DDV

Die treibende Kraft der Data Driven Economy

Branchentrends im Dialogmarketing

Der K(r)ampf mit dem Consent Management

Warum wir über Privacy Innovation sprechen müssen

Autor: **Uwe Roschmann**

Der K(r)ampf mit dem Consent Management

Warum wir dringend über Privacy Innovation sprechen müssen

Spätestens seit Inkrafttreten der DSGVO bzw. GDPR ist Dialogmarketing ein ausgesprochen heißes Eisen! Denn ohne kluges Consent Management wird bilaterale Kommunikation immer schwieriger. Privacy Tech und Privacy Innovation werden daher künftig stark an Bedeutung gewinnen, um die Privatsphäre von (potenziellen) Kunden zu schützen und Datenschutzvorgaben zu erfüllen. Und das betrifft jedes Unternehmen, das digital präsent ist.

„Privacy Tech“ dürfte aktuell nur Expert:innen ein Begriff sein. Dabei ist Privacy Tech zweifellos auf dem Vormarsch. Aber das Verständnis dafür, was die Datenschutztechnologien wirklich ausmacht, ist noch gering. Das wird sich jedoch bald ändern, da wir alle uns mit Privacy Tech auseinandersetzen werden müssen. Die Art und Weise, wie wir den Datenschutz verwalten und belastbare Systeme entwickeln, um die (Datenschutz-)Rechte aller zu respektieren, ändert sich rasant. Die kaskadenartigen Auswirkungen der sich weiter verschärfenden Datenschutzbestimmungen betrifft jede:n digitale:n Akteur:in. Sich umfassend auf das vorzubereiten, was als Nächstes ins Haus steht, wird geradezu geschäftskritisch.

Die Herausforderung besteht für Unternehmen darin, zu beweisen, dass sie die Daten, die sie sammeln, auch wirklich schützen können. Doch was genau ist Datenschutztechnologie? Privacy Tech ist letztlich ein Sammelbegriff, der Technologien zur Umsetzung des Datenschutzes beschreibt. Für eine genauere Definition und zum tieferen Verständnis ist es wichtig, den zentralen Begriff dahinter zu verstehen: Privatsphäre. So wird schnell deutlich, warum sich Privacy Tech von Cyber Security unterscheidet, auch wenn beide Bereiche sich intrinsisch bedingt natürlich überlappen. Die Privatsphäre zu schützen, ist etwas anderes als Hacker-Angriffe auf IT-Umgebungen abzuwehren. Denn Privatsphäre bezieht sich auf die individuelle Kontrolle des Einzelnen über persönliche Informationen, die er bzw. sie einem Unternehmen überlassen – oder eben nicht. Und Privatsphäre ist ein komplexes Gebilde, das Vertrauen, Selbstbestimmung und vor allem Kontext umfasst. Oder eben auch Verweigerung und Abgrenzung.

Wir müssen dringend unsere Perspektive auf den Datenschutz ändern

An Datenschutzgesetzen wird kontinuierlich gearbeitet, bestehende werden regelmäßig aktualisiert, neue werden erlassen. Datenschutzgesetze regeln unter anderem, welche Informationen gesammelt werden dürfen, und wie Betroffene welche Kontrolle über ihre Daten haben, sobald diese einmal an ein Unternehmen übertragen wurden. Diese Richtlinien, Gesetze und Vorgaben führen stets zu neuen Anforderungen, vom Umgang mit Einwilligungen (= Consent) zur Datenspeicherung auf individueller Ebene bis hin zu deren Datenverwaltung und -löschung.

So heißt es zum Beispiel in Artikel 7 der General Data Protection Regulation (GDPR): „Beruht die Verarbeitung von Daten auf einer Einwilligung, muss der für die Verarbeitung Verantwortliche in der Lage sein nachzuweisen, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat." Diese Formulierung soll mit einer vermeintlich einfachen Lösung vor Missbräuchen schützen. Eine einfache Lösung ist aber nicht immer die gründlichste: Die Debatte darüber, ob eine Zustimmung als erteilt gilt, ohne dass Betroffene wirklich allumfassend verstehen (können), was mit ihren Daten passiert, wird lauter. Und mal ehrlich: wer von uns liest und versteht schon eine Datenschutzerklärung Satz für Satz, Seite für Seite – noch dazu ohne Jura-Abschluss? Und selbst wenn: Heißt das, dass ein Unternehmen mit den Daten mehr oder weniger tun kann, was es will, solange es um Erlaubnis bittet?

Wie sich die Rechtsprechung rund um das Consent Management und damit auch das Consent Management selbst weiterentwickeln wird, kann niemand so recht voraussagen. Und dennoch sind Unternehmen gezwungen, sich intensiv damit auseinanderzusetzen und zu überdenken, was sie über ihre Kund:innen tatsächlich wissen und auch wissen wollen. Obwohl seit Anbeginn des Internets das Paradigma galt, „vom Unbekannten zum Bekannten" zu gelangen, ist das Ziel heute dazu vollkommen konträr. Es besteht darin, als Allererstes sicherzustellen, dass man die Person, mit der man in Kontakt steht, unkenntlich oder „unknowable" machen kann, bevor man sich überhaupt das Recht verdient, Daten über sie zu generieren.

Privatsphäre und Vertrauen als neue Erfolgswährung

Im Internet klicken Nutzer:innen auf alles, was sie sehen, lesen, kaufen, weiterleiten wollen. Immer schon. Aber inzwischen klickt das Web zurück. Das Internet ist zu einem skalierbaren Verteilernetzwerk geworden. Chatbots und andere KI-basierte Interaktionen sind griffige Beispiele dafür, wie sich das Internet von einer Einbahnstraße hin zu einer in beide Richtungen befahrbaren Autobahn entwickelt. Datenschutzgesetze greifen diese neue Art der bilateralen Beziehung auf und versuchen notwendige Leitplanken zu setzen, die den Einzelnen und seine Individualität, seine Daten und seine Würde schützen sollen. Grundsätzlich ist das auch gut so. Vor fünfzehn Jahren hätten wir wohl kaum erwartet, dass das Internet heute so ist, wie es ist. Parallel hat sich eben auch der Datenschutz weiterentwickelt.

Und seien wir mal ehrlich: Hätten wir uns selbst vor fünfzehn Jahren gefragt, was „digitale Denke“ in Zukunft bedeuten wird, wir hätten wohl sensationell danebengelegen. Höchste Zeit also, einmal innezuhalten und die Veränderungen zu verdauen, die nicht erst in der letzten Dekade über uns hereingebrochen sind. Heute ist „digitales Denken“ kein vages Konzept mehr, es ist vielmehr die übliche, die „normale“ Denkweise. Und ebenso muss auch die Denkweise zum Datenschutz auf die nächste Stufe gehoben werden.

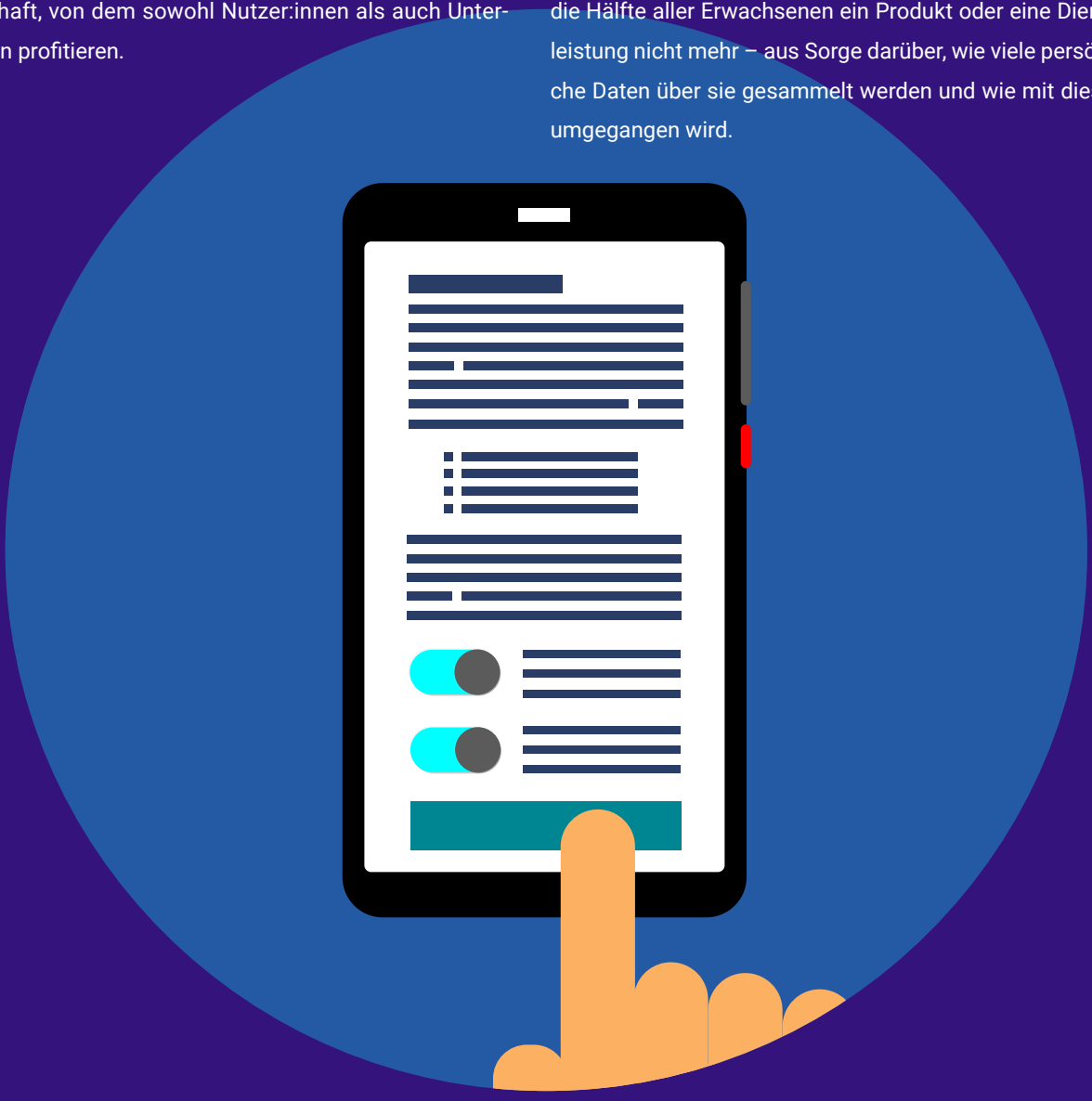
Das bedeutet aber auch: Nutzer:innen sind nicht länger Objekte, die einfach nur datenmäßig erfasst und bei der Stange gehalten werden können. Nutzer:innen sind zu einer Macht geworden. Während es früher im Internet eher wie auf einer Safari zuging, bei der man aus einem Geländewagen heraus überall in der großen weiten Internetwildnis Nutzer:innen entdecken konnte, sitzen die Nutzer:innen heute mit im Geländewagen. Diese Nähe bedeutet allerdings nicht, dass es einfacher geworden ist. Im Gegenteil, sie können aus dem Jeep aussteigen, sie können erzwingen, dass wir direkt vergessen, dass sie jemals im selben Wagen saßen, und sie können das Fahrzeug beim Aussteigen sogar so fahruntauglich machen, dass wir Spuren nicht mehr folgen können und Retargeting keinerlei Sinn macht.

Unternehmen müssen heute also unter ganz anderen Voraussetzungen und zu ganz anderen Bedingungen agieren, und sie müssen sich Nutzer:innen auf Augenhöhe nähern. Welche Informationen möchten Nutzer:innen überhaupt preisgeben, und welche Daten geben sie bewusst zur Speicherung und Nutzung frei? Welche (guten) Gründe liefern Unternehmen dafür, dass sie wissen wollen, was sie wissen wollen? Unternehmen müssen einfühlsamer und vor allem verantwortungsbewusster werden. Wer würde schon wollen, dass das eigene 13-jährige Kind von einem Unternehmen vollständig getrackt und dass dessen Daten auf dem freien Markt verkauft werden?

Was jetzt zu tun ist

Wie groß der Wunsch von Nutzer:innen nach der Hoheit über die eigenen Daten ist, zeigt sich am Erfolg von Anbietern wie z. B. DuckDuckGo, die eine Privatsphäre-freundliche Suchmaschine anbieten. Sozusagen „Privacy as a Service“ und zugleich Datenschutz als definierendes Unterscheidungsmerkmal. Privatsphäre wird hier zum zentralen Bestandteil digitaler Wertschöpfung. Privacy Innovation par excellence. Und das ist sehr wohl auf jedes Unternehmen übertragbar: Ein datenschutzkonformer Umgang mit Informationen sollte nicht als lästige Pflicht wahrgenommen werden. Vielmehr ergibt sich aus einem gut strukturierten Schutz der Privatsphäre ein Wettbewerbsvorteil, der sich langfristig auszahlen wird. Kluges Consent Management ist daher ein wichtiger Baustein der digitalen Wirtschaft, von dem sowohl Nutzer:innen als auch Unternehmen profitieren.

Datenschutztechnologien sind unumgänglich, um das endlos wachsende Datenuniversum effektiv zu verwalten. Internetnutzer:innen achten immer penibler darauf, was Unternehmen mit (ihren) Daten machen. Welche Unternehmen erfassen Kundendaten, um sie an andere Unternehmen weiterzugeben und zu verkaufen? Ein Verdacht genügt, um das Vertrauensverhältnis zwischen Unternehmen oder Marke zu schädigen und kann zu großen Imageschäden führen. Unternehmen müssen also die Datenschutzrechte ihrer Kund:innen bedingungslos respektieren, weil Nutzer:innen es erwarten und es schlicht auch verdienen. Dass der Umgang mit Daten von Konsument:innen einen direkten Einfluss auf weitere Käufe hat, zeigt z. B. **diese Studie aus den USA**. Danach nutzen die Hälfte aller Erwachsenen ein Produkt oder eine Dienstleistung nicht mehr – aus Sorge darüber, wie viele persönliche Daten über sie gesammelt werden und wie mit diesen umgegangen wird.



Der Datenschutz erzwingt aber nicht nur eine fortwährende Anpassung des Einwilligungsmanagements. Auch die der Datensammlung zugrunde liegenden Technologien entwickeln sich entsprechend weiter. Unternehmen müssen also darüber nachdenken, was sie infrastrukturell tun müssen, um dieses neue Denken anzunehmen und umzusetzen. Wie wollen sie Privatsphären wirklich respektieren und schützen, wie und welche Daten sollen letztlich verwendet und welche weitergegeben werden (dürfen)? Privacy Tech als wesentlicher Baustein des digitalen Geschäfts wird darüber mitentscheiden, welche Unternehmen das Vertrauen der Verbraucher:innen gewinnen und langfristig behalten – und welche nicht.

Verglichen mit anderen Anwendungen und digitalen Angeboten mag die Privacy-Tech-Landschaft hinsichtlich der Marktfähigkeit gerade noch im Entstehen sein, doch darf man nicht außer Acht lassen, dass sie aus jahrzehntelangen Entwicklungen des Datenschutzes und dessen juristischen Rahmenbedingungen gespeist wird. Diese Entwicklungen verhelfen Privacy Tech zu einer einzigartigen Ausgangsposition. Sie haben den Weg für Datenschutzinnovationen längst geebnet und einen Markt für Lösungen von Datenschutzproblemen geschaffen.

Tatsache ist, dass Transparenz darüber, wie Daten erfasst, gespeichert und genutzt werden, das Vertrauen der Kund:innen massiv stärkt. Nutzer:innen erwarten einen absolut rechtskonformen Umgang mit persönlichen Daten. Es gibt somit einen mächtigen Treiber hinter Consent Management, Privacy Tech und Privacy Innovation: Das Vertrauen der Kund:innen. Das Wahren der Privatsphäre ist keine Pflichtübung, sondern die angemessene und geforderte Reaktion von Wirtschaftsunternehmen auf die Wünsche der Verbraucher:innen. Es gilt jetzt, das richtige Fundament zu gießen, auf dem eine echt vertrauensvolle digitale Beziehung zwischen beiden Seiten künftig wachsen und gedeihen kann.

Autor:

Uwe Roschmann
Digitas Pixelpark GmbH
Heidi-Kabel-Platz 2
20099 Hamburg
Tel. +49 40 341 01 0
uwe.roschmann@digitaspixelpark.com
www.digitaspixelpark.com

Uwe Roschmann (36) verantwortet als Managing Director bei Digitas Pixelpark das Neugeschäft, die strategische Ausrichtung sowie das Produkt- und Serviceportfolio der Agentur und entwickelt maßgeschneiderte, kundenindividuelle Lösungen im digitalen Bereich, insbesondere für Zukunftsthemen. Aktuell treiben ihn neben Social Commerce insbesondere die Bereiche Commerce, hier in aktiver Funktion auch für Publicis Commerce Germany, aber auch Marketing-Automatisierung, Data-driven Marketing Solutions sowie Consumer Journey, Content und Social Media um. Der diplomierte Wirtschaftswissenschaftler hatte zuvor verschiedene Positionen in den Bereichen Digital, Media und Kreation bei der Publicis Groupe inne und betreute unter anderem Etats wie Daimler/Mercedes-Benz, Telefónica/O2, Zalando, Novartis und L'Oréal. Uwe Roschmann ist außerdem Geschäftsführer des Online-Spirituosen-Vertriebs somelio.de.