

Unternehmerische Haftung für Verstöße gegen datenschutzrechtliche Vorgaben

Christiane Bierekoven

Inhaltsverzeichnis

I.	Zivilrechtliche Haftungsgrundlagen	24
1.	Schadensersatzanspruch gemäß § 7 BDSG	24
2.	Haftung wegen Verletzung des allgemeinen Persönlichkeitsrechtes	29
II.	Bußgeldtatbestände	31
1.	Der allgemeine Bußgeldtatbestand des § 43 BDSG	31
2.	Die bereichsspezifischen Bußgeldtatbestände des § 16 TMG und § 149 TKG	36
III.	Strafrechtliche Sanktionen, § 44 BDSG	37
1.	Täter	37
2.	Tatbestandsvoraussetzung	38
3.	Strafantrag, § 44 Abs. 2 BDSG	38
4.	Praxisfälle	39
IV.	Kontrolltätigkeit der Aufsichtsbehörden, § 38 BDSG	39
1.	Überblick	39
2.	Auskunftsrechte, § 38 Abs. 3 BDSG	39
3.	Zutritts- und Einsichtsrechte, § 38 Abs. 4 BDSG	40
4.	Anordnungs- und Untersagungsrechte, § 38 Abs. 5 BDSG	40
5.	Mitwirkungspflichten des Unternehmens	40
6.	Mögliche Vorgehen der Aufsichtsbehörde	41
7.	Praxisfälle	42
V.	Geplante Änderungen durch die BDSG-Novelle	43
VI.	Zusammenfassung und Ausblick	43

Die unternehmerische Haftung für Verstöße gegen datenschutzrechtliche Vorgaben ergibt sich aus dem Bundesdatenschutzgesetz (BDSG), den bereichsspezifischen Datenschutzgesetzen, insbesondere Telemedien-(TMG) und Telekommunikationsgesetz (TKG) sowie dem allgemeinen Persönlichkeitsrecht. Auf der Rechtsfolgenseite können Datenschutzverstöße zivilrechtliche sowie straf- und ordnungsrechtliche Rechtsfolgen nach sich ziehen.

Als zivilrechtliche Rechtsfolge für Verstöße kommen Schadensersatzansprüche nach § 7 BDSG und Ansprüche aus Deliktsrecht, insbesondere § 823 BGB bei Verletzung des allgemeinen Persönlichkeitsrechtes, in Betracht. Straf- und ordnungsrechtliche Sanktionen sind die Verhängung von Bußgeldern gemäß § 43 BDSG, § 16 Abs. 3 TMG und § 149 Abs. 2 TKG

sowie strafrechtliche Sanktionen gemäß § 44 BDSG und aufsichtsbehördliche Maßnahmen nach § 38 BDSG.

I. Zivilrechtliche Haftungsgrundlagen

1. Schadensersatzanspruch gemäß § 7 BDSG

Gemäß § 7 S. 1 BDSG hat eine verantwortliche Stelle oder ihr Träger Schadensersatz zu leisten, wenn dem Betroffenen durch eine nach dem Bundesdatenschutzgesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten ein Schaden entstanden ist. Dies gilt dann nicht, wenn die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat, § 7 S. 2 BDSG.

a) Voraussetzungen

Für einen Schadensersatzanspruch nach dieser Vorschrift müssen zunächst einmal zwei Voraussetzungen erfüllt sein:

Zum einen muss die verantwortliche Stelle personenbezogene Daten in unzulässiger oder unrichtiger Weise erhoben oder verwendet haben. Sodann muss dieser Verstoß kausal für einen Schaden des Betroffenen sein.

(1) Anspruchsberechtigter

Anspruchsberechtigter i. S. d. § 7 BDSG ist ausschließlich der Betroffene selbst. Dies ist gemäß § 3 Abs. 1 BDSG eine bestimmte oder bestimmbare natürliche Person. Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer solchen bestimmten oder bestimmbaren natürlichen Person. Weitere Personen außer dem Betroffenen werden vom Schutzbereich des § 7 BDSG ebenso wenig erfasst wie juristische Personen.¹

(2) Anspruchsgegner

Anspruchsgegner ist die verantwortliche Stelle oder ihr Träger. Verantwortliche Stelle ist gemäß § 3 Abs. 7 BDSG jede Person/Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Im hier relevanten privatwirtschaftlichen Bereich ist danach verantwortliche Stelle in der Regel das Unternehmen, das die Daten erhebt, verarbeitet und nutzt.

Die Haftung nach § 7 BDSG erstreckt sich andererseits auch nur auf das Unternehmen. Eine Haftung der Mitarbeiter oder des betrieblichen Datenschutzbeauftragten kommt nicht in Betracht. Diese können jedoch nach all-

¹ Däubler, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG Basiskommentar, 2. Aufl. 2007, § 7, Rn. 6; Simitis, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Aufl. 2006, § 7, Rn. 12, 13; Gola/Schomerus, Bundesdatenschutzgesetz: Kommentar, 8. Aufl. 2005, § 7, Rn. 6; Simitis, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Aufl. 2006, § 7, Rn. 9.

gemeinen vertrags- und deliktsrechtlichen Grundsätzen haften.² Diese Haftungsmöglichkeiten sind nicht Gegenstand dieses Beitrages.

(3) Sonderfall: Auftragsdatenverarbeitung

Zu beachten ist, dass die verantwortliche Stelle, also das Unternehmen, auch dann verantwortliche Stelle i. S. d. § 7 BDSG bleibt, wenn ein externes Unternehmen seine Unternehmensdaten im Auftrag nach § 11 BDSG verarbeitet.

Etwas anderes gilt nur dann, wenn dieses externe Unternehmen die Weisungen des Auftraggebers, also des beauftragenden Unternehmens, missachtet und die Daten für eigene Zwecke verwendet. In diesem Fall wird das externe Unternehmen selbst zur verantwortlichen Stelle und kann demgemäß nach § 7 BDSG haften.³

b) Anspruchsgrundende Handlungen und Schaden

Voraussetzungen für einen Schadensersatzanspruch des Betroffenen sind, dass die verantwortliche Stelle gegen datenschutzrechtliche Vorschriften verstoßen hat (1) und dieser Verstoß kausal für einen Schaden des Betroffenen ist (2).

(1) Verstoß gegen datenschutzrechtliche Vorschriften

Ein solcher Verstoß liegt insbesondere dann vor, wenn personenbezogene Daten entgegen der einschlägigen datenschutzrechtlichen Regelungen des BDSG erhoben, verarbeitet oder genutzt werden.⁴ Zu beachten ist, dass dies mangels Konzernprivilegs auch gilt, wenn personenbezogene Daten innerhalb eines Konzerns ohne Einwilligung oder nicht gemäß § 28 BDSG übermittelt werden, insbesondere wenn eine solche Übermittlung im Rahmen eines internationalen Konzerns an die Mutter- oder Tochtergesellschaften erfolgt, die ihren Sitz in einem unsicheren Drittstaat haben.

Unerheblich ist hingegen, auf welcher Verarbeitungsstufe der Verstoß erfolgt, also bei der Erhebung, Verarbeitung oder Nutzung.⁵

(2) Kausalität des Schadens und allgemeine Beweisprobleme

Sodann muss der Verstoß für einen dem Betroffenen entstandenen Schaden kausal sein.

2 Däubler, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG Basiskommentar, 2. Aufl. 2007, § 7, Rn. 9; Simitis, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Aufl. 2006, § 7, Rn. 12, 13.

3 Däubler, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG Basiskommentar, 2. Aufl. 2007, § 7, Rn. 8; Simitis, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Aufl. 2006, § 7, Rn. 11.

4 Däubler, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG Basiskommentar, 2. Aufl. 2007, § 7, Rn. 10; Gola/Schomerus, Bundesdatenschutzgesetz: Kommentar, 8. Aufl. 2005, § 7, Rn. 3–5; Simitis, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Aufl. 2006, § 7, Rn. 18–20.

5 Däubler, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG Basiskommentar, 2. Aufl. 2007, § 7, Rn. 11; Simitis, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Aufl. 2006, § 7, Rn. 14.

Problematisch ist insoweit, dass der Schadensersatzanspruch gemäß § 7 BDSG nach herrschender Auffassung *ausschließlich materielle* Schäden erfasst.⁶ Rechtsprechung existiert zu dieser Schadensersatzproblematik wohl gerade aufgrund dieser Beschränkung kaum.

Der datenschutzrechtliche Verstoß muss zudem *kausal* für einen beim Betroffenen entstandenen materiellen Schaden sein. Dies bedeutet, dass der geschädigte Betroffene nicht nur den Datenschutzverstoß und einen materiellen Schaden, sondern vor allem auch nachweisen muss, dass dieser Verstoß für den materiellen Schaden ursächlich war. Dies ist regelmäßig nur schwer nachzuweisen. Werden personenbezogene Daten beispielsweise innerhalb eines Konzerns datenschutzwidrig von einer Gesellschaft an die andere weitergegeben, ist zunächst kein materieller Schaden erkennbar, der dem Betroffenen hieraus entstehen könnte.

Etwas anderes würde möglicherweise dann gelten, wenn eine derartige Übermittlung von personenbezogenen Daten eines Mitarbeiters die Kündigung dieses Mitarbeiters zur Folge hätte, weil bspw. seine finanziellen Verhältnisse der empfangenden Gesellschaft nicht zusagen oder seine Gesundheitsdaten den erwarteten Anforderungen des Unternehmens nicht entsprechen. Hier entsteht durch den Wegfall des Arbeitsverhältnisses zwar ein materieller Schaden, da der Betroffene keine Vergütung mehr erhält, etwaige Gratifikationen wegfallen und auch die anteiligen Beiträge des Arbeitgebers/Unternehmers zur Kranken-, Renten- und Sozialversicherung. Problematisch ist in diesen Fällen jedoch, dass der Mitarbeiter, der lediglich seine Kündigung erhält, von der konzerninternen Weitergabe seiner personenbezogenen Daten in der Regel keinerlei Kenntnis hat. Er wird deswegen in der Regel nicht auf den Gedanken verfallen, dass seine Kündigung hierauf beruhen könnte und dementsprechend auch keine Schadensersatzansprüche geltend machen. Selbst wenn er Kenntnis von einer solchen konzerninternen Datenübermittlung haben sollte, wird er im Regelfall jedoch kaum nachweisen können, dass diese bzw. das aufgrund dieser Übermittlung weitergeleitete Ergebnis der Grund für seine Kündigung war.

Eine ähnliche Problematik stellt sich bei datenschutzwidrigen Veröffentlichungen von personenbezogenen Daten im Internet. So unangenehm dies im Einzelfall sein kann, führen solche Veröffentlichungen jedoch nicht notwendiger Weise zu einem *materiellen* Schaden i. S. einer konkreten Vermögenseinbuße. Ein Anspruch aus § 7 BDSG läuft in diesen Fällen deshalb vielfach leer. Es verbleiben eventuell Ansprüche wegen Verletzung des allgemeinen Persönlichkeitsrechtes (dazu unten Ziffer 8.).

⁶ *Däubler*, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG Basiskommentar, 2. Aufl. 2007, § 7, Rn. 19; *Gola/Schomerus*, Bundesdatenschutzgesetz: Kommentar, 8. Aufl. 2005, § 7, Rn. 12; *Simitis*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Aufl. 2006, § 7, Rn. 30–32.

Etwas anderes gilt nach dem LG Bonn, wenn der Schufa unbefugt die Kündigung eines Kreditkartenvertrages mitgeteilt wird und der Betroffene deshalb dort schlechter eingestuft wird. Den aus dieser Eintragung in die Schufa-Liste dem Betroffenen entstandenen Schaden kann dieser von der Schufa als in diesem Fall verantwortlichen Stelle ersetzt verlangen. Das Gericht gründete diesen Schadensersatzanspruch jedoch auf eine positive Forderungsverletzung.⁷

c) Die Beweissituation des Betroffenen im Besonderen

Problematisch ist für den Betroffenen, dass er die Voraussetzungen des § 7 BDSG darlegen und beweisen muss.

Deswegen wird teilweise die Auffassung vertreten, dass es genügen müsse, wenn der Betroffene Indizien für einen Verstoß darlegt und beweist und sodann von einem Prima-Facie-Beweis hinsichtlich der Kausalität des Schadenseintritts auszugehen ist. Zudem soll die verantwortliche Stelle zu einer verstärkten Mitwirkung verpflichtet sein, wenn der Betroffene Anhaltspunkte für einen Verstoß hat.⁸ Nach anderer Ansicht soll es ausreichen, wenn der Betroffene beweist, dass die rechtswidrige Datenverarbeitung aus der Sphäre der verantwortlichen Stelle resultiert⁹ oder der Betroffene darlegt, dass die verantwortliche Stelle seine Daten verwendet hat.¹⁰

Die Indizien soll der Betroffene bei einem Verdacht auf eine rechtswidrige Datenverarbeitung durch sein Auskunftsrecht gegen die verantwortliche Stelle nach § 34 BDSG in Erfahrung bringen können.¹¹ Fraglich ist jedoch zum einen, ob der Betroffene überhaupt Kenntnis von Anhaltspunkten für eine rechtswidrige Datenverarbeitung erhält, was in vielen Fällen, wie die angegebenen Beispiele zeigen, schon fraglich sein wird. Zum anderen ist jedoch auch fraglich, ob ihm der Auskunftsanspruch bei der Sammlung von Beweisen für eine rechtswidrige Datenverarbeitung und den ihm entstandenen Schaden überhaupt weiterhilft. Zu beachten ist, dass der Auskunftsanspruch nicht uneingeschränkt besteht und zudem das Interesse der verarbeitenden Stelle an der Wahrung des Geschäftsgeheimnisses der Auskunftserteilung entgegenstehen kann, § 34 Abs. 1 S. 3 BDSG. Insofern kann es für den Betroffenen also bereits schwierig werden, seinen Auskunftsanspruch überhaupt durchzusetzen und damit erst

⁷ *LG Bonn*, NJW-RR 1994, 1392 (1393). Anders aber *OLG Frankfurt*, CR 1989, 19 (19), wenn falsche Angaben an die Schufa folgenlos bleiben; so auch *Simitis*, in: *Simitis* (Hrsg.), *Bundesdatenschutzgesetz*, 6. Aufl. 2006, § 7, Rn. 30.

⁸ *Däubler*, in: *Däubler/Klebe/Wedde/Weichert* (Hrsg.), *BDSG Basiskommentar*, 2. Aufl. 2007, § 7, Rn. 18.

⁹ *Niedermeier/Schröcker*, RDV 2002, 218 (219).

¹⁰ *Simitis*, in: *Simitis* (Hrsg.), *Bundesdatenschutzgesetz*, 6. Aufl. 2006, § 7, Rn. 23.

¹¹ *Däubler*, in: *Däubler/Klebe/Wedde/Weichert* (Hrsg.), *BDSG Basiskommentar*, 2. Aufl. 2007, § 7, Rn. 18., *Simitis*, in: *Simitis* (Hrsg.), *Bundesdatenschutzgesetz*, 6. Aufl. 2006, § 7, Rn. 23.

recht den kausalen Schaden zu beweisen, weshalb es hierzu kaum veröffentlichte Entscheidungen gibt.

Im Ergebnis ist daher festzuhalten, dass der Betroffene in der Praxis bereits erhebliche Schwierigkeiten haben wird, die Voraussetzungen des § 7 BDSG überhaupt darzulegen und zu beweisen und somit einen Anspruch nach § 7 BDSG durchzusetzen.

d) Exkulpation

Hinzu kommt, dass selbst wenn der Betroffene die Voraussetzungen des § 7 S. 1 BDSG darlegen und beweisen kann, die verantwortliche Stelle nach § 7 S. 2 BDSG die Möglichkeit hat, sich zu exkulpieren, indem sie nachweist, dass sie die nach den Umständen gebotene Sorgfalt beachtet hat.

Dies ist etwa dann der Fall, wenn auch die korrekte Einhaltung der datenschutzrechtlichen Vorschriften den Schaden nicht hätte verhindern oder ein etwaiger Einbruch Dritter in das System nicht hätte verhindert werden können.¹² Entsprechendes gilt, wenn eine technische Störung, die zu einem Schaden beim Betroffenen geführt hat, nicht zu vermeiden war. Wird also die Datenbank mit Kunden- und gegebenenfalls Mitarbeiterdaten gehackt und werden diese Daten sodann im Internet verbreitet, könnte sich die verantwortliche Stelle exkulpieren, wenn sie nachweist, dass dieser Vorgang nicht zu vermeiden war, obwohl sie die erforderlichen Schutzmaßnahmen, insbesondere nach der Anlage zu § 9 BDSG ergriffen hat. Hierzu gilt grundsätzlich, dass die Vorkehrungen gegen unberechtigten Zugriff und Zugang zu personenbezogenen Daten umso effektiver sein müssen, je höher die potentiellen Gefahren für die Betroffenen sind.¹³

Andererseits dürfte eine Exkulpation der verantwortlichen Stelle gemesen an diesen Anforderungen bei einer unzulässigen Übermittlung von Daten im zuvor dargestellten Sinn (siehe oben Ziffer e) (1) und (2)) wohl kaum möglich sein. Die verantwortliche Stelle hat sich vor der Übermittlung von personenbezogenen Daten zu informieren, ob die Übermittlung als solche zulässig ist. Hinzu kommt, dass sie sich dann nicht exkulpieren kann, wenn der Datenschutzbeauftragte seine Aufgabe nur mangelhaft erfüllt, da er Teil der verantwortlichen Stelle ist.¹⁴ Von einer solchen mangelhaften Aufgabenerfüllung dürfte bei einer Übermittlung im genannten Sinne auszugehen sein, da der Datenschutzbeauftragte dafür Sorge tragen muss, dass derartige Übermittlungen nur erfolgen, wenn die hierfür erforderlichen Maßnahmen eingehalten werden.

12 Däubler, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG Basiskommentar, 2. Aufl. 2007, § 7, Rn. 14.

13 Däubler, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG Basiskommentar, 2. Aufl. 2007, § 7, Rn. 15.

14 Däubler, in: Däubler/Klebe/Wedde/Weichert (Hrsg.), BDSG Basiskommentar, 2. Aufl. 2007, § 7, Rn. 16; Simitis, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 6. Aufl. 2006, § 7, Rn. 26.

e) Zusammenfassung

Zusammenfassend ist festzuhalten, dass Rechtsprechung zu Ansprüchen nach § 7 BDSG kaum existiert. Dies dürfte wohl zum einen darauf zurückzuführen sein, dass, wie die Beispiele Fälle zeigen, ein materieller Schaden beim Betroffenen selten vorliegen wird. Zum anderen wird er von der rechtswidrigen Datenübermittlung vielfach erst gar keine Kenntnis erhalten oder selbst wenn er Anhaltspunkte hierfür hat, die Voraussetzungen des § 7 BDSG kaum nachweisen können, da ihm hierzu die erforderlichen Einblicke in die Datenverarbeitungsprozesse der verantwortlichen Stelle in der Regel fehlen.¹⁵

2. Haftung wegen Verletzung des allgemeinen Persönlichkeitsrechtes

a) Allgemeine Grundsätze

Ansprüche auf Ersatz des immateriellen Schadens können bei einer Verletzung des allgemeinen Persönlichkeitsrechtes bestehen, wenn die Verletzung des Persönlichkeitsrechtes schwerwiegend ist und eine Genugtuung anders nicht angemessen gewährt werden kann.¹⁶ So hat die Rechtsprechung Schadensersatzansprüche zuerkannt bei einer unzulässigen Speicherung von Daten per Videokamera¹⁷ oder bei nicht genehmigter Bildberichterstattung.¹⁸

Entscheidungen dazu, ob eine Veröffentlichung von im Unternehmen gespeicherten personenbezogenen Daten, insbesondere Kunden- und Mitarbeiterdaten im Internet, die ohne Einwilligung des Betroffenen erfolgt und auch ansonsten nicht durch datenschutzrechtliche Vorschriften gedeckt ist, eine Verletzung des allgemeinen Persönlichkeitsrechtes darstellen und deswegen zum Schadensersatz verpflichten, liegen soweit ersichtlich nicht vor.

b) Die „spickmich.de“-Entscheidung des BGH vom 23. 06. 2009¹⁹

Der für Datenschutz und den Schutz des Persönlichkeitsrechtes zuständige VI. Zivilsenat des Bundesgerichtshofes hat am 23. 06. 2009 in seiner Entscheidung „spickmich.de“ zu der besonderen Thematik der Veröffent-

¹⁵ So ähnlich auch *Simitis*, in: *Simitis* (Hrsg.), *Bundesdatenschutzgesetz*, 6. Aufl. 2006, § 7, Rn. 23, der deshalb vom Betroffenen lediglich verlangt darzulegen, dass die verantwortliche Stelle seine Daten verwendet hat.

¹⁶ *Gola/Schomerus*, *Bundesdatenschutzgesetz: Kommentar*, 8. Aufl. 2005, § 19; ständige Rechtsprechung des BGH seit BGHZ 26, 349; anders jedoch *Simitis*, in: *Simitis* (Hrsg.), *Bundesdatenschutzgesetz*, 6. Aufl. 2006, § 7, Rn. 33f., 59.

¹⁷ *OLG Frankfurt*, NJW 1987, 1087–1089; *OLG Köln*, NJW 1989, 720–722.

¹⁸ *LG Köln*, NJW 1992, 443–444.

¹⁹ *BGH*, CR 2009, 593–598.

lichung von personenbezogenen Daten in einem Internetforum Stellung bezogen.

aa) Hierbei ging es um die Zulässigkeit der Bewertung von Leistungen der Klägerin als Lehrerin mit Namensnennung durch Schüler auf der Webseite www.spickmich.de. Zugang zu diesem Portal hatten nur registrierte Nutzer, wobei die Registrierung nach Eingabe des Namens, der Schule, des Schulorts eines Benutzernamens und einer E-Mail-Adresse erfolgte.

In diesem Portal hatten Schüler die Möglichkeit, ihre Lehrer anonym zu bewerten, wobei die Schulnoten 1 bis 6 an vorgegebene Kriterien wie „cool und witzig“, „beliebt“, „motiviert“, „menschlich“, „gelassen“ und „guter Unterricht“ gebunden waren. Ein eigener Textbeitrag des Bewertenden war nicht möglich. Es bestand jedoch die Möglichkeit, auf einer Zitateseite angebliche Zitate der bewerteten Lehrer einzustellen.

bb) Die Klägerin machte eine Verletzung ihres allgemeinen Persönlichkeitsrechtes geltend.

Der VI. Zivilsenat des Bundesgerichtshofes hat in seiner Entscheidung als Prüfungsmaßstab das Datenschutzrecht herangezogen. So ist es als eine wesentliche Aussage zu werten, dass der Senat unter den Begriff der personenbezogenen Daten nicht nur klassische Daten wie etwa den Namen oder den Geburtsort, sondern auch Meinungsäußerungen und Beurteilungen, die sich auf einen bestimmten oder bestimmbaren Betroffenen beziehen, fasst. Deshalb sind nach seiner Ansicht für die Erhebung und Übermittlung solcher Daten in automatisierten Verfahren grundsätzlich die Vorschriften des Bundesdatenschutzgesetzes heranzuziehen. Als weitere wesentliche Aussage ist festzuhalten, dass der BGH für die Erhebung und Speicherung von Daten zur Übermittlung an Dritte eine Einwilligung des Betroffenen nicht für erforderlich hält. Vielmehr bejaht er die Zulässigkeit der Übermittlung nach § 29 BDSG, wenn ein Grund zu der Annahme eines schutzwürdigen Interesses an dem Ausschluss der Datenerhebung und -speicherung nicht gegeben ist. Ein solches schutzwürdiges entgegenstehendes Interesse hat der BGH in diesem Fall verneint. Er nahm eine Abwägung des Rechtes auf informationelle Selbstbestimmung einerseits und des Rechts auf freie Meinungsäußerung andererseits vor und war der Auffassung, die Bewertungen stellten Meinungsäußerungen dar, die lediglich die berufliche Tätigkeit der Klägerin betreffen würden, im Rahmen derer die Klägerin nicht den gleichen Schutz wie in der Privatsphäre genießen würde. Da konkrete Beeinträchtigungen der Klägerin nicht geltend gemacht worden seien und die Äußerungen weder schmähend noch beleidigend seien, gehe das Recht auf freie Meinungsäußerung vor, denn dieses umfasse auch das Recht, das Verbreitungsmedium frei zu bestimmen.²⁰

20 BGH, CR 2009, 593–598.

cc) Nach diesen Grundsätzen des VI. Zivilsenates des BGH ist jedenfalls im Rahmen von Onlinebewertungsportalen davon auszugehen, dass eine Einwilligung des Betroffenen zur Übermittlung seiner Daten in ein solches Bewertungsportal jedenfalls dann nicht erforderlich ist, wenn und soweit solche Bewertungsportale sich auf den beruflichen Bereich beziehen. Vielmehr ist die Übermittlung personenbezogener Daten nach § 29 BDSG zulässig. Demnach sind Online-Bewertungsportale wohl als eine Art „Auskunft“ i. S. d. § 29 Abs. 1 BDSG anzusehen.

Sodann liegt wohl keine Verletzung des allgemeinen Persönlichkeitsrechts vor, wenn die Bewertungen in diesen Portalen als Meinungsäußerung zu qualifizieren sind und die Grenze zur Schmähkritik nicht überschreiten. In diesen Fällen hat die Meinungsfreiheit Vorrang vor dem Recht auf informationelle Selbstbestimmung.

Deshalb ist wohl davon auszugehen, dass sich die Angehörigen sämtlicher Berufsstände im Internet in derartigen Bewertungsportalen bewerten lassen müssen und Unterlassungsansprüche wegen einer Verletzung des allgemeinen Persönlichkeitsrechts nur bei Schmähkritik geltend machen können. Ob diese Grundsätze jedoch auch für solche Fälle gelten, in denen ohne Kenntnis und ohne Einwilligung der Betroffenen im Unternehmen gespeicherte Kundendaten oder Arbeitnehmerdaten in Bewertungsportalen oder allgemein im Internet veröffentlicht werden, bleibt abzuwarten.

II. Bußgeldtatbestände

1. Der allgemeine Bußgeldtatbestand des § 43 BDSG

Gemäß § 43 Abs. 3 BDSG können Verstöße gegen Vorschriften des Bundesdatenschutzgesetzes mit einer Geldbuße geahndet werden. Dabei ist zwischen Verstößen gegen Verfahrensvorschriften des § 43 Abs. 1 BDSG und materiell-rechtlichen Datenschutzvorschriften des § 43 Abs. 2 BDSG zu unterscheiden.

Bei Verstößen gegen Verfahrensvorschriften kann eine Geldbuße von bis zu EUR 50 000,00 verhängen werden, bei Verstößen gegen materielles Datenschutzrecht sogar bis zu EUR 300 000,00, § 43 Abs. 3 BDSG.

a) Verstöße gegen Verfahrensvorschriften, § 43 Abs. 1 BDSG

§ 43 Abs. 1 BDSG enthält einen Katalog, in dem in den Nummern 1 bis 11 aufgeführt wird, welche Verfahrensverstöße mit einem Bußgeld geahndet werden können. Nachfolgend werden zwei ausgewählte dargestellt:

(1) Bestellung eines betrieblichen Datenschutzbeauftragten

Hierzu gehört gemäß § 43 Abs. 1 Nr. 2 BDSG insbesondere ein Verstoß gegen die Verpflichtung, einen Datenschutzbeauftragten zu bestellen oder nicht in der vorgeschriebenen Weise oder nicht rechtzeitig bestellt zu haben.

Der Datenschutzbeauftragte ist gemäß § 4 f Abs. 1 S. 1, 3 BDSG in einem Unternehmen zu bestellen, wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, in allen anderen Verarbeitungsfällen, wenn mindestens 20 Personen hiermit beschäftigt sind. Zu beachten ist, dass die Bestellung spätestens einen Monat nach Aufnahme der Tätigkeit zu erfolgen hat. Wird hiergegen verstoßen, kann ein Bußgeld verhängt werden.

Sodann ist zu beachten, dass der Datenschutzbeauftragte nach § 4 f Abs. 2 BDSG die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen muss und direkt dem Leiter des Unternehmens zu unterstellen ist, § 4 f Abs. 3 BDSG.

Er darf jedoch nicht – was vielfach angedacht oder auch durchgeführt wird – dem Leiter der IT- oder Rechtsabteilung unterstellt werden.²¹ Geschieht dies dennoch, kann auch dieser Verstoß mit einem Bußgeld von bis zu EUR 50 000,00 geahndet werden. Streitig ist hingegen, ob eine nicht oder nicht ordnungsgemäße Bestellung vorliegt, wenn die erforderliche Zuverlässigkeit und Fachkunde beim Datenschutzbeauftragten nicht vorhanden ist.

Hier ist mangels dahingehender Rechtsprechung davon auszugehen, dass jedenfalls eine nicht ordnungsgemäße Bestellung des Datenschutzbeauftragten nach § 43 Abs. 1 Nr. 2 BDSG vorliegt, die bußgeldbewehrt ist.²² Dies rechtfertigt sich bereits deswegen, weil die Stellung des Datenschutzbeauftragten im Unternehmen eine erhebliche Vertrauensstellung darstellt.

Dies ergibt sich zum einen aus seiner Pflicht zur Verschwiegenheit gemäß § 4 f Abs. 4 BDSG sowohl über die Identität des Betroffenen als auch über Umstände, die Rückschlüsse auf Betroffene zulassen. Zudem besteht seine Hauptaufgabe darin, die praktische Umsetzung des Datenschutzrechtes zu kontrollieren und vor allem die im Unternehmen vorhandenen Datenflüsse transparent und somit kontrollierbar zu machen.²³ Diese Aufgaben kann er ohne die erforderliche Fachkunde, insbesondere bei Datenflüssen in internationalen Konzernen, wie sie oben unter Ziffer 7 e) (1) dargestellt wurden, aber auch nicht ohne die erforderliche Zuverlässigkeit durchführen, die die Gewähr dafür bietet, dass der Datenschutzbeauftragte regelmäßige Kontrollen zur Einhaltung des Datenschutzrechtes sicherstellt.

21 *Däubler*, in: *Däubler/Klebe/Wedde/Weichert* (Hrsg.), *BDSG Basiskommentar*, 2. Aufl. 2007, § 4f, Rn. 31.

22 *Däubler*, in: *Däubler/Klebe/Wedde/Weichert* (Hrsg.), *BDSG Basiskommentar*, 2. Aufl. 2007, § 4f, Rn. 35 und § 43 Rn. 7; *Gola/Schomerus*, *Bundesdatenschutzgesetz: Kommentar*, 8. Aufl. 2005, § 43, Rn. 6; *Simitis*, in: *Simitis* (Hrsg.), *Bundesdatenschutzgesetz*, 6. Aufl. 2006, § 4f, Rn. 111f., anders dagegen *Ehmann*, in: *Simitis* (Hrsg.), *Bundesdatenschutzgesetz*, 6. Aufl. 2006, § 43, Rn. 34.

23 *Däubler*, in: *Däubler/Klebe/Wedde/Weichert* (Hrsg.), *BDSG Basiskommentar*, 2. Aufl. 2007, § 4 g, Rn. 7.