INTERVIEW

WORAUF MÜSSEN UNTERNEHMEN

KÜNFTIG ACHTEN?

Egal ob Internet of Things (IoT) oder neue Geschäftsmodelle – letztendlich basiert alles auf dem Austausch und der Auswertung von (Kunden-) Daten. Aber neben den Chancen, die damit verbunden sind, birgt dies auch Gefahren. Vor allem auch, was Datenschutz und Sicherheit betrifft. Welche Stolpersteine und Aufgaben hier auf die Unternehmen zukommen können, erläutert Bernd Fuhlert, Geschäftsführer von @-yet, im Gespräch.

DATENVERMEIDUNG UND -SPARSAMKEIT /// DATENSCHUTZ UND -SICHERHEIT /// ANONYMISIERUNG

DB: Herr Fuhlert, Kunden machen sich immer häufiger Gedanken darüber, wie ihre Daten verwendet und ausgewertet werden. Was bedeutet dies für die Unternehmen?

BERND FUHLERT: Grundsätzlich denke ich, dass der Ansatz von Unternehmen dahin gehen sollte, nur so viele Daten wie nötig zu erheben. Allein, weil die Zusammenführung großer Datenmengen nicht nur einen Nutzen bringt, sondern daraus ebenfalls vielfältige technische sowie vor allem auch datenschutzrechtliche Risiken resultieren können – sowohl für Betroffene, aber auch für die Unternehmen selbst. Generell sind Unternehmen per se in ihrer Handlungsfreiheit eingeschränkt, weil vieles in den Datenschutzgesetzen geregelt ist, so schreibt unter anderem § 3a BDSG den Grundsatz der Datenvermeidung und -sparsamkeit vor.

DB: Bei datenbasierten Geschäftsmodellen und der entsprechenden Menge an Informationen weichen Unternehmen zunehmend auf Cloud-Lösungen aus. Muss in diesem Kontext noch mehr Sorgfalt angewandt werden?

BERND FUHLERT: Auf jeden Fall. Bei einer externen Datenverwaltung in der Cloud sind auch extrem umfassende Sicherheitsanforderungen relevant. Denn wenn hier die Prozesse nicht richtig aufgesetzt sind, kann es leicht zu Datenpannen oder – durch kriminelle Angriffe – sogar zu massiven Datenverlusten kommen. Hierfür stehen die Unternehmen in der Verantwortung, nicht der beauftragte Dienstleister. Von daher muss bei dem Aufsetzen der Sicherheitsstandards das Gefahrenpotential auf allen Ebenen durchleuchtet werden: etwa auch, inwieweit Mitarbeiter beim Dienstleister die Möglichkeit haben, auf Nutzerdaten zuzugreifen – Vorfälle dieser Art sind in der letzten Zeit häufiger aufgetreten, zum Beispiel der Mitarbeiter eines Telekommunikationsanbieters, der jahrelang Datensätze gegen Geld verkauft hat.

Um sich bestmöglich abzusichern, sollten Unternehmen genau im Vertragswerk fixieren, wie die Abläufe alle gesetzeskonform durchgeführt und welche adäquate Maßnahmen zum Schutz der Daten unternommen werden. Zum Beispiel, dass bei der Speicherung von allen Daten konsequent eine Verschlüsselung mittels aktueller Technologie obligatorisch ist. Oder auch, dass ein Berechtigungsmanagement aufgesetzt wird, in dem sich nachweislich regeln lässt, welcher Mitarbeiter überhaupt Zugriff auf die Kundendaten haben darf.

DB: 2018 tritt die EU-Datenschutz-Grundverordnung in Kraft. Was bedeutet das für die Unternehmen – werden ihnen dadurch noch mehr Pflichten auferlegt?

BERND FUHLERT: Ja, die neue Verordnung bringt einige gravierende Veränderungen mit sich. Das zieht zum einen organisatorische Konsequenzen nach sich, unter anderem auch, was die Rolle des Datenschutzbeauftragten anbelangt. Mit Inkrafttreten der EU-Datenschutz-Grundverordnung erhält er eine andere Position im Unternehmen – die Aufgaben werden detailliert in Artikel 39 Abs. 1b benannt. Statt auf die Einhaltung des Datenschutzes hinzuwirken, soll er diesen künftig überwachen.

Aber insbesondere sollen hierdurch die Rechte der Kunden grundsätzlich gestärkt werden. Von daher weitet die aktuelle Fassung der Datenschutz-Grundverordnung in manchen Bereichen die Rechte noch aus, etwa, wenn es um Informationen über die Verarbeitung personenbezogener Daten geht. Genau diese neuen Informationspflichten der Unternehmen führen zu einem deutlich stärkeren Schutz.

PROFIL

BERND FUHLERT

Seit 2016 ist Bernd Fuhlert Geschäftsführer der @-yet GmbH. Seine zentralen Handlungsfelder sind Online Reputation Management sowie Datenschutz – unter anderem ist er als externer Datenschutzbeauftragter renommierter Unternehmen bestellt und verfügt über ein breites Netzwerk an Partnern und Kontakten. Als freier Dozent ist er an der Quadriga Hochschule Berlin sowie für den Management Circle tätig und gilt als gefragter Experte zu den Themen Reputation Management/Datenschutz/Social Media. Für den BvD e.V. doziert er zum Thema Neue Medien bundesweit an Schulen der Sekundarstufe I & II. Zudem ist er Autor zahlreicher Veröffentlichungen zum Thema Datenschutz und Reputation Management und publiziert monatlich eine Kolumne in der Zeitung „Datenschutz Digital" des VNR Verlages.

DB: Wie schätzen Sie die Sachlage ein – welche Wirkung wird das für Unternehmen haben?

BERND FUHLERT: Ich denke, Unternehmen werden sich von dem Gedanken an ein Mittelmaß verabschieden müssen. Mittelmaß sichert keine Existenz. Heute ist in puncto Datennutzung vieles machbar, allein über die Möglichkeiten der Anonymisierung. Es ist kein Geheimnis, dass hier eine Überwachung nicht in dem Maße durchführbar ist, wie es eigentlich notwendig wäre – im Prinzip wird der gesamte Prozess nur einmal validiert, aber eine kontinuierliche Kontrolle der Ablaufroutinen ist nicht möglich. Ich gehe davon aus, dass sich Unternehmen künftig jedoch einen laxen Umgang mit Daten nicht mehr erlauben können – denn die Gefahr eines Reputationsverlusts ist einfach zu groß.

> **„Grundsätzlich denke ich, dass der Ansatz von Unternehmen dahin gehen sollte, nur so viele Daten wie nötig zu erheben. Allein, weil die Zusammenführung großer Datenmengen nicht nur einen Nutzen bringt, sondern daraus ebenfalls vielfältige Risiken resultieren können.**

Außerdem sind mit dem IT-Sicherheitsgesetz allgemeine Rahmenbedingungen für branchenspezifische Sicherheitsstandards festgelegt worden. Hieraus wird sich künftig auch für alle anderen Unternehmen ableiten, welche technisch-organisatorischen Maßnahmen zur Realisierung eines angemessenen Sicherheitsniveaus zu treffen sind. Darüber hinaus sind die Sanktionen bei Nichteinhaltung der Vorschriften in der neuen Datenschutz-Grundverordnung drastisch angehoben worden. Derzeit sind nach § 43 BDSG Bußgelder von bis zu 300.000 Euro pro Einzelfall möglich, aber nach neuer Rechtslage beträgt die maximale Geldbuße bis zu 20 Millionen Euro oder bis zu 4 Prozent des gesamten weltweit erzielten Jahresumsatzes im vorangegangenen Geschäftsjahr. Es bleibt zwar abzuwarten, ob diese Strafen ausgesprochen werden, aber welches Unternehmen will schon als erstes in dieser Größenordnung bestraft werden?

DB: Wird das die Handlungsfreiheit der Unternehmen einschränken?

BERND FUHLERT: Ich bin schon der Meinung, dass sich daraus komplexe Aufgabenstellungen für die Unternehmen ergeben werden, insbesondere bei der Zweckbindung. Zum Beispiel können aufgrund der Auswertungsmöglichkeiten mittels Big Data neue Muster entstehen, was das Kundenverhalten anbelangt. Um diese zu validieren, müssen Kundendaten verwendet werden. Auch wenn diese im Prinzip vorhanden sind, dürfen sie nicht ohne weiteres dafür genutzt werden, da hierfür keine Einwilligung seitens des Kunden vorliegt.

DB: Was raten Sie den Unternehmen – wie können sie aus solchen Zwickmühlen herauskommen?

> **„Selbst wenn die Abläufe bei der Anonymisierung nicht extern kontrollierbar sind, sollte das nicht zum Anlass genommen werden, dies für Unternehmenszwecke zu missbrauchen. Hier könnte eine Selbstverpflichtung abgegeben werden, die ein solches (unmoralisches) Handeln ausschließt.**

BERND FUHLERT: Ich glaube, einer der essentiellen Grundsätze für Unternehmen sollte lauten, dass sie nicht den Kontakt zu ihren Kunden verlieren dürfen. Dies ist unter verschiedenen Aspekten wichtig. Zum einen garantiert eine aktive Beziehung, dass der Datenbestand bedeutend besser gepflegt ist. Zum anderen lässt sich nur auf diesem Wege ein Vertrauensverhältnis zu den Kunden aufbauen. Gerade weil heutzutage schon so viel möglich ist, sollten Unternehmen mit den gegebenen Optionen innovativ, aber auch sensitiv umgehen. Kommen wir noch einmal zurück auf das Thema Anonymisierung. Selbst wenn die Abläufe – wie ja bereits erläutert – nicht extern kontrollierbar sind, sollte das seitens der Unternehmen nicht zum Anlass genommen werden, dies für ihre Zwecke zu missbrauchen. Im Gegenteil, hier könnte eine Selbstverpflichtung abgegeben werden, die ein solches (unmoralisches) Handeln ausschließt – also eine Datenethik, der sich Unternehmen verschreiben.

DB: Aus welchem Grund glauben Sie, dass eine konstruktive Kooperation zwischen Unternehmen und Konsumenten notwendig ist? Und kann sich diese realisieren lassen?

BERND FUHLERT: Meines Erachtens ist es nicht nur vom Grundsatz her unabdingbar, dass jeder Einzelne die Kontrolle über seine Identität behält. Je mehr ökonomische Nachteile für die Betroffenen durch die Datennutzung entstehen, desto sensibler werden sie reagieren. Von daher denke ich, die Unternehmen sollten hier gewappnet sein und so kann es mittelfristig nur in deren Sinne sein, Daten und Privatsphäre ihrer Kunden zu respektieren und so umfassend wie möglich zu schützen. Dies muss im Zusammenspiel zwischen beiden Parteien geschehen und ist darüber hinaus nur möglich, wenn Unternehmen nicht individuell agieren. Aus diesem Grund sind wir gerade in der Gründungsphase eines Verbands, um gemeinsam mit den Verantwortlichen die relevanten Fragen, auch ethische im Bezug auf die Datennutzung, zu klären. Unser Ziel ist es, hier Wege zu finden sowie Modelle zu entwickeln, die beiden Seiten gerecht werden. Ich denke, dass es heute wichtig ist, die Vorteile ebenso zu diskutieren wie die Nachteile und zu klären, was wir wollen und was nicht.