gfm

Forschungsreihe 2/22

Privacy as Strategy

Ein Framework für das kundenzentrierte Datenmanagement

ABSTRACT

Datenschutz und datengetriebenes Marketing müssen kein Widerspruch sein. Marketers können mit einer Ausrichtung der eigenen Datenverarbeitungsprozessen auf die Bedürfnisse der Kundschaft nicht nur das Vertrauen in dieselben stärken, sondern auch ein Fundament für effizientere Marketingpraktiken legen. Dieser Artikel zeigt auf, wie ein kundenzentriertes Datenmanagement über die strategische Ebene auf einzelne Customer Journeys, Mitarbeitende und schliesslich Touchpoints übersetzt werden kann. Das Ziel: ein stärkeres Kundenengagement in Einklang mit modernen Datenschutzgesetzen.

EINLEITUNG

Mit dem wachsenden Bewusstsein für die informationelle Privatheit in der Bevölkerung, wird die Verankerung derselben im Unternehmen zu einer wichtigen Herausforderung des Marketings. Die Wissenschaft empfiehlt schon lange, dass sich Marketers stärker im Schutz der digitalen Privatheit engagieren sollten[1–3] – besonders wenn sie die notwendige Vertrauensbasis für den Einsatz noch datenintensiverer Innovation (wie z.B. AI getriebene Personalisierung) aufbauen möchten.
Der Schutz der informationellen Privatheit – definiert aus Kundensicht als die Fähigkeit zu steuern, wieviel von einem selbst Drittpersonen wahrnehmen können – wurde bereits in vielen Staaten als grundlegendes Recht verankert (z.B. DSGVO Art. 1, California Consumer Privacy Act [CCPA] § 1798.100., Personal Information Protection Law der Volksrepublik China). Auch wenn sich die grossen Klagen unter der Europäischen Datenschutz-Grundverordnung (DSGVO) bisher hauptsächlich gegen Konzerne wie Google und Amazon richteten (vgl. Abb. 1), bedeutet dies nicht, dass Datenschutz kein Thema für alle anderen Unternehmen ist. Der Zugang zu, sowie die Instrumente für professionelle Datenverarbeitung stehen immer mehr Branchen zur Verfügung. Das entsprechende Datenschutz- und Cyber Security-Wissen hinkt bei diesen Firmen allerdings weit hinter der Big Tech Konkurrenz hinterher.

Gleichzeitig werden bisher einfach nutzbare Instrumente zur Datenabfrage, wie Third-Party-Cookies, vermehrt verschwinden. Einerseits wegen entsprechenden Urteilen unter der DSGVO und andererseits, weil wichtige Browseranbieter wie Google, Apple und Mozilla diese nicht mehr unterstützen wollen. Dieses «Cookiemageddon» wird sowohl kleine als auch grössere Agenturen dazu zwingen, eine eigene Basis an First Party Daten zu schaffen.

Dabei wären Kunden durchaus bereit mehr mit Unternehmen zu teilen. In einer aktuellen Studie von McKinsey gab eine Mehrheit der Befragten an, dass sie persönliche Daten im Austausch gegen tangible Vorteile preisgeben würden[4]. Google kommt zu dem gleichen Schluss – in ihrer Studie gaben knapp 9 von 10 Befragten an, dass sie wahrscheinlicher öfters bei

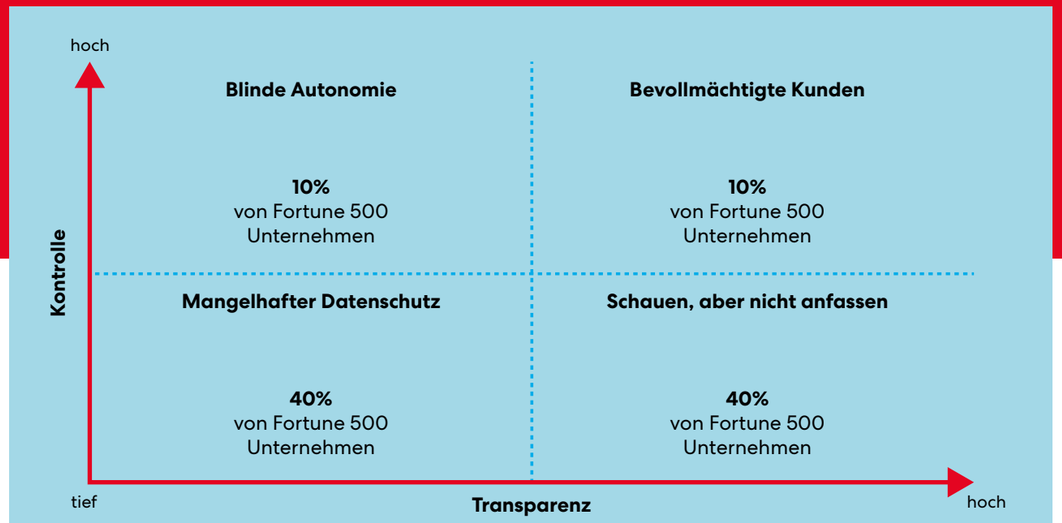

Abbildung 1: Datenmanagement aus Kundensicht 2019 [7]

einer Marke einkaufen würden, wenn diese ihnen relevante Personalisierungen im Austausch gegen Daten bieten würde[5]. Trotzdem wird dieses Potenzial von den meisten Unternehmen momentan nicht adäquat ausgeschöpft. Dies liegt daran, dass informationelle Privatheit von vielen Unternehmen noch hauptsächlich als Compliance Problem gesehen wird und nicht als zentraler Bestandteil der Customer Experience[6]. Datenverarbeitung treibt die Personalisierung vieler nachgefragter Dienste, doch der Schutz dieser Daten sollte nicht als Einschränkung für diesen Prozess gesehen werden, sondern als einen essentiellen Teil davon.

KUNDENZENTRIERTES DATENMANAGEMENT

Aus Sicht des Marketings und des Managements bedeutet ein kundenzentriertes Datenmanagement, dass Datenverarbeitungen den Privatheitsbedürfnissen der Kundschaft entsprechen und zum Kundenengagement beitragen. Das Ziel ist eine «kontinuierliche Interaktion zwischen Unternehmen und Kunden - welche vom Unternehmen angeboten und vom Kunden gewählt»[8] wird.

Tech-Konzerne verfolgen vielfach das Konzept der datengetriebenen Marketingautomatisierung, welche auf der Abfrage von Unmengen an überschüssigen Kundendaten[9] beruht und somit auch die die Kompetenzen, diese Daten zu schützen und zu analysieren, voraussetzt. Nicht viele Unternehmen sind heute bereits in der Lage diese Mischung an Fähigkeiten aufzubieten. Allerdings ist es Unternehmen möglich, mittels eines kundenzentrierten Datenmanagements ein nachhaltiges Kundenengagement zu erreichen. Zwar müssen hierfür auch verschiedene Aktivitäten neu ausgerichtet werden, jedoch scheint es keine Alternative zu geben. Wer in Zukunft versucht, ohne legalen Zugang zu den Daten seiner Kundschaft eine Kundenbeziehung aufzubauen und zu pflegen, verkennt die Grösse der Herausforderung.

In unseren Studien am Institut für Marketing & Customer Insight konnten wir vier Ebenen identifizieren, die ein kundenzentriertes Datenmanagements unterstützen und ermöglichen[10]. Im Mittelpunkt steht

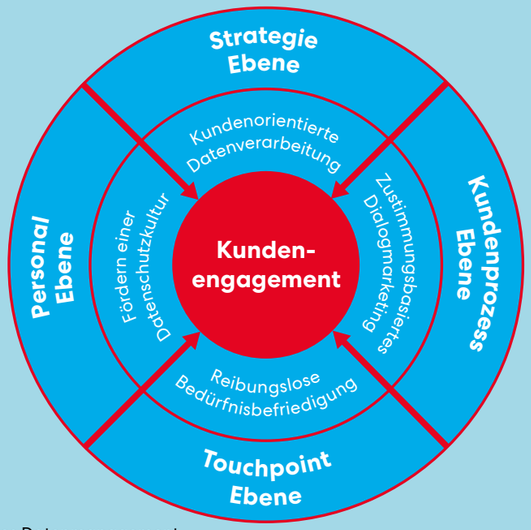

Abbildung 2: Kundenzentriertes Datenmanagement

dabei das Ziel, einen erlaubten Austausch zu etablieren, bei dem die Weitergabe von persönlichen Daten mit einem persönlichen Mehrwert für die Kundschaft verbunden ist. Dieses positive «Customer Engagement» (im folgenden Kundenengagement genannt) ist dann in der Konsequenz der integrierten und ganzheitlichen Gestaltung der folgenden Unternehmens- und Marketingaktivitäten zu verstehen:

- **Strategie Ebene:** Kundenzentrierte Datenverarbeitung – i.e. Zweckgebundenheit der Datenstrategie garantieren und signalisieren.
- **Kundenprozess Ebene:** Zustimmungsbasiertes Dialogmarketing – i.e. Effektivität der Datenverarbeitung garantieren.
- **Personal Ebene:** Fördern einer Datenschutzkultur – i.e. die notwendigen Unternehmensressourcen zur Datenverarbeitung nachhaltig im Unternehmen verankern.
- **Touchpoint Ebene:** Reibungslose Bedürfnisbefriedigung – i.e. Effizienz der Datenverarbeitung garantieren.

Dieser Prozess ist anspruchsvoll und gelingt nur, wenn der Status Quo des eigenen Unternehmens realistisch analysiert wird. Falls keiner der in diesem Artikel angesprochenen Aspekte im eigenen Unternehmen anzutreffen ist, braucht es vermutlich einiges an Vorarbeit, bevor eine Basis für ein kundenzentriertes Datenmanagement gebaut werden kann. Aus unserer Erfahrung können wir aber davon ausgehen, dass die notwendigen «Zutaten» in den meisten Unternehmen bereits vorhanden sind.

CUSTOMER CENTRICITY ALS STRATEGISCHER WEGWEISER

Ein strategischer Fokus ist für die Entwicklung jeglicher Unternehmensressourcen notwendig, denn nur so können «schwer zu imitierende interne und externe Kompetenzen»[11] geschaffen werden. Dasselbe trifft auf das kundenzentrierte Datenmanagement eines Unternehmens zu: es braucht eine extern kommunizierte und intern gelebte Vision, welche die Basis für alle Datenschutzbelangen bildet[10]. Intern bedeutet dies, dass Datenschutzziele nicht einfach als legale Grundlage definiert

Aktuelles Datenschutz-Paradigma	Kundenzentriertes Datenschutz-Paradigma
• **Motto:** Datenschutz als rechtliches Problem	• **Motto:** Datenschutz als Marketing-Strategie
• **Zentrales Anliegen:** Wer erhebt welche Daten?	• **Zentrales Anliegen:** Wie und für was werden die Daten verwendet?
• **Werkzeuge:** Benachrichtigung & Zustimmung	• **Werkzeuge:** Dialog- & Dienstleistungsmentalität
• **Ansatz:** Reaktiv	• **Ansatz:** Proaktiv
• **Zentraler Treiber:** Gesetze & Politik	• **Zentraler Treiber:** Kundenbedürfnisse
• **Fokus:** Datenmenge	• **Fokus:** Datenqualität

Abbildung 3: Eigenschaften kundenzentriertes Datenschutzparadigma [6]

werden, sondern wie andere strategische Ziele direkt adressiert werden. Das Resultat soll eine Unternehmenskultur sein, die Datenschutz als Gruppenaufgabe und nicht individuelle Verantwortung sieht. Datenerhebende und datenverarbeitende Mitarbeitende müssen wissen, wie viele Daten für welchen Zweck erhoben werden. Einerseits um zukünftigen Bedarf zu steuern und «Datenüberschüsse» zu vermeiden - andererseits um der Kundschaft den Zweck der Erhebung ohne legales Kauderwelsch vermitteln zu können.

Gleichzeitig sollten sich Unternehmen für mehr Verantwortung innerhalb der eigenen Industrie einsetzen, wenn sie sich glaubwürdig von der Konkurrenz abheben möchten. Kurzfristig bedeutet dies, sich von Konkurrenten oder Lieferanten mit zweifelhaften Datenschutzpraktiken zu distanzieren. Ein prominentes Beispiel wäre der Kampf von Apple gegen Facebook über transparentere Datenerhebung auf iOS Geräten[12].
Langfristig kann eine effektive Datenschutzstrategie nur glaubwürdig aufrechterhalten werden, wenn sich das Unternehmen für bessere Datenschutzstandards in seinem Markt einsetzt; entweder durch die freiwillige Adoption von anerkannten Privatheitslabels oder dem proaktiven Etablieren von neuen Sicherheitsstandards. Dass dies mit vergleichsweise einfachen Mitteln möglich ist, haben letztes Jahr die Schweizer Unternehmen Migros, Swisscom, SBB und Credit Suisse mit ihrer «Privacy Icons» Initiative bewiesen. Diese etablierte eine einheitliche Bildsprache, um die Kundschaft effizienter über Datenabfragen von Dienstleistungen zu informieren[13].

Der Treiber für solche Initiativen sollte aus einer kundenzentrierten Denkweise kommen. Sprich, eine Ausrichtung der Geschäftstätigkeit auf die Bedürfnisse der Kundschaft und nicht den Verkauf von Produkten. Auf der strategischen Ebene bedeutet dies, die Makro-Customer Journey der eigenen Produkte zu kennen und die eigene Datenverarbeitung entsprechend abzustimmen. Je nach Unternehmen lassen sich die folgenden vier «Extreme» von Makro-Journeys abbilden[14]:

- **Gebrauchsgüter:** Für Low-Involvement Produkte mit einem hohen Substitutionsgrad (z.B. Lebensmittel) ist die Entscheidungs- und Kaufphase meist sehr

kurz. Dementsprechend sollten sich Datenverarbeitungsprojekte darauf konzentrieren, die notwendigen Daten zur Elimination von Friktionen im Kaufprozess zu finden und das Upselling zu erleichtern.

- **Konsumgüter:** Low-Involvement Produkte mit einem tiefen Substitutionsgrad (z.B. Medikamente) haben eine etwas längere Abwägungsphase. Dementsprechend ist es wichtig, dass erhobene Daten dazu verwendet werden, sowohl das Produkt selbst als auch die Betreuung an den einzelnen Touchpoints zu verbessern.

- **Loyalitätsgüter**: Güter mit einem hohen Substitutionsgrad und hohem Involvement (z.B. Unterhaltungselektronik) haben eine lange Entscheidungsphase. Da weitere Käufe von einer hohen Loyalität der Kundschaft abhängig sind, sollten Datenverarbeitungsprozesse nicht nur zu der Verbesserung der Customer Journey beitragen, sondern auch zu der kontinuierlichen Verbesserung der eigenen Produkte.

- **Evaluationsgüter:** Je niedriger der Substitutionsgrad für ein High-Involvement Produkt ist (z.B. Finanzdienstleistungen), desto länger und wichtiger ist die Vorkaufsphase. Datenerhebungen sollten deshalb die Prozesse stützen, welche der Kundschaft in der Recherche, Evaluation und Abwägung helfen.

In all diesen Prozessen ist es essentiell, dass Datenverarbeitungsprozesse möglichst komplett auf den beschriebenen Zweck gebunden werden. Konkret bedeutet dies, dass keine Daten spekulativ erhoben werden, um zukünftige Änderungen der Makro-Journeys vorauszuahnen. Zur Überprüfung der Datenschutzorientierung ihrer Makro-Journeys sollten sich Marketers dementsprechend die folgenden Fragen stellen:

- Nennen wir den Schutz der digitalen Privatheit unserer Kundschaft als strategisches Ziel und können wir den Zweck unserer Verarbeitungsprozesse präzise formulieren?

- Ist unser Unternehmen strukturell kundenzentriert und nicht produktorientiert ausgerichtet?

- Verfügen wir über eine interne Anleitung zur fairen Nutzung von Personendaten, die jedem datenverarbeitenden Mitarbeitenden bekannt ist?

- Messen wir Privatheitskennzahlen (z.B. Anzahl an Datenschutzanfragen) welche in einem regelmässigen Audit oder von einer unabhängigen Stelle überprüft werden?

- Engagieren wir uns in Privatheitsprojekten (z.B. Cyber Security Data Clean Rooms) und distanzieren wir uns von Industrieteilnehmenden mit unbekannten Datenschutzpraktiken?

- Kaufen wir keine Personendaten ein und verkaufen wir keine unserer Personendaten weiter?

KUNDENPROZESSE OPTIMIEREN

Eine oft zitierte Ursache für Kundenunzufriedenheit in Bezug auf kommerzielle Datenverarbeitung, ist das einseitige Machtverhältnis zwischen Kundschaft und Unternehmen[10]. Gleichzeitig ist auch bekannt, dass dieses Machtverhältnis oft akzeptiert werden kann, wenn die Kundschaft den Wert in der Gegenleistung sieht oder bereits eine Verbundenheit zu dem Unternehmen fühlt. Die strategische Ausrichtung stützt dabei hauptsächlich die Vertrauensdimension, aber sie trägt wenig zu der Kommunikation des Kundennutzens bei. Dies liegt daran, dass aus Kundensicht der erwartete Gegenwert einer Datenfreigabe zwischen den Phasen der Customer Journey nicht konstant bleibt. Dementsprechend ist es essentiell, dass Datenabfragen innerhalb der einzelnen Customer Journeys den Prinzipien des Permission Marketings folgen[15]:

- **Vorhersehbar:** Angebote, Formulare und sonstige Datenabfragen sollten nur in Kontexten präsentiert werden, in denen Kunden mit ihnen rechnen können (z.B. im Shop, aber nicht auf der Startseite). Die Risiken einer Datenfreigabe sollten zudem genauso vorhersehbar sein (z.B. wird bei der Anmeldung zu einem Newsletter nicht erwartet, dass die eigene Emailadresse weiterverkauft werden könnte).

- **Relevant:** Datenabfragen sollten Informationen oder Personalisierungen bieten, welche eine bereits demonstrierte Relevanz für die entsprechende Kundschaft haben (z.B. Zugang zu einem neuen Artikel anstatt Verkauf eines gesamten Abonnements). Die Frequenz des Kontaktes ist hier zentral, da die Relevanz von Inhalten durch übermässige Konfrontation (z.B. jeden Tag eine Erinnerung schicken) oder schlechtem Timing (z.B. immer erst vor Feierabend) ebenfalls geschmälert wird.

- **Persönlich:** Wenn persönliche oder tiefere Kundendaten abgefragt oder Angebote gemacht werden, sollten sich diese explizit auf die Person hinter den Daten beziehen (z.B. ein Anruf eines Beraters anstatt einer schriftlichen Abfrage über das Onlineportal). Nur so hat die Kundschaft einen Anreiz, Datenabfragen ernsthaft abzuwägen und ist weniger wahrscheinlich sich z.B. durch falsche Angaben zu schützen[16].

Aus Datenschutzsicht ist eine informierte Abwägung der Datenteilung für die Kundschaft nur in diesem eher engen Wirkungsbereich möglich. Aus Marketingsicht ist dies nichts Neues: sowohl die Idee der «kleinen Jas» aus dem Dialogmarketing als auch das Pull-getriebene Permission Marketing[15] sind inzwischen über zwanzig Jahre alt. Im Zeitalter des Web 2.0 verloren beide diese Ansätze allerdings aufgrund der vergleichbaren Einfachheit der Push Werbung über Plattformen wie Amazon, Google und Facebook, an Relevanz.

Dennoch ist die Idee hinter diesen Ansätzen relativ simpel: innerhalb der Customer

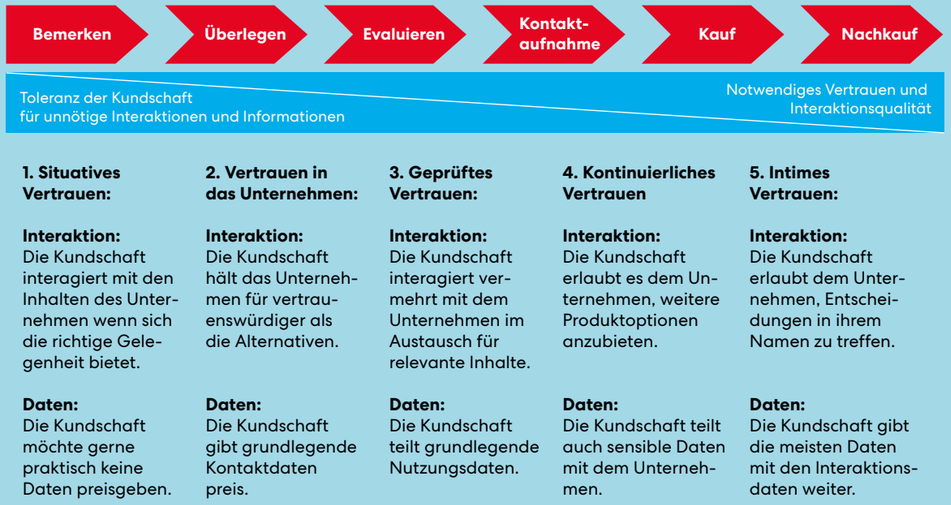

Abbildung 4: Vertrauensmomente in der Customer Journey

Journey hat die Kundschaft eine sinkende Toleranz für unnötige Datenabfragen und ein steigendes Bedürfnis nach Vertrauen in das Unternehmen (siehe Abb. 4). Je nach Makro-Journey und Zielgruppe mag diese Balance unterschiedlich sein, aber grundsätzlich lassen sich in jeder Journey neben den «Moments of Truth» - also, wenn die Kundschaft sich erstmals für ein Unternehmen entscheidet – auch mehrere «Moments of Trust» abbilden. Dies sind all die Momente, in denen sich die Kundschaft aktiv entscheidet, mehr Daten mit einem Unternehmen zu teilen und zu weiteren Kontaktaufnahmen einzuwilligen.

Je mehr Zustimmung ein Unternehmen an diesen «Moments of Trust» generieren kann (d.h. wie viele «kleine Jas» es erhält), desto grösser ist die Chance eines Vertragsabschlusses und einer langwährenden Kundenbeziehung. Dabei ist es wichtig zu beachten, dass die Art der Datenabfragen transparent, kontrollierbar und zu den einzelnen Customer Journeys passend sind. Die Privatheitsfreundlichkeit der eigenen «Moments of Trust» können Marketers anhand der folgenden Fragen überprüfen:

- Werden unsere Personendaten stets zu einem klaren Zweck und nur selten doppelt erhoben?

- Bieten wir genügend Zeit in unserer Customer Journey um die Kundschaft über mehrere «kleine Jas» zu relevanten Datenabfragen graduell zu dem «grossen Ja» eines Kaufs zu führen?

- Führen wir mit unserer Kundschaft einen Datenschutzdialog meistens schon bevor ein Kauf getätigt wurde?

- Hat unsere Kundschaft direkte Kontrolle über ihre bei uns gespeicherten Daten, um diese selbst zu aktualisieren oder bearbeiten?

- Kann unsere Kundschaft Fragen zur Datenverarbeitung einfach & schnell mit unseren Mitarbeitenden besprechen?

VERANKERUNG IM PERSONALMANAGEMENT

Die Akquise und Förderung von Fähigkeiten im Human Ressourcen Pool leisten einen direkten Beitrag zur Umsetzung der operativen und strategischen Ziele eines Unternehmens. Bereits für die Umsetzung der einfachsten Datenverarbeitungsstrategien braucht es eine Vielzahl an entsprechenden Fähigkeiten (z.B. einen CPO, Datenanalysten, IT-Spezialisten). Die genaue Zusammensetzung der notwendigen Fähigkeiten ergibt sich aus den strategischen Zielen, doch tendenziell sollte die interne Nachfrage nach Analysten und IT-Personal in Tandem mit erschlossenen Datenquellen steigen. «Es ist möglich, qualitativ hochwertige, räumlich explizite Daten (...) bereitzustellen und gleichzeitig sensible Informationen so zu schützen, dass die Privatheit und die Ressourcen (von natürlichen Personen) geschützt werden. Dies erfordert jedoch erhebliche Investitionen in technologische Lösungen, Datenpolitik und Transparenzbemühungen»[17]. Klassische Softskills sind dabei besonders in Unternehmen mit intensivem Kundenkontakt (z.B. Finanzdienstleistungen) nicht zu vernachlässigen – schliesslich ist die Kommunikation des Kundennutzens bezüglich der Verarbeitung von Kundendaten ein wichtiger Bestandteil des Kundenerlebnisses.

Wenn diese Fähigkeiten im Unternehmen vorhanden sind, müssen diese wiederum durch eine transparente Datenarchitektur und lenkende Kennzahlen in der Anreizstruktur des Unternehmens verankert werden. Als letzter Schritt im Prozess der Verankerung von Datenschutzkenntnissen im Personalbestand eines Unternehmens dienen persönliche Interaktionen als wichtige Lernquelle für Mitarbeitende und tragen so dazu bei, den Datenschutz einer Firma mit den Anforderungen ihrer Kundschaft in Einklang zu bringen[10].

Die Wirksamkeit einer unternehmerischen «Datenschutzkultur» ist schwierig messbar, da diese stark von den jeweiligen Datenverarbeitungszielen abhängt. Marketers können die grundlegenden Eigenschaften jedoch trotzdem anhand der folgenden Fragen abschätzen:

- Führt unser/e Chief Privacy Officer (CPO) oder Datenschutzbeauftrage/r ein eigenes Team?

- Ist in unserem Unternehmen klar geregelt, welche Personen weshalb zu welchen Personendaten Zugang haben?

- Müssen alle Mitarbeitenden ein Datenschutztraining oder Datenschutzseminar abschliessen?

- Besteht üblicherweise genügend Zeit, um die Daten in unserem CRM (oder ähnlichem System) aktuell zu halten?

- Wissen Mitarbeitende mit Kundenkontakt welche Personendaten für welchen Zweck erhoben werden?

VERBESSERUNG DER EINZELNEN TOUCHPOINTS

Sowohl in der Praxis als auch in der Wissenschaft wurde bisher am meisten Aufmerksamkeit dem Datenschutz am Punkt der Erhebung, also an den einzelnen Touchpoints, geschenkt[10]. Wenn allerdings keine Datenverarbeitungsstrategie vorhanden ist, welche über die Customer Journeys hinunter auf einzelne Touchpoints übersetzt wird, kommen diese Bemühungen der «Reparatur eines tropfenden Wasserhahns auf einem sinkenden Schiff gleich»[18]. Aus der Erfahrung vieler Unternehmen mit der Implementation der DSGVO-Grundprinzipien wissen wir, dass das Fehlen einer klaren Datenmanagementstrategie sowie mangelnde Übersetzung derselben auf die operative Ebene eine enorme Hürde darstellt. Dies ist auch der Grund, weshalb der Strom an Klagen aufgrund nicht gesetzeskonformer Verarbeitungsprozesse auch vier Jahre nach der Ratifizierung der DSGVO noch nicht abgebrochen ist.

Dafür stehen Unternehmen, welche diese Schritte bereits vollzogen haben, eine breite Palette an Instrumenten zur Verfügung, welche ihrer Kundschaft transparentere und einfacher kontrollierbare Datenverarbeitungsprozesse ermöglichen. Aufgezählt sind die am häufigsten genannten Privatheitspraktiken auf Touchpointebene eine transparente (sprich, nicht legalistisch formulierte) Kommunikation, einfaches Datenmanagement (sprich, DSGVO-konform) und Verzicht auf manipulative Nudges. Best-Practices für einzelne Aspekte des Datenschutzes sind hier überraschenderweise bei den Big-Tech Unternehmen zu finden. Von Apples App Tracking Transparenz, zu Googles Datenschutzcheck bis hin zu Facebooks schrittweisen Tour der Privacy Features gibt es für die meisten Unternehmen genügend Ideen, wie sie ihre eigenen Touchpoints kundenzentrierter gestalten können. Zur Überprüfung der Datenschutzorientierung der eigenen Touchpoints können Marketers folgende Fragen in Betracht ziehen:

- Ist unsere Datenschutzerklärung über alle Touchpoints hinweg einfach einsehbar und verständlich?

- Kann unsere Kundschaft über jeden Touchpoint einfach einsehen, welche Daten wir über sie gespeichert haben?

- Hat unsere Kundschaft während einer Transaktion genügend Zeit, um sich mit unserer Datenschutzerklärung und unseren Datenschutzeinstellungen vertraut zu machen?

- Können unsere Dienstleistungen oder Produkte getestet werden, ohne dass eine potenzielle Kundschaft vorher irgendwelche Daten preisgeben muss?

- Wird unsere Kundschaft informiert, falls über einen ausgelösten Prozess neue Daten über sie erhoben werden?

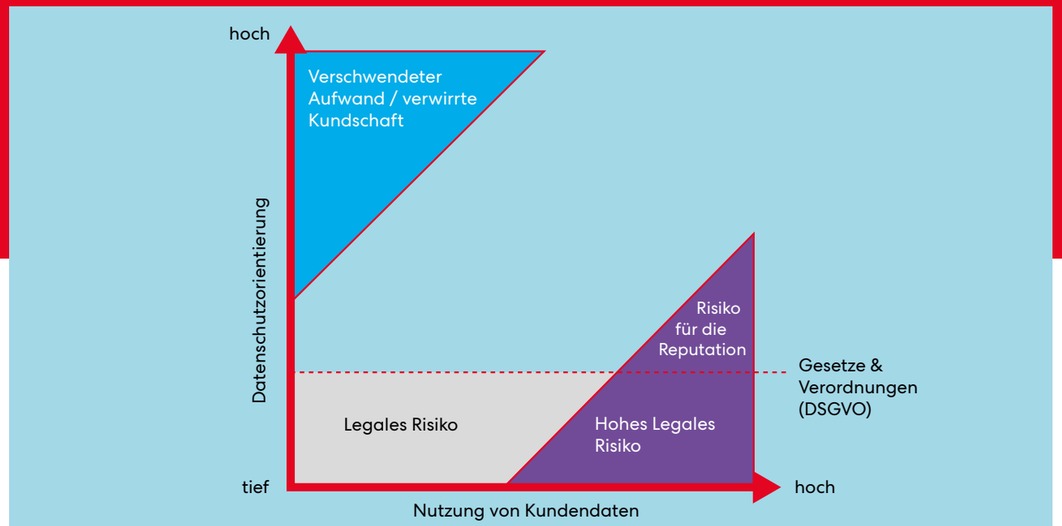

Abbildung 5: Der Spielraum verschiedener Datenschutzstrategien

UMSETZUNG & KUNDENENGAGEMENT

In den letzten zwanzig Jahren wurde in allen Industrien viel in die Digitalisierung von Prozessen und Geschäftsmodellen investiert. Für viele Unternehmen ist und war der Datenschutz dabei eine weitere Hürde, die mit viel Investitionen und Ressourcenakquise überwunden werden musste. Mit dem wachsenden Datenökosystem in allen Industrien ist jetzt der richtige Zeitpunkt, diese Ansicht zu ändern. Die in diesem Artikel angeführten Empfehlungen sind weder neu noch unerreichbar für die meisten Unternehmen – sie verlangen aber eine bewusste und rechtzeitige Verpflichtung des Marketing Managements, die Privatheit der Kundschaft als zentralen Teil des Kundenengagements zu verstehen.

Dies bedeutet nicht, dass Unternehmen auf Datenerhebungen verzichten sollten oder dass jedes KMU mit den Sicherheitsstandards von Apple mithalten muss. Die tatsächliche Ausprägung der eigenen Datenschutzstrategie wird immer auch von dem Ausmass der Nutzung von Kundendaten abhängig sein (siehe Abb. 5). Das Ziel für jedes Unternehmen sollte es allerdings sein, dass es mit seiner Kundschaft einen offenen Dialog über Datenverarbeitung führen kann, ohne dass es diesen unangenehm wird. Tim Cook, Apples CEO, arbeitete bereits vor knapp 10 Jahren an den Fundamenten für einen solchen Dialog mit seiner Kundschaft:

“Wir bei Apple sind der Meinung, dass ein großartiges Kundenerlebnis nicht auf Kosten Ihrer Privatsphäre gehen sollte. Unser Geschäftsmodell ist sehr einfach: Wir verkaufen großartige Produkte. Wir erstellen keine Profile auf der Grundlage Ihrer E-Mail-Inhalte oder Internetgewohnheiten, um sie an Werbekunden zu verkaufen. Wir „monetarisieren“ die Informationen, die Sie auf Ihrem iPhone oder in iCloud speichern, nicht. Wir lesen weder Ihre E-Mails noch Ihre Nachrichten, um an Informationen zu gelangen, mit denen wir Sie bewerben können. Unsere Software und Dienste sind dazu da, unsere Geräte besser zu machen. Schlicht und einfach.»[19] Das Resultat ist ein Konzern, der trotz immenser Datenabfragen das Vertrauen seiner Kundschaft geniesst. Wer eine solche Vertrauensbasis in seiner eigenen Industrie

aufgebaut hat, besitzt nicht nur einen im jetzt schwierig aufzuholenden Vorsprung gegenüber seiner Konkurrenz, sondern eine zukunftsfähige Ressource, die noch viel weiter ausgebaut werden kann.

FAZIT

Vor der Ratifizierung der DSGVO wurde in vielen Artikeln vorhergesagt, dass das neue Gesetz die Art und Weise, wie Daten gesammelt werden, dramatisch beeinflussen und vielen der zuvor verwendeten Big-Data-Erfassungs- und Monetarisierungstaktiken ein Ende setzen würde[6]. Die Idee, dass Big Data mit modernen Datenschutzbestimmungen unvereinbar ist, ist intuitiv richtig, aber nur teilweise wahr. Aus einer ökonomischen Perspektive betrachtet, hat die breite Verfügbarkeit personenbezogener Daten dazu geführt, dass der Informationswert einzelner Datenpunkte gesunken ist. Der Verlust der Datenqualität kann bereits heute beobachtet werden: wenn eine Kundschaft mit einer Situation konfrontiert wird, in der Risiko und Belohnung einer Datenteilung miteinander verwoben sind, entscheiden sie sich oft dafür sich zu schützen (z.B. durch die Verfälschung der eigenen Angaben) anstatt sich ganz gegen die Nutzung eines Dienstes zu entscheiden. Zudem steigt das Wissen der Kundschaft, sich mit rudimentären Instrumenten wie Adblockern und VPN gegen unerwünschte Datenabfragen zu schützen, stetig.

Daher wird seit langem argumentiert, dass es für die Abfrage qualitativ hochwertiger Daten notwendig sein wird, dass unternehmerisches Datenmanagement Vertrauen in die Datenverarbeitung aufbaut. Es gibt zwar viele Faktoren, die Kunden eher dazu bewegen, ihre Daten zu teilen (z.B. einen unmittelbaren Nutzen), aber ein tiefes Vertrauen zu dem Unternehmen oder mehr Kontrolle über gespeicherte Daten erreichen dieses Ziel noch effizienter. Dieses Vorgehen bietet den zusätzlichen Vorteil, dass mögliche negative Auswirkungen eines Datenlecks geschmälert werden. Darüber hinaus gibt es starke Indizien, dass ein erhöhter Schutz der Privatheit nicht nur die Menge der bereitwillig preisgegebenen Daten erhöht, sondern möglicherweise auch die Qualität dieser Daten.

Zusammen mit den sich verschärfenden Privatheitsnormen besteht somit ein starker Anreiz für Marketers, das eigene Datenmanagement als zentraler Aspekt des Kundenengagements zu verstehen.

AUTOREN

Mauro Luis Gotsch, M.A HSG
mauro.gotsch@unisg.ch
Institut für Marketing und Customer Insight an der Universität St. Gallen
Dufourstrasse 40a
CH-9000 St. Gallen

Prof. Dr. Marcus Schögel
marcus.schoegel@unisg.ch
Institut für Marketing und Customer Insight an der Universität St. Gallen
Dufourstrasse 40a
CH-9000 St. Gallen

LITERATUR

1. Solove, D. J. Privacy Self-Management and the Consent Dilemma. *Harvard Law Review* **126**, 1880–1903 (2013).

2. Solove, D. J. The Myth of the Privacy Paradox. *George Washington Law Review* **89**, 1–51 (2021).

3. Sarathy, R. & Robertson, C. J. *Strategic and Ethical Considerations in Managing Digital Privacy. Source: Journal of Business* Ethics vol. **46** (2003).

4. Brodherson, M., Broitman, A., Cherok, J. & Robinson, K. *Marketing in a privacy-first world.* https://www.mckinsey.com/business-functions/marketing-and-sales/our-insights/a-customer-centric-approach-to-marketing-in-a-privacy-first-world (2021).

5. van Troost, D., Asare-Anderson, Y. & van der Wel, P. Privacy by design : exceeding customer expectations. *Think With Google* 1–40 (2021).

6. Gotsch, M. Was hat das Marketing nach 2 Jahren DSGVO gelernt? *Swiss Marketing Review 4–9* (2020).

7. Palmatier, R. W. & Martin, K. D. *The Intelligent Marketer's Guide to Data Privacy.* (palgrave macmillan, 2019).

8. Greenberg, P. *The Commonwealth of Self-Interest: Business Success through Customer Engagement.* (56G Press, 2019).

9. Zuboff, S. Surveillance Capitalism and the Challenge of Collective Action. *New Labor Forum* **28**, 10–29 (2019).

10. Gotsch, M. L. & Schögel, M. Addressing the privacy paradox on the organizational level: review and future directions. *Management Review Quarterly 2021* 1–34 (2021) doi:10.1007/S11301-021-00239-4.

11. Teece, D. J., Pisano, G. & Shuen, A. Dynamic capabilities and strategic management. *Strategic Management Journal* **18**, 509–533 (1997).

12. Rodriguez, S. Facebook strikes back against Apple privacy change, prompts users to accept tracking to get 'better ads experience.' CNBC (2021).

13. Hotz, J. & Glatthaar, M. Verkehrsschilder für den Datenschutz – Privacy Icons. *Privacy Icons* (2020).

14. Hassler, M. Von Data-Driven zu *People-Based Marketing.* (mitp, 2021).

15. Godin, *S. Permission Marketing: Turning Strangers into Friends and Friends into Customers.* (Simon & Schuster, 1999).

16. Richards, N. M. & Hartzog, W. The Pathologies of Digital Consent. *Washington University Law Review* 1461–1503 (2019).

17. Anhalt-Depies, C., Stenglein, J. L., Zuckerberg, B., Townsend, P. M. & Rissman, A. R. Tradeoffs and tools for data quality, privacy, transparency, and trust in citizen science. *Biological Conservation* **238**, 1–7 (2019).

18. Shastri, S., Wasserman, M. & Chidambaram, V. The Seven Sins of Personal-Data Processing Systems under GDPR. in *11th USENIX Workshop on Hot Topics in Cloud Computing* 1–7 (2019).

19. Kovach, S. Apple's Tim Cook Takes a Swipe at Google's Business Model | Inc.com. *Inc* (2014).

gfm
Postfach 8021 Zürich 1
Telefon +44 202 34 25
www.gfm.ch | info@gfm.ch