„Datenschutzpanne" – was ist zu tun?

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

Bruno Schierbaum // BTQ Niedersachsen

Seit 2009 müssen Unternehmen Datenschutzpannen unverzüglich mitteilen. Und zwar nicht nur der zuständigen Aufsichtsbehörde, sondern vor allem den jeweils von den Pannen Betroffenen. Damit sollen diese bei Datenschutzverletzungen vor möglichen Beeinträchtigungen ihrer Rechte und Interessen besser geschützt und eine effektivere Durchsetzung datenschutzrechtlicher Regelungen erreicht werden. Doch wie sollen in der Praxis diese hehren Ziele des Gesetzgebers umgesetzt werden? Dieser Beitrag klärt auf.

Durch das am 3. Juli 2009 vom Bundestag beschlossene „Gesetz zur Änderung datenschutzrechtlicher Vorschriften" wurde der § 42a in das Bundesdatenschutzgesetz (BDSG) aufgenommen. Diese neue Vorschrift enthält besondere Informationspflichten bei unrechtmäßiger Kenntniserlangung von personenbezogenen Daten durch Dritte. Die Informationspflicht soll gegenüber dem Betroffenen selbst und der Aufsichtsbehörde gewährleistet werden. Der § 42a BDSG ist zum 1. September 2009 in Kraft getreten.

Die Regelung ist angelehnt an einen Vorschlag der Europäischen Kommission zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.[1] Sie orientiert sich auch an vergleichbaren Vorschriften in den Vereinigten Staaten, wo es auf Bundesstaatenebene eine Vielzahl von sogenannten „Security Breach Laws" (deutsch: „Sicherheits-Verstoß-Gesetze") gibt.[2]

Parallelregelungen sind in den §§ 93 Abs. 3 Telekommunikationsgesetz (TKG) und 15a Telemediengesetz (TMG) enthalten. Ziel des § 42a BDSG ist es, die Betroffenen bei Datenschutzverletzungen vor möglichen Beeinträchtigungen ihrer Rechte und Interessen zu schützen sowie für eine effektivere Durchsetzung datenschutzrechtlicher Regelungen zu sorgen – so die Gesetzesbegründung.[3] Die Regelung des § 42a BDSG gilt auch für Beschäftigtendaten.[4]

Anwendungsbereich des § 42a BDSG

Die in § 42a BDSG verankerte Informationspflicht gilt für nicht-öffentliche Stellen – also insbesondere Unternehmen der Privatwirtschaft – und ihnen datenschutzrechtlich gleichgestellten öffentlich-rechtlichen Wettbewerbsunternehmen. Mit öffentlich-rechtlichen Wettbewerbsunternehmen sind Einrichtungen des Bundes gemeint, die am Wettbewerb teilnehmen, wie z.B. Einrichtungen/Behörden aus den Bereichen der Kredit- und Versicherungswirtschaft. Andere öffentliche Stellen haben den § 42a BDSG nicht anzuwenden. Ein Grund dafür ist nicht ersichtlich, da auch ähnliche Datenschutzverletzungen bei öffentlichen Stellen auftreten können.[5]

Informationspflicht nur bei bestimmten Daten

Die Informationspflicht besteht jedoch nur hinsichtlich bestimmter Arten personenbezogener Daten, die vom Gesetzgeber als besonders sensibel angesehen werden. Man bezeichnet diese Daten auch als „Risikodaten".[6] Diese Daten sind in § 42a BDSG abschließend aufgelistet. Es handelt sich hierbei um

- besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG,
- personenbezogene Daten, die einem Berufsgeheimnis unterliegen,
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder einen entsprechenden Verdacht beziehen,
- personenbezogene Daten zu Bank- oder Kreditkartenkonten.

In Bezug auf Kunden, Patienten, Klienten usw. werden entsprechende Daten in Unternehmen, wie in Krankenhäusern, in Arztpraxen, bei Banken, bei Versicherungen oder in Anwaltskanzleien erhoben, verarbeitet, übermittelt oder sonst genutzt. Aber auch hinsichtlich der im Unternehmen verarbeiteten Daten der Beschäftigten fallen entsprechende „Risikodaten" an.

Denn „besondere Arten personenbezogener Daten" sind nach § 3 Abs. 9 BDSG Angaben über

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder philosophische Überzeugungen,
- Gewerkschaftszugehörigkeit,
- Gesundheit oder Sexualleben.

Zu diesen Daten gehören also Gesundheitsdaten von Beschäftigten, die durch den Betriebsarzt erhoben oder verarbeitet werden oder auch Arbeitsunfähigkeitsbescheinigungen, die der Beschäftigte bei Krankheiten an den Arbeitgeber weitergeben muss.

Zu diesen Daten zählen aber auch Mitgliedschaft oder Nichtmitgliedschaft in Kirchen, die im Beschäftigungsverhältnis im Rahmen der Lohn- und Gehaltsabrechnung verarbeitet werden.

Bei Daten, die einem „Berufsgeheimnis" unterliegen, geht es unter anderem um die in § 203 Strafgesetzbuch (StGB) verankerte sogenannte „ärztliche Schweigepflicht", die eigentlich mit „Verletzung von Privatgeheimnissen" überschrieben ist. Das sind Daten, die der Betriebsarzt über Beschäftigte vorhält. Es sind aber auch Daten, die andere

Berufsgruppen, die in § 203 StGB genannt werden, über Klienten/Beschäftigte vorhalten. Das können Pädagogen oder Psychologen sein.

Daten über „strafbare Handlungen oder Ordnungswidrigkeiten" können hinsichtlich der Beschäftigten erhoben bzw. gespeichert werden, wenn der Arbeitgeber im Rahmen des Bewerbungsverfahrens rechtmäßigerweise nach sogenannten einschlägigen Vorstrafen fragen darf. Bei Benutzung von Firmenfahrzeugen gelangen die Strafzettel in der Regel auch an den Arbeitgeber.[7] Daten zu „Bank- und Kreditkartenkonten" sind für jeden Arbeitnehmer in der Lohnbuchhaltung vorhanden.

Unrechtmäßige Übermittlung – unrechtmäßige Kenntniserlangung

Die Informationspflicht knüpft an der Feststellung der verantwortlichen Stelle an, dass bei ihr gespeicherte Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten, das heißt Personen oder Stellen außerhalb der verantwortlichen Stelle, unrechtmäßig zur Kenntnis gelangt sind.

Übermitteln von Daten ist das Bekanntgeben gespeicherter Daten oder durch Datenverarbeitung gewonnener personenbezogener Daten in der Weise, dass die Daten an einen Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft (§ 3 Abs. 4 Nr. 3 BDSG).

Werden personenbezogene Daten übermittelt, ohne dass die rechtlichen Voraussetzungen nach § 4 BDSG gegeben sind, kann dies eine Informationspflicht nach § 42a BDSG auslösen. Denn Daten dürfen nur verarbeitet oder auch übermittelt werden, wenn

- das BDSG selbst dies vorsieht (z. B. gemäß § 32 BDSG),
- eine andere Rechtsvorschrift dies erlaubt oder anordnet oder
- der Betroffene eingewilligt hat.

„Unrechtmäßige Kenntniserlangung durch Dritte" umfasst all die Fälle, in denen Daten ohne oder gegen den Willen der verantwortlichen Stelle an Dritte gelangen. Dieses kann durch unbefugten Zugriff auf Daten durch einen Dritten von Außen geschehen oder in der Form, dass ein ein-

§ 42 A BUNDESDATENSCHUTZGESETZ (BDSG)

Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten

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. 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. Die Benachrichtigung der Betroffenen muss eine Darlegung der Art der unrechtmäßigen Kenntniserlangung und Empfehlungen für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Die Benachrichtigung der zuständigen Aufsichtsbehörde muss zusätzlich eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung und der von der Stelle daraufhin ergriffenen Maßnahmen enthalten. 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. 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.

§ 93 ABS. 3 TELEKOMMUNIKATIONSGESETZ (TKG)

Informationspflichten

(3) Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestandsdaten oder Verkehrsdaten 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 § 42 a des Bundesdatenschutzgesetzes entsprechend.

§ 15 A TELEMEDIENGESETZ (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 § 42 a des Bundesdatenschutzgesetzes entsprechend.

zelner Mitarbeiter die Daten unbefugt an Dritte weitergibt.

Schwerwiegende Beeinträchtigungen

Die Kenntniserlangung durch Dritte ist für sich genommen nicht ausreichend, um eine Informationspflicht nach § 42a BDSG zu begründen. Eine Informationspflicht kommt nur dann zum Tragen, wenn schwerwiegende Beeinträchtigungen für die Rechte oder schützwürdigen Interessen der Beschäftigten drohen. Die Gefahr für die Beeinträchtigung bestimmt sich unter anderem nach der Art der betroffenen Daten und den möglichen Auswirkungen für den Betroffenen.

Der Begriff „schwerwiegende Beeinträchtigung" wirft Auslegungsschwierigkeiten auf. Deshalb wird empfohlen, dass die verantwortliche Stelle im Zweifelsfall die Aufsichtbehörde hinzuzieht, bevor sie eine Informationspflicht gegenüber dem Betroffenen unterlässt.[8]

Aber nach allen bekannt gewordenen Datenschutzskandalen wird sehr wahrscheinlich dieser unbestimmte Rechtsbegriff „schwerwiegende Beeinträchtigungen" zur Folge haben, dass – auch bei gutem Willen des Gesetzgebers – in der Praxis alles „beim Alten bleibt". Denn die schwerwiegenden Beeinträchtigungen werden durch die verantwortliche Stelle – das Unternehmen – selbst festgestellt.

Informationspflicht gegenüber dem Betroffenen und der Aufsichtsbehörde

Die Vorschrift schreibt die Information gegenüber zwei Adressaten vor, nämlich dem Betroffenen sowie der zuständigen Aufsichtsbehörde.

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. Die Information des Betroffenen muss mindestens folgenden Inhalt haben:

- eine Darlegung möglicher nachteiliger Folgen der unrechtmäßigen Kenntniserlangung,
- Empfehlungen für den Betroffenen, welche Maßnahmen er zur Minderung möglicher Nachteile ergreifen kann.

Der Inhalt wird je nach Empfänger variieren, das heißt die Benachrichtigung muss vom Empfänger/Betroffenen verstanden werden können. Im Idealfall erhält der Betroffene über diesen Weg die Möglichkeit, sich selbst vor möglichen Schäden zu sichern.[9]

Im Gegensatz zur Benachrichtigung des Betroffenen muss die Benachrichtigung der zuständigen Aufsichtsbehörde ohne weitergehende Einschränkungen unverzüglich erfolgen. Zudem müssen der zuständigen Aufsichtsbehörde die möglichen Folgen der unrechtmäßigen Kenntniserlangung und die von der Stelle daraufhin ergriffenen Maßnahmen mitgeteilt werden.

Information über die Tagespresse

Erfordert die Benachrichtigung der von einer Datenschutzpanne Betroffenen einen unverhältnismäßigen Aufwand, kann eine Information durch eine Anzeige in der Tagespresse erfolgen. Ein unverhältnismäßiger Aufwand kann unter anderem durch einen hohen Aufwand an Zeit und Kosten entstehen, wenn z. B. die Adressdaten der Betroffenen erst ermittelt werden müssen.

Anstelle der direkten Information der Betroffenen tritt eine Information der Öffentlichkeit. Das muss durch Schalten von halbseitigen Anzeigen in mindestens zwei bundesweit erscheinenden Tageszeitungen geschehen.

Datenschützer und Belegschaftsvertretung sind einzubinden

Der interne Datenschutzbeauftragte hat auf die Einhaltung des BDSG hinzuwirken. Daher wird er in das Verfahren bei Datenschutzpannen eingebunden werden müssen. Es kann aber auch sein, dass der Datenschutzbeauftragte die Datenschutzpanne entdeckt, diese an die Geschäftsleitung weiterleitet und somit von Anfang an beteiligt ist.

Da ein Betriebsrat die Einhaltung des BDSG zu überwachen hat (§ 80 Abs 1 Nr. 1 BetrVG), wird der Arbeitgeber die Interessenvertretung nach § 80 Abs. 2 BetrVG informieren müssen. Dies gilt jedenfalls dann, wenn Beschäftigte bei Datenschutzpannen betroffen sind. Im Einzelfall können je nach eingesetzter Technik auch weitergehende Mitbestimmungsrechte zur Anwendung kommen.

„Da ein Betriebsrat die Einhaltung des BDSG zu überwachen hat, wird der Arbeitgeber die Interessenvertretung nach § 80 Abs. 2 BetrVG informieren müssen."

Autor

Bruno Schierbaum, BTQ Niedersachsen GmbH, Donnerschweer Straße 84, 26123 Oldenburg, fon 0441 82068, schierbaum@btq.de, www.btq.de

Fußnoten

1 KOM (2007) 698 endg.
2 Vgl. Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Auflage, § 42a Rn. 1; Taeger/Gabel (Hg.), BDSG, 1. Auflage, § 42a Rn. 1; Gola/Schomerus, BDSG, 10. Auflage, § 42a Rn. 1; Greß, Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten (§ 42a BDSG), 3, in: Kongehl (Hg.), Datenschutz-Management, Loseblatt
3 BT-Drs. 16/12011, S. 73.
4 Vgl. Gola, Information über Datenschutzpannen auch gegenüber Arbeitnehmern, in: CuA 2/2010, 33 f.
5 Vgl. Taeger/Gabel (Hg.), aaO., § 42a Rn. 10
6 Vgl. Taeger/Gabel (Hg.), aaO., § 42a Rn. 11
7 Vgl. Ehmann, Die neue Informationspflicht bei Datenschutzverstößen, in: Datenschutz Praxis, 12/2009, 14
8 So Weichert, aaO., § 42a Rn. 6
9 Vgl. Taeger/Gabel (Hrsg), aaO., § 42a Rn. 24