abrufbar unter http://www.encryptionreports.com/costofdatabreach.html.
32 California Computer Security Breach Notification Act, Cal. Civ. Code Ann. § 1798.82 ff. (2009).
33 Siehe Endnote 3.
34 S.1490, 111. Kongress (2009) (mit dem Titel: „Ein Gesetzentwurf zur Verhinderung und Verringerung von Identitätsdiebstahl, zum Schutz der Privatsphäre, zur Benachrichtigung über Sicherheitsverstöße und zur Verschärfung von strafrechtlichen Sanktionen, Unterstützung bei der Strafverfolgung und andere Schutzmaßnahmen gegen Sicherheitsverstöße, unberechtigten Zugriff auf und Missbrauch von personenbezogenen Daten").
35 Richtlinie 95/46/EG des Rates, 1995 Amtsblatt (L281)31, unter http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_de.pdf.
36 Legislative Entschließung des Europäischen Parlaments vom 6. Mai 2009 zu dem Gemeinsamen Standpunkt des Rates im Hinblick auf die Annahme einer Richtlinie des Europäischen Parlaments und des Rates zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, EUR. PARL. DOC. (TA 360) 6 (2009), abrufbar unter http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//DE.
37 Personal Data Act 2000, § 27 (Nor.), abrufbar unter http://www.legislationline.org/download/action/download/id/1102/file/2e3d6bb37cf550acba8549d9759d.pdf.
38 Das Büro des Informationsbeauftragten (Information Commissioner's Office) liefert keine genaue Definition, wann es sich um einen „schwerwiegenden" Verstoß handelt, sondern bietet allgemeine Richtlinien und Beispiele zur Einschätzung der Handlung; wesentliche Faktoren zur Bestimmung eines „schwerwiegenden" Verstoßes sind u. a. der mögliche Schaden für die Betroffenen sowie der Umfang und die sensiblen Inhalte der betroffenen Daten. Siehe Information Commissioner's Office, Notification of Data Security Breaches to the Information Commissioner's Office, 27.03.2008, abrufbar unter http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/breach_reporting.pdf.
39 Siehe z. B., Tom Espiner, „Data Breach Law: IT Managers Say ‚No'", ZDNet UK, 05.06.2008, abrufbar unter http://community.zdnet.co.uk/blog/0,1000000567,1000837o-2000331828b,00.htm.
40 Siehe z. B. House of Commons Justice Committee, First Report 2007-08, H.C. 154 (Empfehlung zu Informationspflichten bei Datenschutzverletzungen im Rahmen des Data Protection Act 1998), abrufbar unter http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf.
41 § 32 BDSG.
42 Id.

Vertragliche Bestimmungen für das Outsourcing. Wenn ein Unternehmen sein Direktmarketing an Dritte auslagert, müssen die Vertragsparteien einen schriftlichen Vertrag über die Verarbeitung der personenbezogenen Daten abschließen. Dieser Vertrag muss zehn neue Bedingungen erfüllen, um gültig und rechtlich durchsetzbar zu sein.[43] Diese Bedingungen umfassen u. a. den Umfang, Zweck, Sicherheitsmaßnahmen, Verpflichtungen, die Berechtigung zur Begründung von Unterauftragsverhältnissen, die Rückgabe und Löschung der Daten sowie das Erfordernis, den Auftragnehmer zu prüfen.[44] Wird ein solcher Vertrag nicht geschlossen, so kann beiden Parteien ein Bußgeld auferlegt werden.[45] Experten glauben, dass die Aufsichtsbehörden diese Vorschrift am ehesten vollstrecken werden, da (1) die Öffentlichkeit in Deutschland stets Bedenken bezüglich des Direktmarketings äußert und (2) die Aufsichtsbehörden schnell feststellen können, ob die Parteien dieses Erfordernis einhalten.

Schutz des Beauftragten für den Datenschutz. Der Datenschutzbeauftragte, der die Einhaltung der deutschen Datenschutzgesetze durch das Unternehmen sicherstellt und als Kontaktperson für die Aufsichtsbehörde tätig ist, darf nur aus wichtigem Grund gekündigt werden.[46] Dieser besondere Schutz gilt ein Jahr nach der Beendigung der Bestellung zum Datenschutzbeauftragten des Unternehmens fort, es sei denn, der Geschäftsführung liegen „wichtige Gründe" für die Kündigung des Datenschutzbeauftragten vor.[47] Unternehmen müssen außerdem die Teilnahme ihrer Datenschutzbeauftragten an Fort- und Weiterbildungsveranstaltungen ermöglichen und deren Kosten übernehmen.[48] Eine natürliche, jedoch wahrscheinlich nicht beabsichtigte Folge dieser neuen Bestimmung ist, dass viele Unternehmen häufig externe Datenschutzbeauftragte gegenüber internen bevorzugen werden, da externe Datenschutzbeauftragte ab sofort einfacher zu kündigen sind.

Erweiterte Befugnisse der Aufsichtsbehörden. Aufsichtsbehörden können Unternehmen anweisen, Maßnahmen zur Beseitigung festgestellter Verstöße bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten sowie technischer oder organisatorischer Mängel zu ergreifen.[49] In Abhängigkeit von den Umständen des Verstoßes können sie außerdem besondere Datenverarbeitungsverfahren vorschreiben oder den Unternehmen die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten untersagen.[50]

Höhere Bußgelder. Das Bußgeld bei Nichtbeachtung der Datenschutzgesetze beläuft sich nun auf maximal € 50 000 (vorher € 25 000) für einfache Ordnungswidrigkeiten, wie das Unterlassen der Bestellung eines Datenschutzbeauftragten, das Unterlassen der Verschlüsselung einer Datenübermittlung oder der unterlassenen Sicherstellung, dass ein Auftragnehmer die vom Gesetz vorgeschriebenen technischen und organisatorischen Maßnahmen einhält. Für schwere Ordnungswidrigkeiten, wie dem Zugriff auf nicht allgemein zugängliche Daten und die Erhebung oder Verarbeitung solcher Daten, sowie die Erhebung und Verarbeitung von Daten für nicht vorgesehene Zwecke oder das Unterlassen der Benachrichtigung Betroffener über einen Verstoß, der ihnen einen „wesentlichen Schaden" zufügen könnte, beträgt das Bußgeld nun maximal € 300 000 (vorher € 250 000).[51] Außerdem können die Behörden, wenn die verantwortliche Stelle Gewinne erwirtschaftet hat, die € 50 000 bzw. € 300 000 übersteigen, das Bußgeld im Verhältnis dazu erhöhen.[52]

Diese Neuregelungen traten am 1.9.2009 in Kraft, wobei für Daten, die vor diesem Zeitpunkt für Zwecke der Markt- und Meinungsforschung erhoben wurden, eine Übergangsregelung gilt, gemäß der die bisherigen Vorschriften bis 31.8.2012 in Kraft bleiben.

IV. Fazit

Es scheint in Europa, sowie in den Vereinigten Staaten und in anderen Ländern weltweit,[53] eine Tendenz zu geben, Datenschutzgesetze zu verabschieden, die eine allgemeine Verpflichtung enthalten, staatliche Behörden, Betroffene oder beide über den unbefugten Zugriff oder die Nutzung von personenbezogenen Daten zu informieren. Die II.-Novelle spiegelt ein wachsendes Bewusstsein für Datenschutzfragen in der europäischen Öffentlichkeit und das Potenzial für eine höhere Bereitschaft zur Umsetzung von Datenschutzgesetzen durch die europäischen Aufsichtsbehörden wider. Im September 2009 demonstrierten beispielsweise 25 000 Menschen in Berlin für einen besseren Schutz personenbezogener Daten[54] und die neue CDU/FDP-Koalition hat bereits erklärt, dass eine spezieller Arbeitnehmerdatenschutz im BDSG in nicht allzu ferner Zukunft verankert werden soll. Dies alles deutet darauf hin, dass Verletzungen der Datenschutzvorschriften in Zukunft wohl riskanter werden.

Um eine Einhaltung dieser Novelle und einer möglichen zukünftigen Gesetzgebung der Europäischen Union zu gewährleisten, sollten Unternehmen mindestens

- allgemeine Richtlinien und Arbeitsabläufe für die Aufdeckung und Behebung von Datenschutzverletzungen in Verbindung mit personenbezogenen Daten und für die Benachrichtigung darüber erstellen und zwar auch für Daten, die über diejenigen hinausgehen, die im US-amerikanischen Recht eine Informationspflicht auslösen;
- die Nutzung oder Übermittlung von Datenlisten oder anderen personenbezogenen Daten auswerten und neu strukturieren; sowie
- sämtliche datenbezogenen Dienstleistungs- und Arbeitsverträge überprüfen und ggf. neu verhandeln.

Wenn die Unternehmen diese Veränderungen vornehmen, kann es sinnvoll sein, die Gelegenheit zu ergreifen, um die gesamte Datenschutzpraxis zu überprüfen und die Umsetzung eines ganzheitlicheren Ansatzes bezüglich der Einhaltung von Datenschutzvorschriften in Erwägung zu ziehen, der zukünftigen Gesetzen in diesem Gebiet vorweggreift. Um Geschäftsrisiken, einschließlich Bußgelder, Betriebsprüfungen und Rufschädigungen als Folge einer Nichteinhaltung der Gesetze zu vermeiden, müssen Unternehmen den Schwerpunkt ihrer Bemühungen in diesem Bereich richtig setzen.

43 § 11 Abs. 2 BDSG.
44 Id.
45 § 43 Abs. 1 Nr. 2b BDSG.
46 § 4f Abs. 3 BDSG. Gemäß Gesetz müssen (1) alle Unternehmen, die mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen, (2) alle Unternehmen, die in der geschäftsmäßigen Übermittlung von personenbezogenen Daten tätig sind, und (3) alle Unternehmen, die in der geschäftsmäßigen Übermittlung von personenbezogenen Daten für Zwecke der Markt- und Meinungsforschung tätig sind, einen Beauftragten für den Datenschutz bestellen.
47 Id.
48 Id.
49 § 38 Abs. 5 BDSG.
50 Id.
51 § 43 Abs. 3 BDSG. Einfache Verletzungen sind unter § 43 Abs. 1 aufgelistet; schwere Verletzungen sind in § 43 Abs. 2, § 44 aufgelistet.
52 § 43 Abs. 3 BDSG.
53 Neben den Vereinigten Staaten und der Europäischen Union verfügen Länder wie Australien, Kanada und Japan über Gesetze, die unmittelbar die Pflicht zur Information über Datenschutzverletzungen auferlegen. Alana Maurushat, Data Breach Notification Law Across the World from California to Australia, Univ. of New S. Wales L. Research Series (Paper No. 11), April 2009, abrufbar unter http://law.bepress.com/cgi/viewcontent.cgi?article=1153&context=unswwps.
54 Süddeutsche Zeitung v.14.9.2009, S.14.