

September 2009

WHITE PAPER

Rechtsfolgen von Pannen
in der Datensicherheit



I. Executive Summary

Dieses White Paper betrachtet die wichtigsten Rechtsfolgen von Sicherheitspannen, in deren Folge personenbezogene Daten oder vertrauliche Unternehmensdaten für Außenstehende zugänglich werden oder sogar an die Öffentlichkeit gelangen. Als "Sicherheitspanne" werden dabei gleichermaßen von außen veranlasste Eingriffe verstanden wie auch nicht erkannte oder sogar durch Mitarbeiter verschuldete "undichte" Stellen im Unternehmen selbst, die typischerweise auf unzureichende Datensicherheitsmaßnahmen zurückgehen.

Unter den Stichworten "security breach", "data leakage" und "notification requirements" wurden bisher vor allem Benachrichtigungspflichten aufgrund US-amerikanischen Rechts diskutiert, die sich auch für europäische Unternehmen im Falle von Sicherheitslecks im Umgang mit personenbezogenen Daten ergeben können.

Benachrichtigungspflichten im Falle von Sicherheitspannen können sich neuerdings aber auch aus dem deutschen Datenschutzrecht ergeben. Aufgrund einer Gesetzesänderung zum 1. September 2009 verpflichtet das Bundesdatenschutzgesetz (BDSG) Unternehmen, bei denen eine Sicherheitspanne eintritt, unter bestimmten Voraussetzungen nunmehr zur umfassenden Benachrichtigung sowohl der zuständigen Datenschutzbehörde als auch der natürlichen Personen, deren Daten von der Sicherheitspanne betroffen sind. Auch auf der Ebene der EU werden Benachrichtigungspflichten im Falle von Sicherheitspannen im Rahmen der Überarbeitung der Datenschutzrichtlinie für elektronische Kommunikation konkret diskutiert.

Sicherheitspannen können darüber hinaus weitere gesetzliche Rechtsfolgen auslösen wie etwa eine Haftung des Managements oder den Verlust des wettbewerbsrechtlichen Know-How-Schutzes ungewollt bekannt gewordener Betriebs- oder Geschäftsgeheimnisse. Auch vertragliche Rechtsfolgen wegen des Verstoßes gegen Vertraulichkeitsvereinbarungen (NDA) sind denkbar.

Im Ergebnis lässt sich festhalten, dass die rechtlichen Anforderungen an die Datensicherheit sowohl im Umgang mit Sicherheitspannen als auch – damit verbunden – in der Prävention unübersehbar ansteigen und sich jedes Unternehmen darauf einrichten muss, seine Vorkehrungen und Prozesse im Bereich der Datensicherheit zu überprüfen und erforderlichenfalls zu verbessern.

II. Nationales Datenschutzrecht

1. Benachrichtigungspflichten gemäß § 42 a BDSG

1.1 Regelungsinhalt

Zum 1. September 2009 ist eine Neuregelung des Bundesdatenschutzgesetzes (BDSG) in Kraft getreten, die Unternehmen dazu verpflichtet, bei bestimmten Arten von Sicherheitspannen sowohl die zuständige Datenschutzbehörde als auch die natürlichen Personen zu informieren, deren Daten von der Sicherheitspanne betroffen sind.

(a) Voraussetzungen einer Benachrichtigungspflicht

Die Benachrichtigungspflicht besteht nach dem Gesetzeswortlaut immer dann, wenn bestimmte Arten personenbezogener Daten unrechtmäßig übermittelt oder auf sonstige Weise einem Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende

Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der betroffenen natürlichen Personen ("Betroffene") drohen.

Die Regelung greift, sofern eine Sicherheitspanne personenbezogene Daten zumindest einer der folgenden Arten betrifft:

- (i) sog. "besondere Arten personenbezogener Daten", d.h. Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben (vgl. § 3 IX BDSG);
- (ii) personenbezogene Daten zu Bank- oder Kreditkartenkonten;
- (iii) personenbezogene Daten, die einem Berufsgeheimnis unterliegen, also zum Beispiel Daten über natürliche Personen, die bei einer Versicherung, Wirtschaftsprüfungs- oder Steuerberatungsgesellschaft, einem Arzt, Apotheker oder Rechtsanwalt in Ausübung deren beruflicher Tätigkeit erhoben und gespeichert werden;
- (iv) personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen.

Es bleibt abzuwarten, welche Bedeutung die unbestimmte gesetzliche Voraussetzung einer drohenden "schwerwiegenden Rechts- bzw. Interessenbeeinträchtigung der Betroffenen" in der praktischen Rechtsanwendung erlangen wird. Nach der Gesetzesbegründung der Bundesregierung soll die Entstehung einer Benachrichtigungspflicht letztlich von der Art der betroffenen Daten und den potenziellen Auswirkungen der unrechtmäßigen Kenntniserlangung durch Dritte (z.B. materielle Schäden bei Kreditkarteninformationen oder soziale Nachteile einschließlich des Identitätsbetrugs) abhängen. Nach Ansicht des Bundesrats, dessen Stellungnahme die Bundesregierung allerdings letztlich nicht gefolgt ist, begründet dagegen jede Sicherheitspanne, die personenbezogene Daten einer der oben genannten Kategorien betrifft, in der Regel *per se* eine Missbrauchsgefahr zu Lasten der Betroffenen, so dass es der zusätzlichen, positiven Feststellung einer drohenden Beeinträchtigung nicht bedarf.

Angesichts der Unbestimmtheit des Begriffs der drohenden schwerwiegenden Rechts- bzw. Interessenbeeinträchtigung wird eine gewisse Rechtsunsicherheit hier zumindest für eine Anfangsphase letztlich nicht zu vermeiden sein. Unternehmen, die personenbezogene Daten zumindest einer der oben beschriebenen Kategorien speichern, müssen im Fall einer (auch) diese Daten betreffenden Datenpanne fortan im Rahmen einer Prognoseentscheidung anhand aller bekannten objektiven Umstände beurteilen, ob den betroffenen Personen infolge der konkret eingetretenen Datenpanne eine schwerwiegende Rechts- bzw. Interessenbeeinträchtigung droht. Bis es erste Erfahrungswerte mit der Anwendung des § 42a BDSG durch die Datenschutzbehörden gibt, sollten Unternehmen hierbei im Zweifel von eher niedrigen Anforderungen an das Kriterium der schwerwiegenden Rechts- bzw. Interessenbeeinträchtigung ausgehen.

(b) *Umfang und Inhalt der Benachrichtigungspflicht*

Die Benachrichtigungspflicht gilt sowohl gegenüber der zuständigen Datenschutzbehörde als auch gegenüber jeder einzelnen Person, deren Daten von der Sicherheitspanne betroffen sind. Die Benachrichtigung muss grundsätzlich unverzüglich, d.h. ohne schuldhaftes Zögern, erfolgen, sobald die Sicherheitspanne dem Unternehmen zur Kenntnis gelangt.

Gegenüber den Betroffenen darf mit der Mitteilung allerdings so lange gewartet werden, bis "angemessene Maßnahmen zur Sicherung der Daten" ergriffen worden sind (bzw. hätten ergriffen werden können) und eine Strafverfolgung der etwaigen Täter durch eine Mitteilung an die Betroffenen nicht mehr gefährdet wird. Das Gesetz trägt hier dem Grundsatz des sog. "Responsible Disclosure" Rechnung, nach dem die Entdeckung einer Software-Sicherheitslücke erst dann öffentlich bekannt gemacht wird, wenn der Hersteller die Gelegenheit zu ihrer Behebung sowie zur Information anderer Kunden hatte.

Der erforderliche Inhalt der Benachrichtigung hängt von ihrem Empfänger ab. Die Benachrichtigung der Betroffenen muss in verständlicher Weise die Art der unrechtmäßigen Kenntniserlangung darlegen sowie eine Empfehlung für Maßnahmen zur Minderung möglicher nachteiliger Folgen enthalten. Gegenüber der Datenschutzbehörde muss das verantwortliche Unternehmen zudem die möglichen nachteiligen Folgen der unrechtmäßigen Kenntniserlangung sowie die daraufhin ergriffenen Maßnahmen darlegen.

Würde die individuelle Benachrichtigung der Betroffenen einen unverhältnismäßigen Aufwand erfordern, insbesondere auch aufgrund der Vielzahl der Betroffenen, so muss das verantwortliche Unternehmen die Sicherheitspanne nicht durch individuelle Benachrichtigungen kommunizieren. An die Stelle individueller Benachrichtigungen tritt in diesem Falle die Mitteilung über Anzeigen von mindestens einer halben Seite in mindestens zwei bundesweit erscheinenden Tageszeitungen. Alternativ kann das verantwortliche Unternehmen die Öffentlichkeit durch eine andere, in ihrer Wirksamkeit hinsichtlich der Information der Betroffenen gleich geeignete Maßnahme informieren. Welche Maßnahme "gleich geeignet" ist, ist anhand des konkreten Falls zu entscheiden. Bei regionaler Eingrenzbarkeit der Betroffenen könnte unter Umständen auch eine Veröffentlichung in einem nur regional erscheinenden Medium ausreichen.

(c) *Rechtsfolgen eines Verstoßes gegen die Benachrichtigungspflichten*

Verstößt ein Unternehmen gegen seine Benachrichtigungspflichten gemäß § 42 a BDSG, indem es eine danach erforderliche Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht, so drohen Geldbußen in Höhe von bis zu EUR 300.000 (vgl. § 43 Abs. 2 Nr. 7, Abs. 3 BDSG). Bei der Bemessung der Höhe der Geldbuße gilt grundsätzlich, dass die verhängte Geldbuße den wirtschaftlichen Vorteil, den das Unternehmen aus der Nichterfüllung seiner Benachrichtigungspflichten gezogen hat, übersteigen soll. Reicht eine Geldbuße in Höhe von EUR 300.000 hierfür nicht aus, so kann dieser Betrag auch überschritten werden (vgl. § 43 Abs. 3 Satz 3 BDSG).

1.2 Bedeutung für die Praxis

Die Neuregelung ist von hoher praktischer Relevanz, da sie beinahe jedes Unternehmen betrifft. Es gibt kaum ein Unternehmen, das weder im operativen Geschäft (etwa Bank- oder Kreditkartendaten von Kunden) noch im Personalbereich (etwa Gesundheitsdaten oder Daten zur Religionszugehörigkeit von Mitarbeitern) personenbezogene Daten zumindest einer der oben genannten Datenkategorien erhebt, speichert und/oder verarbeitet.

Im Falle einer Sicherheitspanne sollte sich daher ab sofort jedes Unternehmen die Frage stellen, ob, wann, mit welchem Inhalt und in welcher Form eine Benachrichtigung der zuständigen Datenschutzbehörde und der Betroffenen erforderlich ist. Angesichts der deutlich gestiegenen öffentlichen Aufmerksamkeit und Sensibilität für Fragen der Datensicherheit dürfte allgemein mit einer strengen Ahndung durch die Datenschutzbehörden zu rechnen sein.

Auch im Rahmen der Gestaltung von Auftragsdatenverarbeitungsverträgen sollte der Umgang mit Sicherheitspannen künftig adressiert werden. Zwar ist – trotz des insoweit nicht eindeutigen Wortlauts des § 42a BDSG – eine originäre Benachrichtigungspflicht für den Auftragsdatenverarbeiter wohl zu verneinen. Der Auftragsdatenverarbeiter sollte jedoch vertraglich dazu verpflichtet werden, den Auftraggeber über alle Sicherheitspannen, die Daten des Auftraggebers betreffen können, unverzüglich zu informieren und den Auftraggeber bei

der Erfüllung von dessen etwaigen Benachrichtigungspflichten bei Bedarf auch darüber hinaus zu unterstützen.

2. Technische und organisatorische Schutzmaßnahmen gemäß § 9 BDSG

2.1 Regelungsinhalt

Gemäß § 9 BDSG sind Unternehmen und andere Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, dazu verpflichtet, die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um die Einhaltung der Regelungen des BDSG zu gewährleisten. Die Datensicherheitsanforderungen des BDSG sind in der Anlage zu § 9 Satz 1 BDSG näher dargestellt. Als verschiedene Aspekte der Datensicherheit sind dort eine den Umständen nach geeignete Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle und Verfügbarkeitskontrolle genannt. Gemäß § 9 Satz 2 BDSG sind Maßnahmen nur dann erforderlich, wenn der mit ihnen verbundene Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Dabei ist davon auszugehen, dass der einem Unternehmen zumutbare Aufwand proportional zur Sensibilität der zu sichernden personenbezogenen Daten steigt. Dies gilt insbesondere hinsichtlich der Sicherung personenbezogener Daten vor einer Einsichtnahme durch Dritte und damit für die Aspekte der Zutritts-, Zugangs-, Zugriffs- und Weitergabekontrolle.

2.2 Zusammenspiel mit betrieblicher Mitbestimmung

Bei der Implementierung technischer Schutzmaßnahmen in einem Unternehmen können betriebliche Mitbestimmungsrechte gemäß § 87 Abs. 1 Nr. 6 des Betriebsverfassungsgesetzes (BetrVG) zu beachten sein. Danach hat der Betriebsrat ein Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Nach der Rechtsprechung ist eine technische Einrichtung bereits dann zur Überwachung "bestimmt", wenn ihre Nutzung zu diesem Zweck lediglich möglich ist. Dies ist der Fall, wenn eine technische Einrichtung leistungs- und/oder verhaltensbezogene Daten der Arbeitnehmer so verarbeitet, dass eine Beurteilung bestimmter Leistungen und/oder Verhaltensweisen ermöglicht wird. Unmaßgeblich ist, ob der Arbeitgeber eine solche Beurteilung ermöglichen möchte und anschließend tatsächlich vornimmt.

Ob eine technische Maßnahme zum Schutz personenbezogener Daten diesen Tatbestand erfüllt, ist im Einzelfall zu prüfen. An die Mitbestimmung ist etwa zu denken, wenn im Rahmen der Zugangskontrolle zu einem Server-Raum, in dem personenbezogene Daten gespeichert sind, eine Beobachtungskamera oder ein biometrisches Fingerabdruck-System eingeführt wird. Auch bei der Einführung von Softwareprogrammen zum Zweck der Weitergabekontrolle kann unter Umständen das Mitbestimmungsrecht eingreifen, wenn die Software zur Überwachung des Verhaltens einzelner Arbeitnehmer geeignet ist. Dies gilt insbesondere etwa dann, wenn die Weitergabekontrolle an den E-mail-Ausgängen der Arbeitnehmer anknüpft und der Arbeitgeber die private Nutzung der dienstlichen E-mail-Accounts zumindest duldet.

2.3 Verstoß gegen die Bildschirmarbeitsverordnung (BildscharbV)

Zu erwähnen ist ferner die wenig bekannte Regelung in Ziffer 22 des Anhangs zur Bildschirmarbeitsverordnung (BildscharbV). Gemäß dieser Regelung dürfen an Bildschirmarbeitsplätzen ohne Kenntnis der Beschäftigten keine Vorrichtungen zur qualitativen oder quantitativen Nutzung des Bildschirmarbeitsplatzes verwendet werden. Der Begriff des Bildschirmarbeitsplatzes umfasst dabei gemäß § 2 Abs. 2 BildscharbV auch die Software, die den Beschäftigten bei der Ausführung ihrer Arbeitsaufgaben zur Verfügung steht.

Eine Monitoring-Software, die die Beschäftigten in der Nutzung der ihnen zur Verfügung gestellten Softwareprogramme kontrolliert, darf folglich nur mit Kenntnis der Beschäftigten eingeführt werden.

2.4 Rechtsfolgen eines Verstoßes

Ein Verstoß gegen § 9 BDSG erfüllt per se noch keinen Bußgeldtatbestand des § 43 BDSG. Die zuständige Datenschutzbehörde kann die Umsetzung der gemäß § 9 BDSG erforderlichen Maßnahmen jedoch überprüfen, ggf. anordnen und unter Verhängung von Zwangsgeldern durchsetzen. Kommt es infolge unzureichender technischer oder organisatorischer Schutzmaßnahmen zu einem unberechtigten Zugriff auf personenbezogene Daten einer der oben unter Ziffer 1.1(a) genannten Kategorien oder werden solche Daten unberechtigt weitergegeben oder auf sonstige Weise von einem Sicherheitsleck betroffen, so greifen zudem die Benachrichtigungspflichten gemäß § 42 a BDSG ein.

3. Haftung von Vorstand, Geschäftsführung und Aufsichtsrat

Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) aus dem Jahr 1998 verpflichtet Vorstände von Aktiengesellschaften sowie die Geschäftsführung großer und mittelgroßer Kapitalgesellschaften zur Einrichtung eines funktionsfähigen IT-Sicherheitssystems. Die Konzeption und Einführung eines solchen IT-Sicherheitssystems ist Teil der allgemeinen Pflicht des Managements zur Einrichtung eines Überwachungssystems, das die frühzeitige Erkennung von Entwicklungen ermöglicht, die den Unternehmensfortbestand gefährden. Diese Pflicht ist für den Vorstand einer Aktiengesellschaft in § 91 Abs. 2 AktG ausdrücklich normiert. Entsprechende Pflichten gelten aber auch für die Geschäftsführung einer GmbH sowie für das Management anderer Kapitalgesellschaften. Der Aufsichtsrat hat die Pflicht, den Vorstand bei der Erfüllung seiner Pflicht zur Einrichtung einer IT-Sicherheitsstruktur zu überwachen (vgl. § 111 Abs. 1 AktG).

Im Rahmen dieses sog. "Business Continuity Management" (BCM) muss ein IT-Risikomanagementsystem eingerichtet werden, bei dessen Konzeption auch weniger offensichtliche Sicherheitsrisiken (etwa ein Fernzugriff auf IT-Systeme im Rahmen der Fernwartung) aufzuspüren und zu berücksichtigen sind.

Geschäftsführer und Vorstände haften gegenüber ihrem Unternehmen persönlich, falls sie ihre Pflicht zur Einführung eines tauglichen IT-Sicherheitssystems verletzen. Sie haben dabei grundsätzlich mit der "Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters" zu handeln. Entsprechendes gilt für den Aufsichtsrat, sofern er seine diesbezüglichen Überwachungspflichten verletzt.

Kommt es in einem Unternehmen zu einer Sicherheitspanne, so sollte das Management nachweisen können, dass es die der Komplexität des Unternehmens angemessene "Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters" angewendet, ein umfassendes IT-Sicherheitssystem eingeführt und auch für dessen regelmäßige Aktualisierung und Beachtung (etwa die Einhaltung von Sicherheitsregeln) gesorgt hat.

4. Verlust des Schutzes betrieblichen Know-hows als Geschäftsgeheimnis (§ 17 UWG)

Sicherheitspannen können dazu führen, dass betriebliches Know-How ungewollt an die Öffentlichkeit gelangt. In rechtlicher Hinsicht kann daraus folgen, dass Know-How den Charakter eines "Betriebs- oder Geschäftsgeheimnisses" und damit den wettbewerbsrechtlichen Know-How-Schutz gemäß § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) verliert.

5. Verstoß gegen vertragliche Vertraulichkeitsvereinbarungen (NDA)

Ein ungewollter Abfluss vertraulicher Informationen im Rahmen einer Sicherheitspanne kann ferner zu vertraglichen Ansprüchen Dritter führen, mit denen das Unternehmen, bei dem die Sicherheitspanne eingetreten ist, eine Vertraulichkeitsvereinbarung (*Non-Disclosure Agreement, NDA*) abgeschlossen hatte. Voraussetzung ist natürlich, dass gerade die von der Sicherheitspanne betroffenen Daten bzw. Informationen von der Vertraulichkeitsvereinbarung umfasst waren. Häufig werden in Vertraulichkeitsvereinbarungen auch Vertragsstrafen für den Fall einer unautorisierten Preisgabe geschützter Informationen an Dritte vereinbart.

Ist die Sicherheitspanne allerdings trotz eines umfassenden IT-Sicherheitssystems eingetreten und kann dem betroffenen Unternehmen ihre fahrlässige Verursachung auch sonst nicht vorgeworfen werden, so sollten sich vertragliche Ansprüche aus einer Vertraulichkeitsvereinbarung jedenfalls insoweit erfolgreich abwehren lassen, wie sie einen schuldhaften Verstoß gegen die Vertraulichkeitsvereinbarung voraussetzen.

Mit Blick auf Vertragsstrafenklauseln ist zu beachten, dass diese häufig die Beweislastumkehr zulasten des Verpflichteten regeln, so dass von einer Sicherheitspanne betroffene Unternehmen ggf. beweisen müssen, dass sie diese nicht fahrlässig verursacht haben. Gerade dann zeigt sich aber, welchen Wert umfassende Maßnahmen zur IT- und Datensicherheit – und der Nachweis darüber – haben.

III. Entwicklungen auf EU-Ebene

Auch auf EU-Ebene ist mit der Einführung von Mitteilungspflichten im Fall von Pannen in der Datensicherheit konkret zu rechnen. Geplant ist eine Richtlinie, nach der die Mitgliedstaaten der EU Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste verpflichten müssen, im Falle von Sicherheitspannen unverzüglich die zuständigen Aufsichtsbehörden und unter bestimmten Umständen auch die betroffenen Personen zu benachrichtigen.

Das Verfahren zum Erlass dieser Richtlinie (COM (2007) 698) läuft seit 2007 und ist bereits weit fortgeschritten. Für den wahrscheinlichen Fall der Verabschiedung dieser Richtlinie bleibt abzuwarten, inwieweit der deutsche Gesetzgeber bei der Umsetzung der Richtlinie auch Anbieter betriebsinterner Telekommunikationsnetze (sog. "Corporate Networks") oder anderer Telekommunikationsangebote für geschlossene Benutzergruppen erfassen und zur Mitteilung von Sicherheitspannen verpflichten wird. Der Begriff der "öffentlichen" Zugänglichkeit von Telekommunikationsdiensten hat in der Vergangenheit gelegentlich Anlass zur Diskussion gegeben, seitdem das Telekommunikationsgesetz seit 2004 keine generelle Regulierungsausnahme für Angebote an "geschlossene Benutzergruppen" mehr vorsieht. Unabhängig hiervon gelten die spezifisch datenschutzrechtlichen Regelungen des Telekommunikationsgesetzes jedoch mit wenigen Ausnahmen auch für nicht öffentliche, betriebsinterne Telekommunikationsnetze. Es ist somit durchaus vorstellbar, dass der deutsche Gesetzgeber die zu erwartenden EU-Vorgaben in das bisherige telekommunikationsrechtliche Datenschutzsystem einfügen und ggf. auch ihren Anwendungsbereich entsprechend weit gestalten könnte. In diesem Fall wären auch Unternehmen telekommunikationsfremder Branchen im Falle von Sicherheitspannen ggf. von telekommunikationsrechtlichen Benachrichtigungspflichten betroffen.

Soweit derzeit absehbar, werden die Erwägungsgründe der zu erwartenden Richtlinie zudem ausdrücklich anerkennen, dass über den Bereich der elektronischen Kommunikation hinaus ein allgemeines Interesse der Bürger besteht, über Sicherheitspannen benachrichtigt sowie über empfohlene schadensmindernde Maßnahmen informiert zu werden. Auf längere Sicht ist daher mit bereichsübergreifenden Vorgaben der EU zur Einführung von Benachrichtigungspflichten im Falle von Pannen in der Datensicherheit zu rechnen.

IV. Internationale Rechtsfolgen einer nationalen Sicherheitspanne

Eine Sicherheitslücke in einem in Deutschland befindlichen IT-System löst unter Umständen zusätzliche Benachrichtigungspflichten nach US-amerikanischem Recht aus.

1. "Data Breach" – Benachrichtigungspflichten nach US-Recht

Bisher haben 45 Bundesstaaten der Vereinigten Staaten von Amerika sowie Washington, D.C., Puerto Rico und die Virgin Islands "*security breach notification laws*" erlassen. Die Gesetze der einzelnen Bundesstaaten unterscheiden sich hinsichtlich der genauen Voraussetzungen und Anforderungen der normierten Benachrichtigungspflichten. Ihnen gemeinsam ist aber, dass sie Unternehmen, bei denen eine Sicherheitspanne eintritt/auftritt, dazu verpflichten, unverzüglich sämtliche Betroffenen davon in Kenntnis zu setzen. Nach den Gesetzen der meisten Bundesstaaten gelten die Benachrichtigungspflichten für alle Personen oder Unternehmen, die in dem jeweiligen Bundesstaat Geschäfte tätigen. Manche Bundesstaaten schreiben Benachrichtigungspflichten selbst ohne ausdrückliche Bezugnahme auf eine geschäftliche Tätigkeit in dem jeweiligen Bundesland vor.

Der Anwendungsbereich des Rechts der einzelnen Bundesstaaten ist nicht auf Unternehmen beschränkt, die in dem jeweiligen Bundesstaat ihren Sitz oder eine Niederlassung haben. Vielmehr haben alle Bundesstaaten der USA Gesetze zur sog. "long arm" - Jurisdiktion erlassen, nach denen ihre Gesetze unter bestimmten Voraussetzungen auch für Personen und Unternehmen aus anderen US-Bundesstaaten oder anderen Staaten gelten. Die gesetzlichen Voraussetzungen zwischen den Bundesstaaten variieren im Einzelnen, wobei vielfach auf das Bestehen zumindest "minimaler" Kontakte (*minimum contacts*) zu dem jeweiligen Bundesstaat abgestellt wird. Solche "minimalen Kontakte" werden angenommen, wenn Verbindungen (zumindest auch) zu dem jeweiligen Bundesstaat kontinuierlich und systematisch gepflegt werden. Für einen Internetauftritt wird dies nicht erst dann angenommen, wenn über die Webseite Geschäfte mit Ansässigen des jeweiligen Bundesstaats abgeschlossen werden, sondern unter Umständen bereits dann, wenn die Webseite lediglich eine interaktive Kontaktaufnahme vorsieht, ohne dass es zu Geschäftsabschlüssen über die Webseite kommt.

Ob diese Voraussetzungen im Einzelfall gegeben sind, bedarf natürlich der Prüfung anhand der konkreten Umstände und Gegebenheiten. Europäische Unternehmen, die die USA als einen Zielmarkt betrachten, sollten sich jedoch bewusst sein, dass sie im Falle einer Sicherheitspanne selbst dann unter US-bundesstaatliche "*security breach notification laws*" fallen können, wenn sie keine Niederlassung oder sonstige Betriebsstätte in den USA unterhalten.

2. Praktische Erfahrungen

Es kommt vor, dass in Europa ansässige Unternehmen, bei denen eine Sicherheitspanne eintritt, von Betroffenen (oder deren Anwälten) in den USA benachrichtigt und – unter Vorbehalt der Geltendmachung aller Rechte einschließlich Schadensersatz und Mitteilung an die zuständigen Behörden – zur Einhaltung der anwendbaren "*security breach notification laws*" angehalten werden.

Die Vielzahl der "*security breach notification laws*" der einzelnen US-Bundesstaaten und ihrer unterschiedlichen Voraussetzungen stellen in der Praxis hohe Herausforderungen an das Krisenmanagement und die umgehend erforderliche rechtliche Analyse. Dabei ist es schwierig und häufig unverhältnismäßig, die Anwendbarkeit und Rechtsfolgen der Gesetze jedes einzelnen Bundesstaats zu prüfen, zumal die "*security breach notification laws*" in vielen Fällen unverzügliches Handeln erfordern und die einzuhaltenden Fristen zum Teil extrem kurz sind und oft unter zwei Wochen liegen.

Sofern ein Unternehmen geschäftliche Beziehungen in die USA pflegt oder vor Ort sogar eine Niederlassung betreibt, ist es daher im Zweifel ratsam, alle von der Sicherheitspanne betroffenen Personen gleichermaßen zeitnah und in möglichst unaufwendiger und wenig reputationsgefährdender Weise von der Sicherheitspanne zu unterrichten, wobei die logistischen Herausforderungen eines solchen Vorgehens beachtlich sind. Diese Maßnahme ist jedoch zum einen kostengünstiger als eine umfassende Prüfung aller ggf. einschlägigen bundesstaatlichen Gesetze oder als ein etwaiger Rechtsstreit über deren Anwendbarkeit. Zum anderen dokumentiert ein solches Mailing die datenschutzrechtliche "Awareness" des betreffenden Unternehmens sowie sein Bemühen um Compliance mit den entsprechenden US-amerikanischen Regelungen, was sich in einer etwaigen gerichtlichen oder außergerichtlichen Auseinandersetzung mit zuständigen bundesstaatlichen Behörden als nützlich erweisen kann. Es ist ferner darauf hinzuweisen, dass eine Verletzung anwendbarer "security breach notification laws" Geldbußen in Höhe von bis zu USD 250.000 *pro Bundesstaat* zur Folge haben kann.

Liegt es angesichts der geschäftlichen Aktivitäten eines Unternehmens nahe, dass zumindest nach dem Recht eines US-Bundesstaats Benachrichtigungspflichten bestehen, so ist eine vorbeugende Benachrichtigung aller Betroffenen (auch in anderen US-Bundesstaaten) zur Vermeidung umfassender rechtlicher Prüfungen sowie der Kosten und Öffentlichkeitswirkung etwaiger Auseinandersetzungen über die Anwendbarkeit einzelner bundesstaatlicher Regelungen häufig angeraten. Dies gilt nicht zuletzt auch deshalb, weil Präzedenzfälle der Anwendung bundesstaatlicher Benachrichtigungspflichten auf "*Non-US residents*" bisher rar sind, so dass eine entsprechende Auseinandersetzung eine US-weite Aufmerksamkeit seitens der Datenschutzbehörden, der Federal Trade Commission sowie der Medien auf sich ziehen könnte. Demgegenüber erscheint der mögliche Reputationsverlust durch eine einmalige Benachrichtigung der Betroffenen, deren Ton und Formulierung das betreffende Unternehmen letztlich selbst in der Hand hat, unter Umständen hinnehmbar.

* * *

Dr. Alexander Duisberg
Partner

Bird & Bird LLP
Pacellistraße 14
80333 München

Tel: +49 (0)89 3581 6239
Fax: +49 (0)89 3581 6011
Mail: alexander.duisberg@twobirds.com



Mit freundlicher Unterstützung von

