Der iT Rechts-Berater

Informationsdienst
für die EDV-, Multimedia-
und TK-rechtliche
Beratungspraxis

Informationspflichten bei Data Breach

§ 42a BDSG: Handhabung in der Praxis

von Dr. Michael Karger

Vorabdruck aus ITRB 7/2010

Verlag Dr. Otto Schmidt • www.itrb.de

Informationspflichten bei Data Breach

§ 42a BDSG: Handhabung in der Praxis

*von Dr. Michael Karger**

„Data Breaches“, „Identity Theft“ und ähnliche Datenschutzverstöße sind in den meisten US-Bundesstaaten schon lange meldepflichtig und gelangen auf diese Weise rasch in die Schlagzeilen. Deutschland hat entsprechende Informationspflichten erst im September 2009 eingeführt. Der neue § 42a BDSG sorgt für Unsicherheit, wie im Ernstfall mit einer Datenpanne umzugehen ist. Im Folgenden soll auf Einzelfragen in Verbindung mit § 42a BDSG (I.) eingegangen und kurz auf europarechtliche (II.) und internationale Aspekte (III.) hingewiesen werden. Den Abschluss bilden einige praktische Hinweise zum vorbeugenden „Data Breach Notification Management“(IV).

I. Gesetzliche Informationspflichten

1. Rechtsgrundlagen

Die neue Informationspflicht ist in drei Gesetzen geregelt: § 42a BDSG, § 15 TMG und § 93 Abs. 3 TKG. Hierbei ist § 42a BDSG die „Grundnorm“, auf die in § 15a TMG bzw. § 93 Abs. 3 TKG verwiesen wird. Festzuhalten bleibt damit, dass die Informationspflicht auch explizit im Bereich der Telemedien- und der Telekommunikationsdienste gilt.

2. Sanktionen

Datenschutzrechtliche Verpflichtungen interessieren die betroffenen Unternehmen in erster Linie im Hinblick auf die Rechtsfolgen: Welche Konsequenzen kann ein Rechtsverstoß nach sich ziehen? Bislang wurde das Datenschutzrecht häufig deshalb ignoriert, weil die rechtlichen Konsequenzen eines Verstoßes nicht gravierend waren. Insbesondere waren nur geringe Bußgelder vorgesehen. Dies hat sich mit der BDSG-Novelle II jedoch deutlich geändert. Bei einem Verstoß gegen die Informationspflicht des § 42a BDSG droht gem. § 43 Abs. 2 Nr. 7 i.V.m. § 43 Abs. 3 BDSG eine Geldbuße von **bis zu 300.000 €**. Dieser Betrag kann auch überschritten werden, wenn der Täter aus dem Verstoß einen diesen Betrag übersteigenden wirtschaftlichen Vorteil gezogen hat.

3. Verpflichtete Stellen

Die Informationspflicht trifft nicht-öffentliche Stellen i.S.v. § 2 Abs. 4 BDSG, also **Privatunternehmen,** sowie öffentlich-rechtliche Wettbewerbsunternehmen i.S.v. § 27 Abs. 1 BDSG. Sonstige öffentliche Stellen sind nicht verpflichtet.

Unklar ist, ob die Verpflichtung auch **Auftragsdatenverarbeiter** i.S.v. § 11 BDSG erfasst. Relevant ist dies insbesondere für Outsourcing- oder ASP-Provider oder Unternehmen, die Fernwartung erbringen. Eine eigenständige, vom jeweiligen Auftraggeber unabhängige In-

* RA, FA IT-Recht, FA VerwR Dr. Michael Karger ist Partner der Kanzlei Wendler Tremml, München.

formationspflicht für Auftragsdatenverarbeiter ist wohl zu verneinen.[1] Demgemäß ist bei Auftragsdatenverarbeitung **zweistufig** zu verfahren: Der Auftragnehmer teilt dem Auftraggeber den Datenschutzverstoß mit. Die Verpflichtung hierzu ergibt sich aus § 11 Abs. 2 Nr. 8 BDSG. Der Auftraggeber hat aufgrund der mitgeteilten Tatsachen dann seiner Informationspflicht nach § 42a BDSG nachzukommen.

4. Betroffene Daten

Die Informationspflicht nach § 42a BDSG erstreckt sich nicht auf alle Datenpannen bzw. personenbezogene Daten schlechthin, sondern nur auf **bestimmte personenbezogene Daten**. Erfasst werden vier Kategorien:

- besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG), u.a. Angaben über ethnische Herkunft, politische Meinungen, religiöse Überzeugungen und Gesundheit;
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen;
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder einen diesbezüglichen Verdacht beziehen;
- personenbezogene Daten zu Bank- und Kreditkartenkonten.

5. Mitteilungspflichtige Umstände

Die Informationspflicht besteht, wenn die bezeichneten Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen für die Rechte oder schutzfähigen Interessen der Betroffenen drohen.

a) Unrechtmäßige Kenntnisnahme Dritter

Eine unrechtmäßige Kenntnisnahme Dritter liegt vor, wenn sie weder durch Rechtsvorschrift noch durch Einwilligung gedeckt ist. In diesem Zusammenhang sind also alle einschlägigen gesetzlichen Erlaubnistatbestände und gegebenenfalls vorliegende Einwilligungen zu überprüfen.

Für die Feststellung einer unrechtmäßigen Übermittlung oder Kenntnisnahme Dritter bedarf es keiner absoluten Gewissheit, vielmehr entsteht die Informationspflicht bereits dann, wenn **tatsächliche Anhaltspunkte** vorliegen.[2] Demgegenüber sind bloße Vermutungen unerheblich.[3] Ob hingegen fahrlässige Unkenntnis der Informationspflicht entgegensteht,[4] erscheint jedenfalls bei grober Fahrlässigkeit zweifelhaft.

b) Schwerwiegende Beeinträchtigung

Ob eine „schwerwiegende Beeinträchtigung“ droht, ist anhand von objektiven Kriterien und einer **Gefahren-**

---

[1] *Duisberg/Picot*, CR 2009, 823 (825); *Gabe*, BB 2009, 245 (246).

[2] *Gabe*, BB 2009, 245 (247).

[3] *Gabe*, BB 2009, 245 (247).

[4] So jedenfalls *Gabe*, BB 2009, 245 (247).

prognose zu beurteilen. Mit abstrakten Kriterien können die verantwortlichen Entscheidungsträger meist nur wenig anfangen. Allgemein wird man sagen können, dass alle in § 42a BDSG genannten Kategorien von Daten gerade deshalb besonders schutzwürdig sind, weil ihr Missbrauch für den Betroffenen besonders gravierende Konsequenzen haben kann. Im Zweifelsfall ist deshalb davon auszugehen, dass eine schwerwiegende Beeinträchtigung jedenfalls dann droht, wenn die Daten der breiten Öffentlichkeit oder einer unübersehbaren Anzahl von Dritten zugänglich gemacht werden. Bei Daten zu Bankkonten und Kreditkartenkonten wird angesichts des verbreiteten Missbrauchs und der wirtschaftlichen Schäden eine schwerwiegende Beeinträchtigung im Regelfall als gegeben anzusehen sein. Insgesamt wird hinsichtlich des Kriteriums der schwerwiegenden Beeinträchtigung von niedrigen Anforderungen auszugehen sein.[5]

6. Adressaten der Information

Bei der Benachrichtigung ist gem. § 42a BDSG eine **gestufte Reihenfolge** zu beachten: Zuerst ist die Aufsichtsbehörde und dann erst der Betroffene zu informieren.

Die Information hat jeweils unverzüglich zu erfolgen, die Benachrichtigung des Betroffenen allerdings erst dann, wenn angemessene Maßnahmen zur Sicherung der Daten ergriffen worden sind und ggf. eine Strafverfolgung nicht mehr gefährdet ist. Der „Zeitpuffer“ im Hinblick auf die Benachrichtigung des Betroffenen bezweckt, dass zunächst bestehende Sicherheitslücken analysiert und geschlossen werden können und einer erneuten Ausnutzung der bestehenden Lücke durch Dritte vorgebeugt wird.[6]

Da Entscheidungsträger im Ernstfall unter hohem Zeitdruck stehen, kommt der Frage, was in diesem Zusammenhang eine **unverzügliche Information** ist, entscheidende Bedeutung zu. Unverzüglich ist ein Handeln ohne schuldhaftes Zögern (§ 121 Abs. 1 Satz 1 BGB). Dem Benachrichtigungspflichtigen ist eine nach den Umständen des Einzelfalls zu bemessende Prüfungs- und Überlegungsfrist zuzubilligen. Dies schließt die Möglichkeit ein, rechtlichen Rat einzuholen.[7] Dies ist in entsprechenden Fällen angesichts der Konsequenzen einer unrichtigen oder unvollständige Mitteilung (§ 43 Abs. 2 Nr. 7, Abs. 3 BDSG) in jedem Fall geboten.

Welche Fristen im Einzelnen zu wahren sind, kann nicht generell gesagt werden. Da aufgrund der gestuften Vorgehensweise ohnehin zunächst die Aufsichtsbehörde zu informieren ist, empfiehlt es sich, in Zweifelsfällen relativ rasch mit der Behörde in Kontakt zu treten, zumal diese auch die Aufgabe hat, die verantwortlichen Stellen zu **beraten und zu unterstützen** (§ 38 Abs. 1 BDSG).

---

[5] *Duisberg/ Picot*, CR 2009, 823 (824).

[6] *Gabe*, BB 2009, 245 (248).

[7] *Gabe*, BB 2009, 245 (248).

7. Inhalt der Information

Behörde und Betroffener sind über die **Art** der unrechtmäßigen Kenntniserlangung zu unterrichten. In diesem Zusammenhang sind also die konkret aufgetretenen Pannen wie z.B. Pflichtverletzung durch einen Mitarbeiter oder einen externen Dienstleister oder der Verlust von Datenträgern aufzudecken.

Des Weiteren müssen dem Betroffenen **Empfehlungen** gegeben werden, wie er nachteilige Folgen mindern kann, z.B. durch Änderung der Log-In-Daten und Passwörter etc.

Die Behörde ist darüber hinaus über mögliche nachteilige **Folgen** und zwischenzeitlich ergriffene Maßnahmen zu informieren.

8. Form der Benachrichtigung

Das Gesetz gibt keine besondere Form vor. Jedoch ist grundsätzlich zu empfehlen, die entsprechenden Informationen **schriftlich** bzw. jedenfalls in nachweisbarer Form mitzuteilen.

Sofern es eine Vielzahl von Betroffenen gibt, deren individuelle Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde, muss nicht jeder der Betroffenen einzeln benachrichtigt werden. Stattdessen kann die individuelle Benachrichtigung durch die Information der Öffentlichkeit mittels Anzeigen in mindestens zwei bundesweit erscheinenden Tageszeitungen oder durch gleich geeignete Maßnahmen ersetzt werden.

9. Selbstbezichtigung

Bei Datenpannen sieht sich das Unternehmen typischerweise in einer rechtlichen „Zwickmühle“: Kommt es seiner Informationspflicht nicht oder nicht ausreichend nach, so erfüllt es den Bußgeldtatbestand des § 43 BDSG. Informiert es hingegen pflichtgemäß, so werden Umstände dokumentiert, die die Grundlage einer strafrechtlichen oder einer zivilrechtlichen Haftung bilden können.

a) Strafrechtliche Verfolgung

Im Hinblick auf eine Strafverfolgung sieht § 42a Abs. 6 BDSG ein Verwendungsverbot für Straf- und Ordnungswidrigkeitenverfahren vor. Die Benachrichtigung darf nur mit Zustimmung des Benachrichtigungspflichtigen verwendet werden. Aus strafrechtlicher Sicht kann sich deshalb eine rasche und umfassende Information u.U. anbieten, da dann die Chance besteht, einer Strafverfolgung zu entgehen.

b) Zivilrechtliche Haftung

Zivilrechtliche Schadensersatzansprüche sind hingegen nicht von einem Verwendungsverbot betroffen. Das Unternehmen liefert dem Betroffenen mit der Information die erforderlichen Beweise zur Geltendmachung von Schadensersatzansprüchen nach § 7 BDSG.[8] Der Anspruch aus § 7 BDSG ist auf den Ersatz des materiellen Schadens beschränkt. Allerdings sind bei Datenschutz-

[8] Weiterführend *Bierekoven*, ITRB 2010, 88.

verletzungen stets auch das allgemeine Persönlichkeitsrecht sowie die mit Drittwirkung versehenen Grundrechtspositionen aus Art 2 GG tangiert, so dass auch Schadensersatzansprüche nach § 823 Abs. 1 BGB in Betracht kommen, die auch den Ersatz des immateriellen Schadens einschließen.[9] Darüber hinaus kommt auch § 823 Abs. 2 BGB als Anspruchsgrundlage in Betracht.[10]

II. EU-Datenschutzrichtlinie für elektronische Kommunikation

Die §§ 42a BDSG, 93 Abs. 3 TKG und § 15a TMG sind bereits wieder **novellierungsbedürftig**. Grund hierfür ist die geänderte Datenschutzrichtlinie für elektronische Kommunikation (RL 2002/58/EG). Die Änderungen sind bis zum 25.5.2011 in nationales Recht umzusetzen. Allerdings betreffen die anstehenden Änderungen primär den Bereich der Telekommunikationsdienste.[11]

III. Datenpannen mit internationaler Auswirkung

Bei Datenpannen in multinationalen Unternehmen oder im Internetbereich ist neben dem deutschen Datenschutzrecht auch das Recht anderer Staaten zu beachten. Sind etwa die USA tangiert, müssen die dortigen Security Breach Notification Laws beachtet werden. Dies kann deshalb zu großen praktischen Problemen führen, weil es sich hierbei um Gesetze der Einzelstaaten handelt, die untereinander nicht synchronisiert sind. In der Praxis müssen deshalb oft die Vorschriften aller betroffenen Bundesstaaten geprüft werden, was zu einem extrem hohen Zeit- und Kostenaufwand führen kann.[12]

IV. Data Breach Notification Management

Angesichts der gesetzlichen Verpflichtungen sollte jedes Unternahmen jedenfalls in Grundzügen auf eine Data Breach-Situation vorbereitet sein.[13] Hierbei empfehlen sich folgende **Vorkehrungen**, die für sich gesehen banal erscheinen mögen, aber in der Praxis alles andere als selbstverständlich sind:

- Information der Entscheidungsträger einschließlich des Datenschutzbeauftragten und des Compliance-Beauftragten über die Pflichten nach § 42a BDSG;
- Bestimmung der/des für die Formulierung und Herausgabe der Information Verantwortlichen;
- Identifikation, welche der unter § 42a BDSG fallenden Daten im Unternehmen wo und wie gehalten werden;
- Instruktion von Mitarbeitern im Hinblick auf die sofortige Meldung von Datenpannen an die verantwortlichen Personen;

---

[9] Vgl. *Karger*, in Conrad (Hrsg.), Inseln der Vernunft, Liber Amicorum für Jochen Schneider, 159 ff.

[10] *Duisberg/Picot*, CR 2009, 823 (825).

[11] Weiterführend hierzu *Hanloser*, MMR 2010, 300 ff.

[12] Weiterführend hierzu *Spies*, MMR 2008, XIX; *Duisberg/Picot*, CR 2009, 823 (826 f.).

[13] Vgl. auch *Bierekoven*, ITRB 2010, 88 (89).

- Verpflichtung der Auftragsdatenverarbeiter zur sofortigen Meldung von Datenpannen an die Verantwortlichen;
- Sicherstellung von schnell verfügbarem Rechtsrat im Hinblick auf Datenschutzrecht, Strafrecht und zivilrechtliche Haftung;
- Organisation der Datenbestände zur schnellen Ermittlung von Betroffenen;
- Identifikation der gegebenenfalls zuständigen Aufsichtsbehörde(n);
- Koordination der jeweils national Verantwortlichen im internationalen Konzern;
- Organisation eines begleitenden Public Relation-Krisenmanagements.