

Dr. Bettina Kähler\*

## Schöne neue Online-Welt der Versicherer?

*Datenschutz als Vertrauensfaktor*

Es ist die schöne neue Online-Welt, die uns Stefan Hentschel und Sebastian Schopp von Google kürzlich im Heft 19/2010 dieser Zeitschrift beschrieben haben. Die Empfehlung an die Versicherungen lautet, künftig vorrangig auf die (unterstellten) Bedürfnisse der sog. Digital Natives zu setzen, also derer, die mit dem Internet aufgewachsen sind. Diese Zielgruppe gelte es, mit besseren Online-Angeboten an die Versicherungen zu binden.

Die Versicherungswirtschaft müsse sich „konsequent für das Internet öffnen“. Besucher von Webseiten sollten, so der Rat, in zahlende Kunden „umgewandelt“, ihre Daten „effizient eingesammelt“ und an den Außendienst „weitergeleitet“ werden, Abschlüsse möglichst direkt auf den Webseiten getätigt werden. Damit einher gehen müsse auch eine „Komplexitätsreduktion“ der Angebote der Versicherer. Für die (nähere oder fernere?) Zukunft sollte es nach Ansicht von Google dann etwa dem Skifahrer auch möglich sein, spontan per Smartphone eine Unfallversicherung abzuschließen, unmittelbar bevor sich der Skiflirt in Richtung Berg in Bewegung setzt.

### *Kreativ – aber zu kurz gedacht*

Das alles klingt gut, modern, innovativ. Welcher Verbraucher, der einmal versucht hat, online auch nur ein Angebot für eine Kfz-Versicherung einzuholen, würde sich nicht Komplexitätsreduktion wünschen? Das effiziente Einsammeln von persönlichen Daten nach dem Besuch einer Webseite und deren Weiterverarbeitung zu Werbezwecken dürfte dagegen auf der Wunschliste der potenziellen Kunden nicht sehr weit oben rangieren. Dies gilt im Übrigen nicht nur für die jugendlichen Ureinwohner des digitalen Kontinents, sondern auch für

einen Großteil der Generation der jetzt um die 45jährigen, für die das Internet aus ihrem täglichen Leben ebenfalls nicht mehr wegzudenken ist.

Doch Google's Empfehlungen sind entschieden zu kurz gedacht. Google übersieht, dass auch die Online-Welt an gesetzliche und gesellschaftliche Regeln gebunden ist und zukünftig noch mehr gebunden sein wird. Das muss auch so sein – gerade in einer immer komplexer vernetzten Welt. So ist es nach deutschem (und europäischem) Datenschutzrecht ohne Einwilligung der Nutzer nicht erlaubt, die bei einem Besuch einer Webseite anfallenden Daten zu dem Zweck zu sammeln, die Nutzer anschließend zu bewerben; ganz abgesehen von der Tatsache, dass sich solche Praktiken bei jungen und alten Internetnutzern höchster Unbeliebtheit erfreuen. Die Umsetzung von Datenschutz- und Verbraucherrechten im Internet stellt hohe Anforderungen an rechtliches Wissen und den Einsatz von Technik.

Dabei geht es jedoch nicht um die Einhaltung von Gesetzen um der Gesetze willen. Es geht um den Erhalt und den Gewinn des Vertrauens der Kunden und potenzieller Kunden der Versicherer. Um das Vertrauen, dass die Versicherer mit den ihnen anvertrauten Daten sorgsam umgehen. Dieses Vertrauen ist heute unter Verbrauchern, gerade hinsichtlich des Online-Abschlusses von Rechtsgeschäften, nicht sehr ausgeprägt. Es spricht nicht viel dafür, dass dieses sich ändern würde, sollten die Versicherer im Online-Bereich auf kurzfristige und wenig durchdachte Lösungen setzen.

Hinzu kommt, dass die öffentliche Toleranz gegenüber Datenschutzpannen in Unternehmen in den letzten

Jahren kontinuierlich abgenommen hat. Nach dem Bekanntwerden der Datenskandale bei der Telekom erzwungen Umfragen zufolge über 30% der Telekom Kunden einen Wechsel zu einem anderen Anbieter. Insbesondere die Versicherungen, die wie kaum eine andere Branche elementar vom Vertrauen ihrer Kunden abhängig sind, sind daher gut beraten, vor die Einführung neuer Online-Angebote auf die gründliche Analyse und sorgfältige Planung datenschutzfreundlicher Technologien und Verfahren zu setzen.

### *Versicherungen online: Datenschutz noch unterentwickelt*

Schon jetzt sind die Baustellen des Datenschutzes in der Versicherungswirtschaft kaum zu überschauen. Das gilt einerseits für die Offline-Welt – Bonitätsprüfungen, der Einsatz von Scoringverfahren, Datenaustausch im Versicherungskonzern seien nur als Stichworte genannt. Zu diesen Themen besteht ein etablierter und kontinuierlicher Dialog zwischen Versicherungswirtschaft und den Datenschutzaufsichtsbehörden, der im Laufe der Jahre Verbesserungen gebracht hat.

Die auch nur flüchtige Durchsicht von Online-Angeboten verschiedener Versicherungen macht jedoch deutlich, dass dies für den Online Bereich offensichtlich nicht gilt. Das Beispiel der Datenschutzerklärung, die jeder Anbieter einer kommerziellen Webseite auf dieser einfach auffindbar verfügbar halten muss, mag dieses verdeutlichen. § 13 des Telemediengesetzes (TMG) schreibt vor, dass jeder Anbieter einer kommerziellen In-

\* Die Autorin ist Rechtsanwältin und Geschäftsführerin der PrivCom Datenschutz GmbH, Hamburg, E-Mail: [bettina.kaehler@privcom.de](mailto:bettina.kaehler@privcom.de), [www.privcom.de](http://www.privcom.de)

ternetseite den Nutzer „vor Beginn des Nutzungsvorganges“ darüber zu informieren hat, was mit den personenbezogenen Daten geschieht, die beim Besuch der Seite anfallen.

Gleichzeitig werden Beschränkungen im Umgang mit den Daten festgeschrieben. So dürfen Nutzerprofile beispielsweise nur unter Pseudonym erstellt werden und der Nutzer hat dagegen ein Widerspruchsrecht. Die online Datenschutzerklärung kann als Indikator angesehen werden, wie sorgfältig die Versicherung, die das Angebot verantwortet, mit den personenbezogenen Daten ihrer (potenziellen) Kunden umgeht.

Keines von insgesamt zwölf stichprobenartig analysierten Online-Angeboten von Versicherungen konnte im Hinblick auf die Einhaltung dieser eigentlich sehr einfachen Anforderungen des § 13 Telemediengesetz überzeugen. Zwei Angebote wiesen überhaupt keine Datenschutzerklärung auf. Die übrigen sind weit überwiegend inhaltlich unvollständig, sie enthalten in weiten Teilen rechtswidrige Inhalte und Verweise auf Gesetze, die schon seit über drei Jahren nicht mehr gelten. An keiner Stelle findet sich ein Hinweis auf das Widerspruchsrecht gegen das Erstellen von pseudonymen Nutzungsprofilen zu Marketingzwecken.

Die Information über den Umgang mit online erhobenen personenbezogenen Daten wird in allen Datenschutzerklärungen vermischt mit Erklärungen zur Datenverarbeitung im Zusammenhang mit einem Versicherungsvertrag. Letzteres ist sicherlich auch von Interesse, muss aber von der Frage des Umgangs mit den Daten, die beim Besuch der Webseite anfallen, klar getrennt werden. Der Sinn der Vorschrift des § 13 TMG, den Nutzer über den Umgang mit seinen persönlichen Daten zu informieren und ihn vor intransparenten Praktiken zu schützen, wird mit so gestalteten Datenschutzzinformationen genauso konterkariert, wie die von § 13 TMG geforderte „allgemein verständliche Form“ der Unterrichtung.

Davon abgesehen werden einfachste technische Sicherheitsvorkehrungen missachtet. Sensible Daten (Gehalts- und Gesundheitsdaten), die die Nutzer für die Berechnung eines Angebots online in Formulare eintragen können, werden teilweise unverschlüsselt und damit für Dritte sichtbar, übertragen. Nur für das Einholen eines Angebotes für eine Kfz-Versicherung werden Informationen abgefragt, die für diesen Zweck völlig ohne Belang sind (Anzahl der Kinder, deren Alter?). Für den Nutzer, der den Versicherungen online teilweise sehr persönliche Inhalte übermitteln soll, ist das nicht sehr vertrauenswürdig.

Die Einhaltung der Datenschutzvorschriften des TMG stellt dabei nur die Minimalanforderung an ein überzeugendes Online-Angebot einer Versicherung dar – weitere, sich aus europäischen Rechtsvorschriften (Europäische Datenschutzrichtlinie für die elektronische Kommunikation, Richtlinie über den elektronischen Geschäftsverkehr) ergebende Anforderungen, wurden hier nicht berücksichtigt. Dies gilt umso mehr, wenn eine Versicherung Online-Abschlüsse einfacher und schneller möglich machen will, als dies bisher der Fall ist.

### *Datenschutz – keine Innovationsbremse*

Vor einer Einführung neuer Produkte im Online-Vertrieb sollten die Versicherungen zunächst einmal die bereits existierenden Angebote den Anforderungen des geltenden Rechts anpassen. Vor einer Umsetzung neuer Online-Angebote müssen die damit verbundenen Datenschutzfragen gründlich analysiert und sichere Verfahren geplant werden, die Daten-

**„Es gibt für fast alle Verfahren datenschutzkonforme Lösungen und ausreichende technische Sicherungen“**

schutz und Datensicherheit und den diesbezüglichen Erwartungen der Verbraucher angemessen Rechnung tragen. Nicht alles, was technisch machbar ist, sollte auch gemacht werden. Dies gilt umso mehr, als bei den Online-Angeboten und Abschlüssen der nicht nur Datenschutzgesetz, sondern auch Verbraucherschutzvorschriften, aufsichtsbehördliche Vorgaben, technische Sicherheiten und komplexe zivilrechtliche Fragen zu berücksichtigen sind, die ebenfalls Eingang in ein Online-Verfahren finden müssen.

Wie soll ein Versicherer feststellen können, ob die Unfallversicherung am Skilift tatsächlich von Greta Meier über das Smartphone abgeschlossen wird und nicht von jemandem, der vorgibt, Greta Meier zu sein? Wie soll ein Versicherer feststellen können, ob das Bein tatsächlich beim Skifahren brach und nicht schon vorher? Wie kann umgekehrt Greta Meier darauf vertrauen, dass nicht mit genau diesen Argumenten ihr Vertrag von der Versicherung im Nachhinein in Frage gestellt wird?

Diese Fragen müssen rechtlich gelöst und technisch sicher abgebildet werden. Geschieht dies nicht, werden sich mit großem Aufwand neu eingeführte Verfahren als Rückschritt erweisen. Die von Google geforderte „mutige Fehlerkultur“ kann auf dem sensiblen Feld des Datenschutzes und der Datensicherheit schnell zum Vertrauensverlust der Kunden führen. Für die Versicherungen wäre das fatal.

Daraus zu schließen, dass Datenschutz-Bedenkenträger die Einführung von innovativen Online-Angeboten verhindern sollte, wäre allerdings auch falsch. Es gibt für fast alle Verfahren datenschutzkonforme Lösungen und ausreichende technische Sicherungen. Sollen Innovationen eingeführt werden, müssen diese allerdings erst definiert und an ihrer technischen Umsetzung gearbeitet werden. Mitunter müssen datenschutzkonforme Lösungen tech-

nisch und organisatorisch auch erst ganz neu entwickelt werden. Dieser Prozess ist aufwendiger als das unüberlegte Installieren von allem, was technisch machbar ist, und es erfor-

dert entsprechendes finanzielles Engagement. Aber genau dies wäre für die Versicherungen ein Pfad auf dem Weg in die Moderne: Die nachhaltige Investition in das Vertrauen der Kun-

den unter veränderten technischen Bedingungen. Als angenehmer Nebeneffekt werden nachträgliche böse Überraschungen und finanzielle Einbußen vermieden.

Holger Kunschke\*/Dr. Uwe Korte\*\*

## Der neue Personalausweis im Versicherungsunternehmen – Ein Überblick und ein Anwendungsszenario aus der Praxis

### 1. Einleitung

Ab dem 1. November 2010 wurde der bisherige Personalausweis durch den neuen Personalausweis (nPA) im Scheckkartenformat abgelöst. Der neue Personalausweis verfügt mittels eines integrierten RFID-Chips über Funktionen, die der Bürger bei der elektronischen Kommunikation mit Unternehmen und Behörden über eine hochgradig abgesicherte technische Infrastruktur einsetzen kann: den sicheren elektronischen Identitätsnachweis und die Option, den Ausweis als Signaturkarte für eine qualifizierte elektronische Signatur einzusetzen. Der elektronische Identitätsnachweis ermöglicht ein rechtssicheres „Sich-online-Ausweisen“ im elektronischen Geschäftsverkehr. Diese Funktionalität wird auch eID-Funktion (eID = electronic Identity) genannt.

Seit Anfang des Jahres testen ca. 30 Unternehmen und Behörden die Integration des neuen Personalausweises in ihre Unternehmensapplikationen im zentral koordinierten Anwendungstest des Bundesministeriums des Innern. Ihr Ziel ist es, Bürgern zum 1. November 2010 die ersten Ausweis-unterstützten Dienste bereitzustellen. Mit sechs beteiligten Unternehmen stellt die Versicherungsbranche die größte Gruppe im zentral koordinierten Anwendungstest. Dies verdeutlicht das große Interesse der Branche an den erweiter-

ten Möglichkeiten, die der neue Personalausweis zur Abwicklung von Geschäftsprozessen bietet. Der Fokus der am Anwendungstest beteiligten Versicherungsunternehmen liegt auf der Integration der eID-Funktion. Abgesehen von der einmaligen Ausweisgebühr verursacht diese Funktion im Gegensatz zur elektronischen Signatur für den Bürger keine zusätzlichen Kosten. Daher wird hier eine hohe Akzeptanz erwartet.

### 2. Datenkategorien und Berechtigungszertifikat

Im Zuge der Nutzung der eID-Funktion kann ein Unternehmen zum Beispiel Datenkategorien auslesen, wie man sie typischerweise in einer Kundendatenbank findet: Familienname, Vornamen, Doktorgrad, Tag der Geburt und Anschrift. Neben weiteren Datenkategorien gibt es zusätzlich ein so genanntes dienste- und kartenspezifisches Kennzeichen. Dies ist eine Zahlenfolge, die der Chip im Ausweis generiert. Als eine Art dienste-spezifische „Kundennummer“ erlaubt sie es einem Unternehmen, den Ausweis bei wiederholter Benutzung eines Dienstes eindeutig wiederzuerkennen, ohne dass erneut personenbezogene Daten übertragen werden müssen.

Die Nutzung der eID-Funktion durch ein Unternehmen sowie das Auslesen der Datenkategorien, die der

neue Personalausweis zur Verfügung stellt, erfolgt niemals ohne Einwilligung des Bürgers. Bei der Verwendung der eID-Funktion muss sich auch das Unternehmen vor der Datenübermittlung gegenüber dem Bürger elektronisch ausweisen. Darüber hinaus bestätigt der Bürger sein Einverständnis zur Datenübermittlung über die Eingabe einer sechsstelligen PIN, die nur ihm bekannt ist.

Das Unternehmen wiederum weist sich über ein so genanntes Berechtigungszertifikat aus, in dem die Datenkategorien festgelegt sind, die es aus dem Ausweis auslesen darf. Damit wird zum einen sichergestellt, dass auch der Bürger, der einen elektronischen Dienst nutzt, Gewissheit hinsichtlich der Identität seines Gegenübers hat. Zum anderen wird damit unterbunden, dass Daten übermittelt werden, die nicht zur Durchführung des Geschäftszwecks notwendig sind.

Das Berechtigungszertifikat muss von jedem Unternehmen, das für eine Dienstleistung die eID-Funktion nutzen möchte, bei der staatlichen Vergabestelle für Berechtigungszerti-

\* Projektleiter & Gruppenleiter, Provinzial Rheinland Versicherung AG. Er leitet das Projekt, in das der zentral vom BMI koordinierte Anwendungstest für den neuen Personalausweis eingegliedert ist.

\*\* Manager, BearingPoint. Er betreut im Kompetenzzentrum neuer Personalausweis die am Anwendungstest beteiligten Unternehmen der Versicherungswirtschaft.