

Fotos: Markus Spiske/raumrot.com

# Privacy-Paradox

▲ Deutsche Verbraucher genießen ein Recht auf informationelle Selbstbestimmung. Doch das kollidiert immer öfter mit handfesten wirtschaftlichen Interessen auf Seite der Unternehmen. Ist **Datenschutz** in Zeiten digitaler Geschäftsmodelle tatsächlich ein Hemmschuh? Oder doch eher ein **Wettbewerbsvorteil**? >

▲ Der Streit um den Datenschutz wird an vielen Fronten leidenschaftlich geführt. Das gilt für den NSA-Skandal, die EU-Datenschutzreform, Safe Harbor oder die diversen Auseinandersetzungen um Datenkraken wie Facebook oder Google. Experten sind sich einig: Das Vertrauen der Nutzer in Online-Anbieter ist eine essenzielle Geschäftsgrundlage. Das deckt sich mit vielen Umfragen. Nach einer Studie des US-Forschungs-

zentrums Ponemon Institute teilt die Hälfte der deutschen Verbraucher ihre Daten nur mit Unternehmen, denen sie vertraut. Sogar 76 Prozent achten laut dem Marktforschungsinstitut Forsa sehr darauf, wem sie Daten über sich zur Verfügung stellen. Zu welchen Konsequenzen fehlendes Vertrauen führen kann, verdeutlicht eine Studie des amerikanischen IT-Sicherheitsanbieters Symantec: 38 Prozent der Nutzer machen

online absichtlich falsche persönliche Angaben und somit Datenanalysen wertlos. „Man muss die Akzeptanzprobleme ernst nehmen. Das digitale Tempo ist enorm. Da ist Transparenz und Datensouveränität wichtig“, sagt Jan Christian Sahl, Referent für Digitalisierung beim Bundesverband der Deutschen Industrie. „Nicht nur die Bürger, auch viele Unternehmen wollen ihre Daten schützen und über ihre Verwendung selbst

bestimmen.“ Beide treibt die Sorge um die Datensicherheit um.

**Deutsche Anbieter können** hier punkten. Ein Beispiel sind deutsche Cloud-Anbieter, die ihren Marktanteil nach dem NSA-Skandal massiv ausgebaut haben. Andererseits kennt Sahl den Wunsch vieler Unternehmen, gerade in Zeiten von Big Data die Datenschätze selbst zu heben. Unproblematisch sind neue Geschäftsmodelle zur Datenanalyse in der Industrie 4.0, denn hier werden in vielen Fällen auch nicht-personenbezogene Daten verarbeitet, die nicht dem Datenschutzrecht unterliegen. Erfolgversprechend können auch Zertifikate sein, zum Beispiel für Dienstleister der Auftragsdatenverarbeitung. Die Auftraggeber sind nämlich gesetzlich verpflichtet, die Vertrauenswürdigkeit der Auftragnehmer regelmäßig zu überprüfen. Das machen in der Praxis aber nur wenige, zumal gerade kleine Unternehmen damit in der Regel überfordert sind. „Zertifikate sind geeignet, eine solche Kontrolle zu ersetzen“, sagt Sahl. Für den Endverbraucher stellt sich jedoch das Problem, dass es ihm schwerfällt, im Dschungel der Gütesiegel und Zertifikate einen Überblick zu bewahren. Zudem überfordern die komplexen Kriterien für einen effektiven Schutz der Privatsphäre den Durchschnittsnutzer schnell.

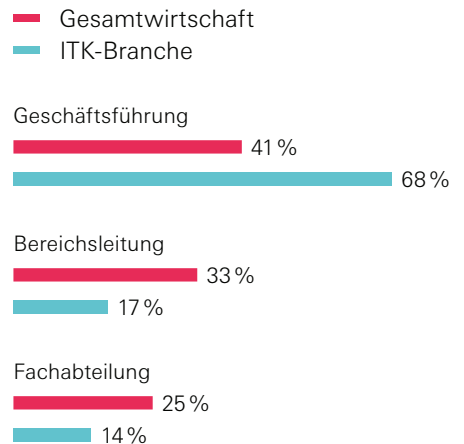
**Auch der Handelsverband Deutschland (HDE)** verweist darauf, dass professioneller Datenschutz das Verbrauchervertrauen eher fördere, betont aber gleichzeitig mögliche Wettbewerbsnachteile. Zwar sei die Datensicherheit im Online-Handel ein Anreiz zu kaufen. Doch der Datenschutz müsse praktikabel sein und dürfe Geschäftsmodelle nicht verhindern, so Peter Schröder, Bereichsleiter Recht und Verbraucherpolitik im HDE. „Nachteilig im internationalen Wettbewerb ist es, wenn deutsche Unternehmen Serviceleistungen nicht anbieten dürfen, die eine Datenerhebung voraussetzen.“ Als Beispiel nennt er zielgerichtete Werbung, die auf der Erhebung und Verarbeitung von Adressen beruht. Für Newsletter ist in Deutschland das aufwendige Verfahren des „double opt-in“ vorgeschrieben, das manchen Interessenten vom Abo-Klick abhalten dürfte. Zudem ist die im Ausland erlaubte Weitergabe von Adressen an andere Unternehmen hierzulande nur eingeschränkt möglich. Damit wäre ein Teil der Nutzer jedoch nicht einverstan-

den und so räumt Schröder ein: „Auch der Verbraucher befindet sich in einem Zwiespalt: Einerseits ist er dagegen, andererseits will er relevante Informationen.“ Kritisch sei ein mögliches Verbot, zum Beispiel bei der Schufa Auskünfte über die Zahlungsfähigkeit von Käufern einzuholen, die auf Rechnung kaufen. Denn das sei die beliebteste Zahlungsart. „Ohne Informationen und Sicherheit kann der Händler den Kauf auf Rechnung nicht anbieten, da sonst das Risiko des Zahlungsausfalls für ihn zu hoch ist.“ Zumindest die Sorge, dass deutsche Unternehmen generell durch strenge Datenschutzgesetze benachteiligt werden, hat die EU-Datenschutzreform obsolet gemacht. Künftig gelten für alle Unternehmen in der EU die gleichen Regeln.

**Eine große Herausforderung** für Anbieter, die auf mehr Datenschutz im Vergleich zur Konkurrenz setzen möchten, ist das Privacy-Paradox. Danach geben Verbraucher zwar in Umfragen an, dass ihnen der Schutz ihrer Privatsphäre wichtig sei, tun aber in der Praxis wenig dafür. Einer der Gründe ist, dass es neben dem Datenschutz noch andere, meist wichtigere Kriterien gibt, weshalb sich Nutzer für einen Anbieter oder Händler entscheiden. Ist das deutsche Unternehmen also in anderen Bereichen nicht konkurrenzfähig, wird ihm der bessere Datenschutz allein kaum helfen. Ebenfalls paradox waren zum Beispiel die Reaktionen der deutschen Autohersteller auf die Frage nach dem möglichen Wettbewerbsvorteil. Meist mit Verweis auf die Sensibilität des Themas fand sich auf Anfrage der Schwesterzeitschrift automotiveIT kein Unternehmen bereit, offen Stellung

## /// Datenschutz auf der Managementebene

Auf welcher Managementebene ist das Thema Datenschutz bei Ihnen angesiedelt?



zu nehmen. Lieber versteckten sie sich hinter schriftlichen, offiziös klingenden Statements. Diese Zurückhaltung steht im Kontrast zur einheitlichen Einschätzung, dass der Schutz der Privatsphäre einen Standortvorteil darstelle. Klare Worte dagegen fand Stefan Römmele, Leiter des Kompetenzzentrums Security und Privacy des Zulieferers Continental: „Die Datenschutzgesetze in Deutschland sind ein klarer Standortvorteil, wenn es darum geht, Sicherheitslösungen für unsere Kunden zu entwickeln. Wenn entsprechende Systeme den hiesigen Gesetzen genügen, dann ist das das beste Aushängeschild, um auch für andere Regionen der Welt Produkte und Systeme zu entwickeln.“

■ Autor: Ulrich Hottel

## /// Anteil der häufigsten Datenschutzverletzungen

2008 bis 2015 in Prozent

