

Opt-out ist demnächst absolut out

Informationspflichten der Unternehmen bei Datenlecks sowie etwaige Schadensersatzansprüche der Betroffenen bei Fehlhandeln der Unternehmen sind wichtige Elemente der Datenschutzgesetz-Novelle. Und auf den Adresshandel kommen harte Zeiten zu.

von stefan hanloser* | juergen.hoefling@informationweek.de



Das Verlieren oder Verschieben von sensiblen Kundendaten ist kein Kavaliersdelikt.

Im Herbst 2008 rückten verschiedene Datenkandale das eher spröde Thema Datenschutz in den Fokus der öffentlichen Diskussion. Rechtswidrig übermittelte Kundendatensätze samt Kontoverbindungsdaten – salopp als Datendiebstahl bezeichnet – beherrschten die Schlagzeilen. Dass ein Datendiebstahl bereits nach geltendem Datenschutzrecht illegal ist und die Hauptakteure gegen das Bundesdatenschutzgesetz (BDSG) verstoßen hatten, stand von Anfang an außer Frage. Gleichwohl wurde auf dem Datenschutzgipfel vom 4. September 2008 eine Verschärfung des Gesetzes beschlossen.

Seit dem 10. Dezember 2008 liegt nun der Regierungsentwurf für ein »Gesetz zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften« vor. Das BDSG soll nach den Plänen der Bundesregierung in seiner endgültigen Fassung am 1. Juli 2009 in Kraft treten. Bis dahin müssen

die Unternehmen ihre technischen und organisatorischen Prozesse an die strengeren Regelungen anpassen. Und das ist mit einigem Aufwand verbunden.

Informationspflicht bei Datenlecks

Ein wesentlicher Aspekt des neuen Gesetzes ist die sogenannte »security breach notification«. Diese Pflicht der Unternehmen, Datenschutzbehörden und betroffene Kunden proaktiv über einen Datenverlust zu informieren, hat ihren Ursprung in den USA. Die meisten US-Bundesstaaten versuchen damit dem drängenden Problem des Identitätsdiebstahls beizukommen. Die Benachrichtigungspflicht ist aus Unternehmenssicht allerdings zweischneidig. Einerseits dient die Benachrichtigung der Schadensbegrenzung. Ignoriert der Kunde die empfohlenen Sicherheitsvorkehrungen, trifft ihn ein anteiliges Mitverschulden. Dies entlastet das Unternehmen finanziell. Andererseits schädigt eine Benachrichtigung zwangsläufig die Kundenbeziehung und führt schlimmstenfalls zu Kundenverlusten. Statistiken aus den USA zeigen aber, dass noch mehr Kunden abwandern, wenn ein Datenkandal ungesteuert durch die Medien veröffentlicht wird.

US-Unternehmen benutzen »security breach notifications« deshalb mittlerweile als Instrument zur gezielten Kundenbindung oder -rückgewinnung in Fällen von Datenverlusten. Es ist nicht unüblich, dass die Unternehmensleitung eine Arbeitsgruppe aus den Bereichen IT, Recht und Marketing einberuft, die präventiv einen Notfallplan entwirft. Im Fall der Fälle braucht der Notfallplan samt Musterbenachrichtigung dann nur noch aus der Schublade gezogen zu werden. Ein klug formuliertes Benachrichtigungsschreiben, das sich im Rahmen der rechtlichen Vorgaben hält, kann so verlorenes Kundenvertrauen wieder gewinnen. Und das rechtfertigt den zeitlichen und finanziellen Aufwand eines Notfallplans allemal.

Wann tritt Melde- und Informationspflicht ein?

Nach dem Entwurf der Bundesregierung tritt die Meldepflicht gegenüber den Datenschutzbehörden und die Benachrichtigungspflicht gegenüber den Kunden dann ein, wenn ein Dritter unrechtmäßig personenbezogene Daten zur Kenntnis nimmt. Dabei macht es

keinen Unterschied, ob die Daten zuvor von einem Mitarbeiter rechtswidrig übermittelt wurden oder dem Unternehmen sonst wie verloren gegangen sind oder gestohlen wurden.

Die Bundesregierung greift allerdings die Erfahrungen aus den USA auf, dass eine Mitteilungs- und Benachrichtigungspflicht in Bagatellfällen unweigerlich einen Abstumpfungseffekt hat und sich auf Dauer kontraproduktiv auswirkt. Der Regierungsentwurf beschränkt die Mitteilungs- und Benachrichtigungspflicht deshalb auf einen abschließenden Katalog besonders sensibler Risikodaten. Risikodaten sind zunächst die sogenannten »besonderen Arten personenbezogener Daten«, wobei das weite Feld der gesundheitsbezogenen Informationen besonders praxisrelevant ist. Auch ein Verlust von personenbezogenen Daten zu Bank- und Kreditkartenkonten soll eine Mitteilungs- und Benachrichtigungspflicht auslösen.

Für Telemediendienste und Telekommunikationsdienste werden bereichsspezifische Parallelvorschriften eingeführt, die den Verlust von Bestands- und Nutzungs- sowie Verkehrsdaten erfassen. Ein Unternehmen wird im Falle eines Datenverlusts also zunächst prüfen, ob solche Risikodaten abgefließen sind. Sollte dies der Fall sein, müssten künftig eine Meldung an die Datenschutzbehörde und die Benachrichtigung der Kunden unverzüglich erfolgen.



Für Fehlhandlungen der Unternehmen können Bußgelder bis zu 300 000 Euro verhängt werden.

Allerdings räumt der Regierungsentwurf den Unternehmen in zwei Fällen eine Karenzzeit für die Benachrichtigung der Kunden (nicht aber für die Meldung an die Datenschutzbehörde!) ein. Sie können zunächst einmal unverzüglich technische Maßnahmen zur Datensicherung treffen. Auch kann die Benachrichtigung aufgeschoben werden, wenn ansonsten strafrechtliche Ermittlungen gefährdet würden, etwa weil dem Täter eine Falle gestellt werden soll.

Mindestinhalte für die Information

Der Regierungsentwurf schreibt zwei Mindestinhalte für die Benachrichtigung der Kunden vor. Das Unternehmen muss zunächst die Art der unrechtmäßigen Kenntniserlangung offenlegen. Gefordert ist aber keine detaillierte Schilderung der Einzelumstände, die zum Datenverlust geführt haben. Eine typisierende Darstellung, wann welche Datenkategorien verloren gingen oder gestohlen wurden beziehungsweise an wen sie unrechtmäßig übermittelt wurden, reicht aus. Als grobe Richtschnur für den Detaillierungsgrad wird man hier auf den Zweck der Benachrichtigungspflicht abstellen müssen. Der Betroffene soll nach Möglichkeit abschätzen können, von wem welche rechtswidri-

ge Nutzung seiner Daten droht und ob gegenwärtig eine konkrete oder nur noch eine abstrakte Gefahr besteht. Zusätzlich muss die Benachrichtigung konkrete Handlungsempfehlungen für Maßnahmen zur Schadensminderung geben, etwa die Aufforderung, Kontoauszüge oder Kreditkartenabrechnungen fortan regelmäßig zu überprüfen und von dem Kreditinstitut oder Kreditkartenunternehmen unverzüglich die Rückabwicklung von Falschbuchungen zu verlangen.



Der Regierungsentwurf beschränkt die Mitteilungs- und Benachrichtigungspflicht auf einen abschließenden Katalog besonders sensibler Risikodaten.

Die Melde- und Benachrichtigungspflicht wird durch einen neuen Bußgeldtatbestand flankiert. Erfolgt die Meldung beziehungsweise Benachrichtigung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig, kann ein Bußgeld von bis zu 300 000 Euro festgesetzt werden. Aus Unternehmenssicht besonders gravierend ist zudem, dass die betroffene Person bei unterlassener, verzögerter, falscher oder unvollständiger Benachrichtigung zivilrechtliche Schadensersatzansprüche gegen das Unternehmen geltend machen kann. Die BDSG-Novelle etabliert damit eine Schutznorm zugunsten der Betroffenen, die bei Nichtbeachtung eine zivilrechtliche Schadensersatzhaftung auslösen kann.

Einschränkung des Listenprivilegs

Die Bundesregierung nimmt die Datenskandale vom Herbst 2008 zum Anlass, die Datennutzung für Werbezwecke erheblich zu reglementieren. Heftigen Widerstand insbesondere aus der Werbewirtschaft haben in diesem Zusammenhang die Pläne zur Einschränkung des Listenprivilegs erregt.

Nach geltendem Recht können insbesondere die Namen, Anschriften und das Geburtsjahr von Personen nach einem Gruppenmerkmal listenmäßig zusammengestellt, für Werbezwecke an ein anderes Unternehmen übermittelt und von diesem genutzt werden (sogenanntes Listenprivileg).

Nach dem neuen Recht muss sich derjenige, der personenbezogene Daten nach dem 1. Juli 2009 erhebt und für Werbezwecke übermitteln oder nutzen möchte, in den meisten Fällen beim Werbeadressaten zuvor eine qualifizierte Einwilligung holen. Das Listenprivileg wird zulasten des Adresshandels erheblich eingeschränkt. Für personenbezogene Daten, die vor dem 1. Juli 2009 erhoben wurden, soll das alte Listenprivileg bis zum 1. Juli 2012 fortgelten. Diese dreijährige Übergangsfrist würde es den Unternehmen ermöglichen, fehlende qualifizierte Einwilligungen bei den Betroffenen – soweit möglich – nachträglich einzuholen.

Das Listenprivileg bleibt nur ganz begrenzt erhalten für die Geschäftswerbung gegenüber freiberuflich und gewerblich Tätigen. Auch soll die Spendenwerbung privi- →

legiert bleiben. Im Übrigen wird es auf die Eigenwerbung gegenüber Bestandskunden beschränkt. Begünstigt sind nur noch Kundendaten, die das werbende Unternehmen selbst erhoben hat; die Werbung gegenüber Neukunden ist nicht mehr erfasst. Für fremde Produkte bleibt ohne qualifizierte Einwilligung nur die Möglichkeit der Beipackwerbung, die der Kommunikation mit dem eigenen Kunden hinzugefügt wird.



Eine Nichtbeachtung der BDSG-Bestimmungen kann eine zivilrechtliche Schadensersatzhaftung auslösen.

Wie bisher kann der Kunde der Übermittlung und Nutzung seiner Daten zu Werbezwecken widersprechen. Neu ist, dass der Kunde bereits beim Vertragsabschluss über sein Widerspruchsrecht zu belehren ist. Versendet das Unternehmen nach einem Widerspruch noch Werbung an den Kunden, kann die Aufsichtsbehörde ein Bußgeld von bis zu 300 000 Euro verhängen. Erteilt der Kunde die Einwilligung mündlich, etwa am Telefon, muss das Unternehmen die erteilte Einwilligung anschließend schriftlich bestätigen. Damit soll späterer Streit über den genauen Wortlaut der

Einwilligung vermieden werden. Wird die Einwilligung elektronisch erteilt, etwa per E-Mail oder durch Ankreuzen einer Check-Box auf einem Online-Formular, muss der Kunde den Einwilligungstext jederzeit abrufen und widerrufen können. Praktisch wird das darauf hinauslaufen, dass das Unternehmen den Einwilligungstext online abrufbar hält und dort auch die Kontaktdaten für einen Widerruf der Einwilligung angibt.

Die Einwilligung muss künftig durch eine aktive Erklärungshandlung des Kunden, etwa ein Ankreuzen erfolgen. Das vom Bundesgerichtshof noch im Sommer 2008 in der Payback-Entscheidung gutgeheißen »Opt-out« ist künftig auch für die Briefwerbung vom Tisch. Unternehmen werden dies bei der Neukonzeption ihrer Formulare zu berücksichtigen haben. Marktbeherrschenden Unternehmen soll es schließlich verboten werden, ihre Leistung an eine qualifizierte Einwilligung für die werbliche Datenverwendung zu koppeln, wie dies bisher nur für Telemediendienste ausdrücklich geregelt war. Damit fällt ein weiterer Unterschied zwischen Online- und Briefwerbung weg. ■

* **Dr. Stefan Hanloser** ist Rechtsanwalt in der Kanzlei Howrey LLP in München