Foto: © iStockphoto

Privacy as Strategy – können Marketers mit Datenschutz strategische Vorteile gewinnen?

Was hat das Marketing nach 2 Jahren DSGVO gelernt?

Vor zwei Jahren ist mit der Datenschutzgrundverordnung der EU (DSGVO) eine der anspruchsvollsten und umfassendsten Datenschutzbestimmungen aller Zeiten in Kraft getreten. Unternehmen weltweit haben seither ihre Bestimmungen angepasst, um dem Wunsch ihrer Kunden nach mehr Kontrolle über persönliche Daten gerecht zu werden. Doch wie haben Marketers auf diese Änderung reagiert und was haben Unternehmen in den letzten 2 Jahren über Kundenorientierung im Datenschutz gelernt?

Von Mauro Gotsch

Seit das Europäische Parlament im April 2016 die neue «Datenschutzgrundverordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten» (DSGVO) verabschiedet hat, spekulieren Fachzeitschriften, was das Ende des «Wilden Westen» der Datensammlung für das Marketing bedeutet[1]. Die DSGVO, welche auf dem Konzept der Privatsphäre (und somit Datenschutz) als grundlegendes Menschenrecht beruht, würde weltweit «die Art und Weise, wie Daten gesammelt werden, dramatisch beeinflussen»[2]. Einerseits, weil sich dieser Schutz auf alle EU-Bürger erstrecken sollte, egal wo ihre Daten verarbeitet werden. Andererseits, weil die 7 DSGVO Grundprinzipien (siehe Abb. 1) die automatische Datenerhebung ohne explizite Zustimmung der Kunden verunmöglichen sollten.

Trotz der potenziell kostspieligen Folgen für unvorbereitete Unternehmen sahen viele Berater die DSGVO als «gute Nachricht fürs Marketing»[3]. So schrieb z.B Goddard[4], dass die neu gewonnene Transparenz in Datenprozessen Unternehmen auf eine Augenhöhe mit ihren Kunden stellen und somit Vertrauen fördern werde. Weiter wurde spekuliert, dass der Know-how-Gewinn durch die Optimierung von Erhebungsprozessen zu einem sichereren Datenmanagement führen würde[5].

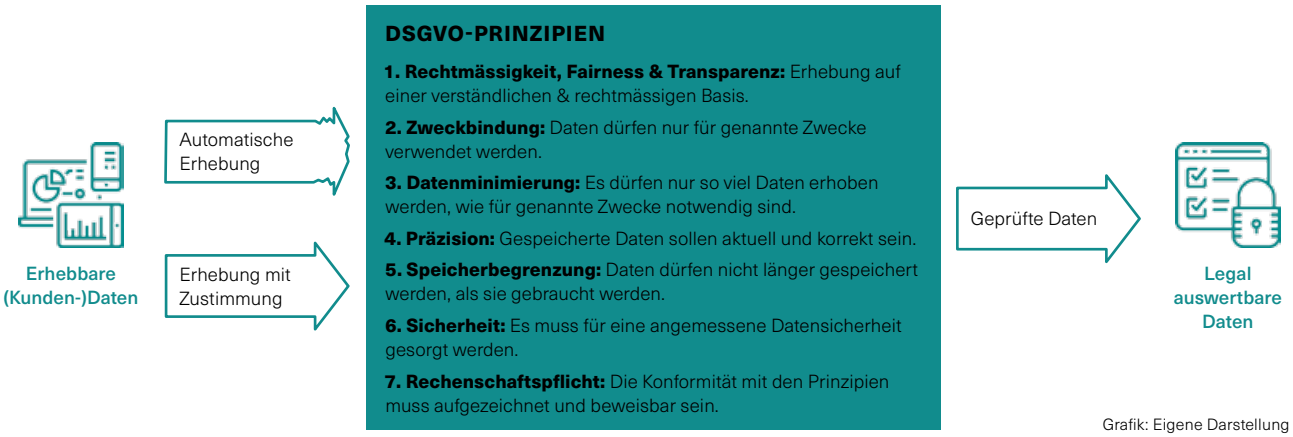
Seither sind über 160 000 Verletzungen der Datensicherheit dem EU-Datenschutzverantwortlichen gemeldet worden. Zudem haben Kundenbefragungen wiederholt gezeigt, dass sich Konsumenten in Bezug auf Datenschutz nicht sicherer fühlen als vor DSGVO[vgl. 6–8]. Natürlich lässt sich ein Teil dieser Unruhe unter Kunden mit dem Medienhype um die neue Gesetzesnorm erklären. In Anbetracht des «exponentiellen Wachstum»[9] von erhobenen Kundendaten scheint es aber wahrscheinlicher, dass sich Kunden auch in Zukunft öfter mit Datenschutz beschäftigen werden. Die Tendenz ist bereits ersichtlich: In einer kürzlich durchgeführten Konsumentenumfrage gaben 72% der Teilnehmenden an, dass sie «aufgrund von Datenschutzbedenken aufhören würden, bei einem Unternehmen einzukaufen»[10,11].

Als einer der grössten Profiteure von Datenerhebungen mussten sich Marketers dank DSGVO zunehmend folgende Fragen stellen: Wie können wir der wachsenden Nachfrage unserer Kunden nach Datenschutz gerecht werden? Was haben wir in den letzten Jahren unter DSGVO über Datenschutz gelernt?

Wie die DSGVO ein altes Marketingproblem ins Licht rückt

Lange vor der DSGVO haben Datenschutzbeauftragte und Forscher gefordert, dass sich Unternehmen stärker mit den Datenschutzbedürfnissen ihrer Kunden beschäftigen. Wang et al.[12] warnten bereits vor 25 Jahren vor der Erosion der Privatsphäre von Kunden durch «Internet Marketing». Sie argumentierten, dass gerade Marketers in einer guten Position seien, die legalen und operationalen Datenschutzanforderungen von Kunden zu sammeln und unternehmensweit umzusetzen. Mit der Verbreitung der ersten sozialen Netzwerke wurde diesen Empfehlungen noch Nachdruck verliehen. So forderten Sarathy et al.[13], dass «Unternehmen ihrem Datenschutz kontinuierlich Aufmerksamkeit widmen, wenn sie das Wohlwollen ihrer Kunden nachhaltig sichern wollen».

Abb. 1: Datenverarbeitung unter DSGVO



Grafik: Eigene Darstellung

Diese Empfehlungen beruhten damals wie heute auf zwei Trends: das bei Konsumenten global steigende Bedürfnis[vgl. 14] nach einem nachhaltigen Datenschutz[15] sowie die eskalierte Verletzbarkeit der Privatsphäre von Konsumenten durch digitale (Marketing-) Technologien[16].

Studien zeigen, dass sich Konsumenten in Online-Umgebungen oft in ihrer Privatsphäre verletzt fühlen, aber sich gleichzeitig nicht gegen solche Verletzungen zu wehren wissen[17]. Dies ist keine neue Erkenntnis; Acquisti[18] hat bereits in den Anfängen des Webs 2.0 gezeigt, dass Kunden – unabhängig von ihrem Wissensstand – Bedenken hinsichtlich Datenschutz äussern und dennoch datenintensive Dienste (z.B. Social Media) nutzen. Seither hat sich die Untersuchung dieses sog. «Privacy Paradox»[19] zu einem eigenen Forschungszweig entwickelt – mit inkonsequenten Ergebnissen. In einer Literaturübersicht von Barth et al.[20] wurden 32 Entscheidungsmodelle aus Studien zum Thema «Privacy Paradox» untersucht. Sie kamen zu dem Ergebnis, dass die Definition eines allgemeinen Entscheidungsprozesses nur begrenzt möglich ist, da zu viele Variablen das Konsumentenverhalten beeinflussen.

Eine der am häufigsten zitierten Erklärungen für das «paradoxe» Verhalten von Konsumenten ist das einseitige Machtverhältnis, wenn es um den Austausch von persönlichen Daten geht[21]. Unternehmen postulieren oft, dass es sich hierbei um einen Marktaustausch wie jeden anderen handelt: Kunden tauschen Daten gegen personalisierte Dienstleistungen. Dies setzt aber voraus, dass dieser Austausch von Konsumenten so initiiert wurde und dass er auf einem ausgeglichenen Machtverhältnis beruht. Da einzelne Datenpunkte an sich fast nichts wert sind, fehlt es Kunden an einer Verhandlungsbasis für einen fairen Handel. Der Wert der Daten entsteht aus ihrer Bündelung und anschliessendem Weiterverkauf. Verstärkt wird das Macht-Ungleichgewicht dadurch, dass ein Verkäufer solcher Daten potenzielle Kosten, die aus dem Verkauf resultieren, ignorieren kann. Der Person, deren Daten verkauft werden, können allerdings (z.B. durch Veröffentlichung heikler Daten) ungefragt Kosten auferlegt werden[22]. Daher sehen sich Kunden oft mit einem Datenaustausch konfrontiert, der «Vermarktern und Werbetreibenden deutlich mehr Nutzen bringt und ein solch unausgewogenes Austauschverhältnis fördert, dass es praktisch als einseitig angesehen werden kann»[23].

Der Wert der Daten entsteht aus ihrer Bündelung und anschliessendem Weiterverkauf.

Doch selbst bei gleichverteiltem Nutzen sind Konsumenten benachteiligt: Die Konditionen des Datenaustauschs sind meist zu undurchsichtig. Sowohl Datenschutzrichtlinien als auch Erhebungsmethoden werden stets komplexer zu verstehen[24–26]. Zusätzlich nutzen viele digitale Plattformen dieses Informationsungleichgewicht durch ihr Design gezielt aus, um die Zustimmung von Konsumenten leichter zu erhalten[27]. Dabei wären Kunden durchaus bereit, mit Daten für Dienstleistungen zu bezahlen. In der EU gab es bereits vor der DSGVO einen leichten Trend hin zu einer Akzeptanz, persönliche Daten im Austausch für tangible Vorteile zu teilen. Derselbe Bericht zeigte aber auch, dass Kunden solche Entscheidungen nicht gerne treffen, da gefühlt alleine die Unternehmen die Konditionen des Austausches bestimmen[28].

Die direkten Auswirkungen der DSGVO

Die Implikationen der DSGVO wurden Unternehmen weltweit schnell deutlich: Wer weiterhin mit EU-Bürgern Geschäfte machen will, muss seine Datenerhebungsprozesse verstehen. Dementsprechend war die sofortige Auswirkung für Unternehmen hauptsächlich monetär: Anwaltskosten und Prozessumstrukturierungen. Online-Unternehmen mit Freemium-Modellen, welche auf den Weiterverkauf von Kundendaten angewiesen waren, mussten ihr Geschäftsmodell überdenken. Offline-Unternehmen, welche sich nur selten mit der Pflege ihrer Datenbanken beschäftigen mussten, sahen sich plötzlich zu drastischen Schritten gezwungen. So z.B die Pub-Kette Wetherspoon, welche es als effizienter befand, ihre E-Mail-Datenbank zu löschen, als die unter Zustimmung erhaltenen Kundendaten von allen anderen zu trennen[29]. Insgesamt wurde geschätzt, dass «Fortune 500»-Unternehmen im Durchschnitt über US-$ 16 Millionen in DSGVO Anpassungsprojekten ausgegeben haben [30]. Teixeira et al.[31] zeigten auf, dass dabei die meisten Schwierigkeiten in der kanalübergreifenden Anwendung auf Datenerhebungsprozesse entstanden. Oft fehlte es an technischem und rechtlichem Know-how. Shastri et al.[32] erklärten das damit, dass die DSGVO mit bisherigen Datenarchitekturen grundlegend inkompatibel sei. Anpassungen müssten dementsprechend von Grund auf und unternehmensweit umgesetzt werden. Alles andere «käme der Reparatur eines undichten Wasserhahns in einem sinkenden Schiff gleich»[32].

Diese Schwierigkeiten spiegelten sich auch in Datenschutzerklärungen wider. In einer Untersuchung von 6278 Unternehmen in und ausserhalb der EU zeigte sich, dass zwar praktisch alle untersuchten Unternehmen ihre Datenschutzerklärungen erweitert haben, aber die Vorteile für Konsumenten mager ausfielen. So konnten im Durchschnitt Verbesserungen in der Transparenz und Spezifität der Erklärungen festgestellt werden (besonders innerhalb der EU), aber trotzdem erreichten viele Erklärungen noch immer nicht das von der DSGVO angestrebte Ziel der vollständigen Offenlegung und Transparenz[33].

Gleichzeitig demonstrierte die Meldepflicht der DSGVO, dass die Aktualisierung der Datenschutzpraktiken für viele Unternehmen notwendig war. Letztes Jahr betrug die durchschnittliche Zahl der in der EU gemeldeten Datenlecks pro Tag 278. Dies entspricht einem Anstieg von 12,6% im Vergleich zum Vorjahr[34]. Trotzdem war der Datenschutzbeauftragte der EU bisher eher zurückhaltend, Verstösse in vollem Ausmass zu strafen. Die 2019 gegen Google verhängte Geldbusse von € 50 Mio. machte im ersten Jahr der DSGVO 89% der Gesamtstrafen aus. Weit entfernt von der möglichen Höchststrafe von € 3,7 Mrd. (4% der weltweiten Google-Einnahmen)[35].

Dies könnte sich jedoch in absehbarer Zeit ändern: Sobald Modelle zur automatischen und objektiven Prüfung der DSGVO-Konformität eine breitere Anwendung geniessen, wird es weitere Instanzen geben, welche Datenschutzverstösse verlässlich aufdecken können[36]. Da auch Gesetzgeber immer vertrauter mit den Vorschriften werden, kann eine strengere Ahndung von Verstössen erwartet werden[37].

Was bedeutet dies für die Zukunft des Marketings?
Trotz bisheriger Auswirkungen der DSGVO könnte es sein, dass sich die Situation für Konsumenten nicht verbessern wird. Palmatier und Martin vermuten, dass der verstärkte Einsatz von «Big Data»-Technologien (z.B. Gesichtserkennung, Spracherkennung, IoT) die Verwundbarkeit von Konsumenten in Bezug auf Datenschutz noch weiter eskalieren wird – egal ob diese zustimmungsbasiert sind oder nicht[16]. Diese Technologien haben ein hohes Nutzungspotenzial im Marketing, sind aber auf das Vertrauen der Konsumenten angewiesen. Demnach könnten sich Unternehmen mit dem Aufbau der notwendigen Infrastruktur für datenschutzorientierte Strategien (z.B Anonymisierungsprozesse), einen strategischen Vorteil am Markt verschaffen[5, 38].

> Aus der Perspektive des Marketings besteht das Ziel darin, «zuerst den Kunden zufrieden zu stellen» und den Datenschutzdialog mit ihm auf einer Augenhöhe zu führen.

Trotzdem wurde das attestierte Potenzial von Datenschutz nur selten in die Praxis übersetzt. Dies, obwohl erste Forschungsergebnisse auf die Vorteile einer datenschutzorientierten Marketingstrategie hinweisen. Ein stärkerer Fokus auf die digitale Privatsphäre von Kunden wurde bisher mit höherem Vertrauen und Kundenzufriedenheit[39–42], einer höheren Bereitschaft Daten zu teilen[43–45], der Schadensbegrenzung bei Datenlecks[46] und der wirtschaftlichen Leistung von Unternehmen[47] in Verbindung gebracht.

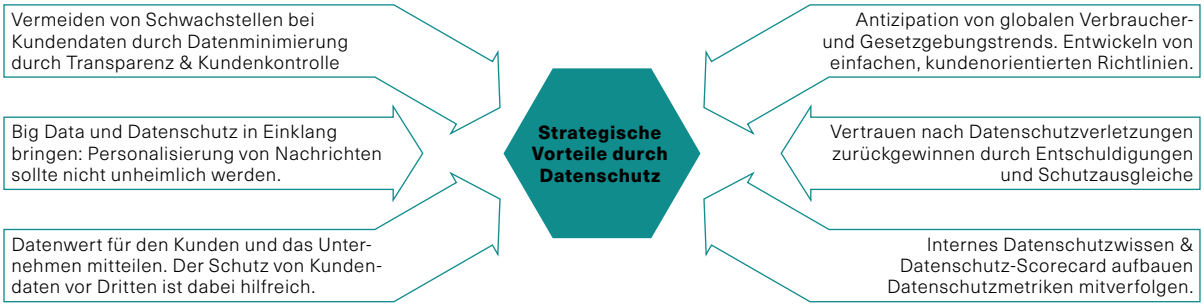
Wenn sich Unternehmen diese strategischen Vorteile sichern möchten, braucht es zuerst ein kulturelles Umdenken. Wie viele DSGVO-Umstrukturierungsprojekte

Abb. 2: Paradigmenwechsel im Datenschutzdenken

AKTUELLES DATENSCHUTZ-PARADIGMA	KUNDENZENTRIERTES DATENSCHUTZ-PARADIGMA
· **Motto:** Datenschutz als rechtliches Problem	· **Motto:** Datenschutz als Marketingstrategie
· **Zentrales Anliegen:** Wer erhebt welche Daten?	· **Zentrales Anliegen:** Wie, wofür werden die Daten verwendet?
· **Werkzeuge:** Benachrichtigung & Zustimmung	· **Werkzeuge:** Dialog- & Dienstleistungsmentalität
· **Ansatz:** Reaktiv	· **Annäherung:** Proaktiv
· **Zentraler Treiber:** Gesetze & Politik	· **Zentraler Treiber:** Kundenbedürfnisse
· **Fokus:** Datenmenge	· **Fokus:** Datenqualität

Grafik: Adaptiert von Matz et. al.[50]

Abb. 3: Datenschutz als Strategie[16]



Grafik: Eigene Darstellung

gezeigt haben, reicht es nicht, sich nur an der minimalen Compliance zu orientieren. Marketers sollten lernen, Datenschutz nicht nur durch eine rechtliche Linse zu betrachten, da diese Sicht «die von ihm verlangten Ziele nicht erreichen kann»[48]. Stattdessen sollten Marketers auf der Grundlage der DSGVO aufbauen und Kunden aktiv helfen, «sich in einem ansonsten sehr ungleichen Spielfeld zurechtzufinden»[49]. Dies erfordert einen Wechsel von der Frage «Wer sammelt welche Daten?», zur Frage «Wie werden diese Daten verwendet?»[50].

Anfangs wurde die DSGVO Kunden hauptsächlich durch zahlreiche Informations-Mails über neue Bestimmungen verständlich gemacht. Seither sind Marketers aber tendenziell nicht besser geworden, ihre Datensammlungsprozesse Kunden als vorteilhaft zu verkaufen. Das «Privacy Paradox» wird solange bestehen, wie Kunden das Gefühl haben, dass Unternehmen ihnen in Sachen Datenschutz nicht entgegenkommen. Die DSGVO bleibt eine Chance für Marketers, innerhalb des eigenen Unternehmens ein nachhaltiges Datenschutzbewusstsein zu schaffen. Marketers verfügen über Instrumente, um Kunden in der Customer-Journey bei ihren Datenschutzentscheidungen zu unterstützen. Alte Ideen, wie das zustimmungsorientierte Dialogmarketing[51], der Verzicht auf Dateneinkauf und -verkauf oder der Ermächtigung des Kunden (z.B durch erhöhte Transparenz, mehr Kontrolle, einfacheres Opt-out) «kann Kunden helfen, paradoxes Verhalten zu vermeiden»[52].

Es gibt viele philosophische, rechtliche, technologische und ethische Gründe für die Förderung des Datenschutzes. Doch aus der Perspektive des Marketings besteht das Ziel darin, «zuerst den Kunden zufrieden zu stellen»[53] und den Datenschutzdialog mit ihm auf einer Augenhöhe zu führen. Nicht weil die DSGVO es verlangt, sondern weil es ein essenzieller Bestandteil der Customer-Experience vieler Unternehmen ist. ●

LITERATUR

1. Murphy, M. & Field, M. GDPR: After the Wild West rush for data, a law for the digital age. The Telegraph (2018).

2. Downes, L. GDPR and the End of the Internet's Grand Bargain. Harv. Bus. Rev. (2018).

3. Gilbert, D. Why GDPR is great news for marketers and will create a more efficient data economy – Econsultancy. Econsultancy (2017).

4. Goddard, M. Viewpoint: The EU general data protection regulation (GDPR): European regulation that has a global impact. Int. J. Mark. Res. 59, 703–706 (2017).

5. Seo, J., Kim, K., Park, M., Park, M. & Lee, K. An Analysis of Economic Impact on IoT Industry under GDPR. Mob. Inf. Syst. 1–6 (2018). doi:10.1155/2018/6792028

6. Insight Intelligence. Delade Meningar – Svenska folkets attityder till digital integritet 2020. (2020).

7. Orange. L'Observatoire des usage du digital. (2019).

8. SUSE. 84 Prozent der Teilnehmer in Deutschland halten EU-DSGVO nicht für eine Verbesserung – SUSE Communities. SUSE Newsroom (2019). Available at: https://www.suse.com/c/de/news/suse-umfrage-84-prozent-der-teilnehmer-in-deutschland-halten-eu-dsgvo-nicht-fuer-eine-verbesserung/. (Accessed: 25th September 2020)

9. Reinsel, D., Gantz, J. & Rydning, J. The Digitization of the World – From Edge to Core. (2018).

10. Salesforce. State of the connected customer. (2019).

11. Cisco. Consumer Privacy Survey – The growing imperative of getting data privacy right. (2019).

12. Wang, H., Lee, M. K. O. & Wang, C. Consumer Privacy Concerns about Internet Marketing. Commun. ACM 41, 63–70 (1998).

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

14. Clemons, E. K., Wilson, J. & Jin, F. Investigations into Consumers Preferences Concerning Privacy: An Initial Step Towards the Development of Modern and Consistent Privacy Protections Around the Globe. in 47th Hawaii International Conference on System Science (ed. IEEE) 4083–4092 (2014). doi:10.1109/HICSS.2014.504

15. Goldfarb, A. & Tucker, C. Shifts in Privacy Concerns. 102, 349–353 (2012).

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

17. Lombardi, D. B. & Ciceri, M. R. More than defense in daily experience of privacy: The functions of privacy in digital and physical environments. Eur. J. Psychol. 12, 115–136 (2016).

18. Acquisti, A. Privacy in Electronic Commerce and the Economics of Immediate Gratification. in Pre-proceedings to EC'04, May 17-20, New York 1–9 (2004).

19. Barnes, S. B. A privacy paradox: Social Networking in the United States. First Monday 11, (2006).

20. Barth, S. & Jong, M. De. The Privacy Paradox – Investigating Discrepancies between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review. Telemat. Informatics 34, 1038–1058 (2017).

21. Martin, K. D. & Murphy, P. E. The role of data privacy in marketing. J. Acad. Mark. Sci. 45, 135–155 (2017).

22. Varian, H. R. Economic Apsects of Personal Privacy. Economic Apsects of Personal Privacy (1996).

23. Rapp, J., Hill, R. P., Gaines, J. & Wilson, R. M. Advertising and Consumer Privacy: Old Practices and New Challenges. J. Advert. 38, 51–61 (2009).

24. Milne, G. R., Culnan, M. J. & Greene, H. A Longitudinal Assessment of Online Privacy Notice Readability. J. Public Policy 25, 238–249 (2006).

25. Slepchuk, A. N. & Milne, G. R. Informing the design of better privacy policies. Current Opinion in Psychology 31, 89–93 (2020).

26. Milne, G. R. & Boza, M. Trust and concern in consumers' perceptions of marketing information management practices. J. Interact. Mark. 13, 5–24 (1999).

27. Nouwens, M., Liccardi, I., Veale, M., Karger, D. & Kagal, L. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. in CHI (ed. Association for Computing Machinery) 1–13 (Association for Computing Machinery, 2020). doi:10.1145/3313831.3376321

28. Ridley-Siegert, T. Data privacy: What the consumer really thinks. J. Direct, Data Digit. Mark. Pract. 17, 30–35 (2015).

29. Manthorpe, R. Wetherspoons just deleted its entire customer email database – on purpose | WIRED UK. Wired (2017).

30. Smith, O. The GDPR Racket: Who's Making Money From This $9bn Business Shakedown. Forbes Mag. (2018).

31. Teixeira, G. A., da Silva, M. M. & Pereira, R. The Critical Success Factors of GDPR Implementation : a Systematic Literature Review. Digit. Policy, Regul. Gov. 21, 402–418 (2020).

32. 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).

33. Linden, T., Khandelwal, R., Harkous, H. & Fawaz, K. The Privacy Policy Landscape After the GDPR. Proc. Priv. Enhancing Technol. 1, 47–64 (2020).

34. DLA Piper. DLA Piper GDPR Data Breach Survey: January 2020. (2020).

35. Herrle, J. & Hirsh, J. The Peril and Potential of the GDPR. Center for Internation Governance Innovation 1–4 (2019).

36. Torre, D. et al. Using Models to Enable Compliance Checking against the GDPR: An Experience Report. in Proceedings – 2019 ACM/IEEE 22nd International Conference on Model Driven Engineering Languages and Systems, MODELS 2019 1–11 (IEEE, 2019). doi:10.1109/MODELS.2019.00-20

37. Vinocur, N. 'We have a huge problem': European tech regulator despairs over lack of enforcement – POLITICO. Politico News (2019).

38. Li, H., Yu, L. & He, W. The Impact of GDPR on Global Technology Development. J. Glob. Inf. Technol. Manag. 22, 1–6 (2019).

39. Dehghanpouri, H., Soltani, Z. & Rostamzadeh, R. The impact of trust, privacy and quality of service on the success of E-CRM: the mediating role of customer satisfaction. J. Bus. Ind. Mark. 1–17 (2020). doi:10.1108/JBIM-07-2019-0325

40. Eastlick, M. A., Lotz, S. L. & Warrington, P. Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. J. Bus. Res. 59, 877–886 (2006).

41. Featherman, M. S., Miyazaki, A. D. & Sprott, D. E. Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility. J. Serv. Mark. 24, 219–229 (2010).

42. Wu, K. W., Huang, S. Y., Yen, D. C. & Popova, I. The effect of online privacy policy on consumer privacy concern and trust. Comput. Human Behav. 28, 889–897 (2012).

43. Dinev, T. & Hart, P. An Extended Privacy Calculus Model for E-Commerce Transactions. Inf. Syst. Res. 17, 61–80 (2006).

44. Hui, K., Teo, H. H. & Lee, S.-Y. T. The Value of Privacy Assurance: An Exploratory Field Experiment. MIS Q. 31, 19–33 (2007).

45. Morlok, T. Sharing is (not) caring – The role of external privacy in users' information disclosure behaviors on social network sites. in PACIS 75–92 (2016).

46. Malhotra, A. & Malhotra, C. K. Evaluating Customer Information Breaches as Service Failures: An Event Study Approach. J. Serv. Res. 14, 44–59 (2011).

47. Martin, K. D., Borah, A. & Palmatier, R. W. Data Privacy: Effects on Customer and Firm Performance. J. Mark. 81, 36–58 (2017).

48. Solove, D. J. Privacy Self-Management and the Consent Dilemma. Harv. Law Rev. 126, 1880–1903 (2013).

49. Acquisti, A. & Varian, H. R. Conditioning Prices on Purchase History. Mark. Sci. 24, 367–381 (2005).

50. Matz, S. C., Appel, R. E. & Kosinski, M. Privacy in the age of psychological targeting. Curr. Opin. Psychol. 31, 116–121 (2020).

51. Gerdes, J. & Hesse, J. Dialogmarketing im Dialog. (Gabler, 2013). doi:10.1007/978-3-658-02000-2

52. Barth, S., de Jong, M. D. T., Junger, M., Hartel, P. H. & Roppelt, J. C. Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources. Telemat. Informatics 41, (2019).

53. Gunther, R. E. Peter Drucker-the grandfather of marketing: an interview with Dr. Philip Kotler. J. Acad. Mark. Sci. 37, 17–19 (2009).

DER AUTOR

Mauro Gotsch ist Doktorand und Seminarleiter am Institut für Marketing an der Universität St. Gallen. In seiner Forschung beschäftigt er sich mit den strategischen Vorteilen des Datenschutzes aus einer Marketing-Management-Perspektive. Zusätzlich leitet er das Intensivstudium für Einkaufsleiter (CAS) und ist involviert in der Organisation verschiedener Kurse im Master für Marketing-Management an der Universität St. Gallen.