GDD-RATGEBER

2. AUFLAGE

© iStock.com – Milan Lipowski

Datenpannen

- Informationspflichten nach § 42a BDSG, IT-Sicherheitsgesetz und verwandten Vorschriften -

GDD
Gesellschaft für Datenschutz
und Datensicherheit e.V.

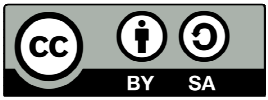
Datenpannen

Informationspflichten nach § 42a BDSG, IT-Sicherheitsgesetz und verwandten Vorschriften

2015

Datenpannen. Informationspflichten nach § 42a BDSG, IT-Sicherheitsgesetz und verwandten Vorschriften

2. Auflage, 2015
Herausgeber: **Gesellschaft für Datenschutz und Datensicherheit e.V.**
Verfasser: **Dr. iur. Lorenz Franck, GDD-Geschäftsstelle**



Heinrich-Böll-Ring 10 • 53119 Bonn

Telefon: (0228) 96 96 75-00
Telefax: (0228) 96 96 75-25
E-Mail: info@gdd.de
Internet: www.gdd.de

Vorwort

> *Toto […] tipped over the screen that stood in a corner. As it fell with a crash they looked that way, and the next moment all of them were filled with wonder. For they saw, standing in just the spot the screen had hidden, a little old man, with a bald head and a wrinkled face, who seemed to be as much surprised as they were.* (Baum, The Wonderful Wizard of Oz)

Der Grundsatz der Transparenz in der Datenverarbeitung ist gleichermaßen Folge und zwingende Voraussetzung des Rechts auf informationelle Selbstbestimmung. Der Begriff der „Selbst-Bestimmung" besitzt insofern mehrere Schattierungen. Er rekurriert einerseits auf ein Entscheidungs- und Interventionsrecht des Betroffenen. Andererseits meint er aber auch eine Bestandsaufnahme und Verortung im Hinblick auf die eigenen Daten.

Das Bundesdatenschutzgesetz ist mehrfach von Transparenzvorschriften durchzogen und vermittelt den Betroffenen in unterschiedlichen Stadien der Datenverarbeitung die Möglichkeit, Datentransfers und -verwendungen nachzuverfolgen. Die Bezeichnungen wechseln dabei stetig. So ist von Unterrichtungen, Informationen, Benachrichtigungen, Auskünften oder Mitteilungen die Rede. Das Ziel ist jedoch immer das gleiche: Der Blick hinter die Kulissen.

Die Informationspflicht bei unrechtmäßiger Kenntnisnahme durch Dritte nimmt eine Sonderstellung unter den Betroffenenrechten ein. Die datenverarbeitenden Stellen sind bei Pannen nicht nur verpflichtet, den Informationsabfluss gegenüber Betroffenen und Aufsichtsbehörden offenzulegen, sie müssen auch geeignete Hilfestellungen zur Verhinderung schwerwiegender Folgen anbieten. Die zweite Auflage des Ratgebers berücksichtigt insbesondere das jüngst in Kraft getretene IT-Sicherheitsgesetz, welches mit eigenständigen Meldepflichten aufwartet.

Bonn, im September 2015 Der GDD-Vorstand

Inhaltsverzeichnis

1. Informationspflichten nach § 42a BDSG

1.1 Gesetzliche Grundlagen

§ 42a BDSG: 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.

§ 15a TMG: Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend.

§ 93 Abs. 3 TKG: Informationspflichten

[…] (3) Im Fall einer Verletzung des Schutzes personenbezogener Daten haben die betroffenen Teilnehmer oder Personen die Rechte aus § 109a Absatz 1 Satz 2 in Verbindung mit Absatz 2.

§ 109a TKG: Datensicherheit

(1) [1]Wer öffentlich zugängliche Telekommunikationsdienste erbringt, hat im Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit von der Verletzung zu benachrichtigen. [2]Ist anzunehmen, dass durch die Verletzung des Schutzes personenbezogener Daten Teilnehmer oder andere Personen

schwerwiegend in ihren Rechten oder schutzwürdigen Interessen beeinträchtigt werden, hat der Anbieter des Telekommunikationsdienstes zusätzlich die Betroffenen unverzüglich von dieser Verletzung zu benachrichtigen. [3]In Fällen, in denen in dem Sicherheitskonzept nachgewiesen wurde, dass die von der Verletzung betroffenen personenbezogenen Daten durch geeignete technische Vorkehrungen gesichert, insbesondere unter Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens gespeichert wurden, ist eine Benachrichtigung nicht erforderlich. [4]Unabhängig von Satz 3 kann die Bundesnetzagentur den Anbieter des Telekommunikationsdienstes unter Berücksichtigung der wahrscheinlichen nachteiligen Auswirkungen der Verletzung des Schutzes personenbezogener Daten zu einer Benachrichtigung der Betroffenen verpflichten. [5]Im Übrigen gilt § 42a Satz 6 des Bundesdatenschutzgesetzes entsprechend.

(2) [1]Die Benachrichtigung an die Betroffenen muss mindestens enthalten:

1. *die Art der Verletzung des Schutzes personenbezogener Daten,*
2. *Angaben zu den Kontaktstellen, bei denen weitere Informationen erhältlich sind, und*
3. *Empfehlungen zu Maßnahmen, die mögliche nachteilige Auswirkungen der Verletzung des Schutzes personenbezogener Daten begrenzen.*

[2]In der Benachrichtigung an die Bundesnetzagentur und den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit hat der Anbieter des Telekommunikationsdienstes zusätzlich zu den Angaben nach Satz 1 die Folgen der Verletzung des Schutzes personenbezogener Daten und die beabsichtigten oder ergriffenen Maßnahmen darzulegen.

(3) [1]Die Anbieter der Telekommunikationsdienste haben ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen, das Angaben zu Folgendem enthält:

1. *zu den Umständen der Verletzungen,*
2. *zu den Auswirkungen der Verletzungen und*

3. zu den ergriffenen Abhilfemaßnahmen.

[2]Diese Angaben müssen ausreichend sein, um der Bundesnetzagentur und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit die Prüfung zu ermöglichen, ob die Bestimmungen der Absätze 1 und 2 eingehalten wurden. [3]Das Verzeichnis enthält nur die zu diesem Zweck erforderlichen Informationen und muss nicht Verletzungen berücksichtigen, die mehr als fünf Jahre zurückliegen.

[…] (5) Vorbehaltlich technischer Durchführungsmaßnahmen der Europäischen Kommission nach Artikel 4 Absatz 5 der Richtlinie 2002/58/EG kann die Bundesnetzagentur Leitlinien vorgeben bezüglich des Formats, der Verfahrensweise und der Umstände, unter denen eine Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten erforderlich ist.

§ 83a SGB X: Informationspflicht bei unrechtmäßiger Kenntniserlangung von Sozialdaten

[1]Stellt eine in § 35 des Ersten Buches genannte Stelle fest, dass bei ihr gespeicherte besondere Arten personenbezogener Daten (§ 67 Absatz 12) 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 unverzüglich der nach § 90 des Vierten Buches zuständigen Aufsichtsbehörde, der zuständigen Datenschutzaufsichtsbehörde sowie den Betroffenen mitzuteilen. [2]§ 42a Satz 2 bis 6 des Bundesdatenschutzgesetzes gilt entsprechend.

§ 18a BlnDSG: Informationspflicht bei unrechtmäßiger Kenntniserlangung von Dritten

(1) Wird einer datenverarbeitenden Stelle bekannt, dass bei ihr gespeicherte personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen, so hat sie dies unverzüglich

dem Betroffenen und dem Berliner Beauftragten für Datenschutz und Informationsfreiheit mitzuteilen.

(2) [1]Die Benachrichtigung des Betroffenen nach Absatz 1 darf nur solange aufgeschoben werden, wie die verantwortliche Stelle zunächst angemessene Maßnahmen zur Sicherung der Daten ergreifen muss. [2]Ergreift sie diese Maßnahmen nicht unverzüglich, so duldet die Benachrichtigung des Betroffenen keinen Aufschub. [3]Satz 1 gilt entsprechend, soweit eine unverzügliche Benachrichtigung des Betroffenen die Strafverfolgung gefährden würde. [4]Die Betroffenen sind über die Art der unrechtmäßigen Kenntniserlangung und über Maßnahmen zur Minderung möglicher nachteiliger Folgen zu unterrichten. [5]Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, tritt an ihre Stelle eine angemessene Information der Öffentlichkeit.

§ 23 DSG MV: Pflicht zur Benachrichtigung Betroffener

Hat eine Daten verarbeitende Stelle Grund zur Annahme oder Kenntnis, dass unrichtige, unzulässig erhobene oder unzulässig gespeicherte personenbezogene Daten in der Weise genutzt wurden, dass dem Betroffenen daraus ein Nachteil entstanden ist oder zu entstehen droht, so hat sie diesen unverzüglich zu benachrichtigen.

§ 18a DSG Rlp: Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

(1) Wird einer verantwortlichen Stelle bekannt, dass bei ihr gespeicherte personenbezogene Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für diese Rechte oder schutzwürdigen Interessen der Betroffenen, hat sie dies unverzüglich den Betroffenen und dem Landesbeauftragten für den Datenschutz und die Informationsfreiheit mitzuteilen.

(2) [1]Die Benachrichtigung der Betroffenen muss erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder

nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet wird. [2]Die Betroffenen sind über die Art der unrechtmäßigen Kenntniserlangung und über Maßnahmen zur Minderung möglicher nachteiliger Folgen zu unterrichten. [3]Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, tritt an ihre Stelle eine angemessene Information der Öffentlichkeit. [4]§ 18 Abs. 5 gilt entsprechend.

§ 27a DSG SH: Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

[1]Stellt eine datenverarbeitende Stelle fest, dass bei ihr gespeicherte personenbezogene Daten im Sinne von § 11 Abs. 3 Satz 1 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 unverzüglich den Betroffenen sowie dem Unabhängigen Landeszentrum für Datenschutz mitzuteilen. [2]§ 42a Satz 2 bis 4 und 6 des Bundesdatenschutzgesetzes gilt entsprechend. [3]Soweit die Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, insbesondere aufgrund der Vielzahl der betroffenen Fälle, tritt an ihre Stelle eine Veröffentlichung auf der Internetseite des Unabhängigen Landeszentrums für Datenschutz.

1.2 Literatur

Albrecht, Informationspflicht öffentlicher Stellen bei Datenpannen?, DSB 2010, 15; *Bierekoven*, Schadensersatzansprüche bei Verletzung von Datenschutzanforderungen nach der BDSG-Novelle, ITRB 2010, 88; *Dorn*, Informationspflicht bei Datenschutzpannen: Wie geht man mit § 42a BDSG um?, DSB 2011, 16; *Duisberg/Picot*, Rechtsfolgen von Pannen in der Datensicherheit, CR 2009, 823; *Eckhardt*, Security Breach Notification – Evaluation durch die Bundesregierung, ZD-Aktuell 2013, 03494; *Eckhardt/Schmitz*, Informationspflicht bei „Datenschutzpannen", DuD 2010, 390; *Ernst*, Datenverlust und die Pflicht zur Öffentlichkeit, DuD 2010, 472; *Gabel*, Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten, BB 2009, 2045; *Gliss*, Datenabfluss und Datenschutzpannen: Veröffentlichungspflicht nach § 42a BDSG, DSB 2009, 11; *Gliss*, Umgang mit Datenpannen und Datenklau, DSB 2013, 246; *Hanloser*, Security Breach Notification: Neue Informationspflichten bei Datenpannen, DSB 2009, 11; *Hanloser*, Datenschutz-Compliance: Security Breach Notification bei Datenpannen, CCZ 2010, 25; *Hanloser*, Europäische Security Breach Notification, MMR 2010, 300; *Hornung*, Information 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; *Koch*, Datenpannen müssen öffentlich gemacht werden - § 42a BDSG, DSB 2009, 9; *Krupna*, IT-Compliance – Informationspflichten nach dem Bundesdatenschutzgesetz nach Hackerangriffen, BB 2014, 2250; *Marschall*, Datenpannen – „neue" Meldepflicht nach der europäischen DS-GVO?, DuD 2015, 183; *Marschall*, Wann drohen schwerwiegende Beeinträchtigungen im Rahmen von § 42a BDSG? Mehr Rechtssicherheit durch mehr Informationen?, RDV 2015, 17; *Schierbaum*, „Datenschutzpanne" – was ist zu tun?, CuA 2011, 28; *Wanagas*, Ein Jahr BDSG-Novelle II – Rückblick unter besonderer Berücksichtigung der Fragen der Auftragsdatenverarbeitung und der Informationspflichten, DStR 2010, 1908; *Zahrte/Selig*, Keine Meldepflicht von Skimming-Fällen nach § 42a BDSG, BKR 2014, 185; *Zimmer-Goertz*, Datenleck – Im Krisenfall richtig reagieren, PinG 2013, 77.

1.3 Entstehung und Regelungszweck

Sog. **Security Breach Notification Laws** existieren im US-amerikanischen Raum bereits seit 2002[1]. Im Jahr 2007 regte dann die EU-Kommission eine Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation an. Demnach könnten Sicherheitsverletzungen, die zum Verlust oder zur Preisgabe personenbezogener Daten führen, erhebliche wirtschaftliche Schäden und soziale Nachteile einschließlich des Identitätsbetrugs nach sich ziehen. Betroffene müssten also in die Lage versetzt werden, entsprechende Gegenmaßnahmen zu ergreifen[2].

Der deutsche Gesetzgeber übernahm diese Überlegungen im weiteren Fortgang bei den Arbeiten am BDSG. Vordergründig ging es dabei darum, potenzielle Schäden bei Betroffenen einzudämmen. Gleichsam erhoffte man sich verstärkte Anstrengungen der Unternehmen zur Sicherung der Daten[3].

Die sog. **BDSG-Novelle II**[4] trat am 1. September 2009 in Kraft. Zu den damaligen Neuerungen gehörte die Benachrichtigungspflicht bei Datenpannen nach § 42a BDSG. Zusätzlich wurden Verweisketten aus dem TKG und TMG angelegt, damit die BDSG-Vorschrift zugleich auf datenverarbeitende Stellen aus diesem Sektor Anwendung finden kann. 2010 folgte die Neufassung des § 83a SGB X, der für den Bereich des Sozialdatenschutzes ebenfalls auf die Benachrichtigungsregelung des BDSG verweist.

Gemäß § 48 BDSG war die Bundesregierung verpflichtet, den neu eingefügten § 42a des BDSG bis zum Ende des Jahres 2012 zu evaluieren und einen entsprechenden Bericht vorzulegen. In 177 Fällen bejahten demnach die befragten Aufsichtsbehörden eine Meldepflicht. Zu den

---

1 Übersicht online unter http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. Zu den Erfahrungen in den USA siehe Duisberg/Picot, CR 2009, 827.

2 KOM (2007) 698, Rn. 29.

3 BT-Drs. 17/12319, S. 2.

4 Verabschiedet in Gestalt des Entwurfs in BT-Drs. 16/12011 mit Änderungen in BT-Drs. 16/13657.

typischen Fällen gehörten dabei der **Verlust von Hardware, der falsche Versand bzw. der Verlust von Dokumenten sowie der unberechtigte Zugriff auf Webserver**[5]**.** Die Einführung der Benachrichtigungspflicht wird, obwohl anfangs als Datenschutzpranger verrufen, von den Beteiligten überwiegend positiv bewertet. Zwar sind sowohl von Seiten der Aufsichtsbehörden als auch von Seiten der Meldepflichtigen vereinzelt Anpassungen vorgeschlagen worden. Diese haben die Bundesregierung jedoch nicht veranlassen können, entsprechende Änderungen am Gesetzestext in Angriff zu nehmen[6].

Das Konzept der Security Breach Notification setzt sich durch. In den Artt. 31 und 32 der Entwürfe von Kommission, Rat und Parlament für eine **EU-Datenschutzgrundverordnung** ist eine ähnliche Regelung vorgesehen[7].

Das im Juli 2015 in Kraft getretene Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (ITSG) enthält weitere Meldepflichten[8]. Betreiber sog. Kritischer Infrastrukturen müssen zukünftig Sicherheitsvorfälle an das Bundesamt für Sicherheit in der Informationstechnik (BSI) weiterleiten. Telekommunikationsdiensteanbieter sind zudem gehalten, ihre Nutzer benachrichtigen, wenn Störungen von deren Datenverarbeitungssystemen ausgehen und Möglichkeiten zur Beseitigung aufzeigen.

Ende März 2014 veröffentlichte die Artikel-29-Datenschutzgruppe bei der Europäischen Kommission auf Grundlage der Richtlinie 2002/58/EG eine Stellungnahme zum Verfahren bei Datenpannen[9]. Diese kann als besonders datenschutz- und betroffenenfreundlicher Leitfaden dienen.

---

5 BT-Drs. 17/12319, S. 2.

6 BT-Drs. 17/12319, S. 5.

7 Eingehend *Marschall*, DuD 2015, 183 ff.; ferner *Kaufmann*, ZD 2012, 358 ff. Vergleich der Fassungen bei *BayLDA*, Synopse der DS-GVO, 2015, S. 238 ff., https://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/BayLDA_Synopse_DS-GVO_KOMM-EU-Parlament-Rat_160623TK.pdf;

8 BGBl. I, 2015, S. 1324 ff.

9 *Article 29 Data Protection Working Party*, Opinion 3/2014 on Personal Data Breach Notification, 693/14/EN, vom 25.03.2014, online unter http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf.

1.4 Anwendungsbereich – Kreis der Pflichtigen

Isoliert betrachtet trifft die Informationspflicht des § 42a Satz 1 BDSG ausschließlich **nicht-öffentliche Stellen** im Sinne des § 2 Abs. 4 sowie öffentliche Stellen nach § 27 Abs. 1 Satz 1 Nr. 2 BDSG. § 2 Abs. 4 BDSG erfasst natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, also im Wesentlichen alle Unternehmen. § 27 Abs. 1 Satz 1 Nr. 2 BDSG meint hingegen die öffentlichen Stellen lediglich insoweit, als es sich um **öffentlich-rechtliche Unternehmen** handelt**, die am Wettbewerb teilnehmen**. Dass hierdurch weite Teile der öffentlichen Verwaltung vom Anwendungsbereich der Vorschrift ausgeschlossen werden, stieß auf gerechtfertigte Kritik[10]. Der Wortlaut der Norm ist dennoch eindeutig und die Intention des Gesetzgebers ausdrücklich dokumentiert.

Über die Verweise in § 15a TMG und § 109a TKG werden zumindest sämtliche **Telemedien- und Telekommunikationsanbieter** in den Kreis der Benachrichtigungspflichtigen einbezogen, vollkommen unabhängig von ihrer privat- oder öffentlich-rechtlichen Natur. Über § 83a SGB X werden sodann auch alle Sozialleistungsträger im Sinne von § 35 SGB I erfasst.

Berlin, Mecklenburg-Vorpommern, Rheinland-Pfalz und Schleswig-Holstein haben in den jeweiligen Landesdatenschutzgesetzen Benachrichtigungspflichten auch für **öffentliche Stellen auf Landesebene** implementiert, die § 42a BDSG nachgebildet sind[11]. Parallele Regelungen in anderen Bundesländern stehen noch aus.

Eine **allgemeine Benachrichtigungspflicht öffentlicher Stellen** kann jedoch möglicherweise aus den Artt. 19 Abs. 4, 20 Abs. 3 GG sowie § 839 BGB bzw. §§ 311, 241 Abs. 2 BGB abgeleitet werden[12].

Auftragsdatenverarbeiter unterfallen nach ganz herrschender Meinung[13] sowie der Praxis der Aufsichtsbehörden[14] nicht dem § 42a BDSG.

---

[10] *BfDI*, RDV 2011, 263; *BfDI*, 24. TB 2013, S. 58; *Gabel*, BB 2009, 2046; *Hornung*, NJW 2010, 1842; *Hullen* in: Plath, BDSG, 2013, § 42a Rn. 3; Dix in: *Simitis*, BDSG, 8. Aufl. 2014, § 42a Rn. 2; *Scheffczyk* in: Wolff/Brink, Datenschutzrecht, 2013, § 42a Rn. 11.

[11] Hierzu im Einzelnen unter 2.8.

[12] Hierzu im Einzelnen unter 2.1, 2.2.

Stattdessen ist im ADV-Vertrag gemäß § 11 Abs. 2 Satz 2 Nr. 8 BDSG eine Regelung zu vereinbaren, wie Verstöße beim Auftragnehmer an den Auftraggeber weitergeleitet werden[15]. Der Auftraggeber selbst bleibt benachrichtigungspflichtige (verantwortliche) Stelle.

1.5 Die Bestimmung im Einzelnen

1.5.1 Datenkategorien

Die Benachrichtigungspflicht gemäß § 42a BDSG greift grundsätzlich nur, wenn eine der in der Vorschrift genannten Datenkategorien betroffen ist. Der Gesetzgeber hat sich dabei auf besonders sensible Informationen beschränkt.

- In § 42a Abs. 1 Satz 1 Nr. 1 BDSG sind zunächst die sog. **besonderen Arten personenbezogener Daten** aufgeführt, welche in § 3 Abs. 9 BDSG legaldefiniert sind. Dabei handelt es sich um Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, Gesundheit oder das Sexualleben.
- Nr. 2 betrifft **personenbezogene Daten, die einem Berufsgeheimnis unterliegen**. Dies ist ein indirekter Verweis auf die §§ 203, 204 StGB. Bestimmte Berufsgruppen, die regelmäßig mit besonders sensiblen Informationen in Berührung kommen, sind strafrechtlich zur Verschwiegenheit verpflichtet. Hierzu zählen unter anderem Ärzte, Apotheker, Rechtsanwälte, Wirtschaftsprüfer oder Steuerberater. Dabei ist zu beachten, dass die verantwortliche Stelle gar nicht selbst dem Berufsgeheimnis unterliegen muss[16]. Gemäß § 39 Abs. 1 BDSG können die

---

[13] *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 3; *Duisberg/Picot*, CR 2009, 825; *Eckhardt/Schmitz*, DuD 2010, 393; *Gabe*l, BB 2009, 2046; *Gola/Schomerus*, BDSG, § 42a Rn. 2; *Hanloser*, DSB 2009, 14; *ders.*, CCZ 2010, 26; *Hornung*, NJW 2010, 1842; *Karger*, ITRB 2010, 162; *Krupna*, BB2014, 2250; *Scheffczyk* in: Wolff/Brink, Datenschutzrecht, 2013, § 42a Rn. 8; *Zimmer-Goertz*, PinG 2013, 78.

[14] *BlnDSB*, TB 2013, S. 174; *Hessischer DSB*, 42. TB 2014, S. 178.

[15] Hierzu im Einzelnen unter 2.4.

[16] *Ernst*, DuD 2010, 472.

Daten zweckgebunden auch von der zur Verschwiegenheit verpflichteten Stelle zur Verfügung gestellt worden sein.

Prozessuale Schweigerechte, etwa für Geistliche oder Journalisten (vgl. § 53 Abs. 1 StPO), begründen **keine** Berufsgeheimnisträgerschaft. Das Bankgeheimnis ist ebenfalls nicht von § 203 StGB geschützt[17], Kontoinformationen unterfallen stattdessen weitgehend § 42a Satz 1 Nr. 4 BDSG.

- Nr. 3 bezieht **personenbezogene Daten ein, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten bzw. einen diesbezüglichen Verdacht beziehen**. Dies meint unter anderem Informationen, die der Arbeitgeber nach § 32 Abs. 1 Satz 2 BDSG zur Aufdeckung von Straftaten erhoben hat[18].
- Nr. 4 erfasst schließlich **personenbezogene Daten zu Bank- bzw. Kreditkartenkonten**. Daten zu Bankkonten sind sowohl der Name der Bank, bei der das Konto besteht, als auch die Kontonummer[19]. Da es sich um Daten „zu" und nicht „von" Bank- oder Kreditkartenkonten handelt, werden auch Zugangsdaten von Bezahlsystemen erfasst, die ihrerseits per Lastschrift agieren[20].

Gilt § 42a BDSG hingegen im Wege der Verweisung über § 15a TMG bzw. § 109a TKG, genügt es, wenn **Bestands- oder Verkehrsdaten** betroffen sind. § 83a SGB X stellt ausschließlich auf **besondere Arten von Sozialdaten** im Sinne von § 67 Abs. 12 SGB X ab.

1.5.2 Unrechtmäßige Übermittlung oder Kenntniserlangung auf sonstige Weise

§ 42a BDSG setzt die Offenbarung der Daten an einen Dritten voraus. Negative Folgen, die bei bloßem Verlust aus der Nichtverfügbarkeit der

17 BGH, Urteil vom 27.10.2009, XI ZR 225/08, (= NJW 2010, 361).

18 *Scheffczyk* in: Wolff/Brink, Datenschutzrecht, 2013, § 42a Rn. 22.

19 *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 5.

20 *Zimmer-Goertz*, PinG 2013, 78.

Daten resultieren könnten, bleiben unberücksichtigt[21]. Die Offenbarung kann durch Übermittlung oder Kenntniserlangung auf sonstige Weise geschehen.

Der Begriff der **Übermittlung** ist in § 3 Abs. 4 Satz 2 Nr. 3 BDSG definiert. Hierunter ist jedes Bekanntgeben von personenbezogenen Daten an Dritte zu verstehen, ganz gleich ob durch Weitergabe der Daten oder Abruf durch die Gegenseite. Unrechtmäßig ist die Übermittlung, wenn sie nicht auf einem Erlaubnistatbestand wie der Einwilligung nach § 4a BDSG oder etwa den §§ 28 ff. BDSG beruht. Die irrtümliche Annahme eines Erlaubnistatbestandes ändert an der Rechtswidrigkeit nichts. Anwendungsfälle sind etwa der **Datendiebstahl** auf Serversystemen oder der **irrtümliche Versand** personenbezogener Informationen an eine falsche Adresse.

Mitarbeiter der verantwortlichen Stelle (und insoweit auch Auftragsdatenverarbeiter) sind grundsätzlich nicht als Dritte anzusehen. Verwendet ein Mitarbeiter jedoch Informationen seines Arbeitgebers missbräuchlich zu privaten Zwecken, handelt er jedoch nicht mehr als Teil der verantwortlichen Stelle[22]. Vertreten wird auch, dass die Einschaltung eines Auftragsdatenverarbeiters unter Verwendung eines unwirksamen Vertrages nach § 11 Abs. 2 Satz 2 BDSG eine unrechtmäßige Übermittlung darstellen kann[23]. Hält sich der Dienstleister allerdings auch ohne wirksamen Vertrag an die Weisungen seines Auftraggebers, wird es zumindest an der weiteren Voraussetzung des § 42a BDSG fehlen, dass schwerwiegende Beeinträchtigungen für die Rechte bzw. schutzwürdigen Interessen des Betroffenen drohen.

Die **Kenntniserlangung auf sonstige Weise** ist keine eigenständige Fallgruppe, sondern ein Auffangtatbestand, der alle anderen Sicherheitsverletzungen, insbesondere Angriffe von außen abdecken soll. Hierun-

---

[21] Die Artikel-29-Datenschutzgruppe skizziert etwa den Fall, dass medizinische Dokumentation abhandenkommt und dadurch eine Behandlung gefährdet wird, sog. „availability breach“, *dies.*, Opinion 3/2014 on Personal Data Breach Notification, 693/14/EN vom 25.03.2014.

[22] *Eckhardt/Schmitz*, DuD 2010, 391; *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 6; *BlnBDI*, TB 2010, S. 177; *BlnBDI*, TB 2012, S. 156.

[23] *Eckhardt/Schmitz*, DuD 2010, 391.

ter ist letztlich jeder Zugriff ohne den Willen der verantwortlichen Stelle zu fassen[24].

In § 42a Satz 1 BDSG heißt es, dass die Kenntniserlangung von der datenverarbeitenden Stelle festgestellt worden sein muss. Gleichwohl wird die Vorschrift weit überwiegend dahingehend verstanden, dass bereits **eine hohe Wahrscheinlichkeit der Kenntnisnahme durch Dritte genügt**[25]. Solch eine Interpretation entspricht dem Schutzzweck der Norm, Betroffene rechtzeitig vor einem möglichen Datenmissbrauch zu warnen. Im Falle geschickter Angreifer, die ihre Spuren auf dem datenverarbeitenden System weitgehend verwischen, bliebe eine Benachrichtigung nach § 42a BDSG sonst aus, obwohl eine unrechtmäßige Verwendung der gewonnenen Informationen umso wahrscheinlicher ist. Die Aufsichtsbehörden teilen durchweg dieses Verständnis[26].

Vor demselben Hintergrund wird der **Verlust von Datenträgern** häufig als Fall des § 42a BDSG angeführt[27]. Nur sofern die Daten dem Stand der Technik entsprechend verschlüsselt sein sollten, sei nicht von einer Kenntnisnahme durch Dritte auszugehen[28]. Das BayLDA weist in diesem Zusammenhang ausdrücklich auf AES-256 als einem dem Stand der Technik entsprechenden Verschlüsselungsalgorithmus hin[29].

---

[24] *Eckhardt/Schmitz*, DuD 2010, 391.

[25] So die Stellungnahme der Bundesregierung, BT-Drs. 17/12319, S. 4; ferner auch *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 8; *Gabel*, BB 2009, 2047; *Gola/Schomerus*, BDSG, § 42a Rn. 4; *Karger*, ITRB 2010, 162; *Krupna*, BB 2014, 2251; *Scheffczyk* in: Wolff/Brink, Datenschutzrecht, 2013, § 42a Rn. 30; *Zimmer-Goertz*, PinG 2013, 78. Andere Ansicht: *Eckhardt/Schmitz*, DuD 2010, 393; *Hanloser*, CCZ 2010, 26. *Eckhardt/Schmitz*, a.a.O., gehen indes irrig davon aus, dass „Betroffene" im Sinne des § 42a BDSG nur die Opfer von Datenpannen sein können, tatsächlich ist aber der „Betroffene" im Sinne von § 1 Abs. 1 BDSG gemeint.

[26] *BayLDA*, 4. TB 2011, S. 95; *BlnBDI*, TB 2010, S. 176; *BlnBDI*, TB 2011, S. 165; *Hessischer DSB*, 40. TB 2012, S. 161, *LDI NRW*, 20. TB 2011, S. 61; *LVwA Sachsen-Anhalt*, 5. TB 2011, S. 20.

[27] *Dorn*, DSB 2011, 16; *Hanloser*, DSB 2009, 11 f.; *ders.*, CCZ 2010, 26; *Hornung*, NJW 2010, 1842; *Wanagas*, DStR 2010, 1910.

[28] *Dorn*, DSB 2011, 16; *Eckhardt/Schmitz*, DuD 2010, 391; *Hornung*, NJW 2010, 1842; *Wanagas*, DStR 2010, 1910; ferner auch die *Artikel-29-Datenschutzgruppe*, Opinion 3/2014 on Personal Data Breach Notification, 693/14/EN, vom 25.03.2014, S. 12. Andere Ansicht: *Ernst*, DuD 2010, 473.

[29] *BayLDA*, 6. TB 2015, S. 153

Die Feststellung, dass sich eine Datenpanne (zumindest mit hoher Wahrscheinlichkeit) ereignet hat, muss nicht zwingend von der Geschäftsleitung getroffen werden. Die Grundsätze der Wissenszurechnung im Unternehmen greifen unter Umständen auch beim jeweiligen Datenverarbeiter, betrieblichen oder externen Datenschutzbeauftragten, Mitarbeitern der IT- oder Compliance-Abteilung etc.[30] Insoweit bedarf es der Implementierung eines geeigneten Verfahrens, um die zügige **betriebsinterne Kommunikation** zu gewährleisten.

1.5.3 Drohen schwerwiegender Beeinträchtigungen

Allein der Verlust von Daten der in § 42a Satz 1 BDSG genannten Kategorien löst noch keine Benachrichtigungspflicht aus. Der Gesetzgeber hat vielmehr ein Korrektiv eingezogen dahingehend, als auf Grund des Datenverlustes schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen müssen.

Der Bundesrat hatte angeregt, das Tatbestandsmerkmal „Drohen schwerwiegender Beeinträchtigungen“ ersatzlos zu streichen[31]. Die aufgezählten Risikodaten wiesen bereits eine inhärente Missbrauchsgefahr auf, so dass für eine zusätzliche Gefahrenprognose durch die datenverarbeitende Stelle kein Bedarf bestehe. Die Bundesregierung hielt indes Konstellationen für möglich, in denen Daten im Sinne von § 42a Satz 1 BDSG Dritten unrechtmäßig zur Kenntnis gelangen, ohne dass hieraus schwerwiegende Beeinträchtigungen erwüchsen[32].

Eine Gefahr „droht“ grundsätzlich immer dann, wenn ein Schaden noch nicht eingetreten ist und daher noch abwendbar erscheint[33]. Dies bedeutet jedoch nicht, dass die Mitteilungspflicht entfällt, wenn der Schaden tatsächlich bereits eingetreten ist[34]. Zum einen erscheint eine

---

30 *Hanloser*, DSB 2009, 12; *ders.*, CCZ 2010, 27.

31 BT-Drs. 16/12011, S. 45.

32 BT-Drs. 16/12011, S. 52, so etwa, wenn die Daten verschlüsselt seien. Die Regierung verkennt freilich, dass bei ordnungsgemäßer Verschlüsselung schon keine Kenntnisnahme vorliegt.

33 *Marschall*, RDV 2015, 18.

34 Gewissermaßen in Parallelwertung zu § 315b Abs. 1 StGB: Es besteht kein Zweifel an der Gefährdung, wenn sich die Gefahr verwirklicht hat.

Vertiefung des Schadensereignisses noch möglich, zum anderen würde eine solche Wertung dem im BDSG niedergelegten Transparenzgedanken widersprechen. Es wäre auch nicht erklärbar, warum die Aufsichtsbehörde über all jene Fälle unterrichtet werden sollte, in denen die Beeinträchtigung von Betroffeneninteressen noch abgewendet werden konnte, die echten Schadensfälle aber durch einen Mantel des Schweigens verdeckt werden dürften.

Die Bedrohungslage ist anhand objektiver Kriterien zu bewerten. Ein allzu strenger Maßstab sollte hierbei freilich nicht angelegt werden[35]. Nach Ansicht des BayLDA soll diese besondere Einschränkung lediglich **Bagatellfälle** ausschließen[36].

Insbesondere **je größer der potenzielle Schaden** ausfallen könnte, **desto geringer** sollten **die Anforderungen an die Eintrittswahrscheinlichkeit** veranschlagt werden[37]. Auch das Alter der Daten kann eine Rolle bei der Gefahrenprognose spielen[38].

Die Gefahrenprognose obliegt der verantwortlichen Stelle. Bei Rechtsunsicherheit kann es sinnvoll sein, vor der offiziellen Meldung die zuständige Aufsichtsbehörde informell um Rat zu fragen[39].

Das Risiko sozialer Nachteile wird in der Regel nur schwer vorherzusehen sein[40]. Hier kommt es auf individuelle Beziehungen des Betroffenen zu seinem Soziotop an, die von der datenverarbeitenden Stelle kaum überblickt werden können. § 42a BDSG ermächtigt jedenfalls nicht zur Ausforschung des Betroffenen, um eine Risikoprognose auf eine geeignete Tatsachengrundlage stellen zu können.

35 *Duisberg/Picot*, CR 2009, 824.
36 *BayLDA*, 4. TB 2011, S. 96.
37 *Gabel*, BB 2009, 2047; *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 42a Rn. 4; *Wanagas*, DStR 2010, 1910.
38 *BlnBDI*, TB 2013, S. 171.
39 *Dorn*, DSB 2011, 16; *Schierbaum*, CuA 2011, 30; *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 10; *Scheffczyk* in: Wolff/Brink, Datenschutzrecht, 2013, § 42a Rn. 39.
40 *Holländer*, RDV 2009, 220;

Indizien zur Gefahrenprognose[41]:

Auf **Seite der Betroffenen** sind zu berücksichtigen:

- übermittelte Datenkategorie(n)
- abstraktes Missbrauchsrisiko[42] (Geeignetheit der Informationen):
  - Risiko materieller Schäden
  - Risiko des Identitätsbetruges
  - Risiko sozialer Nachteile
- Gefahr von Erpressbarkeit, Bloßstellung, Rufschädigung

Auf **Seite der Empfänger** sind zu berücksichtigen:

- Zahl der Empfänger
- Konkretes Missbrauchsrisiko, z.B.:
  - Handelte es sich um einen vorsätzlichen Angriff durch Dritte oder eine unachtsame Herausgabe durch die datenverarbeitende Stelle?
  - Hat der Empfänger selbst auf das Datenleck aufmerksam gemacht?
  - Ist die datenverarbeitende Stelle ein allgemein lohnendes Ziel für Angriffe?
- Risiko der Weitergabe und/oder Veröffentlichung.

Der BlnBDI geht etwa bei **Gesundheitsdaten** per se davon aus, dass schwerwiegende Beeinträchtigungen drohen[43].

[41] In Anlehnung an *Dorn*, DSB 2011, 16; *Hornung*, NJW 2010, 1843; *Karger*, ITRB 2010, 162. Eingehend hierzu *Marschall*, RDV 2015, 18 ff.

[42] Es sollten Verwendungsszenarien für die betreffenden Daten entwickelt werden, die sodann auf ihr Missbrauchspotential hin untersucht werden, so ausdrücklich *BlnBDI*, TB 2010, S. 175 sowie *LVwA Sachsen-Anhalt*, 5. TB 2011, S. 20.

[43] *BlnBDI*, TB 2011, S. 166; *BlnBDI*, TB 2014, S. 150.

Umstritten ist, ob **reine Vermögensschäden** ausreichen können, um eine schwerwiegende Beeinträchtigung herbeizuführen. Richtigerweise wird man dies bejahen müssen[44]. Zwar mögen reine Vermögensschäden keine schwerwiegenden Beeinträchtigungen im Sinne von § 14 Abs. 2 Nr. 8 BDSG darstellen[45], jedoch sind Bank- und Kreditkarteninformationen als eigene Risikokategorie in § 42a Satz 1 Nr. 4 BDSG aufgenommen worden. Dieser Teil der Vorschrift liefe praktisch leer, wenn reine Vermögensschäden nicht umfasst sein sollten. Gerade bei Bank- und Kreditkarteninformationen wird in der Regel immer eine Bedrohungslage erzeugt[46]. So besteht bei dem Verlust derartiger Informationen insbesondere regelmäßig die Gefahr unzulässiger Abbuchungen.

1.5.4 Problem: Skimming

Skimming bezeichnet eine Vorgehensweise, bei der ein Bankautomat bzw. ein EC-Kartenterminal so manipuliert werden, dass der Magnetstreifen der Bankkarte heimlich ausgelesen werden kann und die vom Kunden eingegebene PIN abgefangen wird.

Die Meldepflicht bei Skimming-Fällen ist umstritten[47]. Einige **Datenschutzbehörden** gehen pauschal von einer Meldepflicht nach § 42a Satz 1 Nr. 4 BDSG aus[48]. Die Stellungnahmen erschöpfen sich jedoch in der Feststellung, dass ein bestehender Versicherungsschutz nicht die schwerwiegende Beeinträchtigung entfallen lasse.

Diese Darstellung greift zu kurz. Bei der Prüfung ist genau darauf zu achten, wie die Manipulation technisch vor sich gegangen ist. Sofern es

---

44 *Hanloser*, CCZ 2010, 26 f.; *Hornung*, NJW 2010, 1843; *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 9.

45 *Holländer*, RDV 2009, 220; wohl auch *Ernst*, DuD 2010, 473.

46 So bereits die Stellungnahme des Bundesrats, BT-Drs. 16/12011, S. 45; ferner *Karger*, ITRB 2010, 162.

47 Ablehnend *Zahrte/Selig*, BKR 2014, 185 ff., die jedoch fälschlicherweise sowohl den Personenbezug der Daten als auch die schwerwiegende Beeinträchtigung von Betroffeneninteressen verneinen.

48 *BayLDA*, 5. TB 2013, S. 86; *BayLDA*, 6. TB 2015, S. 153; *HmbBfDI*, 23. TB 2012, S. 203; *Hessischer DSB*, 42. TB 2014, S. 177/179 f.; *Sächsischer DSB*, 5. TB NÖB 2011, S. 133; *Sächsischer DSB*, 6. TB NÖB 2013, S. 109; *LfDI Thüringen*, 10. TB 2014, S. 216.

sich um eine vollständige **Attrappe** oder einen Aufbau mit zweitem Tastenfeld und Kartenleser handelt, scheidet die Meldepflicht nach § 42a Satz 1 Nr. 4 BDSG aus. Die Vorschrift fordert ausdrücklich, dass **bei der verantwortlichen Stelle gespeicherte Daten** Dritten unrechtmäßig zur Kenntnis gelangen. Die beim Skimming abgegriffenen Daten sind zwar auch bei der verantwortlichen Stelle gespeichert, dort ist aber nicht der Ort des Datenlecks[49]. Vielmehr gibt der Kunde die Daten von sich aus preis, wenngleich in der irrigen Vorstellung, es handele sich um ein legitimes Terminal.

Original und Attrappe allein wegen ihrer räumlichen Nähe zueinander als einheitliche Datenverarbeitungsanlage ansehen zu wollen, ginge zu weit. Es macht daher keinen Unterschied, ob die Bankkarte einen Zentimeter oder einen Kilometer vom echten Kartenschlitz entfernt durch Dritte ausgelesen wird. Die PIN des Kunden ist zudem gar nicht auf der Karte gespeichert. Sie wird durch ein gefälschtes Tastenfeld, eine versteckte Videokamera oder zukünftig sogar durch eine Wärmebildkamera[50] gesondert ermittelt.

Eine Benachrichtigungspflicht gegenüber dem Kunden ergibt sich daher allein aus **vertraglichen Rücksichtnahme- und Schutzpflichten** nach den §§ 241 Abs. 2 BGB bzw. **Verkehrssicherungspflichten** nach den §§ 823 BGB[51]. Die Aufsichtsbehörden bleiben dabei außen vor.

Wird hingegen **keine Attrappe** verwendet, sondern ein funktionierendes Gerät derart manipuliert, dass die Daten intern abgezweigt und ausgeleitet werden, etwa bei präparierten EC-Karten-Terminals im Einzelhandel[52], findet § 42a Satz 1 Nr. 4 BDSG Anwendung. Verantwortliche (meldepflichtige) Stelle ist der Betreiber des Terminals, nicht hingegen die Bank des jeweiligen Kunden[53].

---

49 So auch *Zahrte/Selig*, BKR 2014, 185, 187.

50 Siehe *Güler*, Fingerzeig für Kriminelle, http://www.sueddeutsche.de/geld/bankautomaten-fingerzeig-fuer-kriminelle-1.2628495.

51 Hierzu näher unten, 2.2. Die regelmäßige Kontrolle auf Attrappen oder Zusatzgeräte entspricht der Produktbeobachtungspflicht der jeweiligen Bank.

52 Vgl. Heise Security vom 18.08.2011, http://heise.de/-1324866.

53 Ebenso *Nink* in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 42a Rn. 9.

1.5.5 Art und Weise der Information

Adressaten

Als Benachrichtigungsempfänger sieht § 42a Satz 1 BDSG **die zuständige Datenschutzaufsichtsbehörde wie auch den Betroffenen** selbst vor. Die zeitlichen Vorgaben und die inhaltlichen Anforderungen sind im Detail jeweils unterschiedlich ausgestaltet. An die Stelle der Betroffenen treten im Falle von Minderjährigen die Eltern[54], im Falle von Betreuungsverhältnissen die Betreuer[55].

Zeitliche Vorgabe

Die Benachrichtigung hat **„unverzüglich"** zu erfolgen. Die Verwendung dieses zivilrechtlichen Begriffs ist ein indirekter Verweis auf § 121 Abs. 1 Satz 1 BGB. Unverzüglich ist demnach eine Handlung, die „ohne schuldhaftes Zögern" erfolgt. Dies strafft einerseits den Entscheidungsfindungsprozess bei der verantwortlichen Stelle, bedeutet jedoch andererseits, dass die Benachrichtigung keineswegs „sofort" zu erfolgen hat. Stattdessen ist ein nach den Umständen des Einzelfalles zu bemessendes beschleunigtes Verhalten an den Tag zu legen[56]. Zu den Umständen, die eine Mitteilung verzögern können, gehört unter anderem auch die Pflicht, dem Betroffenen Handlungsempfehlungen zu erteilen, um sich gegen den Missbrauch seiner Daten zu schützen.

Hinsichtlich der Mitteilung an den Betroffenen modifiziert § 42a Satz 2 BDSG den zeitlichen Ablauf etwas. Danach muss die Mitteilung unverzüglich erfolgen, sobald angemessene Maßnahmen zur Sicherung der Daten ergriffen worden oder (ihrerseits) nicht unverzüglich erfolgt sind und die Strafverfolgung nicht mehr gefährdet ist. Der Gesetzgeber hatte hier das sog. **„responsible disclosure"**-Konzept vor Augen, bei welchem Sicherheitslücken erst publik gemacht werden, wenn die datenverarbeitende Stelle genug Zeit hatte, Fehler zu beheben[57]. Versäumt es der Pflichtige, entsprechende Datensicherungsmaßnahmen vorzu-

54 *BlnBDI*, TB 2014, S. 151.
55 *BlnBDI*, TB 2012, S. 152.
56 Reichsgericht, Urteil vom 22.02.1929, II 357/28 (= RGZ 124, 115, 118).
57 BT-Drs. 16/12011, S. 34.

nehmen, greift wieder die kürzere Frist. In aller Regel wird aber die Aufsichtsbehörde die Meldung zuerst erhalten[58].

In jedem Falle sollte intern dokumentiert werden, warum ein bestimmter Zeitpunkt für die Benachrichtigung gewählt wurde[59].

Je nachdem kann die unverzügliche Meldung durchaus mehrere Monate beanspruchen. Die niedersächsische Datenschutzaufsicht berichtet, dass der Nachmieter einer Geschäftsimmobilie Unterlagen der zuvor dort ansässigen Bank in Besitz genommen hatte. Die Bank war gezwungen, auf Herausgabe zu klagen, sodass erst nach zehn Monaten überhaupt geprüft werden konnte, ob es sich um Risikodaten im Sinne des § 42a BDSG handelte. Die Behörde ging bei diesem atypischen Verlauf von einer unverzüglichen Meldung aus[60].

Inhalt

Gemäß § 42a Satz 3 BDSG muss die Benachrichtigung der Betroffenen eine **Darlegung der Art der unrechtmäßigen Kenntniserlangung sowie Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen** enthalten. Dabei ist es insbesondere im Hinblick auf etwaige Nachahmer nicht erforderlich, zu sehr in technische Details zu gehen[61]. Die Betroffenen sollen erkennen können, was Ursache für das Datenleck war und wer hierfür verantwortlich ist[62]. Es genügt also z.B. die Angabe, dass ein Datendiebstahl, ein Angriff auf das IT-System oder eine irrtümliche Übermittlung stattgefunden hat.

Nach dem reinen Wortlaut des § 42a Satz 1 BDSG bezieht sich die Benachrichtigung allein auf die aufgezählten – besonders sensiblen – Datenkategorien[63]. Richtigerweise wird die Benachrichtigung jedoch auch die betroffenen Nichtrisikodaten umfassen müssen, wenn die Meldepflicht erst einmal besteht. Dies ergibt sich aus der Schutzdimension

---

58 *Karger*, ITRB 2010, 162; *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 10.

59 *Eckhardt/Schmitz*, DuD 2010, 394; *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 10.

60 *LfD Niedersachsen*, 21. TB 2015, S. 34.

61 *Eckhardt/Schmitz*, DuD 2010, 394; *Hornung,* NJW 2010, 1843; *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 12.

62 *Hornung*, NJW 2010, 1843

63 „[…] hat sie *dies* […] mitzuteilen."

der Vorschrift. So drohen schwerwiegende Beeinträchtigungen möglicherweise gerade erst durch das Zusammentreffen von Risiko- und Nichtrisikodaten. Eine effektive Eigensicherung ist den Betroffenen nur möglich, wenn sie umfassend informiert werden.

Die Benachrichtigung der zuständigen Aufsichtsbehörde muss gemäß § 42a Satz 4 BDSG zunächst alle Informationen enthalten, die dem Betroffenen mitgeteilt werden. Zudem ist eine **Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen** anzufügen.

Form

Eine bestimmte Form für die Benachrichtigung von Betroffenen und Aufsichtsbehörden ist **im Gesetz nicht vorgeschrieben**. Freilich empfiehlt sich regelmäßig **zumindest** die **Textform**[64] (§ 126b BGB, z.B. eMail ohne qualifizierte elektronische Signatur). Um einem etwaigen Datenmissbrauch rechtzeitig vorzubeugen, kann auch eine telefonische Mitteilung angezeigt sein[65]. Erfolgt die Benachrichtigung mündlich, sollte der Inhalt dennoch dokumentiert werden, da die Aufsichtsbehörde nur so die Ordnungsmäßigkeit überprüfen kann[66].

Soweit die individuelle Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern würde, genügt nach § 42a Satz 5 BDSG auch eine **Information der Öffentlichkeit**. Als gesetzliches Fallbeispiel wird auf die Vielzahl der Betroffenen rekurriert, um den unverhältnismäßig hohen Aufwand zu begründen. Ein unverhältnismäßiger Aufwand lässt hingegen **nicht die Benachrichtigungspflicht insgesamt** entfallen[67]. Auch wenn unklar ist, wessen Daten konkret von der Sicherheitsverletzung betroffen sind, ist nach dem Sinn und Zweck der

64 *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 15; *Hornung*, NJW 2010, 1843; *Scheffczyk* in: Wolff/Brink, Datenschutzrecht, 2013, § 42a Rn. 50. Für Schriftform nach § 126 Abs. 1 BGB *Karger*, ITRB 2010, 163 sowie *Krupna*, BB 2014, 2253.

65 *Dix* in: Simitis, BDSG, § 42a Rn. 15

66 *BlnBDI*, TB 2012, S. 160.

67 *BlnBDI*, TB 2013, S. 170.

Norm eine öffentliche Bekanntmachung geboten (§ 42a BDSG analog)[68].

Die öffentliche Information wird nach Vorstellung des Gesetzgebers sichergestellt durch Anzeigen in mindestens zwei bundesweit erscheinenden Tageszeitungen, welche jeweils mindestens eine halbe Seite umfassen müssen[69]. Die Kosten für eine solche Maßnahme belaufen sich auf ca. 25.000 bis 30.000 €. Alternativ sollen auch andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahmen ausreichen können. Dies könnte etwa bei der Benutzung elektronischer Medien der Fall sein[70] oder auch bei der Verwendung regionaler Zeitungen, wenn der Kreis der Betroffenen entsprechend lokal angesiedelt ist[71].

1.5.6 Verwendungsverbot

Weder der Inhalt noch der Umstand einer Benachrichtigung darf gemäß § 42a Satz 6 BDSG in einem Straf- oder Ordnungswidrigkeitenverfahren ohne Zustimmung des Pflichtigen verwendet werden. Derselbe Schutz erfasst zugleich Angehörige im Sinne des § 52 Abs. 1 StPO[72].

Die Freiheit, sich nicht selbst bezichtigen zu müssen, besitzt Verfassungsrang und stellt eine notwendige Prämisse des Strafprozesses dar. Der sog. **nemo-tenetur-Grundsatz**[73] ergibt sich zunächst aus Art. 14 Abs. 3 lit. g) des Internationalen Pakts über bürgerliche und politische

---

[68] *Dorn*, DSB 2011, 16. Dorn ist sich jedoch bewusst, dass die Begründung einer Ordnungswidrigkeit wegen Verstoßes gegen eine analog angewandte Vorschrift nicht mit dem Vorbehalt des Gesetzes vereinbar wäre.

[69] *Scheffczyk* in: Wolff/Brink, Datenschutzrecht, 2013, § 42a Rn. 52 zählt die (wenigen) in Frage kommenden Zeitungen auf.

[70] *Ernst*, DuD 2010, 475; *Hornung*, NJW 2010, 1843.

[71] *Duisberg/Picot*, CR 2009, 825; *Hanloser*, DSB 2009, 13; *Hornung*, NJW 2010, 1843.

[72] Verlobte (auch zwecks eingetragener Lebenspartnerschaft); Ehegatten; Ex-Ehegatten; Lebenspartner; Ex-Lebenspartner; Verwandte, Verschwägerte und Ex-Verschwägerte in gerader Linie; Verwandte in der Seitenlinie bis zum dritten Grad; Verschwägerte und Ex-Verschwägerte bis zum zweiten Grad.

[73] Lat.: „nemo tenetur se ipsum accusare“, niemand ist gehalten, sich selbst anzuklagen.

Rechte (IPbpR) sowie aus Art. 6 Abs. 1 Satz 1 der Europäischen Menschenrechtskonvention. Das deutsche Verfassungsrecht bietet Anknüpfungspunkte in der Menschenwürdegarantie (Art. 1 Abs. 1 GG), der freien Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG), der Freiheit als solcher (Art. 2 Abs. 2 Satz 2 GG), dem allgemeinen Persönlichkeitsrecht (Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG), der Gewissensfreiheit (Art. 4 Abs. 1 Var. 2 GG) sowie dem Rechtsstaatsprinzip (Art. 20 Abs. 3 GG).

Die bisherigen Bundesregierungen sahen in § 42a Satz 6 BDSG eine verfassungskonforme Auflösung des Spannungsverhältnisses von Mitteilungspflicht und Selbstbezichtigungsfreiheit[74]. Die Formulierung der Norm ist jedoch missverständlich. Bemängelt wird, dass der Wortlaut **allein die pflichtige Stelle selbst** schützt. Es seien bei juristischen Personen aber zugleich auch die **Organe und Mitarbeiter** von einer straf- bzw. ordnungswidrigkeitenrechtlichen Verfolgung bedroht[75]. Hierin sei ein offensichtlicher Verstoß gegen Menschenrechte zu erblicken[76].

Aus diesem Grund ist § 42a Satz 6 BDSG dahingehend **verfassungskonform auszulegen**, dass die mitgeteilten Tatsachen in keiner Form für ein straf- oder ordnungswidrigkeitenrechtliches Verfahren nutzbar gemacht werden dürfen. Es handelt sich also keineswegs um ein bloßes Beweisverwertungsverbot, sondern um ein vollumfängliches Verwendungsverbot, welches zugleich Fernwirkung für alle anderen hierdurch aufgefundenen Beweismittel besitzt.[77] (Diese Lesart deckt sich mit derjenigen, die bereits zum gleichlautenden § 97 Abs. 1 Satz 3 InsO vertreten wird.)[78]

Das Verwendungsverbot bezieht sich allerdings ausschließlich auf solche Tatsachen, die in der Benachrichtigung offengelegt werden. Es greift nicht, wenn gegen § 42a BDSG als solchen verstoßen wird. Wäre

[74] BT-Drs. 16/12011, S. 35; BT-Drs. 17/12319, S. 5.

[75] *Eckhardt*, ZD-Aktuell 2013, 03494; *Eckhardt/Schmitz*, DuD 2010, 395; *Ernst,* DuD 2010, 475.

[76] *Eckhardt/Schmitz*, DuD 2010, 396

[77] *Gabel*, BB 2009, 2049; *Gola/Schomerus*, BDSG, 12. Aufl. 2015, § 42a Rn. 9; *Hanloser*, CCZ 2010, 29; *Hornung*, NJW 2010, 1844; *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 20; *Scheffczyk* in: Wolff/Brink, Datenschutzrecht, 2013, § 42a Rn. 58.

[78] *Hanloser*, CCZ 2010, 29; *Hornung*, NJW 2010, 1844.

dem nicht so, gäbe es für § 43 Abs. 2 Nr. 7 BDSG („…nicht richtig, nicht vollständig oder nicht rechtzeitig…“) keinen Anwendungsbereich.

Auch **im Zivilprozess gilt das Verwendungsverbot nicht**[79]**.** Der Wortlaut ist ausdrücklich auf Straf- und Ordnungswidrigkeitenverfahren bezogen. Eine Ausdehnung auf bürgerliche Rechtsstreitigkeiten ist wegen der weniger drastischen Folgen eines solchen Verfahrens auch nicht angezeigt.

Ebenso wenig sperrt die Benachrichtigung eine **Prüfung durch die Aufsichtsbehörde** nach § 38 BDSG. Zufallsfunde, die bei einer solchen Prüfung zutage treten, und die mit dem gemeldeten Sachverhalt nicht in Beziehung stehen, können durchaus mit Bußgeldern geahndet werden[80].

1.5.7 Irrtümliche und missbräuchliche Meldungen

Das Verwendungsverbot muss auch gelten, wenn die verantwortliche Stelle **irrtümlicherweise** eine Meldung abgibt, etwa weil das Missbrauchsrisiko zu hoch eingeschätzt wurde. § 42a Satz 6 BDSG setzt zwar einen „Benachrichtigungspflichtigen“ voraus. Jedoch darf der Verantwortliche, der sich irrig für pflichtig hält, in seinem Streben nach Rechtskonformität nicht schlechter behandelt werden als ein echter Pflichtiger im Sinne des § 42a Satz 1 BDSG.

Unter den tatsächlich gemeldeten Pannen finden sich häufig solche, die eigentlich keine Meldepflicht nach § 42a BDSG begründen. Dies war bereits bei der Evaluation durch die Bundesregierung der Fall[81] und setzt sich in den Tätigkeitsberichten der Aufsichtsbehörden fort[82]. Der Verdacht liegt nahe, dass bestimmte Versäumnisse gemeldet werden,

---

[79] *Ernst*, DuD 2010, 475; *Scheffczyk* in: Wolff/Brink, Datenschutzrecht, 2013, § 42a Rn. 59.

[80] *Krupna*, BB 2014, 2254.

[81] BT-Drs. 17/12319, S. 2.

[82] *BayLDA*, 4. TB 2011, S. 96; *BlnBDI*, TB 2012, S. 149; *HmbBfDI*, 23. TB 2012, S. 199; *HmbBfDI*, 24. TB 2014, S. 252; *Hessischer DSB*, 40. TB 2012, S. 162; *Hessischer DSB*, 42. TB 2014, S. 23; *Sächsischer DSB*, 5. TB NÖB 2011, S. 133; *Sächsischer DSB*, 6. TB NÖB 2013, S. 109.

um gemäß § 42a Satz 6 BDSG einem entsprechenden Bußgeld zu entgehen. Die insoweit **missbräuchliche Meldung** stellt jedoch keine „nicht richtige“ Meldung im Sinne des Bußgeldtatbestandes § 43 Abs. 2 Nr. 7 BDSG[83] dar. Eine derartige Ausweitung der Ordnungswidrigkeit scheitert, da hiervon auch die fahrlässige „nicht richtige“ Meldung erfasst wäre, die nach dem oben Gesagten aber gerade privilegiert werden muss.

1.6 Haftung und Schadensersatz

1.6.1 Ordnungswidrigkeit

Gemäß § 43 Abs. 2 Nr. 7 BDSG stellt es eine Ordnungswidrigkeit dar, wenn entgegen § 42a Satz 1 BDSG eine Mitteilung **nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig** gemacht wird. Der Verstoß kann gemäß § 43 Abs. 3 BDSG mit einer Geldbuße bis zu 300.000 € geahndet werden. Sollte dieser Betrag nicht ausreichen, um die wirtschaftlichen Vorteile aus dem Verstoß abzuschöpfen, können ggf. auch höhere Bußgelder verhängt werden. Maßgeblich ist insofern der wirtschaftliche Vorteil durch die unterbliebene Meldung gemäß § 42a BDSG, nicht etwa der Vorteil durch unterbliebene Sicherheitsmaßnahmen, welche die Datenpanne verursacht haben.

Auch die nicht richtige Mitteilung kann teuer werden. Nachdem Patientenunterlagen im Hausmüll gefunden worden waren, erweckte der verantwortliche Arzt in seinem Benachrichtigungsschreiben den Eindruck, die Unterlagen seien gestohlen worden. Der BlnBDI setzte ein Bußgeld in vierstelliger Höhe fest[84].

§ 43 Abs. 2 Nr. 7 BDSG greift ausschließlich bei positiver Kenntnis vom Vorliegen der Voraussetzungen des § 42a BDSG. Ein sog. „Kennenmüssen“, also die **fahrlässige Unkenntnis** wird nicht erfasst[85]. Der Fahrläs-

[83] Näher unten, 1.6.1.

[84] *BlnBDI*, TB 2013, S. 169.

[85] *Eckhardt/Schmitz*, DuD 2010, 393; *Gabel*, BB 2009, 2047; *Hanloser*, DSB 2009, 11; *ders.*, CCZ 2010, 27. A.A. ohne triftige Begründung *Nink* in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015, § 42a Rn. 5

sigkeitstatbestand des § 43 Abs. 2 Nr. 7 BDSG greift hingegen dann, wenn ungeeignete Kommunikationsstrukturen im Unternehmen die Benachrichtigung verhindern oder die Meldung inhaltlich falsch ist.

Die verantwortliche Stelle steht schlechterdings nicht vor der Wahl, entweder die Mitteilung zu machen oder das Bußgeld einfach hinzunehmen. Da es sich bei Unterlassungstaten um sog. Dauerdelikte handelt, beginnt mit jedem bestandskräftigen Bußgeldbescheid eine neue Ordnungswidrigkeit, die gesondert verfolgt werden kann. Außerdem besitzt die Aufsichtsbehörde gemäß § 38 Abs. 5 Satz 1 BDSG die Möglichkeit, zur Vornahme der Mitteilung zu zwingen[86].

1.6.2 Haftung für Datenpannen

Sofern sie schuldhaft, d.h. vorsätzlich oder fahrlässig erfolgt, kann eine unrechtmäßige Datenoffenbarung einen **Schadensersatzanspruch des Betroffenen** aus §§ 7 f. BDSG bzw. §§ 823 ff. BGB begründen[87].

§ 7 BDSG: Schadensersatz

[1]Fügt eine verantwortliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist sie oder ihr Träger dem Betroffenen zum Schadensersatz verpflichtet. [2]Die Ersatzpflicht entfällt, soweit die verantwortliche Stelle die nach den Umständen des Falles gebotene Sorgfalt beachtet hat.

§ 8 BDSG: Schadensersatz bei automatisierter Datenverarbeitung durch öffentliche Stellen

(1) Fügt eine verantwortliche öffentliche Stelle dem Betroffenen durch eine nach diesem Gesetz oder nach anderen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Erhe-

[86] *Hanloser*, DSB 2009, 12; *ders.*, CCZ 2010, 27. Irrig insoweit *Eckhardt/Schmitz*, DuD 2010, 395, die offenbar keinen organisatorischen Mangel im Sinne des § 38 Abs. 5 Satz 1 BDSG erkennen wollen, wenn die Benachrichtigung ausbleibt.

[87] *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 21.

bung, Verarbeitung oder Nutzung seiner personenbezogenen Daten einen Schaden zu, ist ihr Träger dem Betroffenen unabhängig von einem Verschulden zum Schadensersatz verpflichtet. […]

§ 823 BGB: Schadensersatzpflicht

(1) Wer vorsätzlich oder fahrlässig das Leben, den Körper, die Gesundheit, die Freiheit, das Eigentum oder ein sonstiges Recht eines anderen widerrechtlich verletzt, ist dem anderen zum Ersatz des daraus entstehenden Schadens verpflichtet. […]

Zwar wird im Rahmen des § 7 BDSG bei rechtswidrigem Verhalten der verantwortlichen Stelle ein Verschulden ihrerseits vermutet (Umkehr der Beweislast). Sowohl bei § 7 BDSG als auch bei §§ 823 ff. BGB trägt der Betroffene aber die prozessuale **Beweislast für den Datenschutzverstoß** an sich. In der Praxis wird der Betroffene häufig nicht über genügend Einblick in die Abläufe der verantwortlichen Stelle verfügen, um den Beweis führen zu können. Auch eine in solchen Fällen häufig auferlegte sekundäre Darlegungslast der Beklagtenseite wird das Informationsungleichgewicht nur selten aufheben können. Mit Einführung der Mitteilungspflicht nach § 42a BDSG und der damit verbundenen Darlegung von Ursache und Verantwortlichkeit stehen die Chancen einer Schadensersatzklage wesentlich besser[88].

1.6.3 Haftung für das Verschweigen von Datenpannen

Entsteht dem Betroffenen ein Schaden, weil er entgegen § 42a BDSG oder einer anderweitigen Benachrichtigungspflicht nicht rechtzeitig gewarnt wurde, kann auch dies einen **Schadensersatzanspruch** begründen. Mögliche Anspruchsgrundlagen sind die §§ 280 Abs. 1, 241 Abs. 2 sowie die §§ 823 ff. BGB, wobei § 42a BDSG insbesondere als Schutzgesetz im Sinne von § 823 Abs. 2 BGB eine Rolle spielt.

[88] *Bierekoven*, ITRB 2010, 89; *Eckhardt/Schmitz*, DuD 2010, 396.

§ 280 BGB: Schadensersatz wegen Pflichtverletzung

(1) Verletzt der Schuldner eine Pflicht aus dem Schuldverhältnis, so kann der Gläubiger Ersatz des hierdurch entstehenden Schadens verlangen. Dies gilt nicht, wenn der Schuldner die Pflichtverletzung nicht zu vertreten hat.

§ 241 BGB: Pflichten aus dem Schuldverhältnis

[…] (2) Das Schuldverhältnis kann nach seinem Inhalt jeden Teil zur Rücksicht auf die Rechte, Rechtsgüter und Interessen des anderen Teils verpflichten.

§ 823 BGB: Schadensersatzpflicht

[…] (2) Die gleiche Verpflichtung trifft denjenigen, welcher gegen ein den Schutz eines anderen bezweckendes Gesetz verstößt. Ist nach dem Inhalt des Gesetzes ein Verstoß gegen dieses auch ohne Verschulden möglich, so tritt die Ersatzpflicht nur im Falle des Verschuldens ein.

Unterlässt der Betroffene trotz Benachrichtigung die erforderlichen Schutzmaßnahmen, trifft ihn ggf. ein Mitverschuldensanteil gemäß § 254 Abs. 1 BGB. Die Schadensersatzsumme wird hierdurch gemindert.

2. Datenschutzrechtliche Informationspflichten außerhalb von § 42a BDSG

Über die spezialgesetzliche Skandalisierungspflicht des BDSG hinaus lässt sich eine Mitteilungspflicht gegenüber den Betroffenen auch anderweitig herleiten. Dies betrifft insbesondere die öffentlichen Stellen, die vom § 42a BDSG prinzipiell ausgenommen werden.

2.1 Rechtsstaatsprinzip und unmittelbare Grundrechtswirkung

Die Benachrichtigungspflicht öffentlicher Stellen gemäß § 42a BDSG bleibt nominell hinter derjenigen der nicht-öffentlichen Stellen zurück[89]. Das der Bundesrepublik zu Grunde liegende **Rechtsstaatsprinzip**, welches u.a. in Art. 20 Abs. 3 GG seine textliche Ausprägung erfährt, verpflichtet die Verwaltung nichtsdestotrotz zur Gewährleistung von Grundrechten.

Sowohl das informationelle Selbstbestimmungsrecht aus den Art. 1 Abs. 1, 2 Abs. 1 GG als auch andere Grundrechtsgehalte wie die Berufsfreiheit (Art. 12 GG) oder die Eigentumsgarantie (Art. 14 GG) können bei Datenpannen bedroht sein. Den Staat trifft daher auch ohne § 42a BDSG eine Pflicht zur Schadensminimierung[90]. Unterlässt die verantwortliche Behörde die Information, drohen ggf. Schadensersatzansprüche der Betroffenen, Folgenbeseitigungsansprüche oder dienstaufsichtsrechtliche Konsequenzen.

---

89 Vgl. Abschnitt 1.4.

90 *Albrecht*, DSB 2010, 15; *Gabel*, BB 2009, 2046; *Pötters* in: Thüsing, Beschäftigtendatenschutz und Compliance, 2. Aufl. 2014, § 18 Rn. 45.
Scheffczyk in: Wolff/Brink, Datenschutzrecht, 2013, § 42a Rn. 13 will eine ungeschriebene Informationspflicht nur bei massiven Grundrechtsbeeinträchtigungen bejahen.

2.2 Zivilrechtliche Benachrichtigungspflicht

Aus dem **vertraglichen Rücksichtnahmegebot** kann ebenfalls eine Benachrichtigungspflicht erwachsen.[91] Gemäß § 241 Abs. 2 BGB verpflichten bestehende Schuldverhältnisse zur Rücksicht auf die Rechte, Rechtsgüter und Interessen des anderen Teils. Sofern also ein Schuldverhältnis zwischen verantwortlicher Stelle und Betroffenem besteht, muss ein Datenmissbrauchsrisiko mitgeteilt werden. Wird die Benachrichtigung unterlassen, können Schadensersatzansprüche gemäß § 280 Abs. 1 Satz 1 BGB die Folge sein[92].

Eine Benachrichtigungspflicht kann sich zudem aus **deliktischen Verkehrssicherungspflichten nach den §§ 823 ff. BGB** ergeben. Beruht die unrechtmäßige Kenntniserlangung durch Dritte auf unzureichenden IT-Sicherheitsmaßnahmen, hat die verantwortliche Stelle dadurch eine Gefahrenquelle geschaffen. Sie ist deshalb verpflichtet, weitere Schäden abzuwenden. Für öffentliche Stellen ist dabei der Amtshaftungsanspruch[93] nach § 839 BGB i.V.m. Art. 34 GG von besonderem Interesse.

2.3 Auskunft nach § 34 BDSG

Völlig ungeklärt ist bislang die Frage, inwieweit verantwortliche Stellen unrechtmäßige Datenabflüsse **auf Antrag** des Betroffenen zu beauskunften haben. Sofern ein entsprechender Vorgang mit Bezug zum Betroffenen gespeichert ist[94], dürfte dies bereits nach § 34 Abs. 1 Satz 1 Nr. 1 BDSG der Fall sein („die zu seiner Person gespeicherten Daten“).

§ 34 Abs. 1 Satz 1 Nr. 2 BDSG statuiert zudem ein eigenständiges Recht auf Auskunft über Empfänger (oder Kategorien von Empfängern), an die Daten weitergegeben werden.[95] Im Gegensatz zu § 42a BDSG würde hierbei nicht zwischen Risikodaten und anderen Datenkategorien un-

91 *Gabel*, BB 2009, 2046.

92 Vgl. auch Abschnitt 1.6.3.

93 *Albrecht*, DSB 2010, 15.

94 Vgl. § 109a Abs. 3 TKG mit der Verpflichtung, ein entsprechendes Verzeichnis anzulegen.

95 Für Bundesbehörden gilt gemäß § 19 Abs. 1 Satz 1 Nr. 2 BDSG selbiges.

terschieden. Es wäre auch **keine besondere Gefährdungslage** nötig. Lediglich die positive Kenntnis von Datenleck und Empfänger müsste gegeben sein

Verfehlt wäre es, den Anspruch mit der Begründung vom Tisch zu wischen, § 42a BDSG sei die allein einschlägige **Spezialnorm** bei Datenschutzpannen. Zum einen verfängt dieser Einwand schon bei öffentlich-rechtlichen und vertraglichen Mitteilungspflichten (s.o.) nicht, zum anderen erfasst § 42a BDSG gerade nicht die Fälle eines Auskunftsverlangens durch den Betroffenen sondern verpflichtet zur Eigeninitiative.

Der Auskunftsanspruch soll Datenweitergaben transparent machen. Unerheblich ist nach dem Wortlaut zunächst, ob die Weitergabe an sich legal gewesen ist. Es müssen daher grundsätzlich **sowohl rechtmäßige als auch rechtswidrige Datentransfers** mitgeteilt werden.

Juristisch interessant ist nun, ob auch der Datendiebstahl aus Sicht der verantwortlichen Stelle als „Weitergabe" im Sinne der Vorschrift angesehen werden muss. § 34 BDSG spricht in diesem Zusammenhang von „Empfängern", womit nach der Legaldefinition des § 3 Abs. 8 Satz 1 BDSG schlicht alle Personen oder Stellen gemeint sind, die Daten erhalten. Der Datendieb ist daher ohne weiteres als Empfänger anzusehen. Unschädlich ist ferner, dass nur solche Empfänger genannt sind, an die Daten weitergegeben „werden" (Präsens). Die Formulierung meint keineswegs nur Weitergaben die regelmäßig und auch in Zukunft weiterhin stattfinden. Auch einmalige und in der Vergangenheit liegende Weitergaben sollen offengelegt werden. Die Umschreibung als aktives Tun hat letztlich ebenfalls keine einschränkende Wirkung. Übermittlungen etwa nach § 3 Abs. 4 Satz 2 Nr. 3 lit. b) BDSG, bei denen Daten lediglich zum Abruf bereitgehalten werden, also das passive Element im Vordergrund steht, sind gleichermaßen in § 34 BDSG angesprochen[96].

[96] Im Rahmen einer „Übermittlung" nach § 3 Abs. 4 BDSG muss die Weitergabe das Ergebnis zweckgerichteten Handelns sein, unbefugte Zugriffe sollen dementsprechend nicht genügen (*Dammann* in: Simitis, BDSG, 8. Aufl. 2014, § 3 Rn. 150; *Schild* in: Wolff/Brink, Datenschutzrecht, 2013, § 3 Rn. 71). Der in § 34 BDSG geforderte Begriff der „Weitergabe" ist allerdings weiter als derjenige der „Übermittlung".

Im Hinblick auf das allgemeine datenschutzrechtliche **Transparenzgebot** erscheint die Anwendung des § 34 BDSG in Fällen rechtswidriger Übermittlung bzw. des Datendiebstahls geboten. Ausnahmen hiervon sind nicht auf den ersten Blick erkennbar. Die Datenpanne wird im Zweifel kein **schützenswertes Geschäftsgeheimnis** gem. § 34 Abs. 1 Satz 5 BDSG darstellen. Der illegale Empfänger ist auch nicht schutzwürdiger Dritter im Sinne der §§ 34 Abs. 7, 33 Abs. 2 Satz 1 Nr. 3 BDSG.

Allein nach den §§ 33 Abs. 7, 33 Abs. 2 Satz 1 Nr. 7 lit. b BDSG darf die Auskunft unterbleiben, wenn die **Geschäftszwecke der verantwortlichen Stelle erheblich gefährdet** würden, es sei denn, dass wiederum das Interesse an der Auskunft die Gefährdung überwiegt. Hier kann freilich keine schematische Lösung vorgegeben werden. Unter Berücksichtigung, dass § 42a BDSG mit seinen besonders sensiblen Risikodaten keinerlei Einschränkungen der Benachrichtigung kennt, sollte der Auskunftsanspruch nach § 34 BDSG nicht zu vorschnell abelehnt werden. Die unvollständige Auskunft ist nach § 43 Abs. 1 Nr. 8a BDSG bußgeldbewehrt.

2.4 Mitteilungspflicht des Auftragsdatenverarbeiters (§ 11 Abs. 2 Nr. 8 BDSG)

Wie bereits dargestellt, trifft den Dienstleister einer Auftragsdatenverarbeitung keine originäre Pflicht aus § 42a BDSG[97]. Der formbedürftige **ADV-Vertrag** muss jedoch gemäß § 11 Abs. 2 Nr. 8 BDSG Regelungen über mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Datenschutzvorschriften bzw. gegen die im Auftrag getroffenen Festlegungen enthalten. Der Auftragnehmer versetzt den Auftraggeber in diesen Fällen durch die Weiterleitung des Vorfalls erst in die Lage, der Benachrichtigungspflicht aus § 42a BDSG nachzukommen.

Erleidet der Auftragnehmer Datenverluste, die nicht seiner Sphäre zuzurechnen sind, ist der Wortlaut des § 11 Abs. 2 Nr. 8 BDSG nicht ein-

[97] Vgl. Abschnitt 1.4.

schlägig[98]. Es bietet sich daher an, auch solche Sicherheitsverletzungen in das ADV-Vertragswerk einzubeziehen. Die entsprechende Klausel könnte wie folgt gestaltet sein:

> *„Der Auftragnehmer erstattet dem Auftraggeber in allen Fällen eine Meldung, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind.*
>
> *Es ist bekannt, dass nach § 42a BDSG Informationspflichten im Falle des Abhandenkommens oder der unrechtmäßigen Übermittlung oder Kenntniserlangung von personenbezogenen Daten bestehen können. Deshalb sind solche Vorfälle ohne Ansehen der Verursachung unverzüglich dem Auftraggeber mitzuteilen. Dies gilt auch bei schwerwiegenden Störungen des Betriebsablaufs, bei Verdacht auf sonstige Verletzungen gegen Vorschriften zum Schutz personenbezogener Daten oder anderen Unregelmäßigkeiten beim Umgang mit personenbezogenen Daten des Auftraggebers. Der Auftragnehmer hat im Benehmen mit dem Auftraggeber angemessene Maßnahmen zur Sicherung der Daten sowie zur Minderung möglicher nachteiliger Folgen für Betroffene zu ergreifen. Soweit den Auftraggeber Pflichten nach § 42a BDSG treffen, hat der Auftragnehmer ihn hierbei zu unterstützen."*[99]

Bei der Bemessung des Bußgeldes nach § 43 Abs. 2 Nr. 7 BDSG kann erschwerend berücksichtigt werden, wenn das Unternehmen durch den Dienstleister ausdrücklich auf die Pflicht zur Benachrichtigung hingewiesen wurde, die verantwortliche Stelle dieser Pflicht aber nicht nachgekommen ist[100].

---

98 *Scheffczyk* in: Wolff/Brink, Datenschutzrecht, 2013, § 42a Rn. 10.

99 Ziffer 8 des GDD-Vertragsmusters zur ADV (GDD-Ratgeber Datenschutz beim Outsourcing, 3. Auflage, S. 101 ff.); ähnlich der Formulierungsvorschlag des *Regierungspräsidiums Darmstadt* in dessen Mustervertrag zu § 11 BDSG.

100 *Hessischer DSB*, 42. TB 2014, S. 178.

2.5 Informationspflicht nach § 15a TMG

Mit der BDSG-Novelle II von 2009 wurde nicht nur § 42a BDSG, sondern zugleich eine Neuregelung in § 15a TMG eingeführt, welche die BDSG-Regelung in Bezug nimmt. § 15a TMG gilt für **Telemedienanbieter** (also auch für die Anbieter sämtlicher Bürgerportale der öffentlichen Verwaltung) und bezieht sich auf Bestands- bzw. Nutzungsdaten. § 42a BDSG wird für entsprechend anwendbar erklärt. Von § 42a Satz 1 BDSG bleibt dabei freilich nicht viel übrig, da Normadressaten, Risikodaten und die auslösenden Umstände der Benachrichtigungspflicht vom TMG vorgegeben werden. Lediglich die Empfänger der Benachrichtigung (Betroffene/Aufsichtsbehörde) ergeben sich noch aus § 42a Satz 1 BDSG.

Warum der Gesetzgeber es verabsäumt hat, den Verstoß gegen § 15a TMG gleichzeitig als Ordnungswidrigkeit zu sanktionieren, bleibt unverständlich[101]. Im Verweis auf § 42a BDSG ist keinesfalls zugleich ein Verweis auf § 43 Abs. 2 Nr. 7 BDSG zu erblicken[102].

2.6 Informationspflicht nach § 109a TKG

Die Informationspflicht nach dem TKG ergibt sich seit der Novellierung dieses Gesetzes im Jahr 2012 aus § 93 Abs. 3 i.V.m. § 109a TKG. Die Vorschriften richten sich an **Erbringer öffentlich zugänglicher Telekommunikationsdienste**. Wegen der abweichenden Regelungsgehalte zum TMG wird eine sachdienliche Abgrenzung zwischen diesen Bereichen notwendig. Das TKG ist immer dann einschlägig, wenn der Vorgang der Signalübertragung, also der Netzbetrieb im Vordergrund steht[103].

Die Informationspflicht nach dem TKG kennt **drei Benachrichtigungsempfänger**. Es sind dies die Bundesnetzagentur (BNetzA), der Bundes-

[101] *Ernst*, DuD 2010, 475; *Holländer*, RDV 2009, 221; *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 2., der im Verweis auf § 42a BDSG zugleich einen Verweis auf § 43 Abs. 2 Nr. 7 BDSG erblickt.

[102] Gänzlich verfehlt insoweit a.A. *Müller-Broich*, TMG, 2012, § 15a Rn. 1.

[103] *Geppert/Schütz/Eckhardt*, TKG, 4. Aufl. 2013, § 109a Rn. 9 f.

beauftragte für den Datenschutz und die Informationsfreiheit (BfDI) und die Betroffenen (hier: „Teilnehmer oder andere Personen“).

Die beiden Behörden sind **in allen Fällen** der Verletzung des Schutzes personenbezogener Daten zu informieren (§ 109a Abs. 1 Satz 1 TKG). Die „Verletzung des Schutzes personenbezogener Daten“ ist ein telekommunikationsrechtlicher Spezialterminus und in § 3 Nr. 30a TKG gesetzlich definiert[104].

Die Betroffenen werden lediglich dann informiert, wenn eine **schwerwiegende Beeinträchtigung** der Rechte oder schutzwürdigen Interessen droht (§ 109a Abs. 1 Satz 2 TKG). Die §§ 93 Abs. 3 i.V.m. 109a TKG sind insoweit nicht richtlinienkonform, da die zu Grunde liegende Richtlinie 2009/136/EG ihrerseits nicht auf das Erfordernis schwerwiegender Beeinträchtigungen abstellt[105].

Bei ausreichender Verschlüsselung kann die Meldung gegenüber den Betroffenen gemäß § 109a Abs. 1 Satz 3 TKG wiederum entfallen. Es erscheint nur auf den ersten Blick erstaunlich, dass beim Einsatz von Verschlüsselungstechnik eine meldepflichtige Datenpanne eintreten kann[106]. § 3 Nr. 30a TKG fordert jedoch im Gegensatz zu § 42a Satz 1 TKG gerade keine Kenntnisnahme durch Dritte.

Der **Inhalt der Benachrichtigungen** an Behörden und Betroffene ist in § 109a Abs. 2 Sätze 1 und 2 TKG spezialgesetzlich geregelt. Aufzuführen sind zunächst die Art der Verletzung des Schutzes personenbezogener Daten, Angaben zu Kontaktstellen, bei denen weitere Informationen erhältlich sind sowie Empfehlungen dahingehend, nachteilige Auswirkungen zu begrenzen. Folgen der Schutzverletzung und die beabsichtigten oder ergriffenen Maßnahmen sind nur in der Meldung an die Behörden darzulegen.

---

[104] „[…] eine Verletzung der Datensicherheit, die zum Verlust, zur unrechtmäßigen Löschung, Veränderung, Speicherung, Weitergabe oder sonstigen unrechtmäßigen Verwendung personenbezogener Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste verarbeitet werden sowie der unrechtmäßige Zugang zu diesen;[…]“

[105] *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 2.

[106] Kritisch hierzu *BfDI*, 24. TB 2013, S. 59.

Gemäß § 109a Abs. 3 TKG ist ein Verzeichnis der Verletzungen des Schutzes personenbezogener Daten zu führen, das die gesetzlichen Pflichtangaben umfasst und wenigstens fünf Jahre in die Vergangenheit reicht.

Die Bundesnetzagentur hat entsprechend § 109a Abs. 4 TKG ein **Meldeformular nebst korrespondierender Leitlinien** bereitgestellt[107]. Diese sollen fortan laufend aktualisiert werden.

Ein Verstoß gegen § 109a TKG kann als **Ordnungswidrigkeit** gemäß § 149 Abs. 1 Nr. 21b sowie Nr. 21c TKG geahndet werden. Das **Verwertungs- und Verwendungsverbot** greift gemäß § 109a Abs. 1 Satz 5 TKG i.V.m. § 42a Satz 6 BDSG[108].

2.7 Informationspflicht nach § 83a SGB X

§ 83a SGB X statuiert einen eigenständigen ersten Satz mit speziellen Tatbestandmerkmalen und verweist in Satz 2 vollumfänglich auf § 42a Sätze 2 bis 6 BDSG. Informationspflichtig sind nach dieser Vorschrift die **Sozialleistungsträger**, also Stellen im Sinne des § 35 SGB I[109].

Zu den geschützten Risikodaten gehören **ausschließlich die besonderen Arten personenbezogener Sozialdaten gemäß § 67 Abs. 12 SGB X** (entspricht vollumfänglich § 3 Abs. 9 BDSG). Hierdurch können sich Wertungswidersprüche ergeben. Es ist nicht erklärbar, warum Sozialleistungsträger weniger strengen Meldevoraussetzungen unterliegen sollen als sonstige verantwortliche Stellen[110].

---

[107] Online unter http://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Datenschutz/Datenschutzverletzungenmelden/datenschutzverletzungenmelden-node.html.

[108] Näher oben, 1.5.6.

[109] Leistungsträger, Verbände und Arbeitsgemeinschaften der Leistungsträger, Datenstelle der Träger der Rentenversicherung, gemeinsame Servicestellen, Integrationsfachdienste, die Künstlersozialkasse, die Versicherungsämter und Gemeindebehörden, anerkannten Adoptionsvermittlungsstellen und einige mehr. Nicht jedoch die Leistungserbringer (etwa Kliniken, Arztpraxen oder Pflegeeinrichtungen).

[110] Vgl. *Diering/Timme/Waschull/Seidel*, SGB X, 3. Aufl. 2011, § 83a Rn. 4; *Dix* in: Simitis, BDSG, 8. Aufl. 2014, § 42a Rn. 5.

Der Sozialdatenschutz schützt zugleich die Daten Verstorbener (§ 35 Abs. 5 SGB I). Im Einzelfall kann sich daraus die Pflicht zur **Benachrichtigung der Angehörigen** ergeben[111].

Zu den bereits bekannten Mitteilungsempfängern des § 42a BDSG tritt als weiterer Empfänger die **Aufsichtsbehörde nach § 90 SGB IV** hinzu. Diese ist qua gesetzlichem Verweis (eine) „zuständige Aufsichtsbehörde" nach § 42a Satz 4 BDSG. Der gesetzliche Inhalt der Meldung nach § 83a Satz 2 SGB X i.V.m. § 42a Satz 4 BDSG ist daher für alle Aufsichtsbehörden gleich.

Kommt die verantwortliche Stelle ihren Informationspflichten nicht nach, kann dies gemäß § 85 Abs. 2 Nr. 6 SGB X als **Ordnungswidrigkeit** geahndet werden. Im Übrigen gelten die obigen Ausführungen zur Informationspflicht nach dem BDSG.

Der Sächsische DSB berichtet, dass Empfänger eines Schreibens über die Bewilligung von Sozialleistungen im gleichen Umschlag ein nicht an sie gerichtetes Schreiben erhielten. Die Behörde verneinte die schwerwiegende Beeinträchtigung, da sich die jeweiligen Betroffenen in einer ähnlichen Lebenssituation befanden und nicht in unmittelbarer Nähe zueinander wohnten[112].

2.8 Landesrechtliche Benachrichtigungspflichten

Benachrichtigungspflichten ähnlich derjenigen in § 42a BDSG sind mittlerweile in den **Landesdatenschutzgesetzen** von Berlin, Mecklenburg-Vorpommern, Rheinland-Pfalz und Schleswig-Holstein enthalten. Die Vorschriften richten sich an die öffentlichen Stellen des Landes sowie Private, die Aufgaben der öffentlichen Verwaltung wahrnehmen.

Zu den landesrechtlichen Vorschriften im Einzelnen:

- **§ 18a BlnDSG:** Besondere Risikodaten müssen nicht betroffen sein, allerdings müssen schwerwiegende Beeinträchtigungen

[111] Vgl. *BlnBDI*, TB 2014, S. 152 zu § 18a BlnDSG, welcher ebenfalls die Daten von Verstorbenen erfasst.

[112] *Sächsischer DSB*, 16. TB 2013, S. 98.

drohen. Die Verfahrensweise ähnelt derjenigen des BDSG. Die Vorschrift erfasst auch Daten Verstorbener (§ 4 Abs. 1 Satz 2 BlnDSG)[113]. Ein ausdrückliches Verwendungsverbot ähnlich § 42a Satz 6 BDSG existiert nicht.

- **§ 18a DSG Rlp:** Besondere Risikodaten müssen nicht betroffen sein, allerdings müssen schwerwiegende Beeinträchtigungen drohen. Die Verfahrensweise ähnelt derjenigen des BDSG. Ein ausdrückliches Verwendungsverbot ähnlich § 42a Satz 6 BDSG existiert nicht.
- **§ 23 DSG MV:** Risikodaten müssen nicht betroffen sein. Auf das Merkmal der schwerwiegenden Beeinträchtigung wurde verzichtet, es genügt jeder eventuelle Nachteil. Die konkrete Verfahrensweise ist nicht geregelt. Ein ausdrückliches Verwendungsverbot ähnlich § 42a Satz 6 BDSG existiert nicht.
- **§ 27a DSG SH:** Risikodaten müssen nicht betroffen sein, aber es müssen schwerwiegende Beeinträchtigungen drohen. Satz 2 der Vorschrift verweist sodann vollumfänglich auf § 42a Satz 2 bis 6 BDSG und damit auch auf das Verwendungsverbot.

Für öffentliche Stellen, die am Wettbewerb teilnehmen, bzw. öffentlich-rechtliche Wirtschaftsunternehmen gelten gemäß Verweis in den Landesgesetzen das BDSG und damit auch die Informationspflichten gemäß § 42a (vgl. jeweils die einschlägigen Regelungen zum Anwendungsbereich der Landesdatenschutzgesetze).

So entschied etwa der Bayerische Landesbeauftragte, dass Krankenhäuser in öffentlich-rechtlicher Trägerschaft und Universitätskliniken gemäß Art. 3 Abs. 1 BayDSG der Meldepflicht nach § 42a BDSG unterliegen[114].

[113] *BlnBDI*, TB 2013, 178; *BlnBDI*, TB 2014, S. 152.
[114] BayLfD, 26. TB 2014, S. 65.

3. Meldepflichten nach dem IT-Sicherheitsgesetz

3.1 Gesetzliche Grundlagen

§ 8b BSIG: Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

[…] (4) [1]Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen

1. *führen können oder*
2. *geführt haben,*

über die Kontaktstelle unverzüglich an das Bundesamt zu melden. [2]Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten. [3]Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

§ 109 TKG: Technische Schutzmaßnahmen

[…] (5) [1]Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur unverzüglich Beeinträchtigungen von Telekommunikationsnetzen und -diensten mitzuteilen, die

1. *zu beträchtlichen Sicherheitsverletzungen führen oder*
2. *zu beträchtlichen Sicherheitsverletzungen führen können.*

[2]Dies schließt Störungen ein, die zu einer Einschränkung der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. [3]Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und zu der betroffenen Informationstechnik enthalten. [4]Kommt es zu einer beträchtlichen Sicherheitsverletzung, kann die Bundesnetzagentur einen detaillierten Bericht über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen. [5]Soweit es sich um Sicherheitsverletzungen handelt, die die Informationstechnik betreffen, leitet die Bundesnetzagentur die eingegangenen Meldungen sowie die Informationen zu den ergriffenen Abhilfemaßnahmen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. [6]Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Europäische Agentur für Netz- und Informationssicherheit über die Sicherheitsverletzungen. [7]Die Bundesnetzagentur kann die Öffentlichkeit unterrichten oder die nach Satz 1 Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt. [8]§ 8d des BSI-Gesetzes gilt entsprechend. […]

§ 109a TKG: Daten- und Informationssicherheit

[…] (4) [1]Werden dem Diensteanbieter nach Absatz 1 Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. [2]Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können.

3.2 Literatur

Bartels, Bezugspunkte des IT-Sicherheitsgesetzes – Weichenstellungen einer nationalen Gesetzesinitiative, ITRB 2015, 92; *Beucher/Ehlen*, Der neue Referentenentwurf zum IT-Sicherheitsgesetz, jurisPR-Compl 2/2014, Anm. 3; *Bräutigam/Wilmer*, Big brother is watching you? – Meldepflichten im geplanten IT-Sicherheitsgesetz, ZRP 2015, 38; *Ferik*, Aus der digitalen Agenda der Bundesregierung – das geplante IT-Sicherheitsgesetz, RDV 2014, 261; *Freund*, IT-Sicherheitsgesetz – Zum neuen Entwurf eines Gesetzes gegen Cyberattacken, ITRB 2014, 256; *Gerling*, Das IT-Sicherheitsgesetz: purer Aktionismus oder doch mehr IT-Sicherheit?, RDV 2015, 167; *Heckmann*, IT-Sicherheit auf Raten?, MMR 2015, 289; *Heinickel/Feiler*, Der Entwurf für ein IT-Sicherheitsgesetz – europarechtlicher Kontext und die (eigentlichen) Bedürfnisse der Praxis, CR 2014, 708; *Klett/Ammann*, Gesetzliche Initiativen zur Cybersicherheit Ein Überblick zu den bisherigen regulatorischen Ansätzen auf nationaler und europäischer Ebene, CR 2014, 93; *Leisterer/Schneider*, Der überarbeitete Entwurf für ein IT-Sicherheitsgesetz – Überblick und Problemfelder, CR 2014, 574; *Rath/Kuss/Bach*, Das neue IT-Sicherheitsgesetz K&R 2015, 437; *Roos*, Der Entwurf eines IT-Sicherheitsgesetzes: Regelungsinhalte und ihre Übereinstimmung mit dem Richtlinienvorschlag der EU-Kommission, K&R 2013, 769; *Roos*, Der neue Entwurf eines IT-Sicherheitsgesetzes – Bewegung oder Stillstand?, MMR 2014, 723; *Roth*, Neuer Referentenentwurf zum IT-Sicherheitsgesetz – Dringende Neuregelung der Netz- und Informationssicherheit, ZD 2015, 17; *Seidl*, Mehr Cybersicherheit durch ein IT-Sicherheitsgesetz?, jurisPR-ITR 7/2014 Anm. 2 (Teil I), jurisPR-ITR 9/2014 Anm. 2 (Teil II), jurisPR-ITR 10/2014 Anm. 2 (Teil III), jurisPR-ITR 12/2014 Anm. 2 (Teil IV), jurisPR-ITR 15/2014 Anm. 2 (Teil V); *Selk/Gierschmann*, Stellungnahme der DGRI zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), CR 2015, 273; *Weise/Brühl*, Auswirkungen eines künftigen IT-Sicherheitsgesetzes auf Betreiber Kritischer Infrastrukturen, CR 2015, 290.

3.3 Zweck und Gegenstand des IT-Sicherheitsgesetzes

Das IT-Sicherheitsgesetz (ITSG) ist am 25. Juli 2015 in Kraft getreten[115]. Vermittels der neuen Vorschriften soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme erreicht werden[116]. Das Gesetz schreibt die Einhaltung eines Mindestniveaus an IT-Sicherheit bei Betreibern sog. „Kritischer Infrastrukturen", Telekommunikationsdienstleistern und Telemedienanbietern vor. Zugleich werden Meldepflichten statuiert, sofern Störungen der IT-Sicherheit auftreten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Bundesnetzagentur (BNetzA) erhalten so die Möglichkeit, ein zutreffendes Bild von der **Bedrohungslage** zu zeichnen und entsprechende Hilfestellungen anzubieten.

Es handelt sich hierbei nicht um Datenschutzrecht im eigentlichen Sinne, da die Vorschriften des ITSG nicht auf den Schutz personenbezogener Daten abzielen. Die im ITSG niedergelegten Sicherheitsanforderungen können ggf. Ausstrahlungswirkung auf technisch-organisatorische Maßnahmen nach dem BDSG haben. Es existiert jedoch kein Rangverhältnis zwischen Datenschutz- und IT-Sicherheitsrecht. Ein Vorfall kann daher durchaus nach § 42a BDSG und § 8c BSIG meldepflichtig sein[117].

Das ITSG ist ferner keine einheitliche Kodifikation sondern ein Artikelgesetz, welches lediglich bestehende Gesetze abändert. Es bringt u.a. Neuerungen im BSI-Gesetz (BSIG), dem Atomgesetz (AtomG), dem Energiewirtschaftsgesetz (EnWG), dem Telemediengesetz (TMG), dem Telekommunikationsgesetz (TKG) und dem BKA-Gesetz (BKAG).

Die Vorschriften über Kritische Infrastrukturen und deren Meldepflichten unterliegen gemäß Art. 10 ITSG einer **Evaluationsfrist** von vier Jahren.

Auf europäischer Ebene laufen momentan die Vorbereitungen für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemein-

[115] BGBl. I 2015, S. 1324 ff.

[116] BT-Drs. 18/4096, S. 19.

[117] *Roos*, MMR 2014, 727 sowie *Bartels*, ITRB 2015, 93 zu möglichen Doppelmeldungen nach § 42a BDSG und § 8c BSIG.

samen Netz- und Informationssicherheit in der Union (sog. NIS-RL)[118]. Nach Verabschiedung der Richtlinie wird sich u.U. auf nationaler Ebene weiterer Änderungsbedarf ergeben.

[118] Vorschlag der Kommission unter http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf. Eingehend hierzu *Heinickel/Feiler*, CR 2014, 709 ff.; *Roos*, K&R 2013, 773 ff.; *Seidl*, jurisPT-ITR 12/2014, Anm. 2; *ders.*, jurisPR-ITR, 15/2014, Anm. 2.

3.4 Störungsmeldung an das BSI (§ 8b BSIG)

Die Störungsmeldung an das BSI nach § 8b Abs. 4 BSIG macht den Kern der Meldepflichten im ITSG aus. Die bereichsspezifischen und damit spezielleren Meldepflichten im AtomG[119], dem EnWG[120] und dem TKG[121] sind dem nachgebildet.

Obschon das ITSG insgesamt bereits in Kraft ist, greift die Meldepflicht als solche noch nicht. Grund hierfür ist, dass der genaue Adressatenkreis des ITSG erst durch eine Rechtsverordnung nach § 10 Abs. 1 BSIG festgelegt werden muss. Dies ist bislang noch nicht geschehen. Erst wenn feststeht, wer Betreiber einer Kritischen Infrastruktur ist, muss eine entsprechende Kontaktstelle im Sinne von § 8b Abs. 3 S. 1 BSIG geschaffen werden.[122] Lediglich die Kontaktstelle ist zur Abgabe von Störungsmeldungen berechtigt[123].

3.4.1 Kreis der Pflichtigen

§ 2 Abs. 10 S. 1 BSIG definiert grob, was als **Kritische Infrastruktur** gilt. Gemeint sind Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören (Nr. 1) und zugleich von hoher Bedeutung für das Funktionieren des Gemeinwesens sind (Nr. 2), weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. **Sektorenzugehörigkeit und Gemeinwichtigkeit** müssen dabei zwingend zusammentreffen.

Eine genauere Bestimmung wird durch Rechtsverordnung gemäß § 2 Abs. 10 Satz 2 i.V.m. § 10 Abs. 1 BSIG nachgereicht werden. Auch die Rechtsverordnung wird sich unterdessen auf abstrakte Umschreibun-

[119] Siehe insb. § 44b AtomG (nicht Gegenstand dieses Ratgebers).
[120] Siehe insb. § 11 Abs. 1c EnWG (nicht Gegenstand dieses Ratgebers).
[121] Siehe Abschnitt 3.5.
[122] Transitionszeit: 6 Monate.
[123] § 8b Abs. 4 Satz 1 BSIG.

gen beschränken[124]. Es bestehen freilich erhebliche Zweifel, ob der Umweg über die Rechtsverordnung überhaupt zulässig ist, da der Gesetzgeber grundsätzlich selbst den Adressatenkreis derart einschneidender Gesetze festlegen muss[125].

Die Bewertung der Kritikalität wird daran anknüpfen, ob durch die jeweilige Infrastruktur eine für die Gesellschaft kritische Dienstleistung erbracht wird (Qualität) und ob ihr Ausfall wesentliche Folgen für wichtige Schutzgüter[126] und die Funktionsfähigkeit des Gemeinwesens hätte (Quantität)[127].

Die Bundesregierung hat bereits offengelegt, welche Branchen sie in den einzelnen Sektoren als besonders kritisch ansieht[128]. Es sind dies:

- Energie: Versorgung mit Elektrizität, Gas und Mineralöl;
- Informationstechnik und Telekommunikation: Sprach- und Datenkommunikation, Verarbeitung und Speicherung von Daten;
- Transport und Verkehr: Güterverkehr, Personennahverkehr, Personenfernverkehr;
- Gesundheit: Medizinische Versorgung, Versorgung mit Arzneimitteln und Medizinprodukten;
- Wasser: Trinkwasserversorgung, Abwasserbeseitigung;
- Ernährung: Lebensmittelversorgung;
- Finanz- und Versicherungswesen: Zahlungsverkehr und Zahlungsdienstleistungen, Bargeldversorgung, Kreditvergabe, Geld- und Devisenhandel, Wertpapier- und Derivatehandel, Versicherungsleistungen.

[124] BT-Drs 18/4096, S. 30.

[125] *Heckmann*, MMR 2015, 290; *Roos*, MMR 2014, 725; *Roth*, ZD 2015, 19. Die „sektor- und branchenspezifischen Einbeziehung aller betroffenen Kreise“ in einem gemeinsamen Arbeitsprozess (BT-Drs. 18/4096, S. 23) hätte jedenfalls schon im formellen Gesetzgebungsverfahren Berücksichtigung finden können.

[126] Hier: Leib, Leben, Gesundheit und Eigentum, BT-Drs 18/4096, S. 31.

[127] BT-Drs 18/4096, S. 30.

[128] BT-Drs 18/4096, S. 30.

Klar ist dank § 8c Abs. 1 BSIG bislang nur, dass **Kleinstunternehmen** im Sinne der Empfehlung 2003/361/EC der Kommission[129] vom Anwendungsbereich ausgeschlossen sind. Hierbei handelt es sich gemäß Art. 2 Abs. 3 der Empfehlung um Unternehmen, die weniger als zehn Personen beschäftigen und deren Jahresumsatz bzw. Jahresbilanz zwei Millionen Euro nicht überschreitet.

3.4.2 Störung

§ 8b Abs. 4 Satz 1 BSIG fordert eine erhebliche Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen kann (Nr. 1) oder geführt hat (Nr. 2). Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit stellen aus Sicht der Bundesregierung die vornehmlichen Schutzgüter der IT-Sicherheit dar[130].

- Verfügbarkeit = Autorisierte Nutzer dürfen nicht am Zugriff auf Informationen oder Systeme gehindert werden.
- Integrität = Informationen müssen vollständig und unverändert sein, Systeme müssen korrekt funktionieren.
- Authentizität = Kommunikationspartner oder Informationsquellen müssen eindeutig feststehen.
- Vertraulichkeit = Informationen dürfen Unbefugten nicht zur Kenntnis gelangen oder weitergegeben werden.

Eine **Störung** liegt vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken[131]. Die Gesetzesbegründung zählt hierzu insbesondere Sicherheitslücken, Schadpro-

[129] *Europäische Kommission*, Empfehlung vom 06.05.2003, online unter http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32003H0361.

[130] BT-Drs 18/4096, S. 19; u.a. definiert im IT-Grundschutzkatalog des *BSI*, Glossar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Glossar/glossar_node.html.

[131] BT-Drs 18/4096, S. 27 f.

gramme und Angriffe auf die IT- Sicherheit sowie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug[132].

Erheblich sind solche Störungen, die die nicht etwa bereits automatisiert oder mit wenig Aufwand abgewehrt werden können[133]. Das Merkmal der **Erheblichkeit** stellt insoweit eine reine Tautologie dar, da kaum unerhebliche Störungen denkbar sind, die einen Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit befürchten lassen.

Der Betreiber trägt die Verantwortung für die korrekte **Risikoeinschätzung**. Vor allem die Abgrenzung zwischen erheblichen Störungen, die nicht zur Beeinträchtigung geführt haben und gänzlich unerheblichen Störungen stellt Betreiber vor unwägbare Herausforderungen. Das Bundesinnenministerium rät daher, im Zweifel stets zu melden[134]. Die hieraus möglicherweise resultierende Flut von überobligatorischen Meldungen könnte freilich den eigentlichen Gesetzeszweck konterkarieren[135]. Immerhin war im Referentenentwurf angedacht, dass das BSI einen Kriterienkatalog zur Bestimmung der Meldepflichtigkeit erarbeitet[136].

3.4.3 Art und Weise der Meldung

Adressat

Empfänger der Meldung nach § 8b Abs. 4 Satz 1 BSIG ist **ausschließlich das BSI**. Anders als § 42a BDSG erfüllt die Informationspflicht nicht unmittelbar die Funktion eines Betroffenenrechts. Warnungen und Empfehlungen an die Öffentlichkeit durch das BSI sind stattdessen in § 7 Abs. 1 Satz 1 Nrn. 1 und 2 BSIG vorgesehen.

---

[132] Etwa nach (missglückten) Softwareupdates oder einem Ausfall der Serverkühlung.

[133] BT-Drs 18/4096, S. 28.

[134] *BMI*, Referentenentwurf vom 18.8.2014, S. 42. Zustimmend *Freund*, ITRB 2014, 259; *Rath/Kuss/Bach*, K&R 2015, 438; *Roos*, MMR 2014, 726.

[135] *Heinickel/Feiler*, CR 2014, 713.

[136] *BMI*, Referentenentwurf vom 18.8.2014, S. 42.

Zeitliche Vorgabe

Die Störung ist gemäß § 8b Abs. 4 Satz 1 BSIG **unverzüglich** zu melden. Hierbei handelt es sich – wie bereits bei § 42a BDSG – um einen indirekten Verweis auf § 121 Abs. 1 Satz 1 BGB. Unverzügliches Handeln erfolgt „ohne schuldhaftes Zögern". Dies strafft einerseits den Entscheidungsfindungsprozess bei der verantwortlichen Stelle, bedeutet jedoch andererseits, dass die Benachrichtigung keineswegs „sofort" zu erfolgen hat. Stattdessen ist ein nach den Umständen des Einzelfalles zu bemessendes beschleunigtes Verhalten an den Tag zu legen[137].

Im Falle des § 8b Abs. 4 Satz 1 BSIG muss Zeit bleiben, erste Nachforschungen zum Ausmaß des Vorfalls durchzuführen. Die Entscheidung, ob eine Meldung erforderlich ist, kann nicht aus dem Bauch heraus getroffen werden, sondern bedarf einer umfassenden Kenntnis von den zugrundeliegenden Vorgängen. Ein Aussondern von personenbezogenen Daten[138] und Geschäftsgeheimnissen kann ebenfalls zu Verzögerungen führen[139]. Ein Abwarten von mehr als 24 Stunden soll jedoch nur durch besondere Umstände gerechtfertigt sein[140].

Ähnlich wie bei § 42a BDSG sollte dokumentiert werden, warum ein bestimmter Zeitpunkt für die Meldung gewählt wurde. Anderenfalls läuft der Betreiber Gefahr, wegen fahrlässiger nicht rechtzeitiger Meldung mit einem Bußgeld belegt zu werden[141].

Inhalt

Die Meldung muss gemäß § 8b Abs. 4 Satz 2 BSIG Angaben zu der **Störung** sowie zu den **technischen Rahmenbedingungen**, insbesondere der vermuteten oder tatsächlichen **Ursache**, der **betroffenen Informationstechnik**, der **Art der betroffenen Einrichtung oder Anlage** sowie zur **Branche** des Betreibers enthalten.

---

[137] Reichsgericht, Urteil vom 22.02.1929, II 357/28 (= RGZ 124, 115, 118).
[138] Vgl. § 8b Abs. 7 Satz 3 BSIG.
[139] *Roos*, K&R 2013, 771.
[140] *Roos*, K&R 2013, 771.
[141] Näher hierzu unten, 3.4.4.

Die Nennung des Betreibers ist nach § 8b Abs. 4 Satz 3 BSIG jedoch nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat (Fall des § 8b Abs. 4 Satz 2 BSIG). Nach der Gesetzesbegründung ist hierfür ausdrücklich keine Anonymisierung, sondern lediglich eine Pseudonymisierung vorgesehen[142]. Hierdurch wird der besonderen wirtschaftlichen Sensibilität der Meldungen im Hinblick auf eventuelle Imageschäden Rechnung getragen, ohne dass das BSI auf die Möglichkeit etwaiger Rückfragen verzichten müsste.

Form

Eine bestimmte Form ist für die Meldung nicht vorgesehen. Das BSI hat jedoch gemäß § 3 Abs. 1 Satz 2 Nr. 15 BSIG den gesetzlichen Auftrag erhalten, besondere **Kommunikationsstrukturen** zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zu errichten. Es ist daher damit zu rechnen, dass (gerade unter Berücksichtigung der Eilbedürftigkeit) ein irgendwie geartetes elektronisches Meldeverfahren zur Verfügung gestellt werden wird.

Zur Abgabe der Meldung ist zunächst die **Kontaktstelle** im Sinne von § 8b Abs. 3 S. 1 BSIG berechtigt. Pseudonyme Meldungen nach § 8b Abs. 4 Satz 3 BSIG sind durch sie jedoch nur schwer möglich. Die einzelnen Wirtschaftssektoren können daher zusätzlich gemäß § 8b Abs. 5 Satz 1 BSIG **gemeinsame übergeordnete Stellen** einrichten. Diese vermögen pseudonyme Meldungen zu kanalisieren[143].

3.4.4 Verstoß gegen die Meldepflicht

Sowohl der Verzicht auf eine Kontaktstelle (§ 14 Abs. 1 Nr. 3 BSIG) als auch die ausbleibende, nicht richtige, nicht vollständige oder nicht rechtzeitige Meldung (§ 14 Abs. 1 Nr. 4 BSIG) werden als **Ordnungswidrigkeiten** geahndet. Der Bußgeldrahmen beträgt gemäß § 14 Abs. 2 BSIG jeweils 50.000 Euro.

[142] BT-Drs. 18/4096, S. 28.

[143] Mögliches (verschlüsseltes) Verfahren skizziert bei *BMI*, Referentenentwurf vom 18.08.2014, S. 43.

Anders als in § 42a Satz 6 BDSG bzw. § 109a Abs. 1 Satz 5 TKG wurde jedoch kein Verwertungs- und Verwendungsverbot für den Fall der Selbstbezichtigung aufgenommen[144]. Insoweit dürfte der Bußgeldtatbestand verfassungswidrig und damit unwirksam sein[145].

[144] Zu § 42a Satz 6 BDSG oben, 1.5.6.

[145] So bereits *Eckhardt* in: Geppert/Schütz, TKG, 3. Aufl. 2013, § 109 TKG Rn. 79 zur Meldepflicht nach dem TKG vor Inkrafttreten des ITSG.

3.5 Störungsmeldung an die BNetzA (§ 109 TKG)

Gemäß § 8c Abs. 3 Nr. 1 BSIG gelten die Vorschriften über die Störungsmeldung an das BSI nicht für Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen. An deren Stelle tritt die Meldung an die BNetzA nach § 109 Abs. 5 TKG.

Die Meldepflicht der Telekommunikationsdienstleister ist **kein völliges Novum**. Bis zum Inkrafttreten des ITSG galt bereits nach § 109 Abs. 5 Satz 1 TKG a.F., dass Betreiber Sicherheitsverletzungen einschließlich Störungen von Telekommunikationsnetzen oder -diensten unverzüglich mitzuteilen hatten, sofern durch diese beträchtliche Auswirkungen auf den Betrieb der Telekommunikationsnetze oder das Erbringen von Telekommunikationsdiensten entstanden. Das ITSG weitet die Meldepflicht nunmehr auf den Vorfeldbereich potentieller Sicherheitsverletzungen aus, um ein valides und vollständiges Lagebild der IT-Sicherheit zeichnen zu können[146].

3.5.1 Kreis der Pflichtigen

§ 109 Abs. 5 TKG richtet sich an Stellen die **öffentliche Telekommunikationsnetze** betreiben oder **öffentlich zugängliche Telekommunikationsdienste** erbringen. Öffentliche Telekommunikationsnetze sind gemäß § 3 Nr. 16a TKG solche, die ganz oder überwiegend der Bereitstellung öffentlich zugänglicher Telekommunikationsdienste dienen, die die Übertragung von Informationen zwischen Netzabschlusspunkten[147] ermöglichen. Diese Netze oder Dienste sind öffentlich, wenn sie der Allgemeinheit bzw. einem **unbegrenzten Adressatenkreis** zur Verfügung stehen[148].

3.5.2 Störung

Als meldepflichtige Störung im Sinne des § 109 Abs. 5 Satz 1 TKG gilt jede Beeinträchtigung von Telekommunikationsnetzen und -diensten,

[146] BT-Drs. 18/4096, S. 36.
[147] Siehe § 3 Nr. 12a TKG.
[148] *Ricke* in: Spindler/Schuster, Recht der elektronischen Medien, 3. Aufl. 2015.

die zu einer beträchtlichen Sicherheitsverletzungen führt (Nr. 1) oder führen kann (Nr. 2).

Dies schließt ausweislich des § 109 Abs. 5 Satz 2 TKG solche Störungen mit ein, die zu einer Verfügbarkeitseinschränkung der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der jeweiligen Nutzer führen können.

Potentielle Verletzungen wurden in den Anwendungsbereich der Vorschrift aufgenommen, da sich z.B. Manipulationen der Internet-Infrastruktur oder etwa der Missbrauch einzelner Server oder Anschlüsse zum Betrieb eines Botnetzes zwar nicht gegen die Verfügbarkeit der Netze insgesamt richten, jedoch schwerwiegende Folgen für die IT-Systeme der Nutzer nach sich ziehen können[149].

Die geforderten „beträchtlichen Sicherheitsverletzungen“ sind leider ebenso wenig gesetzlich definiert wie zuvor die beträchtlichen Auswirkungen in § 109 Abs. 5 Satz 1 TKG a.F. Dieses Merkmal unterliegt der Einschätzung und Bewertung des Betreibers.

3.5.3 Art und Weise der Meldung

Adressat

Die Meldung nach § 109 Abs. 5 Satz 1 TKG richtet sich zunächst **ausschließlich an die BNetzA**.

Soweit es sich um Sicherheitsverletzungen handelt, die konkret die Informationstechnik betreffen, leitet die BNetzA ihrerseits gemäß § 109 Abs. 5 Satz 5 TKG sowohl die eingegangenen Meldungen als auch die Informationen zu den ergriffenen Abhilfemaßnahmen an das BSI weiter. Sonstige Regulierungsbehörden in anderen EU-Mitgliedstaaten und die Europäische Agentur für Netz- und Informationssicherheit können gemäß § 109 Abs. 5 Satz 6 TKG informiert werden.

Die BNetzA kann schließlich gemäß § 109 Abs. 5 Satz 7 TKG die Öffentlichkeit unterrichten oder zu einer solchen Unterrichtung auffordern,

[149] BT-Drs. 18/4096, S. 3

wenn die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt, nach § 109 Abs. 5 Satz 8 TKG i.V.m. § 8d Abs. 1 BSIG keine schutzwürdigen Betreiberinteressen entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist.

Zeitliche Vorgabe

Die Meldung hat wie in § 42a Satz 1 BDSG und § 8b Abs. 4 Satz 1 BSIG **unverzüglich** zu erfolgen[150].

Inhalt

Die Meldung muss gemäß § 109 Abs. 5 Satz 3 TKG Angaben zu der **Störung** sowie zu den **technischen Rahmenbedingungen**, insbesondere der vermuteten oder tatsächlichen **Ursache** und zu der betroffenen **Informationstechnik** enthalten. Der Inhalt der Meldung gleicht damit demjenigen, der in § 8b Abs. 4 Satz 2 BSIG vorgesehen ist. Die Möglichkeit einer pseudonymen Meldung wie in § 8b Abs. 4 Satz 3 BSIG ist im TKG allerdings nicht vorgesehen.

Die Meldung muss nicht umfassend sein[151]. Kommt es tatsächlich zu einer beträchtlichen Sicherheitsverletzung (§ 109 Abs. 5 Satz 1 Nr. 1 TKG), kann die Bundesnetzagentur nach § 109 Abs. 5 Satz 4 TKG einen **detaillierten Bericht** über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen.

Form

Eine bestimmte Form ist gesetzlich nicht vorgeschrieben. Insofern wird auf die Ausführungen zu § 8b BSIG verwiesen[152].

[150] Einzelheiten hierzu oben, 1.5.5.

[151] So bereits *Eckhardt* in: Geppert/Schütz, TKG, 3. Aufl. 2013, § 109 TKG Rn. 74 zum Rechtszustand vor dem ITSG.

[152] Siehe oben, 3.4.3.

3.5.4 Verstoß gegen die Meldepflicht

Ordnungswidrig handelt nach § 149 Abs. 1 Nr. 21a TKG, wer entgegen § 109 Abs. 5 Satz 1 Nr. 1 TKG eine Mitteilung **nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig** macht. Fälle der nur potentiellen Sicherheitsverletzung nach § 109 Abs. 5 Satz 1 Nr.2 TKG sind hingegen nicht erfasst. Der Bußgeldrahmen beträgt gemäß § 149 Abs. 2 Satz 1 TKG 50.000 €.

Da anders als in § 42a Satz 6 BDSG bzw. § 109a Abs. 1 Satz 5 TKG kein Verwertungs- bzw. Verwendungsverbot für den Fall der Selbstbezichtigung im § 109 Abs. 5 TKG festgeschrieben wurde, wird der Bußgeldtatbestand z.T. für verfassungswidrig erachtet[153].

[153] *Eckhardt* in: Geppert/Schütz, TKG, 3. Aufl. 2013, § 109 TKG Rn. 79.

3.6 Störungsmeldung an Nutzer (§ 109a TKG)

§ 109a Abs. 4 TKG stellt ein Nutzerrecht dar[154]. Beabsichtigt ist nicht die Lagebestimmung der IT-Sicherheitslandschaft insgesamt, sondern die konkrete Hilfestellung für Nutzer von IT-Systemen. Die vormaligen Empfehlungen der Allianz für Cybersicherheit[155] unter Federführung des BSI erhalten somit Gesetzesrang und können zur Auslegung der neuen Bestimmungen herangezogen werden.

3.6.1 Kreis der Pflichtigen

Die Vorschrift verpflichtet Diensteanbieter im Sinne des § 109a Abs. 1 Satz 1 TKG, also all diejenigen, die öffentlich zugängliche Telekommunikationsdienste erbringen.

3.6.2 Störung

Anknüpfungspunkt der Meldepflicht ist, wie im gesamten ITSG, die Störung. Diese muss von einem Datenverarbeitungssystem des Nutzers ausgehen, also prinzipiell von jedem beliebigen Endgerät, welches zumindest nominell unter der Kontrolle des Nutzers steht.

§ 8b Abs. 4 Satz 1 BSIG verwendet einen Störungsbegriff, der immer dann erfüllt ist, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken[156]. Unter Berücksichtigung der Schutzrichtung von § 109a Abs. 4 TKG muss das Merkmal der „nicht richtigen“ Funktionsweise weit ausgelegt werden (z.B. Inkorporierung in ein Botnetz, DDoS, Proxy für zielgerichtete Hackerattacken). Zugleich muss der Störungsbegriff all diejenigen Fälle erfassen, in denen das System an sich zwar ordnungsgemäß funktioniert, aber nicht in

[154] Die Bezeichnung „Betroffenenrecht“ wäre verfehlt, da es im ITSG insgesamt nicht um den Schutz personenbezogener Daten geht.

[155] *BSI*, Empfehlung Malware-Schutz – Handlungsempfehlungen für Internet-Service-Provider, 2012, S. 1, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/techniker/netzwerk/BSI-CS-046.pdf?__blob=publicationFile.

[156] BT-Drs 18/4096, S. 27 f.

intendierter Weise verwendet wird (z.B. Missbrauch eines regulären Mail-Servers zum Spamversand).

3.6.3 Art und Weise der Meldung

Adressat

Die Störungsmeldung richtet sich an die jeweiligen **Nutzer, soweit diese dem Betreiber bereits bekannt sind**. § 109a Abs. 4 Satz 1 TKG statuiert ausdrücklich keine Nachforschungspflicht, wenn die Störung nicht konkret zugeordnet werden kann.

Zeitliche Vorgabe

Die Meldung hat **unverzüglich** zu erfolgen[157]. Wegen des geringeren Ermittlungsaufwandes dürfte hier ein noch strengerer Maßstab als bei § 42a Satz 1 BDSG oder § 8b Abs. 4 Satz 1 BSIG angelegt werden.

Inhalt

Die Meldung umfasst zunächst die Störung als solche. Da sich die Störungsmeldung auch und insbesondere an IT-Laien richtet, sollten allgemeinverständliche Ausführungen gemacht werden. Die Nutzer sollen erkennen können, was vor sich geht und die Ursache für die Störung eingrenzen.

Soweit technisch möglich und zumutbar, hat der Betreiber seine Nutzer zudem gemäß § 109a Abs. 4 Satz 2 TKG auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können. Dieser Passus wurde im Rahmen des Gesetzgebungsverfahrens kritisiert, da die schiere Masse an möglichen Endgeräten (Router, PCs, Tablets, Netzwerkdrucker, Heimserver, Unterhaltungselektronik u.s.w.) unmöglich vom Diensteanbieter in ausreichendem Maße unterstützt werden könne[158]. § 109a Abs. 4 Satz 2 TKG fordert allerdings keine Schritt-für-Schritt-Anleitung

[157] Hierzu näher oben, 1.5.5.
[158] *Seidl*, jurisPR-ITR 10/2014, Anm. 2.

für das spezifische Endgerät (welches dem Diensteanbieter im Zweifel auch gar nicht bekannt sein dürfte).

Form

Das Gesetz schreibt keine spezifische Form für die Mitteilung vor. Sie kann nach den Vorgaben der Allianz für Cybersicherheit per Brief, eMail oder über eine Vorschaltseite/Walled-Garden vorgenommen werden.[159] Die Kontaktaufnahme sollte allerdings den möglichen Zeitverzug berücksichtigen.

3.6.4 Verstoß gegen die Meldepflicht

Die Störungsmeldung an Nutzer von Telekommunikationsdiensten ist nicht bußgeldbewehrt. Unterlässt ein Betreiber jedoch eine ihm mögliche Benachrichtigung, kann dies ggf. als **Plichtverletzung** im Rahmen der vertraglichen Schadensersatzhaftung nach § 280 Abs. 1 BGB oder einer Schutzgesetzverletzung nach § 823 Abs. 2 BGB berücksichtigt werden. Freilich muss der geltend gemachte Schaden gerade durch das pflichtwidrige Unterlassen hervorgerufen worden sein. Sofern es sich unterdessen um Störungen handelt, die der Nutzer auch selbst hätte bemerken müssen oder verhindern können, kann ein (auch überwiegender) Mitverschuldensanteil nach § 254 Abs. 1 BGB angerechnet werden.

[159] *BSI*, Empfehlung Malware-Schutz – Handlungsempfehlungen für Internet-Service-Provider, 2012, S. 1.

Muster: Handlungsempfehlungen zu § 42a BDSG

Im Falle einer Datenschutzverletzung ist zügiges Handeln geboten. Deswegen ist bereits im Vorhinein ein geeigneter Krisenreaktionsplan zu entwerfen.

Formulierung von internen **Richtlinien** für den Fall einer Datenpanne

- ✓ Definition von Datenpannen
- ✓ Identifizierung der zuständigen Aufsichtsbehörde
- ✓ Festlegung von Data-Breach-Notification-Verantwortlichen und weiteren Ansprechpartnern[160]
- ✓ Ggf. Schaffung eines Krisenteams
- ✓ Unterrichtung sämtlicher Mitarbeiter

Implementierung eines geeigneten **Security Incident Response Systems**[161]

- ✓ Monitoring der IT-Systeme auf sicherheitsrelevante Zugriffe
- ✓ Bestimmung von Art und Umfang des Datenlecks
- ✓ Beseitigung von Datenlecks und Sicherheitsrisiken
- ✓ Sicherstellung computerforensischer Analyse

Implementierung eines geeigneten **Data Breach Notification Management Systems**

- ✓ Festlegung von Kommunikationswegen
- ✓ Kooperation verschiedener Untergliederungen[162]

[160] Wer entscheidet, ob sich eine Datenpanne im Rechtssinne ereignet hat, muss hinreichend geschult sein, so auch *Hanloser*, CCZ 2010, 29.

[161] *Gliss*, DSB 2009, 11 spricht vom Security Incident und Event Management (SIEM) bzw. Security Incident Handling. In der Medizin existieren vergleichbare Critical Incident Reporting Systems (CIRS).

- ✓ Informationsaustausch mit Auftragsdatenverarbeitern
- ✓ Rechtzeitige Benachrichtigung der Entscheidungsträger
- ✓ Regelung von Whistleblowing-Situationen[163]
- ✓ Beteiligung der Mitarbeitervertretung[164]
- ✓ Vorbereitung von Musterbenachrichtigungen

Kontakt zur Aufsichtsbehörde

- ✓ Erörterung von Zweifelsfällen schon vor offizieller Meldung[165]
- ✓ Beachtung behördlicher Hinweise, sofern vorhanden
- ✓ Vermeidung behördlicher Benachrichtigungsanordnungen nach § 38 Abs. 5 Satz 1 BDSG

Kontakt zur Strafverfolgungsbehörde

- ✓ Erstattung einer Strafanzeige/ggf. Stellen eines Strafantrages
- ✓ Abstimmung, ob Betroffenenmitteilung die Ermittlungen gefährden könnte

[162] Es können die Unternehmensleitung, die Rechts-, Compliance-, IT-(Sicherheits-), Datenschutz-, PR-Abteilung u.a. betroffen sein.

[163] Es gilt, Hemmschwellen der Mitarbeiter abzubauen, vgl. *Gliss*, DSB 2009, 11; *Hanloser*, CCZ 2010, 29. Allgemein zum Whistleblower-Schutz nach deutschem Recht siehe *Király*, ZRP 2011, 146 f.; *ders.*, RdA 2012, 236 f.

[164] Die Einführung eines solchen Notification Managements kann gemäß § 87 Abs. 1 Nr. 6 BetrVG mitbestimmungspflichtig sein, vgl. *Duisberg/Picot*, CR 2009, 825; *Gliss*, DSB 2013, 246; *Schierbaum*, CuA 2011, 30.

[165] *Dorn*, DSB 2011, 16; *Scheffczyk* in: Wolff/Brink, BDSG, § 42a Rn. 39; *Schierbaum*, CuA 2011, 30.

Muster: Checkliste des Data-Breach-Notification-Verantwortlichen nach § 42a BDSG

Vorliegen einer Datenpanne:

- ✓ Wann und wo ist die Datenpanne aufgetreten?
- ✓ Wie sind die Daten abhandengekommen?
- ✓ Sind Daten im Sinne des § 42a Satz 1 Nr. 1-4 BDSG betroffen?
- ✓ Wie viele Datensätze sind (ungefähr) betroffen?
- ✓ Ist der Empfänger der Daten bekannt?
- ✓ Besteht das Risiko eines Datenmissbrauchs?
- ✓ Drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen?

Weiteres Vorgehen:

- ✓ Welche Maßnahmen zur Sicherung der Daten wurden ergriffen?
- ✓ Kann der Missbrauch noch verhindert werden oder dessen Folgen eingedämmt werden?
- ✓ Gefährdet die Mitteilung an die Betroffenen laufende Ermittlungen?
- ✓ Welche Abteilungen sind zu informieren und einzubinden?
- ✓ Welche Datenschutzaufsichtsbehörde ist zuständig?
- ✓ Ist Strafanzeige zu erstatten/Strafantrag zu stellen?
- ✓ Bestehen Anzeigenkontakte mit bundesweit erscheinenden Tageszeitungen?

Muster: Mitarbeiterrichtlinie zum Umgang mit Datenpannen nach § 42a BDSG

In unserem Unternehmen werden personenbezogene Daten verarbeitet. Diese bedürfen des besonderen Schutzes. Im Falle einer Datenpanne ist unser Unternehmen verpflichtet, die Betroffenen und die zuständige Datenschutzaufsichtsbehörde zu informieren. Ziel der Regelung ist u.a., bei Datenverlusten Folgeschäden für den Betroffenen in Form von finanziellen Einbußen oder sozialen Nachteilen zu vermeiden.

Personenbezogene Daten sind alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG).

Eine Datenpanne im Sinne des Bundesdatenschutzgesetzes liegt vor, wenn gesetzlich näher bezeichnete sensible personenbezogene Informationen unrechtmäßig an Dritte weitergegeben werden oder Dritte sich diese Daten unrechtmäßig verschaffen. Eine Datenpanne liegt auch vor, wenn Geräte oder Speichermedien mit unverschlüsselten Daten verloren gehen.

Sollten Sie bemerken oder den Verdacht haben, dass personenbezogene Daten unrechtmäßig Dritten zugänglich gemacht wurden, sich Dritte solche Daten unrechtmäßig verschafft haben oder entsprechende Informationen abhandengekommen sind, informieren Sie bitte umgehend:

_____ [Zimmer/Durchwahl]

[Hinweis: Als unternehmensinterne Adressaten der Meldung kommen etwa in Betracht: der/die Vorgesetzte, die Unternehmensleitung, der/die Datenschutzbeauftragte, die IT-Abteilung, die IT-Sicherheitsabteilung, die Rechtsabteilung, andere Ansprechpartner.]

Aus dieser Meldung entstehen Ihnen als Mitarbeiter/in **keinerlei berufliche oder persönliche Nachteile.** Die Namensangabe erfolgt freiwillig.

1.) Wann und wo ist die Datenpanne aufgetreten?

_____
_____
_____

2.) Beschreibung des konkreten Vorfalls

Z.B. Verlust oder Diebstahl von Datenträgern, unrechtmäßige/ irrtümliche Übermittlung, unrechtmäßige Einsichtnahme durch einen Mitarbeiter, Angriff auf Computersysteme

_____
_____
_____
_____
_____

3.) Welche Datenarten sind betroffen?

- □ Angaben über die rassische oder ethnische Herkunft
- □ politische Meinungen
- □ religiöse oder philosophische Überzeugungen
- □ Gewerkschaftszugehörigkeit
- □ Gesundheit
- □ Sexualleben
- □ Daten, die einem Berufsgeheimnis unterliegen
- □ Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen
- □ personenbezogene Daten zu Bank- oder Kreditkartenkonten
- □ Unbekannt
- □ Sonstige: _____

4.) Wie viele Datensätze sind [ungefähr] betroffen?

_____

5.) Besteht aus Ihrer Sicht das Risiko des Datenmissbrauchs?

□ Ja □ Nein

Wenn nein, warum?

_____

6.) Drohen aus Ihrer Sicht schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen (z.B. Identitätsbetrug, unberechtigte Abbuchungen, soziale Nachteile) ?

□ Ja □ Nein

Wenn nein, warum?

_____

7.) Sind Maßnahmen zur Sicherung der Daten ergriffen worden?

□ Ja □ Nein

8.) Sonstige Mitteilungen:

_____
_____

Name (optional) Datum

Muster: Benachrichtigung der Betroffenen nach § 42a BDSG

Beispiel:

Information nach § 42a des Bundesdatenschutzgesetzes

Sehr geehrte/r […],

Am […] / im Zeitraum von […] bis […] sind Ihre bei uns gespeicherten personenbezogenen Daten Dritten unrechtmäßig zur Kenntnis gelangt.

Alternativ: Es ist nicht auszuschließen, dass Ihre bei uns gespeicherten personenbezogenen Daten am […] / im Zeitraum von […] bis […]Dritten unrechtmäßig zur Kenntnis gelangt sind.

In diesem Zeitraum sind Datensicherungsbänder mit Lohn- und Gehaltsinformationen von Unbekannten entwendet worden. Die Bänder enthalten Namen, Adressen, Gehaltsforderungen sowie insbesondere Kontoverbindungen, Kirchensteuer- und/oder Gewerkschaftsbeiträge.

Im Missbrauchsfall sind die Daten möglicherweise geeignet, schwerwiegende Beeinträchtigungen für Ihre Rechte und schutzwürdigen Interessen herbeizuführen. Bitte achten Sie in Ihrem eigenen Interesse auf nichtautorisierte Zahlungsbewegungen auf Ihrem Konto sowie auf unerwartete bzw. verdächtige Kenntnis Dritter von Ihren persönlichen Lebensumständen.

Der Landesdatenschutzbeauftragte und die Staatsanwaltschaft Musterstadt sind über den Vorfall bereits informiert. Bitte teilen Sie etwaige Unregelmäßigkeiten unserer Datenschutzabteilung mit.

[Grußformel]

Notwendige Inhalte der Information:

Nach § 42a Satz 3 BDSG muss die Benachrichtigung des Betroffenen eine **Darlegung der Art der unrechtmäßigen Kenntniserlangung** und **Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen** enthalten.

Die **Art der unrechtmäßigen Kenntniserlangung** umfasst folgende Aspekte:

- Welche **Datenkategorien** sind von der Datenpanne betroffen?

  Sinnvollerweise sind insofern nicht nur die die Informationspflicht auslösenden Risikodaten im Sinne von § 42a Satz 1 BDSG zu nennen, sondern sämtliche von der Datenpanne betroffenen personenbezogenen Informationen, siehe Beispiel.

- Welcher **konkrete Vorfall** hat sich ereignet?

  Z.B. Verlust oder Diebstahl von Datenträgern, unrechtmäßige/ irrtümliche Übermittlung, unrechtmäßige Einsichtnahme durch einen Mitarbeiter, Angriff auf Computersysteme

Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen sind regelmäßig nur verständlich, wenn auch bzgl. möglicher **Missbrauchsszenarien** informiert wird. Dies sind z.B.:

- Identitätsmissbrauch (etwa bei Online-Geschäften)
- Herbeiführung von Vermögensschäden, z.B. durch unberechtigte Abbuchungen
- Herbeiführung soziale und/oder beruflicher Nachteile
- Herbeiführung sonstiger Nachteile

Als mögliche **Schutzempfehlungen** kommen insbesondere in Betracht:

- Änderung von Passwörtern und PIN-Codes
- Kontrolle von Kontoauszügen auf Unregelmäßigkeiten

- Kontrolle von Online-Konten auf Unregelmäßigkeiten
- Information von Geschäftspartnern
- Information von Kreditinstitut bzw. Kreditkartengesellschaft

Sinnvolle **fakultative Informationen** gegenüber dem Betroffenen können sein:

- Information, dass zusätzlich eine Information der zuständigen Datenschutzaufsichtsbehörde über den Vorfall erfolgt
- Sofern zutreffend: Information über die Erstattung einer Strafanzeige bei der Staatsanwaltschaft unter Angabe des Aktenzeichens
- Angabe eines unternehmensinternen Ansprechpartners für Hinweise oder Rückfragen zum Datenschutzvorfall

Muster: Benachrichtigung der Aufsichtsbehörde nach § 42a BDSG

An [die zuständige Datenschutzaufsichtsbehörde]

Am […] / im Zeitraum von […] bis […] sind bei uns gespeicherte personenbezogene Daten im Sinne von § 42a Satz 1 BDSG Dritten unrechtmäßig zur Kenntnis gelangt.

Alternativ: Es ist nicht auszuschließen, dass bei uns gespeicherte personenbezogene Daten im Sinne von § 42a Satz 1 BDSG am […] / im Zeitraum von […] bis […] Dritten unrechtmäßig zur Kenntnis gelangt sind.

Wir haben hiervon seit dem […] Kenntnis.[166]

1.) Beschreibung des konkreten Vorfalls

Z.B. Verlust oder Diebstahl von Datenträgern, unrechtmäßige/ irrtümliche Übermittlung, unrechtmäßige Einsichtnahme durch einen Mitarbeiter, Angriff auf Computersysteme

_____
_____
_____
_____
_____

2.) Welche Datenarten im Sinne von § 42a Satz 1 BDSG sind betroffen?

□ Angaben über die rassische oder ethnische Herkunft

□ politische Meinungen

□ religiöse oder philosophische Überzeugungen

[166] Information gefordert vom *LVwA Sachsen-Anhalt*, 5. TB 2011, S. 20.

- □ Gewerkschaftszugehörigkeit
- □ Gesundheit
- □ Sexualleben
- □ Daten, die einem Berufsgeheimnis unterliegen
- □ Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen
- □ personenbezogene Daten zu Bank- oder Kreditkartenkonten

3.) Wie viele Datensätze sind [ungefähr] betroffen?

_____

4.) Gefahrenpotenzial

Die betroffenen Daten bergen ein Missbrauchsrisiko und könnten dazu verwendet werden,

- □ Identitäten (etwa bei Online-Geschäften) vorzutäuschen
- □ Vermögensschäden herbeizuführen
- □ soziale und/oder berufliche Nachteile herbeizuführen
- □ sonstige Nachteile herbeizuführen:

  _____

  _____

5.) Maßnahmen

Welche Maßnahmen wurden zum Schutz der im konkreten Fall betroffenen personenbezogenen Daten ergriffen (z.B. Information von irrtümlichen Empfängern und Aufforderung zur Datenlöschung)?

_____

_____

_____
_____

Welche Maßnahmen wurden ergriffen, um die Ursache der unrechtmäßigen Kenntniserlangung personenbezogener Daten für die Zukunft zu beseitigen (z.B. Einspielen von Sicherheitspatches, Einführung von Verschlüsselungsverfahren, Penetrationstests)?

_____
_____
_____
_____

Eine entsprechende Strafanzeige ist anhängig.

□ Ja □ Nein

Wenn *ja*, Staatsanwaltschaft: _____

Aktenzeichen: _____

Wenn *nein*, warum nicht ?

_____

Die Betroffenen sind informiert worden.

□ Ja □ Nein

Wenn *ja*, durch

□ individuelle Mitteilung □ öffentliche Bekanntmachung.

Wenn *nein*, warum nicht?

_____

Ein Muster der Benachrichtigung ist als **Anlage** beigefügt. Die Betroffenen sind gebeten worden, sich vor einem eventuellen Missbrauch der Daten durch kriminelle Dritte zu schützen durch

□ Änderung von Passwörtern und PIN-Codes

- □ Kontrolle von Kontoauszügen auf Unregelmäßigkeiten
- □ Kontrolle von Online-Konten auf Unregelmäßigkeiten
- □ Information der Geschäftspartner
- □ Information des Kreditinstituts bzw. der Kreditkartengesellschaft
- □ Sonstiges:
  _____

6.) Kontakt

Bei Rückfragen wenden Sie sich bitte an […].

Satzung

der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. (in der Fassung der Beschlüsse vom 10.11.1983, 16.11.1984, 14.11.1990, 04.11.1991, 20.11.2002, 18.11.2009, 21.11.2012 und 19.11.2014 der ordentlichen Mitgliederversammlung in Köln)

Präambel

Datenschutz und Datensicherheit sind mit Blick auf die modernen Informations- und Kommunikationstechnologien sowie den wachsenden wirtschaftlichen Wert personenbezogener Daten wichtige Grundpfeiler der Informationsgesellschaft. Ein angemessener Datenschutz hat dabei sowohl dem Recht auf informationelle Selbstbestimmung als auch der Informationsfreiheit Rechnung zu tragen. Die Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V. tritt für einen sinnvollen, vertretbaren und technisch realisierbaren Datenschutz ein. Sie hat zum Ziel, die Daten verarbeitenden Stellen und deren Datenschutzbeauftragte bei der Lösung der vielfältigen technischen, rechtlichen und organisatorischen Fragen zu unterstützen, die durch das Erfordernis nach rechtmäßiger, ordnungsgemäßer und sicherer Datenverarbeitung aufgeworfen werden. Die Gesellschaft tritt hierzu für die Prinzipien der Selbstkontrolle und Selbstregulierung ein. Im Rahmen ihrer Aktivitäten pflegt sie eine intensive Zusammenarbeit mit Wirtschaft, Verwaltung, Wissenschaft und Politik. Die Gesellschaft vertritt die Belange der Daten verarbeitenden Stellen - insbesondere auch der mittelständischen Wirtschaft -, deren Datenschutzbeauftragten und der betroffenen Bürger gegenüber Regierungen und Gesetzgebungsorganen; sie will ferner die politische Willensbildung durch fachlichen Rat unterstützen.

§ 1
Name, Sitz, Geschäftsjahr

(1) Der Verein führt den Namen „Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.“ Die Gesellschaft hat ihren Sitz in Bonn; sie ist in das Vereinsregister eingetragen.

(2) Das Geschäftsjahr der Gesellschaft ist das Kalenderjahr.

§ 2
Zweck und Gemeinnützigkeit

(1) Die Gesellschaft mit Sitz in Bonn verfolgt ausschließlich und unmittelbar gemeinnützige Zwecke im Sinne des Abschnitts „Steuerbegünstigte Zwecke“ der Abgabenordnung. Zweck der Gesellschaft ist die Förderung der Volks- und Berufsbildung auf dem Gebiet des Datenschutzes und der Datensicherheit im Sinne der dieser Satzung vorangestellten Präambel. Der Satzungszweck wird verwirklicht insbesondere durch

1. die Zurverfügungstellung von Informationen und Materialien an die betroffenen Bürger und Daten verarbeitenden Stellen zur Meinungsbildung und Entscheidungsfindung,
2. die Bildung von Arbeits- und Erfahrungsaustauschkreisen,
3. die Entwicklung und Veröffentlichung von Methoden zur Sicherung der Qualifikation von Datenschutzverantwortlichen, insbesondere Datenschutzbeauftragten,
4. die Zusammenarbeit mit den in der Datenschutzgesetzgebung vorgesehenen staatlichen Kontrollorganen.

(2) Die Gesellschaft ist selbstlos tätig; sie verfolgt nicht in erster Linie eigenwirtschaftliche Zwecke. Mittel der Gesellschaft dürfen nur für die satzungsmäßigen Zwecke verwendet werden. Die Mitglieder erhalten keine Zuwendungen aus Mitteln der Gesellschaft. Es darf keine Person durch Ausgaben, die dem Zweck der Gesellschaft fremd sind, oder durch unverhältnismäßig hohe Vergütungen begünstigt werden.

§ 3
Mitgliedschaft

(1) Ordentliche Mitglieder der Gesellschaft können natürliche und juristische Personen, Handelsgesellschaften, nicht rechtsfähige Ver-

eine sowie Anstalten und Körperschaften des öffentlichen Rechts werden.
(2) Die Beitrittserklärung erfolgt schriftlich gegenüber dem Vorstand. Über die Annahme der Beitrittserklärung entscheidet der Vorstand. Die Mitgliedschaft beginnt mit Annahme der Beitrittserklärung.
(3) Die Mitgliedschaft endet durch Austrittserklärung, durch Tod von natürlichen Personen oder durch Auflösung und Erlöschen von juristischen Personen, Handelsgesellschaften, nicht rechtsfähigen Vereinen sowie Anstalten und Körperschaften des öffentlichen Rechts oder durch Ausschluss; die Beitragspflicht für das laufende Geschäftsjahr bleibt hiervon unberührt.
(4) Der Austritt ist nur zum Schluss eines Geschäftsjahres zulässig; die Austrittserklärung muss spätestens drei Monate vor Ablauf des Geschäftsjahres gegenüber dem Vorstand schriftlich abgegeben werden.
(5) Die Mitgliederversammlung kann solche Personen, die sich besondere Verdienste um die Gesellschaft oder um die von ihr verfolgten satzungsgemäßen Zwecke erworben haben, zu Ehrenmitgliedern ernennen. Ehrenmitglieder haben alle Rechte eines ordentlichen Mitglieds. Sie sind von Beitragsleistungen befreit.

§ 4
Rechte und Pflichten der Mitglieder

(1) Die Mitglieder sind berechtigt, die Leistungen der Gesellschaft in Anspruch zu nehmen.
(2) Die Mitglieder sind verpflichtet, die satzungsgemäßen Zwecke der Gesellschaft zu unterstützen und zu fördern. Sie sind ferner verpflichtet, die festgesetzten Beiträge zu zahlen.

§ 5
Ausschluss eines Mitgliedes

(1) Ein Mitglied kann durch Beschluss des Vorstandes ausgeschlossen werden, wenn es das Ansehen der Gesellschaft schädigt, seinen Beitragsverpflichtungen nicht nachkommt oder wenn ein sonstiger wichtiger Grund vorliegt. Der Vorstand muss dem auszuschließenden Mitglied den Beschluss in schriftlicher Form unter der Angabe der Gründe mitteilen und ihm auf Verlangen eine Anhörung gewähren.
(2) Gegen den Beschluss des Vorstandes ist die Anrufung der Mitgliederversammlung zulässig. Bis zum Beschluss der Mitgliederversammlung ruht die Mitgliedschaft.

§ 6
Beitrag

(1) Die Gesellschaft erhebt einen Jahresbeitrag. Er ist für das Geschäftsjahr im ersten Quartal des Jahres im Voraus zu entrichten. Das Nähere regelt die Beitragsordnung, die von der Mitgliederversammlung beschlossen wird.
(2) Im begründeten Einzelfall kann für ein Mitglied durch Vorstandsbeschluss ein von der Beitragsordnung abweichender Beitrag festgesetzt werden.

§ 7
Organe der Gesellschaft

Die Organe der Gesellschaft sind
1. die Mitgliederversammlung,
2. der Vorstand.

§ 8
Mitgliederversammlung

(1) Oberstes Beschlussorgan ist die Mitgliederversammlung. Ihrer Beschlussfassung unterliegen
1. die Genehmigung des Finanzberichtes und der Haushaltspläne,
2. die Entlastung des Vorstandes,
3. die Wahl der einzelnen Vorstandsmitglieder,
4. die Bestellung von Finanzprüfern,
5. Satzungsänderungen,
6. die Genehmigung der Beitragsordnung,
7. die Richtlinie für die Erstattung von Reisekosten und Auslagen,
8. Anträge des Vorstandes und der Mitglieder,
9. die Ernennung von Ehrenmitgliedern,
10. die Auflösung der Gesellschaft.

(2) Die ordentliche Mitgliederversammlung findet einmal im Jahr statt. Außerordentliche Mitgliederversammlungen werden auf Beschluss des Vorstandes abgehalten, wenn die Interessen der Gesellschaft dies erfordern, oder wenn ein Viertel der Mitglieder dies unter Angabe des Zweckes schriftlich beantragt. Die Einberufung der Mitgliederversammlung erfolgt schriftlich durch den Vorstand mit einer Frist von mindestens zwei Wochen.

Hierbei sind die Tagesordnung bekannt zugeben und ihr die nötigen Informationen beizufügen, insbesondere Geschäftsbericht, Finanzbericht, Haushaltsplan, Satzungsänderungen, Änderungen der Beitragsordnung und - soweit bekannt - Wahlvorschläge und Anträge an die Mitgliederversammlung. Anträge zur Tagesordnung sind mindestens drei Tage vor der Mitgliederversammlung bei der Geschäftsstelle einzureichen. Über die Behandlung von Initiativanträgen entscheidet die Mitgliederversammlung.

(3) Die Mitgliederversammlung ist beschlussfähig, wenn mindestens 30 stimmberechtigte Mitglieder anwesend sind. Beschlüsse sind jedoch gültig, wenn die Beschlussfähigkeit vor der Beschlussfassung nicht angezweifelt worden ist.

(4) Beschlüsse über Satzungsänderungen und über die Auflösung der Gesellschaft bedürfen zu ihrer Rechtswirksamkeit der Dreiviertelmehrheit der anwesenden und ordnungsgemäß vertretenen Mitglieder. In allen anderen Fällen genügt die einfache Mehrheit.

(5) Jedes Mitglied hat eine Stimme. Juristische Personen haben einen Stimmberechtigten schriftlich zu bestellen. Jedes Mitglied hat das Recht, sich durch eine andere stimmberechtigte natürliche Person vertreten zu lassen; eine Person kann höchstens zehn Stimmen auf sich vereinigen. Die Bestellung des Vertreters hat schriftlich zu erfolgen.

(6) Auf Antrag des Mitglieds ist geheim abzustimmen. Über die Beschlüsse der Mitgliederversammlung ist ein Protokoll anzufertigen, das vom Versammlungsleiter und dem Protokollführer zu unterzeichnen ist; das Protokoll ist allen Mitgliedern zuzustellen und auf der nächsten Mitgliederversammlung genehmigen zu lassen.

§ 9
Vorstand

(1) Der Vorstand besteht aus mindestens sieben und höchstens elf Mitgliedern:

1. dem Vorsitzenden,
2. zwei stellvertretenden Vorsitzenden,
3. dem Schatzmeister,
4. mindestens zwei und maximal sechs Beisitzern und
5. dem Erfa-Repräsentanten.

Der Vorstand ist berechtigt, bei entsprechendem Bedarf bis zu zwei Mitglieder zu kooptieren. Diese haben kein Stimmrecht.

(2) Vorstand im Sinne des § 26 Abs. 2 BGB sind der Vorsitzende, im Verhinderungsfall sein Stellvertreter, zusammen mit einem der anderen Vorstandsmitglieder. Die Vertretungsmacht ist durch Beschlüsse des gesamten Vorstandes begrenzt.

(3) Der Vorstand beschließt mit der Mehrheit seiner satzungsgemäßen Mitglieder. Sind mehr als zwei Vorstandsmitglieder dauernd an der Ausübung ihres Amtes gehindert, so sind unverzüglich Nachwahlen anzuberaumen.

(4) Die Amtsdauer der Vorstandsmitglieder beträgt zwei Jahre; Wiederwahl ist zulässig.

(5) Der Vorstand gibt sich eine Geschäftsordnung.

(6) Der Vorstandsvorsitzende ist Dienstvorgesetzter der Geschäftsführer.

(7) Der Schatzmeister überwacht die Haushaltsführung und verwaltet das Vermögen der Gesellschaft. Er hat auf eine sparsame und wirtschaftliche Haushaltsführung hinzuwirken. Mit Ablauf des Geschäftsjahres stellt er unverzüglich die Abrechnung sowie die Vermögensübersicht und sonstige Unterlagen von wirtschaftlichem Belang den Finanzprüfern der Gesellschaft zur Prüfung zur Verfügung.

(8) Die Vorstandsmitglieder sind grundsätzlich ehrenamtlich tätig; sie haben Anspruch auf Erstattung notwendiger Auslagen im Rahmen einer von der Mitgliederversammlung zu beschließenden Richtlinie über die Erstattung von Reisekosten und Auslagen.

(9) Der Vorstand kann einen 'Wissenschaftlichen Beirat' einrichten, der für die Gesellschaft beratend und unterstützend tätig wird; in den Beirat können auch Nicht-Mitglieder berufen werden.

(10) Auf Vorschlag des Vorstandes kann die Mitgliederversammlung einen Vorsitzenden des Vorstandes nach dessen Ausscheiden aus dem Vorstand wegen herausragender Verdienste um die Gesellschaft zum Ehrenvorsitzenden ernennen. Der Ehrenvorsitzende wird zu den Sitzungen des Vorstandes eingeladen, er hat aber kein Stimmrecht.

§ 10
Geschäftsführung

(1) Die Geschäftsführung besteht aus bis zu zwei Geschäftsführern. Die Rechte und Pflichten werden in einem Dienstvertrag geregelt.

(2) Die Geschäftsführung führt die Geschäfte der Gesellschaft. Sie ist an die Vorgaben und Weisungen des Vorstandes gebunden. Die Geschäftsführung erstellt insbesondere den Jahreshaushaltsplan, den Rechnungsabschluss sowie den Geschäftsbericht und bereitet die Sitzungen des Vorstandes, der Mitgliederversammlung, des wissenschaftlichen Beirates und des Erfa-Beirates vor.

(3) Innerhalb des laufenden Geschäftsverkehrs ist die Geschäftsführung im Rahmen der ihr erteilten Vollmacht ermächtigt, den Verein zu verpflichten und Rechte für ihn zu erwerben.

§ 11
Finanzprüfer

(1) Zur Kontrolle der Haushaltsführung bestellt die Mitgliederversammlung Finanzprüfer. Nach Durchführung ihrer Prüfung geben sie dem Vorstand Kenntnis von ihrem Prüfungsergebnis und erstatten der Mitgliederversammlung Bericht.
(2) Die Finanzprüfer dürfen dem Vorstand nicht angehören.

§ 12
Erfa-Organisation

(1) Die Gesellschaft bildet zur Durchführung ihrer Aufgaben Erfahrungsaustauschkreise (Erfa-Kreise). Aufgabe der Erfa-Kreise ist es insbesondere, in Zusammenarbeit mit den zuständigen Aufsichtsbehörden und sonstigen Fachleuten für Fragen des Datenschutzes und der Datensicherheit,

1. die Teilnehmer bei der Lösung und Klärung bestehender Datenschutzprobleme zu unterstützen,
2. auf lokaler oder regionaler Ebene Ziele und Belange der Gesellschaft und ihrer Mitglieder zu vertreten,
3. auf lokaler oder regionaler Ebene die Belange der betrieblichen und behördlichen Datenschutzbeauftragten zu vertreten.

(2) Aufgabe der Erfa-Kreise ist es ferner,

1. die Entscheidungsbildung in der Gesellschaft zu fördern und vorzubereiten,
2. Mitglieder für die Gesellschaft zu werben.

(3) Beabsichtigt ein Erfa-Kreis, bestimmte Themen oder Aktivitäten mit überregionalem Bezug an die Öffentlichkeit zu tragen, ist dies vorher mit dem Vorstand der Gesellschaft abzustimmen.
(4) Jeder Erfa-Kreis wählt einen Erfa-Kreis-Leiter. Die Erfa-Kreise sollten sich eine Geschäftsordnung geben, die mit dem Erfa-Beirat abzustimmen ist.

§ 13
Erfa-Beirat

(1) Der Erfa-Beirat besteht aus den Erfa-Kreis-Leitern, die Mitglieder der Gesellschaft sind.
(2) Der Erfa-Beirat schlägt der Mitgliederversammlung aus seiner Mitte den Erfa-Repräsentanten zur Wahl in den Vorstand vor.
(3) Der Erfa-Beirat wirkt bei der Führung der Geschäfte der Gesellschaft beratend und unterstützend mit. Er hat insbesondere die Aufgabe, die Belange der Erfa-Kreise zu vertreten.
(4) Der Erfa-Beirat gibt sich eine Geschäftsordnung; in ihr ist die Mitgliederstärke der einzelnen Erfa-Kreise angemessen zu berücksichtigen.

§ 14

Auflösung der Gesellschaft

Bei der Auflösung oder Aufhebung der Gesellschaft oder bei Wegfall steuerbegünstigter Zwecke fällt das Vermögen der Gesellschaft an eine juristische Person des öffentlichen Rechts oder eine andere steuerbegünstigte Körperschaft zwecks Verwendung für die Förderung der Volks- und Berufsbildung.

Nähere Informationen über die GDD finden Sie unter www.gdd.de oder rufen Sie uns an 0228/96 96 75 00.

Mitgliedschaft

GDD-Mitglieder können natürliche und juristische Personen, Personengesellschaften, nicht-rechtsfähige Vereine sowie Einrichtungen des öffentlichen Rechts im In- und Ausland werden. Bei Wirtschaftsunternehmen, Behörden, Verbänden u.ä. wird ein nach Größe der Vereinigung gestaffelter Jahresbeitrag erhoben. Einzelheiten ergeben sich aus unserer Beitragsordnung. Firmenmitglieder können neben den regelmäßigen Serviceleistungen der GDD zusätzlich die Unterstützung bei Datenschutzfragen aus der betrieblichen Praxis ihres Unternehmens in Anspruch nehmen. Wenn Sie Mitglied werden möchten, senden Sie bitte folgende Beitrittserklärung ausgefüllt an die

Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD)
Heinrich-Böll-Ring 10 · 53119 Bonn · F +49 228 96 96 75 25 · info@gdd.de

.....

Beitrittserklärung

Für eine ordentliche Mitgliedschaft gem. § 3 Abs. 1 der GDD-Satzung:

- □ Firmenmitgliedschaft
- □ Anzahl der Beschäftigten: .....
- □ Persönliche Mitgliedschaft (nur Privatpersonen)
- □ Persönliche Mitgliedschaft als betrieblicher Datenschutzbeauftragter

Firma: .....

Name: .....

Straße/Ort: .....

Abteilung/Branche: .....

Telefon-/Fax-Nr.: .....

E-Mail: .....

Wie wurden Sie auf die GDD aufmerksam? .....

Mit der Aufnahme meiner Daten in die offizielle Mitgliederliste erkläre ich mich

□ einverstanden □ nicht einverstanden

.....
Datum und Unterschrift

Wir verarbeiten Ihre Daten zu Ihrer Betreuung im Rahmen der Mitgliedschaft, ggf. auch unter Einsatz von Dienstleistern. Darüber hinaus geben wir Ihre Adressdaten an unseren Kooperationspartner Verlagsgruppe Hüthig Jehle Rehm GmbH - Datakontext - weiter, um Sie über Produkte und Fachveranstaltungen zum Thema Datenschutz und IT-Sicherheit zu informieren. Der Verwendung Ihrer Daten zu Werbezwecken können Sie jederzeit bei uns widersprechen.

Notizen

Notizen

Wie Sie noch mehr erfahren

Gesellschaft für Datenschutz und Datensicherheit e.V.

Heinrich-Böll-Ring 10
53119 Bonn
Telefon (0228) 96 96 75 00
Telefax (0228) 96 96 75 25
E-Mail: info@gdd.de
Internet: www.gdd.de

>> GDD-Support für Wirtschaft, Verwaltung, Wissenschaft und Politik

Die GDD tritt für die Prinzipien der Selbstkontrolle und Selbstregulierung auf dem Gebiet des Datenschutzes ein. Sie unterstützt die politische Willensbildung durch fachlichen Rat.

Bei der Umsetzung der datenschutzrechtlichen Vorgaben bietet die GDD folgende Leistungen:

- >> Beratung in Einzelfragen
- >> Schulungen und Praktikerforen
- >> Online-Datenbanken, u.a.:
  GDD-Rechtsprechungsarchiv
  GDD-Literaturarchiv
- >> GDD-Praxis-Ratgeber
- >> Fachzeitschrift „Recht der Datenverarbeitung (RDV)"
- >> Fachpublikationen
- >> Erfahrungsaustausch

Gesellschaft für Datenschutz und Datensicherheit e.V.