In weniger als einem Jahr gilt EU-weit ein einheitliches Datenschutzrecht. Ja, es macht Datennutzung nicht mehr ganz so einfach wie bisher oft. Ja, bei Verstößen drohen enorme Geldstrafen. Aber die Verordnung ist ein Fortschritt, denn sie stellt Kundenbeziehungen auf transparente Pfeiler.

Nur wer gibt, kann auch nehmen

TEXT PHIL WINTERS

Am 25. Mai 2016 hat die EU das weltweit strengste, weitestreichende Gesetz zum Schutz der bürgerlichen Freiheiten im digitalen Zeitalter verabschiedet. Gleichzeitig soll die Datenschutzgrundverordnung der EU den Boden bereiten für Wirtschaftswachstum, indem sie ein Regelwerk für den gemeinsamen europäischen Digitalen Markt schafft. Bis dato lag es in der Hoheit der einzelnen Mitgliedsstaaten, wie sie das verworrene Netz aus EU-Gesetzen und Empfehlungen in nationales Recht umsetzen wollten. Das hat Unternehmen das grenzüberschreitende Agieren erschwert. Die neue Datenschutzgrundverordnung (DSGVO) wurde von allen EU-Mitgliedsstaaten einstimmig beschlossen. Somit gilt ein Gesetz für die gesamte EU. Und das tritt am 25. Mai 2018 in Kraft – in weniger als einem Jahr!

Zum ersten Mal in der Geschichte gilt die Datenschutzgrundverordnung für alle Unternehmen, Organisationen und Körperschaften, die personenbezogene Daten von EU-Bürgern verarbeiten. Die DGSVO betrifft aber auch den Transfer dieser Daten. Das zielt auf Unternehmen in Ländern wie die USA und Russland, die bis jetzt EU-Regularien geflissentlich ignorieren konnten. Das hat sich mit der Verordnung radikal geändert: Sind Daten von

EU-Bürgern betroffen, greift die Verordnung. Punkt. Ironie der Geschichte: Großbritannien muss die neue EU-Neuordnung befolgen, Brexit hin oder her.

Die DSGVO unternimmt den Versuch, einen modernen und harmonisierten Rahmen für den Datenschutz innerhalb der gesamten EU zu schaffen. Keine Überraschung, dass bei einem solch komplexen Gebilde einige Teile dem Leser Angstschauer über den Rücken laufen lassen – vor allem die astronomisch hohen Geldstrafen, die bei Verstößen gegen Personen und Unternehmen verhängt werden können. Das eröffnet Angstmachern unter Experten und Verkäufern ein weites Feld, die nur darauf warten, Ihnen Produkte und Dienste zu verkaufen, um Sie bei der Compliance zu unterstützen.

Doch was steht denn nun wirklich in der Verordnung? Artikel 6 DSGVO sieht strengere Regeln für die Einwilligung der Betroffenen vor, sowohl bei der Datenerhebung als auch bei der Datennutzung. Auch wenn das einen Mehraufwand bedeutet, sind wir in Deutschland eigentlich damit vertraut, denn in Deutschland galt schon bislang die strengste Auslegung der bisherigen EU-Regeln zum Datenschutz. Für mich eröffnet sich hier ein Spielfeld für Vordenker im Marketing. Wieso? Nun …

Geben und Nehmen

Wenn Daten über MEIN Verhalten und MEINE Bedürfnisse gesammelt und genutzt werden, ohne, dass ich davon weiß, habe ich offensichtlich Angst vor Missbrauch. Wenn aber Organisationen mir nicht nur deutlich sagen, welche Daten sie über mich erheben möchten, sondern auch, warum sie das wollen und welchen Nutzen ich davon habe, dann stimme ich der Datennutzung wahrscheinlich zu, solange ich den Nutzen für mich erkenne. Wir können dieses Verfahren „Informationsreziprozität" nennen. Bislang haben meine Kunden dieses Konzept immer als smartes Marketing begriffen, aber jetzt ist es genau das, was wir tun müssen, um die sehr detaillierten gesetzlichen Vorgaben zur Einwilligung in die Datennutzung zu erfüllen. Sagen und erklären Sie Ihren Kunden offen, welche Daten Sie erheben und nutzen wollen und warum. Je besser Sie Ihre Gründe darlegen, desto wahrscheinlicher erkennen Ihre Kunden die Vorteile und revanchieren sich, indem sie Ihnen die Einwilligungen geben, die Sie haben wollten. »

Foto: UrchenkoJulia/istockphotos.de

Improve your Marketing

Learning 1 Was zählt, ist Informationsreziprozität. Unternehmen müssen den Kunden ganz deutlich sagen, welche Daten sie erheben und wozu. Und erklären, welche Vorteile der Kunde davon hat, wenn er der Datenerhebung und -nutzung zustimmt. Es geht um maximale Transparenz.

Learning 2 Unternehmen müssen alle Daten, die sie erheben, lückenlos dokumentieren. Ebenso die Art, wie sie diese nutzen. Auf Verlangen müssen sie Kunden schnell und umfassend Auskunft über Daten geben und sie ganz oder teilweise löschen.

Learning 3 Große Chance für gute Marketer: Wenn sie genau erklären, welche Vorteile die Datenspeicherung bringt (bessere Suchergebnisse, besserer Service et cetera), werden nur wenige Kunden auf das Recht auf Vergessenwerden bestehen.

Autor

Phil Winters

ist einer der weltweit führenden Experten und Berater rund um Daten, Analytics und Customer Journey Mapping. Er war Mitarbeiter Nr. 7 bei SAS Institute und nennt sich selbst den „Datenflüsterer", andere bezeichnen ihn als Data Vader. Er lebt, schreibt und denkt in Heidelberg, ist aber eigentlich immer unterwegs – als Redner, Berater und Workshop-Leiter.

↗ *www.ciagenda.com*

In Artikel 12 und noch detaillierter in Artikel 15 ist ausgeführt, dass EU-Bürger das Recht haben, ganz genau zu erfahren, welche ihrer Daten erhoben und gesammelt werden und wie diese Daten genutzt werden. Das Glücksteam, das diese Aufgabe übertragen bekommt, muss in der Lage sein, schnell, effizient und umfassend in „klarer und verständlicher Form" Auskunft zu geben. Das Marketing muss diese Daten dem Datenschutzteam also schon vor einer möglichen Anfrage seitens des Kunden zur Verfügung stellen. Das bedeutet für uns Marketer zwar einen einmaligen Initialaufwand, kann und sollte aber dann als beständiger Prozess etabliert werden, der sicherstellt, dass jedes neue Datum, das genutzt wird, und jede neue Nutzung bestehender Daten dokumentiert sind. Wichtig: Diese Artikel der Verordnung schränken uns nicht in der Datennutzung ein, sondern nur in der Art, wie wir das dokumentieren.

Artikel 13 schreibt fest, dass wir „aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person" geben müssen. Müssen wir also in nicht-technischer Sprache erklären, wie unser selbstlernender Algorithmus zu einer Kaufempfehlung gekommen ist oder aus welchem Grund ein bestimmter EU-Bürger kein Sonderangebot erhalten hat? Manch ein Experte wird das bejahen – und so Deep Learning-Algorithmen praktisch unmöglich machen. Andere Experten aber halten es für ausreichend, wenn wir die Daten hinter einer Entscheidung und die Entscheidung selbst offenlegen.

Artikel 17 der Verordnung ist ein weiterer wichtiger Punkt. Er schreibt vor, dass jeder EU-Bürger das Recht auf Vergessenwerden hat. Das geht weit über bestehende Regeln hinaus. Auch beim neuen Recht auf Vergessenwerden gilt, dass das Datenschutzteam schnell reagieren können muss. Wir Marketer, aber auch alle anderen Abteilungen in einem Unternehmen, müssen gemeinsam mit dem Datenschutzteam Prozesse erarbeiten, die sicherstellen, dass jede einzelne Information zu einer bestimmten Person entfernt werden kann – sei es die Kaufhistorie, seien es Cookies oder all die anderen Daten, die wir erheben. Jedes Unternehmen muss in der Lage sein, in ganz kurzer Zeit eine detaillierte Beschreibung aller personenbezogenen Daten bereitzustellen und gegebenenfalls zu löschen, die das Unternehmen über eine Person gespeichert hat, sobald ein EU-Bürger fordert, vergessen zu werden. Das wird am besten vom Datenschutzbeauftragten koordiniert.

Das Recht auf Vergessenwerden

Aber: Sobald jemand erst einmal verstanden hat, was es für ihn heißt, wenn er komplett vergessen wird, wird er diese Forderung gar nicht mehr erheben. Denn wer will keine auf ihn angepassten Sonderangebote statt überhaupt keine Angebote? Wer will auf einer Website nicht schnell zur Antwort auf seine Frage geführt werden statt ewig herumzusuchen? Kunden erwarten allgemein von einem Unternehmen ja, dass es sie kennt, über die Kauf- und Reklamationshistorie Bescheid weiß. Wenn alles gelöscht ist, ist nichts mehr davon möglich. Die ganze Beziehung ist auf Null gestellt. Es wird spannend zu sehen, wie viele Menschen wirklich diese Möglichkeit durchsetzen wollen, wenn sie verstanden haben, was das konkret für sie bedeutet. Damit sind wir wieder beim „Geben und Nehmen".

Die Datenschutzgrundverordnung ist das erste Gesetz, das sich vor allem in Artikel 9 explizit mit den Folgen der Algorithmus-basierten Entscheidungsfindung für „die grundlegenden Rechte und Freiheiten natürlicher Personen" befasst – inklusive algorithmischer Diskriminierung.

Wir finden Algorithmen in Kampagnenmanagement-Systemen, in der Marketing Automation, im CMS und in Websystemen, im Omnichannel Marketing, bei Analytics und Predictive Analytics. Kurz: Wir nutzen Machine Learning, um mit den Daten zu arbeiten und ein Modell zu finden, mit dem sich Vorhersagen machen lassen oder mit dem wir ein Individuum kategorisieren können. Und dann nutzen wir dieses Ergebnis für Aktionen. Am effektivsten ist es, wenn diese Ergebnisse ins System zurückgespielt werden, um den Prozess für die nächste Aktion zu verfeinern. Das ist kein Problem, wenn dieser Ansatz zum Tragen kommt, um die Maschinenwartung in einer Fabrik oder das Pricing bei einer Airline zu verbessern. Aber wann immer es bei regelbasierten Entscheidungen um personenbezogene Daten geht (samt Cookies und IP-Adressen), müssen wir uns intensiv fragen, ob „Daten, die diskriminieren", in unsere Arbeit einfließen.

Keine Diskriminierung!

Diskriminierende Wirkungen erleben wir, wenn wir in Bezug auf natürliche Personen Entscheidungen treffen, die auf ethnischer Herkunft, Religion, politischen Überzeugungen, Gewerkschaftsmitgliedschaft, genetischen Informationen oder dem Gesundheitszustand oder der sexuellen Orientierung beruhen. Wichtig dabei: Das gilt auch dann, wenn wir die entsprechenden Daten auf rechtmäßigem Weg gewonnen haben.

Der erste Schritt für das Marketing ist also zu klären, ob Daten, die wir für Marketingzwecke nutzen, in eine der oben genannten Kategorien fallen. Viel wichtiger aber ist ein zweiter Aspekt – die statistische Diskriminierung. Es kann passieren, dass eigentlich harmlose Daten wie die Postleitzahl auf einmal doch diskriminieren. In manchen Gegenden lassen Postleitzahlen relativ genaue Vorhersagen darüber zu, welcher Herkunft die meisten Bewohner sind. Das heißt: Selbst, wenn wir alle Hinweise auf ethnische Zugehörigkeit aus unseren Datensätzen streichen, kann die Verknüpfung von Postleitzahl und ethnischer Herkunft der Bewohner ethnische Diskriminierung quasi durch die Hintertür zurück ins System bringen. Und so möglicherweise gegen das Gesetz verstoßen – weil wir so harmlose wie nötige Daten wie die Postleitzahl erheben.

Wie können wir das Risiko umgehen? Wir können Predictive Analytics eben nicht nur nutzen, um Next Best Action et cetera zu berechnen, sondern auch dazu zu bestimmen, ob die Verknüpfung von Informationen zu einer ungewollten Diskriminierung führt. Das ist eine Aufgabe für Ihr Data Mining-Team. Wichtig ist, dass Sie einen Prozess etablieren, der (ungewollte) Diskriminierung ausschließt.

↗redaktion@acquisa.de

Service

Internet

- Die EU-Datenschutzgrundverordnung finden Sie hier *↗http://bit.ly/2qm5xUy*
- Einen Überblick über die Anforderungen der DSGVO fürs Marketing haben wir für Sie hier auf acquisa.de zusammengestellt *↗http://bit.ly/2qIbmhL*
- Eine allgemeine Übersicht über die Datenschutzgrundverordnung und ihre Folgen finden Sie bei Haufe *↗http://bit.ly/2pBdXKo*