Anderer Leute Server – irgendwo

TEXT KARSTEN ZUNKE

Marketing ist auf Datenaustausch angewiesen. In Zeiten weltweiter Marketing Clouds stellen sich Fragen zum Datenschutz mehr denn je. Während für Marketer exakte Zielgruppeninformationen im Vordergrund stehen, ist es für User die Privatsphäre. Doch der Spagat kann gelingen.

Foto: peterhowell/istockphoto

Das Prinzip der Datensparsamkeit, wie es vor vielen Jahren galt, könne heute nicht die generelle Leitschnur für die Entwicklung neuer Produkte sein, sagte Bundeskanzlerin Angela Merkel Ende vergangenen Jahres auf dem IT-Gipfel in Saarbrücken. In jüngster Vergangenheit wird immer öfter der Ruf laut, zeitgemäßer mit Daten umzugehen. Auch das Wording passt sich der neuen, digital geprägten Zeit und den damit verbundenen Herausforderungen an: Statt vom Begriff des klassischen Datenschutzes ist von Seiten der Politik jetzt häufig von Datensouveränität die Rede. Aber unabhängig davon, wie die Politik das Thema bewertet – fest steht: Ohne Daten funktioniert die digitalisierte Gesellschaft nicht. Und auch ein modernes Marketing ist ohne sie nicht möglich. Ohne Big Data können Unternehmen heute lediglich mit der Gießkanne werben. Doch das Gießkannenprinzip haben die Nutzer weitgehend abgewählt. Was nicht relevant ist, wird leicht als Spam wahrgenommen und – im schlechtesten Fall für den Marketer – vom Nutzer geblockt. Im Internet ist dies einfacher denn je. Das heißt: Die digitale Wirtschaft braucht Daten, der Nutzer braucht Datenschutz. Auch Firmendaten müssen geschützt sein, beispielsweise wenn Informationen konkurrierender Unternehmen beim gleichen Cloud-Anbieter gespeichert sind. Datenschutz und Big Data sind kein Widerspruch, aber sie in einen harmonischen Einklang zu bringen, ist eine Zukunftsaufgabe.

Cloud-Lösungen mit Vorteilen

Mit der zunehmenden Verbreitung von Marketing Clouds wird diese Aufgabe nicht leichter. Die Cloud-Lösungen versprechen viele Vorteile: Das IT-

Wirrwarr im Marketing wird gelichtet, Datensilos werden abgeschafft und Kampagnen können effizient aus einer Hand gemanagt werden. Der Preis dafür ist vielfach hoch: Eigene Lösungen werden über Bord geworfen, stattdessen setzt man alles auf einen Anbieter – und der speichert auch noch alle Daten. „‚Cloud' heißt nichts anderes als anderer Leute Server, irgendwo'", sagt Michael Heine, Geschäftsführer der Companion Strategieberatung in Berlin. Der damit verbundene Kontrollverlust könne durchaus produktiv und effizient sein, „das gilt aber nicht für alle Daten", sagt Heine. Aus seiner Sicht sind Marketing Clouds eine Riesenchance für die Unternehmen, ihre Prozesse effizienter zu gestalten – allerdings nicht ohne eine interne Reorganisation. Kreations-, Content- und Planungsprozesse dürfen demnach nicht mehr in Mediensilos stattfinden. Wird nicht reorganisiert, sind Marketing-Clouds einfach nur „unproduktive Golfplatz-Software", so der Strategieberater. Außerdem würden dem Top-Management oft große Visionen erfolgreich verkauft, mit denen im Unternehmensalltag – für sehr viel Geld – neue Probleme entstehen.

Aber organisatorische Probleme sind noch eines der geringeren Übel. Ein mangelnder ››

Alles so unübersichtlich hier: Für viele Unternehmen ist die Anbindung einer Marketing Cloud eine Herausforderung, insbesondere für jene, die erst jetzt beginnen, sich mit dem Thema zu befassen.

Datenschutz kann sogar die komplette Existenz eines Unternehmens gefährden. Selbst den kleinen Handwerksbetrieb an der Ecke können Verstöße gegen den Datenschutz künftig teuer zu stehen kommen, denn am 25. Mai 2018 wird die neue EU-Datenschutzgrundverordnung (DSGVO) wirksam. Und damit kommen Bußgelder ins Spiel, die man so bisher nur aus Kartellverfahren kannte: Bei Verstößen gegen das neue Gesetz können Bußgelder bis zu einer Höhe von 20 Millionen Euro beziehungsweise von bis zu vier Prozent des weltweiten Jahresumsatzes eines Unternehmens erhoben werden – je nachdem, welcher Wert der höhere ist. Nach aktueller Regelung liegt der Höchstbetrag bei 300.000 Euro. Kleine Firmen müssen solche Höchststrafen zwar nicht fürchten, aber nach der neuen Regelung kann schon das kleinste Datenschutz-Vergehen geahndet und mit einem Bußgeld belegt werden.

Europaweite Harmonisierung kommt 2018

Aktuell wird der Datenschutz in Deutschland unter anderem von zwei zentralen, nationalen Gesetzen geregelt: Dem Bundesdatenschutzgesetz und dem Telemediengesetz. Die neue EU-Datenschutzgrundverordnung wird dafür sorgen, dass aus diesen beiden Gesetzen „Rumpfgesetze" werden, die nur noch jene Bereiche abdecken, die von der neuen EU-Datenschutzgrundverordnung nicht erfasst sind. Die gute Nachricht: Es wird keine Überschneidungen bei den Gesetzen geben, denn die nationalen Gesetze werden entsprechend angepasst. So dürfen in den EU-Ländern künftig keine Gesetze gelten, die ein höheres oder niedrigeres Datenschutzniveau aufrecht erhalten (siehe Interview Seite 38).

Die schlechte Nachricht: Die neue EU-Datenschutzgrundverordnung enthält sehr viele Regelungen, und es gibt noch keine belastbaren Behördenäußerungen, keine Urteile und darüber hinaus verschiedene Ansichten, wie manche Formulierungen auszulegen seien. „Momentan sind wir mit dem Gesetz allein", kommentiert Dr. Martin Schirmbacher, Fachanwalt für IT-Recht bei Härting Rechtsanwälte in Berlin, die aktuelle Situation. So sei das neue Gesetz in vielen Punkten unklar. „Das ist eine Herausforde-

Ängste auf beiden Seiten

Datenschutz spielt für Unternehmen und Verbraucher gleichermaßen eine immer wichtigere Rolle. Eine Entwicklung, die das Marketing nicht ausblenden darf.

83 Prozent der mittelständischen Unternehmen in Deutschland fordern mehr Sicherheit bei der Nutzung von Cloud-Diensten. Das geht aus dem Report „IT-Sicherheit und Datenschutz 2017" hervor, den die „Nationale Initiative für Informations- und Internet-Sicherheit e.V." (NIFIS) herausgebracht hat. Für 79 Prozent spielt es demnach bei der Auswahl eines Cloud-Anbieters eine entscheidende Rolle, welcher Datenschutzgesetzgebung er unterliegt. 97 Prozent bevorzugen den deutschen Datenschutz, 87 Prozent genügt der EU-Standard, lediglich sieben Prozent geben sich mit dem US-amerikanischen Datenschutzniveau zufrieden.

Für Verbraucher ist das Datenschutz-Thema nicht minder wichtig: Laut einer internationalen Studie von Ovum und dem britischen Marktforschungsunternehmen Opinion im Auftrag von Verint Systems, misstraut etwa jeder zweite Verbraucher (48 Prozent) Unternehmen, wenn es um den Umgang mit Daten geht. Die deutschen Verbraucher sind noch skeptischer. Was die Verwendung persönlicher Daten angeht, misstrauen hierzulande 61 Prozent den Unternehmen. Nur in Großbritannien ist das Misstrauen noch größer. Verlorenes Vertrauen wieder herzustellen, muss daher das Gebot der Stunde sein.

Improve your Marketing

Learning 1 Am 25. Mai 2018 wird in der EU die neue EU-Datenschutzgrundverordnung wirksam. Bei Verstößen drohen sehr hohe Bußgelder. Darum sollten sich Unternehmen schon jetzt mit der neuen Verordnung befassen.

Learning 2 Möchte man mit einem Marketing Cloud-Anbieter zusammenarbeiten, muss transparent geklärt werden, welche Daten erhoben werden, wo sie gespeichert und für welchen Zweck sie verwendet werden dürfen. Juristische Beratung ist ratsam.

Learning 3 Die gesetzlich vorgeschriebenen Datenschutzhinweise sind kein Marketing-Argument. Das Vertrauen der Konsumenten muss mit offensiv kommuniziertem Bekenntnis zum Schutz der Privatsphäre zurückgewonnen werden. Nutzer wollen Datensouveränität, -sicherheit, transparente Prozesse.

rung und lässt Spielraum. Erst Entscheidungen von Gerichten werden zeigen, wie einzelne Regelungen auszulegen sind", sagt Schirmbacher. Aus seiner Sicht ist das Gesetz zwar grundsätzlich gut für die Werbeindustrie, da es die verschiedenen Regelungen innerhalb Europas harmonisiert. Aber die neue Vorlage habe auch viele Schwächen und Unklarheiten. Insbesondere, wenn es um den Transfer und das Verarbeiten personenbezogener Daten geht, wie es für viele Clouds typisch ist. „Für die Verarbeitung personenbezogener Daten gilt weiterhin das Verbotsprinzip", erläutert Schirmbacher. So ist in der EU auch künftig jede Art der Verarbeitung personenbezogener Daten verboten – es sei denn, der Nutzer willigt ein oder es gibt ein Gesetz, das diese Nutzung erlaubt. Aus diesem Grund behilft sich die Branche seit Jahren mit „Verträgen zur Auftragsdatenverarbeitung". Wesentlicher Bestandteil solcher Vereinbarungen ist, dass der Auftragsdatenverarbeiter technische und organisatorische Maßnahmen treffen muss, um diverse Datenschutz-Anforderungen einzuhalten, zum Beispiel die Zutritts- oder die Zugriffskontrolle. Wird eine solche Vereinbarung geschlossen, gilt der Auftragsdatenverarbeiter juristisch nicht wie ein externer Dienstleister, sondern wie ein Teil des eigenen Unternehmens. Somit ist die Datenverarbeitung im Rahmen dieser Vereinbarungen gestattet.

Pikant ist: Der Begriff des Personenbezugs wird laut Schirmbacher nach neuem Recht eher weiter gefasst als nach der derzeitiger Rechtslage. Ein Rückschluss auf eine konkrete natürliche Person und deren Namen ist dem Experten zufolge nicht mehr erforderlich, damit Daten als personenbeziehbar gelten. „Vom neuen Recht betroffen ist also nicht nur jedes Unternehmen, das Arbeitnehmerdaten oder Kundendaten speichert, sondern auch alle Unternehmen, die mit IP-Adressen arbeiten. Das trifft insbesondere die digitale Werbebranche", so Schirmbacher.

Ein bürokratischer Koloss

Während sich an der rechtlichen Frage, wie man Daten verarbeiten darf, mit der neuen Regelung nur wenig ändert, gibt es in Bezug auf die operativen Anforderungen an die Unternehmen große Veränderungen. „Egal ob ein Unternehmen die Daten selbst verarbeitet oder es einem Dienstleister überlässt: Das Unternehmen ist künftig auch zusammen mit dem Dienstleister datenschutzrechtlich verantwortlich. Künftig hat es umfangreiche Abwägungs-, Dokumentations- und Nachweispflichten zu erfüllen", sagt Rechtsanwalt Michael Neuber, Justiziar und Leiter Recht und Regulierung beim Bundesverband Digitale Wirtschaft in Berlin. Dabei steht zunächst die Frage im Raum, wofür ein Unternehmen verantwortlich ist und wofür nicht. Künftig müssen Unternehmen nachweisbar dokumentieren, dass sie sich vorab Gedanken gemacht haben und Abwägungen getroffen haben, welche Daten sie warum und zu welchem Zweck verarbeiten möchten. Dazu gehört auch eine Einschätzung, ob die Daten risikobelastet sind und ob deren Verarbeitung einer Einwilligung bedarf oder nicht. „Die neue EU-Datenschutzgrundverordnung ist zu einem bürokratischen Koloss voller Rechtsunsicherheiten geworden, der für die modernen Anforderungen an einen funktionierenden digitalen Binnenmarkt sowie für die gesamte datengetriebene Ökonomie ein enormes Hindernis darstellt", sagt Neuber.

Wesentlicher Kritikpunkt: Eine Kategorisierung der Daten, nach denen sich gesetzliche Erlaubnisse richten könnten – wie bisher etwa »

für einfache Nutzungsdaten – wird mit der neuen EU-Datenschutzgrundverordnung abgeschafft. „Jedes Unternehmen muss künftig für jeden einzelnen Datenverarbeitungsvorgang separat entscheiden, ob, und wenn ja, welche Einwilligung für die Datenverarbeitung eingeholt werden muss. Das ist ein erheblicher Mehraufwand und mit extremen Rechtsunsicherheiten aufseiten der digitalen Wirtschaft verbunden", sagt Neuber. Beim Bundesverband Digitale Wirtschaft (BVDW) e.V. arbeitet man daran, Leitlinien und Handlungsempfehlungen auszuarbeiten, damit insbesondere standardmäßig wiederkehrende Datenverarbeitungsvorgänge einheitlich betrachtet werden können.

Vor dem Hintergrund der Clouds ergeben sich weitere Herausforderungen, denn Marketing Clouds funktionieren global und somit ist die Rechtslage recht unterschiedlich, wenn es um die Datenschutzanforderungen und die jeweiligen Rollen in den Ländern außerhalb der EU geht. „Welche Daten werden erhoben, wo liegen sie und für welchen Zweck dürfen diese Daten verwendet werden. Das sind Fragen, die zu Beginn jeder Cloud-Partnerschaft geklärt werden müssen", erläutert René Lamsfuß, Chief Research Officer bei Publicis Media, Düsseldorf. Entsprechend sind auch die rechtlichen Regelungen zu beachten. Wenn es beispielsweise früher notwendig war, Daten in die USA zu übermitteln, griff das Safe-Harbour-Abkommen. Dieses wurde mittlerweile durch das sogenannte EU-US Privacy Shield ersetzt. Alle großen Internetkonzerne haben sich mit Eigenerklärungen diesem Privacy Shield unterworfen – insgesamt mehr als 1.200 Firmen.

Rechtssicher in der Cloud

Doch viele Datenschutzbehörden stehen dem Privacy Shield skeptisch gegenüber. Nichtzuletzt hat Safe Harbor gezeigt, wie schnell ein Abkommen gekippt werden kann. Immer mehr Cloud-Anbieter eröffnen bereits Rechenzentren in EU-Ländern. Damit berücksichtigen sie besser die Interessen ihrer Kunden in Bezug auf Datensicherheit und Datenschutz und unterliegen dem strengen europäischen Datenschutzrecht. Denn für EU-weite Datentransfers greift die neue EU-Datenschutzgrundverordnung.

Für Agenturen ist eine rechtssichere Zusammenarbeit mit Marketing Clouds ein wichtiges Thema. „Alle Daten sind zentral abgelegt – man kann auf die gesamte Datenstruktur zugreifen und in Realtime mit den Daten arbeiten", erläutert Lamsfuß die Vorteile. Publicis Media hat frühzeitig eine eigene, offene technische Grundinfrastruktur geschaffen, um für Big Data und Cloud-Services gerüstet zu sein. Denn neben rechtlichen Aspekten ist bei der Anbindung von Marketing-Technologie die Frage wichtig, welche technischen Systeme eingesetzt werden; ob es notwendig ist, Daten zwischen den Systemen zu transferieren und unter welcher Vorgabe dies erfolgen kann. In solchen Fällen wird auch hier zwischen den Beteiligten ein entsprechender Vertrag zur Auftragsdatenverarbeitung geschlossen.

↗ *redaktion@acquisa.de* ‹

Service

Internet

- Europäische Informationsplattform zur grenzüberschreitenden Cloud-Nutzung, unter anderem mit Cloud Privacy Check:
  ↗ *https://cloudprivacycheck.eu*

- Prüfsiegel und Zertifizierungen können eine Entscheidungshilfe für die Zusammenarbeit mit einem Cloud-Anbieter sein:
  ↗ *https://www.trusted-cloud.de/*
  ↗ *https://staraudit.org/*

- Infowebseite der Federal Trade Commission zum EU-US Privacy Shield:
  ↗ *https://www.privacyshield.gov*

- Verzeichnis aller Unternehmen, die sich dem „Privacy Shield" unterworfen haben:
  ↗ *https://www.privacyshield.gov/list*

- EU-Datenschutzgrundverordnung:
  ↗ *https://www.datenschutz-grundverordnung.eu/*