Recht der elektronischen Medien

Kommentar

von

Prof. Dr. Gerald Spindler, Prof. Dr. Fabian Schuster, Katharina Anton, Dr. Harm-Randolf Döpkens, Dr. Jens Eckhardt, Dr. Murad Erdemir, Prof. Dr. Udo Fink, Michael Fricke, Prof. Dr. Marco Gercke, Prof. Dr. Hubertus Gersdorf, Prof. Dr. Ludwig Gramlich, Dr. Andreas Grünwald, Dr. Kathrin Hahne, Jörn Heckmann, Dr. Helmut Hoffmann, Dr. Daniel Hofmann, Prof. Dr. Bernd Holznagel, Florian Hürst, Eike Jahn, Dr. Babette Kibele, Dr. Daniel Krone, Dr. Maxim Kleine, Dr. Roger Mann, Prof. Dr. Ulf Müller, Dr. Monika Namyslowska, Dr. Monika Namys?owska, Dr. Jens Neitzel, Dr. Judith Nink, Dr. Carl Friedrich Nordmeier, Dr. Kerstin Orantek, Prof. Dr. Thomas Pfeiffer, Thorsten Ricke, Prof. Dr. Hans-Wolfgang Micklitz, Lutz Ropeter, Dr. Martin Schirmbacher, Jörg F. Smid, Dr. Axel Sodtalbers, Dr. Christian Volkmann, Dr. Matthias Weller, Prof. Dr. Andreas Wiebe

3. Auflage

Verlag C.H. Beck München 2015

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 406 66383 3

Zu Inhalts- und Sachverzeichnis

verstehen sind.[15] Darunter fallen auch unproblematisch Texte auf CD-ROMs oder anderen **audiovisuellen Trägern,** soweit eine stofflich-gegenständliche Verkörperlichung gegeben ist.[16] Nicht erfasst wird die elektronische Presse. Diese wurde bisher durch den MDStV erfasst und unterfällt nun den Datenschutzvorschriften für Telemedien. Durch den 9. Rundfunkänderungsstaatsvertrag wurde in § 57 RStV für die elektronische Presse ein entsprechendes Medienprivileg eingefügt.[17] So fallen journalistisch-redaktionelle Online-Archive[18] und auch Fanpages sozialer Netzwerke sofern sie journalistisch-redaktionellen Charakter haben[19] unter den Schutz von § 57 RStV.[20] Bewertungsportale im Internet sollen nach der Rechtsprechung indes nicht den Schutz von § 41 genießen, da diese nicht **ausschließlich** journalistisch-redaktionellen Zwecken dienten sondern der journalistisch-redaktionelle Charakter lediglich schmückendes Beiwerke sei (siehe auch Rn. 1).[21] Aufgrund dieser strengen Auslegung und weil das Kriterium der journalistisch-redaktionellen Inhalte insbesondere im **Web 2.0** sehr schwer zu greifen ist, wäre es zum Schutz der Meinungsfreiheit geboten, dass der Gesetzgeber eine deutliche Ausweitung der §§ 41 und 57 RStV vornimmt.[22] Die übrigen datenschutzrechtlichen Bestimmungen ergeben sich aus den §§ 11 bis 15 TMG. Daten die ausschließlich zu eigenen **journalistisch-redaktionellen Zwecken** erhoben, verarbeitet oder genutzt werden sind personenbezogene Informationen, die von Journalisten, Redakteuren und anderen im Presseunternehmen tätigen Personen zu Zwecken der Recherche, Vorbereitung und Herstellung von zur Veröffentlichung bestimmten Artikeln etc entweder erhoben oder aus anderen Quellen beschafft werden.[23] Fraglich ist, ob darunter auch Honorardaten freier Mitarbeiter zu subsumieren sind.[24] Der **literarischen Zweckbestimmung** dienen Daten, wenn sie ausschließlich der Herstellung belletristischer oder Sachliteratur dienen.[25]

Das Medienprivileg hat zur Folge, dass beispielsweise ein präventiver Auskunftsanspruch des potentiell Betroffenen nach § 34 nicht möglich ist. Dies kann insbesondere im Bereich der Boulevardpresse für sog. Medienopfer dazu führen, dass diese kaum eine rechtlich durchsetzbare Möglichkeit haben, Verletzungen ihres allgemeinen Persönlichkeitsrechts vorzubeugen (zu den Anspruchsvarianten bei Vorliegen einer Verletzung ausführlich § 823 BGB Rn. 45 ff.).[26] Höchst fraglich ist, ob der Google-Dienst „Street View" unter das Medienprivileg fällt und damit dem Datenschutzrecht entzogen würde. Denn nach Auffassung des *LG Köln* unterfällt der Online-Dienst „bilderbuch.de", der von **Google Street View** kaum unterscheidbar ist,[27] dem Medienprivileg.[28] Allerdings ist Google Street View's prägender Bestandteil gerade nicht die meinungsbildende Wirkung, so dass es keine Presse ist und daher richtigerweise nicht dem Medienprivileg unterfallen darf.[29] **4**

2. Das Medienprivileg der Deutschen Welle

Abs. 4 befreit die Deutsche Welle, wie die Presse in Abs. 1, von einem Großteil der datenschutzrechtlichen Pflichten und begründet insofern ein Medienprivileg für diese. Durch Abs. 2 wird die Deutsche Welle verpflichtet, Gegendarstellungen zu den gespeicherten Daten aufzunehmen und ebenso lange wie die Daten zu speichern, sofern sie nach § 18 des Deutsche-Welle-Gesetzes eine solche Pflicht trifft. Nach Abs. 3 hat der durch eine Berichterstattung Betroffene ein **Auskunftsrecht** über die der Berichterstattung zugrunde liegenden personenbezogenen Daten. Es besteht aber kein Recht auf Kenntnisvermittlung der Herkunft und Empfänger der Daten, so dass von einem **eingeschränkten Auskunftsanspruch** gesprochen wird.[30] Diese Auskunft kann ihm nach Abwägung der schutzwürdigen Interessen aller Beteiligten auch verweigert werden, soweit eine der Nummern des § 41 Abs. 3 Satz 2 Nr. 1 bis 3 einschlägig ist. Dieses Verweigerungsrecht ist Ausdruck des **Informantenschutzes.**[31] **5**

---

[15] *Simitis/Dix,* § 41 BDSG Rn. 9; *Gola/Schomerus,* § 41 Rn. 7; siehe auch die Definitionen in den Landesdatenschutzgesetzen, zB § 7 Nds. PresseG; Art. 6 BayPrG.

[16] *Simitis/Dix,* § 41 BDSG Rn. 9; *Lauber/Rönsberg,* ZD 2014, 180.

[17] *Caspar,* NVwZ 2010, 1455.

[18] *Lauber/Rönsberg,* ZD 2014, 180.

[19] *Härting,* ITRB 2012, 111; *Spindler,* GRUR-Beil. 2014, 101.

[20] So der *BGH,* NJW 2010, 2432 (2433 f.) Rz. 27 f.; *Lauber/Rönsberg,* ZD 2014, 180; zum Medienprivileg bei Internetdiensten und Blogs mit meinungsbildender Wirkung siehe auch *Spindler,* NJW-Beil. 2012, 100.

[21] *BGH,* MMR 2009, 608 (610) Rz. 19b ff. – spickmich.

[22] Siehe dazu ausf. *Spindler,* DJT, F73; *ders.,* GRUR-Beil. 2014, 101; *ders.,* GRUR 2013, 1000; *Lauber/Rönsberg,* ZD 2014, 181.

[23] *Simitis/Dix,* § 41 BDSG Rn. 12.

[24] *Michel* in: FS Herrmann, S. 113; *Gola/Schomerus,* § 41 BDSG Rn. 11.

[25] *Gola/Schomerus,* § 41 BDSG Rn. 12.

[26] Auch aus Ziff. 3 des Deutschen Pressekodex resultiert kein verbindlicher Rechtsanspruch auf Auskunft, da die Regeln des Pressekodex lediglich ethische, rechtlich unverbindliche Standards darstellen.

[27] *Härting,* BB 2010, 843.

[28] *LG Köln,* K&R 2010, 210 (211), ohne dies aber abschließend zu entscheiden; offenlassend auch *LG Berlin,* ZUM-RD 2011, 418 (419).

[29] *Spiecker gen. Döhmann,* CR 2010, 313; *Moritz,* jurisPR-ITR 13/2010 Anm. 2.

[30] *Simitis/Dix,* § 41 BDSG Rn. 38; *Gola/Schomerus,* § 41 BDSG Rn. 15.

[31] *Michel* in: FS Herrmann, S. 114.

Auch gegenüber der Deutschen Welle besteht also kein präventives sondern lediglich ein späteres Auskunftsrecht, nach bereits erfolgter Persönlichkeitsrechtsverletzung durch eine Berichterstattung.

§ 42 *(vom Abdruck wurde abgesehen)*

§ 42a Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

[1] Stellt eine nichtöffentliche Stelle im Sinne des § 2 Absatz 4 oder eine öffentliche Stelle nach § 27 Absatz 1 Satz 1 Nummer 2 fest, dass bei ihr gespeicherte

1. besondere Arten personenbezogener Daten (§ 3 Absatz 9),
2. personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
3. personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
4. personenbezogene Daten zu Bank- oder Kreditkartenkonten

unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies nach den Sätzen 2 bis 5 unverzüglich der zuständigen Aufsichtsbehörde sowie den Betroffenen mitzuteilen. [2] Die Benachrichtigung des Betroffenen muss unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. [3] Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. [4] Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. [5] Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle die Information der Öffentlichkeit durch Anzeigen, die mindestens eine halbe Seite umfassen, in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme. [6] Eine Benachrichtigung, die der Benachrichtigungspflichtige erteilt hat, darf in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen ihn oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Benachrichtigungspflichtigen nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden.

Übersicht

Literatur: *Bierekoven,* Schadensersatzansprüche bei Verletzung von Datenschutzforderungen nach der BDSG-Novelle, ITRB 2010, 88; *Duisberg/Picot,* CR 2009, 823, (827); *Eckhardt,* Security Breach Notification – Evaluation durch die Bundesregeierung, ZD-Aktuell 2013, 03494; *ders.,* BDSG: Neuregelungen seit 1.9.2009 – Ein Überblick, DuD 2009, 587; *Eckhardt/Schmitz,* Informationspflichten bei „Datenschutzpannen" DuD 2010, 390; *Ernst,* Datenverlust und die Pflicht zur Öffentlichkeit, DuD 2010, 472; *Hanloser,* Europäische Security Breach Notification, MMR 2010, 300; *Gabel,* Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten, BB 2009, 2045; *Höhne,* Benachrichtigungspflichten bei unrechtmäßiger Kenntniserlangung von Daten durch Dritte – Informationspflichten bei Datenpannen nach der BDSG-Novelle II gemäß § 42a BDSG, § 15a TMG und § 93 Abs. 3 TKG, jurisPR-ITR 20/2009 Anm. 3; *Hornung,* Informationen über „Datenpannen" – Neue Pflichten für datenverarbeitende Unternehmen, NJW 2010, 1841; *Karger,* Informationspflichten bei Data Breach, ITRB 2010, 161; *Kaufmann,* Meldepflichten und Datenschutz-Folgenabschätzung, ZD 2012, 358; *Spindler,* Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, Gutachten F zum 69. Deutschen Juristentag (DJT), München 2012; *Zahrte/Selig,* Keine Meldepflicht von Skimming-Fällen nach § 42a BDSG, BKR 2014, 185.

I. Allgemeines

1 Die in § 42a[1] statuierte **Informationspflicht** gegenüber dem Betroffenen sowie der Aufsichtsbehörde bei unrechtmäßiger Kenntniserlangung besonderer Daten durch Dritte, wurde durch die

[1] Eingefügt durch Art. 1 Nr. 16 des Gesetzes zur Änderung datenschutzrechtlicher Vorschriften v. 14.8.2009, BGBl. I S. 2814 (2818).

BDSG-Novelle II[2] neu in das Gesetz aufgenommen. Adressat der Vorschrift sind gleichermaßen nichtöffentliche Stellen und öffentliche Wettbewerbsunternehmen.[3] Im Übrigen wurden öffentliche Stellen nicht in den Anwendungsbereich der Vorschrift aufgenommen. Diese sind im Falle einer unrechtmäßigen Übermittlung oder einer sonstigen unrechtmäßigen Kenntniserlangung der von ihnen gespeicherten besonderen personenbezogenen Daten seitens Dritter dazu verpflichtet, unverzüglich die zuständige Aufsichtsbehörde[4] und die Betroffenen[5] zu informieren.[6] Ziel der Vorschrift ist es, bei Datenschutzverletzungen zum Schutz der Betroffenen mehr Transparenz zu schaffen und die effiziente Durchsetzung datenschutzrechtlicher Regelungen zu gewährleisten.[7] Weiter soll die Vorschrift einen Schutz vor Folgeschäden beim Betroffenen bieten.[8] Der Gesetzgeber räumt mit der Einführung des § 42a dem informationellen Selbstbestimmungsrecht der Betroffenen somit eine vorrangige Stellung vor den Geheimhaltungsinteressen der Datenverarbeiter ein.[9]

Zurückzuführen ist § 42a auf den inzwischen von Parlament und Rat verabschiedeten Entwurf der Richtlinie 2009/136/EG[10] der Europäischen Kommission zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.[11] Angelehnt ist die in § 42a enthaltene Regelung zudem an vergleichbare Regelungen im US-amerikanischen Recht **(security breach notification).**[12] Parallelvorschriften finden sich in § 15a TMG sowie § 93 Abs. 3 TKG. **2**

Die Verfassungsmäßigkeit der Vorschrift wird in der Literatur stark angezweifelt, da nach dem ***BVerfG***[13] niemand zur eigenen Beibringung von Tatsachen, die eine von ihm begangene strafbare/ordnungswidrige Handlung offenbaren, verpflichtet werden kann,[14] genau dies aber durch die Pflicht zur Anzeige von Ordnungswidrigkeiten nach § 42a ermöglicht wird. Der Gesetzgeber wollte diesen Interessenkonflikt durch Abs. 6 ausgleichen (siehe Rn. 8).[15] **3**

II. Regelungsinhalt

1. Erfasste Daten

Die Informationspflicht bezieht sich ausschließlich auf die in Satz 1 Nr. 1 bis 4 aufgelisteten Daten.[16] Diese erfassen besondere Arten personenbezogener Daten gem. § 3 Abs. 9 BDSG (Nr. 1), personenbezogene Daten, die einem Berufsgeheimnis (Patientendaten, Mandatsdaten aus anwaltlichen und steuerrechtlichen Beratungen etc) unterliegen (Nr. 2), sowie personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder einen entsprechenden Verdacht beziehen. Ebenso fallen personenbezogene Daten zu Bank-und Kreditkartenkonten in den Anwendungsbereich der Norm. Gerade Bank- und Kreditkarteninformationen dürften voraussichtlich das größte Spektrum für den Anwendungsbereich von § 42a bieten. **4**

2. Anhaltspunkte für Kenntniserlangung und Beeinträchtigung

Der verantwortlichen Stelle (§ 3 Abs. 7), die die betreffenden Daten speichert, müssen tatsächliche Anhaltspunkte für eine unrechtmäßige Übermittlung oder Kenntniserlangung Dritter vorliegen.[17] Unrechtmäßig ist jede Kenntnisnahme, die nicht durch eine gesetzliche Erlaubnis oder eine explizite Einwilligung des Betroffenen gestattet ist.[18] Wie die Daten zur Kenntnis erlangt sind, ist dabei unerheblich.[19] Erforderlich ist eine hohe Wahrscheinlichkeit der Kenntnisnahme, eine bloße Möglichkeit der Kenntnisnahme oder Vermutungen reichen nicht aus.[20] Aufgrund des Sinn und Zwecks der **5**

---

[2] Allg. zum Inhalt der BDSG-Novelle II siehe *Eckhardt,* DuD 2009, 587 ff.
[3] Siehe die Legaldefinition in § 2.
[4] Siehe § 38 Abs. 6.
[5] Siehe die Legaldefinition in § 3 Abs. 1.
[6] *Taeger/Gabel/Gabel,* § 42a BDSG Rn. 1; *Karger,* ITRB 2010, 162.
[7] *Gola/Schomerus,* § 42a Rn. 1; *Gabel,* BB 2009, 2046.
[8] *Höhne,* jurisPR-ITR 20/2009 Anm. 3.
[9] *Simitis/Dix,* § 42a Rn. 1.
[10] RL 2009/136/EG, ABl. EU Nr. L 337/11 v. 18.12.2009.
[11] KOM (2007) 698 endg., S. 36; *Hanloser,* MMR 2010, 300; *Gabel,* BB 2009, 2045.
[12] *Duisberg/Picot,* CR 2009, 827; *Hornung,* NJW 2010, 1842; Begr. des Entw. der BundesReg für ein Gesetz zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften, BT-Drs. 16/12011, S. 34.
[13] StRspr *BVerfG,* NJW 2002, 1411 (1412); *BVerfG,* NJW 1981, 1431.
[14] *Kaufmann,* ZD 2012, 360; *Eckhardt/Schmitz,* DuD 2010, 396 f.
[15] Dazu ausf. *Eckhardt/Schmitz,* DuD 2010, 396 f.
[16] *Eckhardt/Schmitz,* DuD 2010, 390; eine Erstreckung auf alle Datenverarbeitungsvorgänge fordernd *Spindler,* DJT, F103.
[17] *Eckhardt,* ZD-Aktuell 2013, 03494; *Eckhardt/Schmitz,* DuD 2010, 393.
[18] *Karger,* ITRB, 162.
[19] *Höhne,* jurisPR-ITR 20/2009 Anm. 3.
[20] *Taeger/Gabel/Gabel,* § 42a BDSG Rn. 17; *Karger,* ITRB 2010, 162; *Ernst,* DuD 2010, 473.

Vorschrift muss jedoch eine fahrlässige Unkenntnis,[21] zumindest im Falle eines **Kennenmüssens,** die Informationspflicht auslösen.[22] Eine Möglichkeit der Kenntnisnahme besteht auch dann nicht, wenn die Daten ausreichend verschlüsselt sind.[23] Da es sich aber um teils hoch sensible Daten handelt, müssen an die Verschlüsselung hohe Anforderungen gemäß dem Stand der Technik gestellt werden. Dafür kann und sollte auf die Anforderungen an eine Anonymisierung (siehe ausführlich § 13 TMG Rn. 12) zurückgegriffen werden. Bei Hackerangriffen, und auch der Verwendung eines Rechners in einem **Bot-Netz,** muss sich der Verpflichtete Anhaltspunkte darüber verschaffen, ob die Daten dem Angreifer tatsächlich zur Kenntnis gelangt sind, zB durch die Auswertung von Log-Files etc.[24] In Zweifelsfällen ist der Datenschutzbeauftragte heranzuziehen.[25]

6 Alleine die Kenntniserlangung durch Dritte löst eine entsprechende Informationspflicht der verantwortlichen Stelle nicht aus, hinzukommen muss vielmehr eine drohende, **schwerwiegende Beeinträchtigung** für die Rechte oder schutzwürdigen Interessen des Betroffenen.[26] Die Gefahr der Beeinträchtigung richtet sich insbesondere nach der Art der betroffenen Daten und den zu erwartenden Auswirkungen der unrechtmäßigen Kenntniserlangung.[27] Dazu gehören etwa auch soziale Nachteile einschließlich eines Identitätsbetrugs.[28] Aus dem Wortlaut der Norm ergibt sich, dass die verantwortliche Stelle eine objektive[29] Gefahrenprognose über den zukünftigen hypothetischen Geschehensablauf zu treffen hat.[30] Praktisch ist dies oft schwer prognostizierbar. Sinnvoll erscheint es daher, auch bloße Vermögensinteressen in die Gefahrenprognose einzubeziehen.[31]

3. Benachrichtigungspflichten

7 Die verantwortliche benachrichtigungspflichtige Stelle[32] hat sowohl die Betroffenen als auch die zuständige Aufsichtsbehörde bei Vorliegen der oben genannten Voraussetzungen über die unrechtmäßige Kenntniserlangung zu informieren. Benachrichtigungspflichtig sind nicht öffentliche Stellen iSd § 2 Abs. 4 sowie öffentliche Stellen (öffentlich-rechtliche Wettbewerbsunternehmen) gem. § 27 Abs. 1 Satz 1 Nr. 2. § 42a Satz 2–5 regeln im Einzelnen Art und Umfang der Informationspflicht. Die Benachrichtigung hat grundsätzlich *„unverzüglich"* zu erfolgen, vorausgesetzt wird somit ein Handeln ohne schuldhaftes Zögern iSd § 121 BGB.[33] Für die Benachrichtigung der Betroffenen ordnet Satz 2 an, dass ein schuldhaftes Zögern dann ausgeschlossen ist, soweit Datensicherungspflichten (§ 9) oder Strafverfolgungsinteressen entgegenstehen.[34] Die erste Alternative dient der Schadensbegrenzung, da sich andernfalls Dritte in Kenntnis der Sicherheitslücke ungehindert Daten beschaffen könnten. Die verantwortliche Stelle soll somit zunächst die Möglichkeit erhalten, die Sicherheitslücke in ihrem System zu analysieren und zu beheben (sog. **Responsible Disclosure**).[35] Die zweite Alternative dient hingegen dem reibungslosen Ablauf des strafrechtlichen Ermittlungsverfahrens, welches durch eine Offenlegung beeinträchtigt werden könnte.[36] Die vorgenannten Einschränkungen gelten nicht für Aufsichtsbehörden, da diese einer Verschwiegenheitspflicht unterliegen.[37] Praktisch bedeutet dies, dass gegebenenfalls die Aufsichtsbehörde vor den Betroffenen zu informieren ist, insofern empfiehlt sich hier eine zeitnahe Information.[38]

8 § 42a Satz 3 und 4 enthalten genauere inhaltliche Anforderungen an die Benachrichtigung. Bei einer **Benachrichtigung** des Betroffenen ist die Art der Verletzung darzulegen und eine Empfehlung für Maßnahmen zur Minderung möglicher nachteiliger Folgen auszusprechen.[39] Hierdurch sollen die Betroffenen in Kenntnis der Sachlage die Gelegenheit haben, entsprechende Maßnahmen zu treffen.[40]

---

[21] AA *Ernst,* DuD 2010, 473; *Gabel,* BB 2009, 2047.
[22] Ähnlich auch *Karger,* ITRB 2010, 162, der bei grober Fahrlässigkeit in diese Richtung tendiert.
[23] *Ernst,* DuD 2010, 473.
[24] *Ernst,* DuD 2010, 473.
[25] *Ernst,* DuD 2010, 473.
[26] *Plath/Hullen,* § 42a BDSG Rn. 8.
[27] BT-Drs. 16/12011, S. 34; *Weichert* in: Däubler/Klebe/Wedde/Weichert, § 42a BDSG Rn. 6; *Eckhardt/Schmitz,* DuD 2010, 392.
[28] GesetzesEntw der BundesReg für ein Gesetz zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften v. 18.2.2009, BT-Drs. 16/12011, S. 34; *Spindler,* DJT, F103; *Höhne,* jurisPR-ITR 20/2009 Anm. 3.
[29] *Höhne,* jurisPR-ITR 20/2009 Anm. 3.
[30] *Gola/Schomerus,* § 42a Rn. 4; *Duisburg/Picot,* CR 2009, 823 (824); *Karger,* ITRB 2010, 162; *Ernst,* DuD 2010, 473.
[31] *Gabel,* BB 2009, 2047.
[32] BT-Drs. 16/12011, S. 34.
[33] BT-Drs. 16/12011, S. 34.
[34] BT-Drs. 16/12011, S. 34.
[35] BT-Drs. 16/12011, S. 34; *Gabel,* BB 2009, 2048.
[36] BT-Drs. 16/12011, S. 34.
[37] *Simitis/Dix,* § 42a Rn. 16.
[38] *Karger,* ITRB 2010, 162; siehe auch *Ernst,* DuD 2010, 474.
[39] *Hornung,* NJW 2010, 1843.
[40] *Gola/Schomerus,* § 42a Rn. 6.

§ 42a Satz 5 statuiert eine Ausnahme der individuellen Benachrichtigung der Betroffenen, wenn dies einen unverhältnismäßigen Aufwand (zB bei einer großen Anzahl an Betroffenen) darstellt.[41] Eine solche öffentliche Benachrichtigung kann durch Anzeigen in mindestens zwei überregionalen Tageszeitungen mit mindestens einer halben Seite Umfang oder durch vergleichbar wirksame Maßnahmen erfolgen.[42] Je nach den konkreten Umständen des Einzelfalls kann eine vergleichbare Maßnahme auch eine Benachrichtigung über ein elektronisches Medium sein.[43] Denkbar sind gegebenenfalls auch Informationen über **soziale Netzwerke,** sofern das Unternehmen überwiegend dort aktiv war und somit die Kenntnisnahme der Information durch die Betroffenen über dieses Medium am ehesten zu erwarten ist.

Problematisch sind die Fälle des Skimmings. Unter **Skimming** versteht man das Auslesen oder Kopieren des Inhalts der auf dem Magnetstreifen enthalten von Daten aus einer Bank- oder Kreditkarte sowie das Ausspähen der PIN über Kartenterminals.[44] Aus den ausgelesenen Daten wird dann eine Kopie der Karte hergestellt.[45] Mit dieser Kartenkopie und der ausgespähten PIN können Zahlungen oder Abhebungen durch unberechtigte Dritte erfolgen. Skimming Fälle werden in der Regel sehr schnell entdeckt und die Betroffenen durch die jeweilige Institutsbank umgehend telefonisch kontaktiert und Schäden den Betroffenen ersetzt. Da aufgrund dieses Vorgehens gar keine künftige Beeinträchtigung mehr besteht, erscheint eine Information nach § 42a nicht geboten.[46] Zudem wäre nach dem Wortlaut der Vorschrift, sofern man eine Mittteilungspflicht annehmen wollte, auch gar nicht das Bankinstitut Adressat der Informationspflicht sondern vielmehr der jeweilige Kartenterminalnutzer, denn die Missbrauchsfälle treten gerade bei dem Nutzer des Kartenterminals ein und nicht bei dem Bankinstitut.[47] **9**

Bezüglich der Benachrichtigung der Aufsichtsbehörde verlangt § 42a Satz 4 zusätzlich, dass diese über die möglichen nachteiligen Folgen der unrechtmäßigen Kenntniserlangung durch Dritte und über die ergriffenen Maßnahmen der verantwortlichen Stelle unterrichtet wird. **10**

Für die Form der Benachrichtigung genügt die Textform gem. § 126 BGB, die auch eine Benachrichtigung per E-Mail zulässt. In dringenden Ausnahmefällen kann auch eine telefonische Benachrichtigung genügen.[48] **11**

4. Verwendungsverbot

Satz 6 enthält ein strafrechtliches **Verwendungsverbot.** Das Verbot gilt für Verfahren gegen den Benachrichtigungspflichtigen oder dessen Angehörige, § 52 Abs. 1 StPO. Der Benachrichtigungspflichtige soll somit vor dem Konflikt bewahrt werden, dass er sich selbst belastet („nemo tenetur se ipsum accusare"), oder sich aufgrund einer Nichtanzeige gem. § 43 Abs. 2 Nr. 7 ordnungswidrig verhält.[49] Das Verwendungsverbot erstreckt sich zunächst auf natürliche Personen, eine Selbstbezichtigung ist bei juristischen Personen allenfalls bei einer Ein-Mann-GmbH denkbar.[50] Es wird jedoch, um ein Leerlaufen der Vorschrift zu verhindern, befürwortet, das Verwendungsverbot entsprechend auch auf die Personen und ihre vertretungsberechtigten Organe anzuwenden, die als taugliche Täter einer Ordnungswidrigkeit oder Straftat in Betracht kommen.[51] Das Verwendungsverbot ist äquivalent zum Verwendungsverbot des § 97 Abs. 1 Satz 3 InsO. Es geht über ein Verwertungsverbot hinaus und beansprucht eine Fernwirkung, die jede weitere Verwendung der Informationen für Straf- und Bußgeldverfahren ausschließt.[52] **12**

III. Folgen bei Verstößen

Verstöße gegen die Informationspflicht aufgrund nicht richtiger, nicht vollständiger oder nicht rechtzeitiger Information können durch Aufsichtsbehörden gem. § 43 Abs. 2 Nr. 7 mit Bußgeldern bis zu 300.000 Euro geahndet werden. Interessanterweise fehlen für § 15a TMG und § 93 Abs. 3 TKG entsprechende Bußgeldvorschriften, was wohl auf ein Redaktionsversehen zurückgeführt werden muss.[53] Der Betroffene ist zudem nach § 7 sowie § 823 Abs. 1 und gegebenenfalls auch Abs. 2 (§ 42a **13**

[41] *Simitis/Dix,* § 42a Rn. 17; *Bierekoven,* ITRB 2010, 89.
[42] *Bierekoven,* ITRB 2010, 89; *Karger,* ITRB 2010, 163; *Ernst,* DuD 2010, 474.
[43] *Ernst,* DuD 2010, 475.
[44] *BGH,* NStZ 2011, 154; *Leupold/Glossner/Cornelius,* Teil 10 Rn. 251; ausf. zur Funktionsweise *Zahrte/Selig,* BKR 2014, 186.
[45] *Leupold/Glossner/Cornelius,* Teil 10 Rn. 251.
[46] Bereits keine personenbezogenen Datem beim Entwender sehend *Zahrte/Selig,* BKR 2014, 186.
[47] *Zahrte/Selig,* BKR 2014, 187.
[48] *Weichert* in: Däubler/Klebe/Wedde/Weichert, § 42a BDSG Rn. 11.
[49] BT-Drs. 16/12011, S. 35.
[50] *Simitis/Dix,* § 42a Rn. 19.
[51] *Taeger/Gabel/Gabel,* § 42a BDSG Rn. 31; *Ernst,* DuD 2010, 475; aA *Eckhardt,* ZD-Aktuell 2013, 03494.
[52] *Hornung,* NJW 2010, 1841 (1844); *Höhne,* jurisPR-ITR 20/2009 Anm. 3.
[53] *Gabel,* BB 2009, 2046.

als Schutzgesetz)[54] BGB berechtigt, **Schadensersatzansprüche** geltend zu machen. Der Anspruch nach § 7 ist auf Ersatz des materiellen Schadens begrenzt.

Fünfter Abschnitt. Schlussvorschriften

§ 43 Bußgeldvorschriften

(1) **Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig**

1. entgegen § 4d Abs. 1, auch in Verbindung mit § 4e Satz 2, eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
2. entgegen § 4f Abs. 1 Satz 1 oder 2, jeweils auch in Verbindung mit Satz 3 und 6, einen Beauftragten für den Datenschutz nicht, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt,
2a. entgegen § 10 Absatz 4 Satz 3 nicht gewährleistet, dass die Datenübermittlung festgestellt und überprüft werden kann,
2b. entgegen § 11 Absatz 2 Satz 2 einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt oder entgegen § 11 Absatz 2 Satz 4 sich nicht vor Beginn der Datenverarbeitung von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt,
3. entgegen § 28 Abs. 4 Satz 2 den Betroffenen nicht, nicht richtig oder nicht rechtzeitig unterrichtet oder nicht sicherstellt, dass der Betroffene Kenntnis erhalten kann,
3a. entgegen § 28 Absatz 4 Satz 4 eine strengere Form verlangt,
4. entgegen § 28 Abs. 5 Satz 2 personenbezogene Daten übermittelt oder nutzt,
4a. entgegen § 28a Abs. 3 Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,
5. entgegen § 29 Abs. 2 Satz 3 oder 4 die dort bezeichneten Gründe oder die Art und Weise ihrer glaubhaften Darlegung nicht aufzeichnet,
6. entgegen § 29 Abs. 3 Satz 1 personenbezogene Daten in elektronische oder gedruckte Adress-, Rufnummern-, Branchen- oder vergleichbare Verzeichnisse aufnimmt,
7. entgegen § 29 Abs. 3 Satz 2 die Übernahme von Kennzeichnungen nicht sicherstellt,
7a. entgegen § 29 Abs. 6 ein Auskunftsverlangen nicht richtig behandelt,
7b. entgegen § 29 Abs. 7 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet,
8. entgegen § 33 Abs. 1 den Betroffenen nicht, nicht richtig oder nicht vollständig benachrichtigt,
8a. entgegen § 34 Absatz 1 Satz 1, auch in Verbindung mit Satz 3, entgegen § 34 Absatz 1a, entgegen § 34 Absatz 2 Satz 1, auch in Verbindung mit Satz 2, oder entgegen § 34 Absatz 2 Satz 5, Absatz 3 Satz 1 oder Satz 2 oder Absatz 4 Satz 1, auch in Verbindung mit Satz 2, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder entgegen § 34 Absatz 1a Daten nicht speichert,
8b. entgegen § 34 Abs. 2 Satz 3 Angaben nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt,
8c. entgegen § 34 Abs. 2 Satz 4 den Betroffenen nicht oder nicht rechtzeitig an die andere Stelle verweist,
9. entgegen § 35 Abs. 6 Satz 3 Daten ohne Gegendarstellung übermittelt,
10. entgegen § 38 Abs. 3 Satz 1 oder Abs. 4 Satz 1 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder eine Maßnahme nicht duldet oder
11. einer vollziehbaren Anordnung nach § 38 Abs. 5 Satz 1 zuwiderhandelt.

(2) **Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig**

1. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, erhebt oder verarbeitet,
2. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, zum Abruf mittels automatisierten Verfahrens bereithält,
3. unbefugt personenbezogene Daten, die nicht allgemein zugänglich sind, abruft oder sich oder einem anderen aus automatisierten Verarbeitungen oder nicht automatisierten Dateien verschafft,
4. die Übermittlung von personenbezogenen Daten, die nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht,
5. entgegen § 16 Abs. 4 Satz 1, § 28 Abs. 5 Satz 1, auch in Verbindung mit § 29 Abs. 4, § 39 Abs. 1 Satz 1 oder § 40 Abs. 1, die übermittelten Daten für andere Zwecke nutzt,

[54] *Gabel,* BB 2009, 2046; *Ernst,* DuD 2010, 475.

5a. entgegen § 28 Absatz 3b den Abschluss eines Vertrages von der Einwilligung des Betroffenen abhängig macht,
5b. entgegen § 28 Absatz 4 Satz 1 Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung verarbeitet oder nutzt,
6. entgegen § 30 Absatz 1 Satz 2, § 30a Absatz 3 Satz 3 oder § 40 Absatz 2 Satz 3 ein dort genanntes Merkmal mit einer Einzelangabe zusammenführt oder
7. entgegen § 42a Satz 1 eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(3) **[1]Die Ordnungswidrigkeit kann im Falle des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro, in den Fällen des Absatzes 2 mit einer Geldbuße bis zu dreihunderttausend Euro geahndet werden. [2]Die Geldbuße soll den wirtschaftlichen Vorteil, den der Täter aus der Ordnungswidrigkeit gezogen hat, übersteigen. [3]Reichen die in Satz 1 genannten Beträge hierfür nicht aus, so können sie überschritten werden.**

Übersicht

Literatur: *Bär,* Wardriver und andere Lauscher – Strafrechtliche Fragen im Zusammenhang mit WLAN, MMR 2005, 434; *Gabel,* Informationspflichten bei unrechtmäßiger Kenntniserlangung von Daten, BB 2009, 2045; *Höfinger,* Zur Straflosigkeit des sogenannten „Schwarz-Surfens", ZUM 2011, 212; *Höhne,* jurisPR-ITR 20/2009 Anm. 3; *Hornung,* Informationen über „Datenpannen" – Neue Pflichten für datenverarbeitende Unternehmen, NJW 2010, 1841; *Mathy,* Der problematische Datenrechtsschutz in der Rechtsschutzversicherung, VersR 2010, 318; *Rathsack,* Strafrechtliche Bewertung des Einwählens in fremde unverschlüsselte WLAN-Netze, jurisPR-ITR 1/2011 Anm. 2; *Wybitul,* BGH verurteilt Detektive wegen Überwachungsmaßnahmen zu Haftstrafen, ZD-Aktuell 2013, 03606.

I. Allgemeines

Mit den §§ 43, 44 setzt der Gesetzgeber die Vorgaben aus Art. 24 DSRL 95/46/EG[1] um.[2] Art. 24 DSRL knüpft wiederum an eine US-amerikanische Regelung an, die eine Informationspflicht gegenüber den Betroffenen und der Federal Trade Commission (FTC), einer unabhängige Bundesbehörde für Wettbewerbs- und Verbraucherschutz, vorschreibt.[3] **1**

Sofern andere datenschutzgesetzliche Regelungen kein eigenes Sanktionsregime enthalten, ist § 43 auf diese anwendbar.[4] § 43 soll das Datenschutzrecht stärken[5] und die **informationelle Selbstbestimmung** der Betroffenen schützen.[6] **2**

Als Ordnungswidrigkeitstatbestand erfordert § 43 immer das Vorliegen der Tatbestandsvoraussetzungen, Rechtswidrigkeit und Verschulden.[7] Allerdings wird die Rechtswidrigkeit durch die Tatbestandsverwirklichung indiziert, was sich aus dem Zusatz **„unbefugt"** im Wortlaut ergibt.[8] Ein Verstoß gegen den Tatbestand des § 43 stellt zudem eine Schutzgesetzverletzung dar, weswegen der Betroffene auch nach § 823 Abs. 2 BGB **Schadensersatz** verlangen kann.[9] § 43 und § 44 sind indes **keine Verbotsgesetze** iSv § 134 BGB, da sie die Rechtsfolge einer entsprechenden Gesetzesverletzung bereits selbst regeln.[10] Des Weiteren gilt die allgemeine Verjährungsfrist des § 3 OWiG von drei Jahren.[11] **3**

---

[1] RL 95/46/EG des Europäischen Parlaments und des Rates v. 24.14.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 S. 3 1 ff. v. 23.11.1995.
[2] *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 1.
[3] *Hornung,* NJW 2010, 1842.
[4] *Simitis/Ehmann,* § 43 Rn. 18 f.; aA *Plath/Becker;* § 43 BDSG Rn. 2.
[5] *Schaffland/Wiltfang,* § 43 Rn. 1.
[6] *Hornung,* NJW 2010, 1841; *Höhne,* jurisPR-ITR 20/2009 Anm. 3.
[7] *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 3.
[8] *Taeger/Gabel/Mackenthun* § 43 BDSG Rn. 4.
[9] *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 7; *Schaffland/Wiltfang,* § 43 Rn. 3.
[10] *OLG Celle,* WM 2004, 1384 (1385).
[11] *Roßnagel/Bär,* Kap. 5.7, Rn. 67.

II. Täterschaft

4 Aus dem Wortlaut *(„wer")* ergibt sich, dass grundsätzlich jede **natürliche Person**[12] (außer dem Betroffenen selbst im Hinblick auf seine eigenen Daten) Täter sein kann.[13] Nach den Voraussetzungen des § 30 OWiG kann Bußgeld gegen eine juristische Person oder Personenvereinigung nur dann verhängt werden, wenn die Pflichtverletzung auf deren Bereicherung zielte und der Täter eine Organ-, Vertreter- oder andere Verantwortungsposition inne hatte.[14] Liegt allerdings eine solche Position vor, kann die Geldbuße sogar verdoppelt werden (§ 30 Abs. 2 OWiG).[15]

III. Verfahrensverstöße (Abs. 1)

1. § 11 (Nr. 2b)

5 Bußgeldbewehrt ist die mangelnde Erfüllung der Anforderungen an die **Auftragsdatenverarbeitung.** Erforderlich ist die richtige, vollständige und formgerechte Erteilung des Auftrags gem. § 11 Abs. 2 Nr. 1 bis 10. Zudem muss sich der Auftraggeber vor der Datenverarbeitung von den getroffenen **technischen und organisatorischen** Maßnahmen überzeugen (§ 11 Abs. 2 Satz 4); dazu gehört auch die sorgfältige Auswahl des Auftragnehmers. Die Erfüllung dieses zweiten Tatbestandsteils ist praktisch allerdings schwer nachweisbar. Denn es ist bereits unklar, was unter der Formulierung *„sich überzeugen"* konkret zu verstehen ist (siehe ausführlicher § 11 Rn. 22).[16] Zudem ist lediglich die erstmalige Kontrolle bußgeldbewehrt, nicht aber die Pflicht, die Sicherheitsmaßnahmen regelmäßig zu überprüfen.[17] Der Gesetzgeber geht nämlich davon aus, dass regelmäßige Kontrollen auf der Vorabkontrolle aufbauen und der Handlungszeitpunkt für weitere Kontrollen zu unbestimmt ist.[18] Adressat des Ordnungswidrigkeitentatbestands ist die Person, welche die Vertragsabschlusskompetenz hat und unter Umständen der Datenschutzbeauftragte, falls er seine Aufgabe zur Kontrolle nicht delegiert hat.[19]

2. § 28 (Nr. 3, 3a, 4)

6 § 43 Abs. 1 Nr. 3 bezieht sich auf die Unterrichtungspflicht bei Ansprache zu **Werbe-, Markt-, Meinungsforschungszwecken.** Diese soll den Betroffenen vor unerwünschter Werbung schützen.[20] Hierbei handelt es sich um eine **Organisationspflicht.** Der Tatbestand ist also auch dann erfüllt, wenn durch keine konkrete Person Kenntnis über die Herkunft von personenbezogenen Daten verlangt wird.[21] Waren die für die Ansprache genutzten Daten bei der verantwortlichen Stelle bereits vorhanden, muss sie ihre Identität preisgeben und den Betroffenen auf sein Widerspruchsrecht hinweisen.[22] Stammen die Daten dagegen von einem Dritten, muss die verantwortliche Stelle dem Betroffenen zudem die Möglichkeit aufzeigen, wie er die Herkunft der Daten feststellen kann.[23] Eine Ordnungswidrigkeit liegt dann vor, wenn die **Unterrichtung** fehlt bzw. unrichtig, nicht rechtzeitig oder lückenhaft erteilt wird.[24] Eine mündliche Unterrichtung ist dann noch rechtzeitig, wenn sie derart erfolgt, dass der Widerspruch des Betroffenen noch Konsequenzen haben kann.[25]

7 Denn gem. § 28 Abs. 4 Satz 4 darf für den **Widerspruch** keine strengere Form verlangt werden, als für die Begründung des rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses selbst.[26] Erfolgt das Vertragsangebot etwa im Internet, muss auch der Widerspruch über das Internet erklärbar sein.[27] Auch wenn gegenläufige Allgemeine Geschäftsbedingungen ohnehin an der Inhaltskontrolle scheitern, ist der Tatbestand des § 43 erfüllt, weil zunächst eine strengere Form gefordert wurde.[28]

8 Nach § 43 Abs. Nr. 4 handelt ordnungswidrig, wer **zweckgebundene Daten** unter Verletzung der Zweckbindung übermittelt oder nutzt (§ 28 Abs. 5 Satz 2). Normadressat ist der Dritte, der Daten mit

---

[12] *Schaffland/Wiltfang,* § 43 Rn. 4.
[13] *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 8.
[14] *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 10.
[15] *Schaffland/Wiltfang,* § 43 Rn. 6.
[16] *Simitis/Ehmann,* § 43 Rn. 35.
[17] *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 15; *Simitis/Ehmann,* § 43 Rn. 35.
[18] BT-Drs. 16/13657, S. 22; *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 15.
[19] *Schaffland/Wiltfang,* § 43 Rn. 12b; *Gola/Schomerus,* § 43 Rn. 3.
[20] *Schaffland/Wiltfang,* § 43 Rn. 13.
[21] *Simitis/Ehmann,* § 43 Rn. 36.
[22] *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 17 f.
[23] *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 19 f.
[24] *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 21.
[25] *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 21; *Gola/Schomerus,* § 43 Rn. 7; *Roßnagel/Bär,* Kap. 5.7, Rn. 34.
[26] BT-Drs. 16/12011, S. 33 f.; *Taeger/Gabel/Mackenthun,* § 43 BDSG Rn. 22.
[27] *Simitis/Ehmann,* § 43 Rn. 37.
[28] *Simitis/Ehmann,* § 43 Rn. 37.