ePrivacy und Digital Analytics & Optimization

Leitfaden

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Rebekka Weiß, LL.M. | Bereichsleiterin Datenschutz & Verbraucherrecht
T 030 27576-116 | r.weiss@bitkom.org

Verantwortliche Bitkom-Gremien

AK Digital Analytics & Optimization
AK Datenschutz

Autoren

Martin Buske | Digital Analytics Institute GmbH
Gordon Grill | Deloitte Consulting GmbH
Georg Klassen | Rohde & Schwarz GmbH & Co. KG
Rebekka Weiß, LL.M. | Bitkom e.V.
Tobias Weiß | Deloitte Consulting GmbH

Titelbild

© Fotolia.com – SUNGYOON

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Zielsetzung des Dokuments

Im Mai 2018 wurde die Datenschutzgrundverordnung (DS-GVO) europaweit rechtswirksam. Die datenschutzrechtlichen Änderungen wurden mit immensem Aufwand seitens der Wirtschaft in Europa umgesetzt. Eine der Folgen sind heute teilweise stark hinsichtlich der Nutzung eingeschränkte Webseiten von Technologieanbietern und anderen europäischen Unternehmen. Die besonders auf mobilen Geräten viel Platz einnehmenden Cookie-Banner als Informationspflicht der Unternehmen zur Datenerhebung reduzieren das Nutzererlebnis der Anwender und schaffen zusätzlichen Aufwand.

Während Großkonzerne dabei wohl eher den datenschutzrechtlichen Anforderungen gerecht werden können und richtungsweisende technische und organisatorische Lösungen schaffen, ist der Umsetzungsaufwand vor allem für kleine und mittelständische Anbieter nur schwer zu bewältigen; das liegt unter anderem auch an den vielen noch offenen Rechtsfragen. Diese ergeben sich zum Teil aus der DS-GVO selbst aber auch aus Unklarheiten hinsichtlich der Fortgeltung nationaler Gesetze wie dem Telemediengesetz (TMG), das ganz maßgeblich bisher zum Beispiel die Informationspflichten auf Webseiten geregelt hat.

Gerade der Großteil der europäischen wie auch deutschen Wirtschaft sind Unternehmen mit unter 50 Mitarbeitern. Hier sorgen die ohnehin online im internationalen Wettbewerb geschaffenen und oben beschriebenen Nutzungsbarrieren für einen Wettbewerbsnachteil. Dies wird auch dadurch bestärkt, dass die kleinen und mittleren Unternehmen, die sich vorrangig operativ um ihr Kerngeschäft bemühen müssen, durch den zusätzlichen Umsetzungsaufwand kosten und zeitintensiv Ressourcen binden müssen. Diese Ressourcen zur Erfüllung der Anforderungen fehlen dann natürlich an anderer Stelle.

Schon zum Geltungsbeginn der DS-GVO am 25. Mai 2018 war es – wie beschrieben – für viele Unternehmen schwer bis unmöglich, die gestellten Anforderungen zu erfüllen. In Folge schlossen viele Unternehmen ihre Internetportale oder reduzierten ihre Onlineaktivitäten.[1] Ein weiteres Ungleichgewicht und Wettbewerbsnachteile sind dadurch praktisch wahrnehmbar entstanden. Die derzeit geplanten Regelungen der ePrivacy Verordnung werden diese Effekte noch verstärken, da bisher die komplexen technischen Vorgänge nicht ausreichend differenziert und die gesamtwirtschaftlichen Auswirkungen nicht ausreichend beachtet werden.

Unklare oder zu komplexe Anforderungen an den Betreiber des Online-Angebots führen unter anderem zu aus der Endnutzersicht undurchsichtigen und verwirrenden Implementierungen der Richtlinien auf den Webseiten. So weiß ein Normalverbraucher in der Regel nicht, welche Einstellungen auf der Webseite und direkt im Browser vorgenommen werden müssen, um den gewünschten Grad des persönlichen Datenschutzes und der gewünschten Nutzererfahrung zu erreichen – geschweige denn, wie sich diese Einstellungen gegenseitig beeinflussen.

1 URL: ↗ http://www.faz.net/aktuell/wirtschaft/diginomics/skurrile-folgen-der-dsgvo-15609815.html, zugegriffen am 07.09.2018.

Das irritiert und verunsichert den Nutzer, der mittlerweile einen hohen Standard der Online-Erfahrung und Benutzerfreundlichkeit gewohnt ist. Sinkt dieser hohe Standard, zieht dies nahezu zwangsläufig auch wirtschaftliche Folgen nach sich – wie z. B. Umsatzeinbrüche oder Abwanderung der Kunden. Diese Auswirkungen haben allerdings mit dem eigentlichen Online-Angebot nichts zu tun; die Nutzererfahrung auf Webseiten ist aber essentiell für die Nutzung der Angebote. Eine weitere mögliche Auswirkung ist, dass der Nutzer in seiner Verzweiflung sämtliche Datenschutzmechanismen abschaltet, um überhaupt noch weiter wie gewohnt im Internet surfen zu können. Damit wird dann genau das Gegenteil vom eigentlich angedachten Datenschutz erreicht.

Jedes Unternehmen ist außerdem zugleich Arbeitgeber und gesamtwirtschaftlich damit essentiell für die Betrachtung des Konsumentenschutzes. Durch Wettbewerbsnachteile und faktische Nutzungsnachteile entstehende Umsatzeinbrüche sorgen für weniger Beschäftigung – ein Weniger an Konsumenten oder Konsummöglichkeiten durch verringerte Einkommen.

Durch den technischen Wandel verändern sich ständig die Handlungsweisen und Mediennutzungen der Nutzer. Um diese zu verstehen und bestmöglich auf die Bedürfnisse der Nutzer einzugehen und exzellente Produkte und Dienstleistungen anzubieten, ist die Analyse des Nutzerverhaltens notwendig. Dies erfordert Daten in einem Umfang, der repräsentative Rahmenbedingungen zur Schaffung aussagekräftiger Analysen ermöglicht. Ansonsten würden falsche oder fehlerhafte Ableitungen entstehen, die wiederum für den heutigen digital agierenden Konsumenten ein negatives Kundenerlebnis hervorrufen würden.Zudem ist die Analyse und Anwendung von Erkenntnissen zur Optimierung der Maßnahmen zur Produkt- und Dienstleistungspräsentation und Bewerbung ein fortwährender Prozess mit dem Ziel, dem Nutzer ohne größere Barrieren oder Verzögerungen maximalen Nutzen hinsichtlich seiner Informations- oder Kaufabsichten zu verschaffen.

Durch die wohl gravierenden Auswirkungen der geplanten ePrivacy Verordnung besteht ein Bedürfnis an einer umfassenden Folgenabschätzung. Das vorliegende Dokument soll über die bestehenden technischen Abläufe und rechtlichen Ableitungen informieren, die für die Wettbewerbsfähigkeit eines modernen und kundenorientierten Unternehmens essentiell sind. Die Publikation soll zu mehr Transparenz im Bereich des Webtrackings beitragen. Denn Information und Transparenz schaffen die Basis für Vertrauen, das im digitalen Zeitalter unerlässlich ist.

Das Papier konzentriert sich dabei auf drei Schwerpunkte:

- Die Darstellung der gängigen Tracking-Verfahren und Einsatzgebiete von Tools des Digital Analytics & Optimization. Ein gutes Verständnis der Technologie ist sowohl für die Rechtsanwendung als auch für weitere Regulierungsbestrebungen unerlässlich.

- Den zweiten Schwerpunkt bilden datenschutzrechtliche Fragestellungen, die im Zusammenhang mit Digital Analytics & Optimization diskutiert werden müssen. Die DS-GVO gibt hier einen Rahmen vor, ohne jedoch konkrete Anwendungen zu erlauben oder zu verbieten. Es stellen sich jedoch Fragen, ob die DS-GVO im Bereich des Digital Analytics & Optimization Anwendung findet, oder das Telemediengesetz diesen Bereich noch regelt.

- Den dritten Schwerpunkt bildet die Darstellung der Implikationen DS-GVO und der ePrivacy Verordnung auf Digital Analytics & Optimization.

Der vorliegende Leitfaden »ePrivacy und Digital Analytics & Optimization« adressiert Entscheidungsträger in der Politik und in den Datenschutzbehörden, private Verbraucher sowie die breite Öffentlichkeit. Es wendet sich ebenfalls an die Anwender von Digital Analytics & Optimization-Technologien und -Lösungen aus der Wirtschaft, Tool-Anbieter sowie Datenschutzbeauftragte. Der Leitfaden lädt somit zur Diskussion rund um das Thema der ePrivacy Verordnung ein.

2 Einführung in Digital Analytics & Optimization

Im Zusammenhang mit der Erhebung, Verarbeitung und Analyse von Daten über das Nutzerverhalten auf Webseiten oder Apps wird vielfach lediglich auf die mögliche Sensibilität der erhobenen Daten und eine eventuelle Profilbildung der Nutzer abgestellt. Dabei wird häufig der immense Mehrwert außer Acht gelassen, der durch Analyse und Optimierung der digitalen Interaktionen für Nutzer entstanden ist. Insbesondere die Entwicklung der heute beliebten eCommerce-Angebote und Streaming-Plattformen ist maßgeblich durch Digital Analytics & Optimization beeinflusst.

Als ein Beispiel sei hier die Analyse des Besucherverhaltens eines Nachrichtenportals genannt. Durch die Erhebung und Analyse der Nutzerinteraktionen können Vorlieben und Lesegewohnheiten identifiziert werden. So ist es zum Beispiel möglich, die Interessen und Vorliegen eines Nutzers zu identifizierung und auf diser Basis dann passende Artikel, Themen und Beiträge vorzuschlagen. Letztlich verbessert dies das Kundenerlebnis und erspart dem Nutzer aufwändige Suche.

Da Analyse und Optimierung zunächst sehr breite Anwendungsfelder haben, grenzen wir die im Kontext dieses Faktenpapiers relevanten Anwendungsfelder ab. Bei den hier betrachteten Methoden fokussieren wir uns auf die Analyse und Optimierung der digitalen Kommunikation. Dabei wird als Kommunikation jegliche Interaktion mit dem Nutzer verstanden, die digitale Kontaktpunkte (sog. Touchpoints) einbezieht. Solche Kontaktpunkte können Webseiten, mobile Apps, aber auch Beacons oder NFC-Tags sein. Analyse in diesem Zusammenhang meint, dass an allen diesen Kontaktpunkten, an denen eine Kommunikation zwischen Organisation und Kunde stattfindet, Daten über die Interaktionen gesammelt und sinnvoll ausgewertet werden. Dabei werden typischerweise Daten zu den Rahmenbedingungen der Kommunikation (Uhrzeit, Art und Dauer des Kontakts), Daten über die konkrete Interaktion (Bestellung, Informationsabruf, Beschwerde, Serviceanfrage etc.) und Daten zum Ergebnis der Interaktion (erfolgreicher Abschluss, Abbruch, Zwischenspeicherung auf der Merkliste etc.) gesammelt.

Aus diesen Daten können Profile und Personentypen abgeleitet werden, um die Nutzer besser in ihrem Verhalten zu verstehen. Dabei geht es häufig darum, Muster zu erkennen und zukünftiges Verhalten zu prognostizieren, auch auch um eine Steuerung der Interaktionen. Damit die zukünftige Interaktion sowohl für den Kunden als auch für die Organisation zufriedenstellend verläuft, wird diese laufend optimiert. Auf Basis der gesammelten und analysierten Daten können dem Kunden passgenaue Angebote unterbreitet und insgesamt ein besseres Nutzungserlebnis entlang der gesamten Customer Journey geboten werden.

Digital Analytics & Optimization

Digital Analytics & Optimization beschreibt damit die Erfassung und Auswertung von Nutzungs- sowie Nutzerdaten auf digitalen Kanälen, um die Nutzungsintensität sowie Zielerfüllung zu prüfen und nachhaltig zu verbessern.

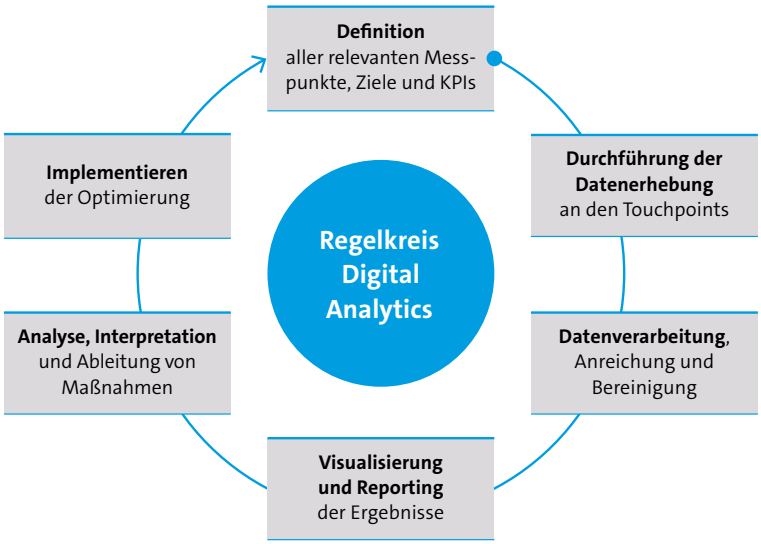

Abbildung 1: Übersicht Digital Analytics, adaptiert von Deloitte

Bei Digital Analytics & Optimization handelt es sich nicht um eine einmalige, sondern um eine beständig begleitende Maßnahme. So wie auch ein klassisches Ladengeschäft immer wieder um kreative Marketingmaßnahmen und deren Reflektion hinsichtlich der Wirksamkeit bemüht sein muss, um über lange Zeit erfolgreich zu bleiben, verstehen wir Digital Analytics & Optimization auf digitalen Kanälen als essentiellen Bestandteil der Erfolgskontrolle.

Wie in Abbildung 1 ersichtlich, können die Aktivitäten in einem Regelkreis abgebildet werden. Dieser beginnt mit der initialen **Datenerhebung**, idealerweise auf jedem Touchpoint, d. h. an jeder Stelle an der bspw. ein Online-Händler mit potentiellen oder bestehenden Kunden in Kontakt gerät – bspw. auf der eigenen Webseite oder im Online-Shop. Hier ist das Nutzerverhalten hochinteressant: für welche Produkte interessiert sich der potentielle Kunde, welche Webseiten schaut er sich an? Die Folgeschritte der **Bereinigung, Strukturierung und Anreicherung** finden i. d. R. in spezialisierten Systemen für Digital Analytics & Optimization statt. Mehrere Datenquellen verschiedener Touchpoints werden dabei miteinander kombiniert und entsprechend angeglichen, damit sie im einheitlichen Kontext genutzt werden können und bspw. auch stets die individuellen Präferenzen desselben Kunden beachten.

Im Anschluss kommt eine wesentliche Kernfunktion dieser Systeme zum Einsatz: die **Visualisierung** (wie beispielhaft dargestellt in Abbildung 2), also Darstellung der gesammelten Daten in einem verständlichen und nutzenstiftenden Format. Klassische Auswertungen zeigen deskriptiv bspw. die Performance der unterschiedlichen Produkte, Verweildauern bei der Betrachtung der Beschreibungen, oder den Bestellprozess.

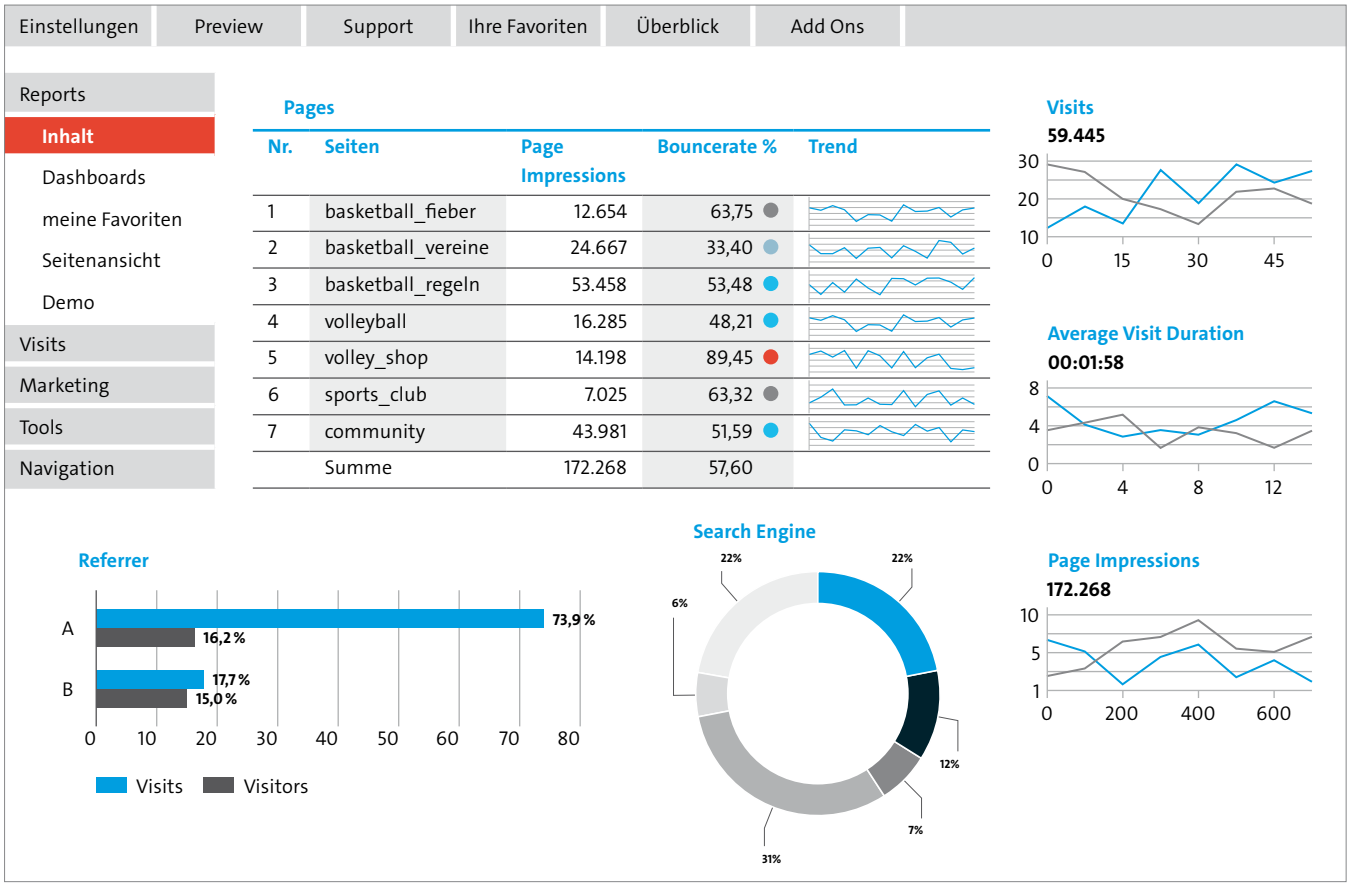

Abbildung 2: Visualisierung und Darstellung der gesammelten und aufbereiteten Daten in einem Dashboard

Die Aufgabe eines Webanalysten innerhalb der Organisation besteht in der **Kommunikation und Interpretation** der Ergebnisse sowie in der Ableitung von konkreten **Handlungsempfehlungen** anhand der Datenlage. Diese führen zu entsprechenden Implikationen im Management, oder bspw. zur Anpassung der Marketingstrategie. Diesen Folgeschritt bezeichnen wir als **Aktion**, im Grunde eine Reaktion auf gelerntes Wissen des vorherigen Durchlaufs, welches anschließend zu einem neuen Durchlauf des Zyklus führt.

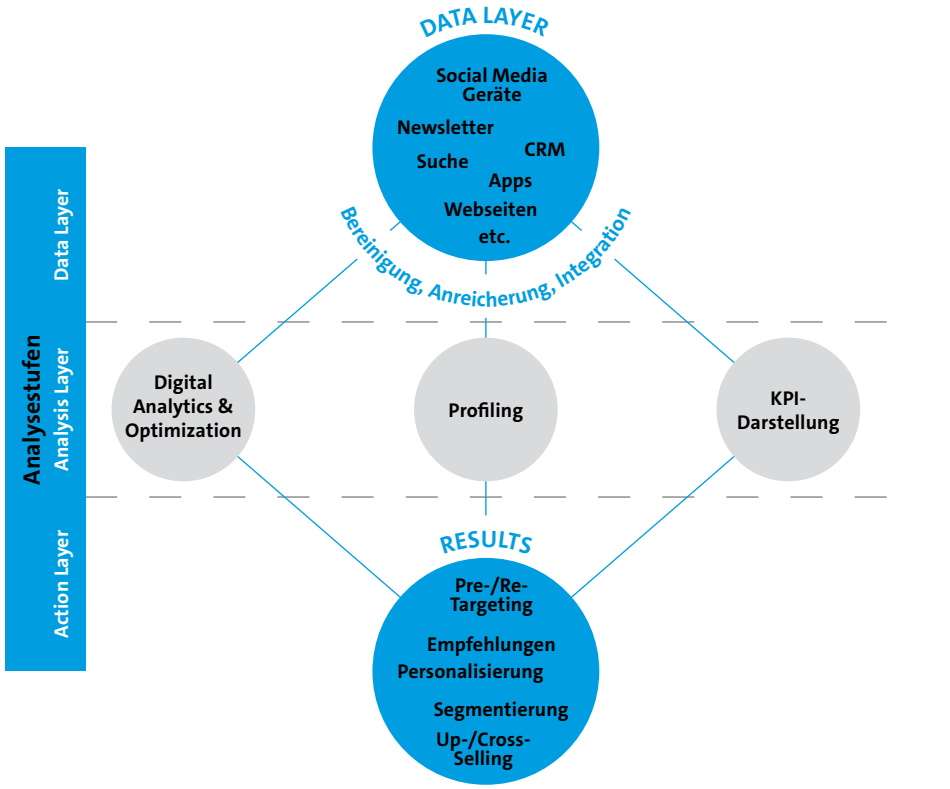

Abbildung 3: Drei Layer der Datenverarbeitung und -nutzung bei Digital Analytics & Optimization, adaptiert von Deloitte

Ergänzend zum oben dargestellten Optimierungskreislauf sollen in Abbildung 3 unterschiedliche aufeinander aufbauende Layer der Datenverarbeitung und -nutzung veranschaulicht werden:

- Im Data Layer erfolgt die Sammlung der Daten aus unterschiedlichen Quellen – sprich digitalen Touchpoints
- Bevor diese Daten sinngemäß im Analysis Layer benutzt werden können, wird die Datenqualität, -vollständigkeit und -konsistenz sichergestellt
- Im Analysis Layer findet die Auswertung, Visualisierung und Interpretation der Daten statt
- Die gewonnenen Erkenntnisse werden im Action Layer in bestimmte Handlungen überführt, die sowohl operativer als auch strategischer Natur sein können

Bei hinreichender Datenbasis und Datenqualität können viele Schritte des Optimierungskreislaufs automatisiert werden. Ein interessantes Spannungsfeld bietet zudem der Einsatz der künstlichen Intelligenz, die z. B. bei der Erkenntnisgewinnung mit Einbezug unterschiedlicher Datenquellen unterstützen könnte. Typischerweise werden Analyseergebnisse heute aufbereitet zur Entscheidungsunterstützung im Austausch zwischen Fachexperten und Entscheidern eingesetzt. Reifere Unternehmen nutzen hier die automatisierte Entscheidungsfindung und Anwendung von Optimierungen, um weitere Reduktionen manueller Aufwände und eine schnelle zeitliche Reaktion und Umsetzung von Verbesserungen zu erreichen.

3 Funktionsweisen von Tracking-Verfahren

Im Folgenden sollen die aktuell meist verbreiteten Tracking-Verfahren anschaulich erklärt werden. Logfile-Analysen und Logfile-basiertes Tracking werden dabei ebenso beleuchtet wie das häufig verwendete Page Tagging und Pixel-basiertes Tracking. Verschiedene Methoden der Nutzeridentifikation werden ebenfalls in diesem Kapitel untersucht und vor allem die sehr bekannten »Cookies« genauer betrachtet und in ihren verschiedenen Ausprägungen dargestellt. Ein umfassendes und präzises Verständnis der unterschiedlichen Methoden ist aus unserer Sicht erforderlich – nicht nur für das wichtige Verständnis der Mehrwerte von Digital Analytics & Optimization sondern auch für die alle regulatorischen Entwicklungen, die in diesem Bereich Auswirkungen haben (werden).

3.1 Logfile-basiertes Tracking

Unter Logfile-Analysen versteht man die Anfangsformen der Erhebung von Daten mit Methoden der Digital Analytics. Dabei findet die Protokollierung und Speicherung der Daten auf Webservern statt, welche üblicherweise die Inhalte von Webseiten ausliefern. Bei einem Aufruf der Webseite stellt der Browser des Besuchers an diesen Webserver eine Anfrage zu den gewünschten Medien wie Bildern und Videodateien, Texten und sonstigen Inhalten. Diese Aufrufe werden durch den Webserver in ein Protokoll – auch Logfile genannt – geschrieben. Es werden sowohl die erfolgreichen als auch die fehlerhaften Aufrufe erfasst.

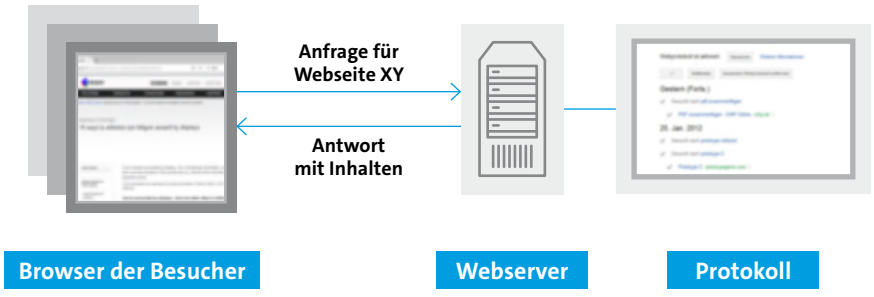

Abbildung 4: Kommunikation zwischen Browser und Webserver und resultierendes Protokoll, adaptiert von Deloitte

Logfiles werden in der Regel dann direkt auf dem Webserver mit Tools wie bspw. AWStats[2] oder Splunk[3] ausgewertet. Sie sind jedoch zur Einschätzung des Nutzerverhaltens aus heutiger Perspektive nicht mehr geeignet, da bei der Auswertung nicht die Benutzersicht, sondern die technische Sicht eingenommen wird. Falls bspw. ein Nutzer die betreffenden Websites aufgrund von lokalen Netzwerk- oder Browser-Problemen nicht angezeigt bekommt, der Server die Inhalte aber korrekt ausgeliefert hat, so findet diese Problematik keine Beachtung. In der Logfile-Auswertung würde dieser Zugriff als erfolgreich gewertet. Des Weiteren gibt es oftmals keine zuverlässige Möglichkeit der Wiedererkennung von Besuchern, da als Identifizierungsmerkmal die IP-Adresse des Nutzers herangezogen wird. Bei im Konsumentenbereich üblichen Internet-anschlüssen wird diese dynamisch vergeben und wechselt i. d. R. alle 24 Stunden. Aktuell sind Logfiles daher primär im Bereich der technischen Auswertungen anzufinden, jedoch nicht mehr im Kontext von Digital Analytics & Optimization.

3.2 Pixel-basiertes Tracking (Page Tagging)

Das Pixel-basierte Tracking ist aktuell der Standard im Bereich der Erfassung von Nutzungs- und Nutzerdaten auf Websites. Die Technologie ist hinreichend erprobt, verbreitet und datenschutzrechtlich beleuchtet. Seinen Namen verdankt es ursprünglich 1×1 Pixel großen transparenten Bilddateien, die meistens am Ende einer jeden Seite integriert werden. Bei jedem Seitenaufruf wird das kleine Bild mit geladen. Dem Bildaufruf werden alle relevanten Tracking-Parameter (Page Tagging) hinzugefügt, die die Interaktion des Nutzers mit der Webseite beschreiben sollen.

Bei dieser Methode werden die JavaScript-Codes auf jeder einzelnen Seite des Webangebotes integriert. Sie werden im Browser des Nutzers aufgerufen und ausgeführt. Damit findet idealer-weise eine Vollerhebung der Nutzung statt. Im Gegensatz zu Logfile-Analysen steht nicht die technische Kommunikation mit dem Webserver im Vordergrund, sondern die Interaktion zwischen dem Nutzer und der Webseite. Da der Tracking-Code erst am Ende der Seite ausgeführt wird, kann z. B. sichergestellt werden, dass der Nutzer tatsächlich die vollständige Seite gesehen hat. Darüber hinaus wird mittels der JavaScript-Codes eine viel umfassendere Nutzungsanalyse möglich, bspw. das Tracking des Mauszeigers, des Fortschritts beim Abspielen eines Videos, des Scrollverhaltens auf der Seite oder die Sammlung von zahlreichen Kontextinformationen des Browsers, des genutzten Computers oder des aktuellen Standorts des Nutzers.

2 ↗ https://de.wikipedia.org/wiki/AWStats, zugegriffen am 06.09.2018.

3 ↗ https://de.wikipedia.org/wiki/Splunk, zugegriffen am 06.09.2018.

Die Pixel-basierten Tracking-Requests können durch den JavaScript-Code bei Bedarf und jederzeit ohne Neuladen der Webseite ausgelöst werden und eröffnen somit neue Möglichkeiten im Gegensatz zur Logfile-Analyse, die nur die Zugriffe der jeweiligen Seitenaufrufe auswerten kann.

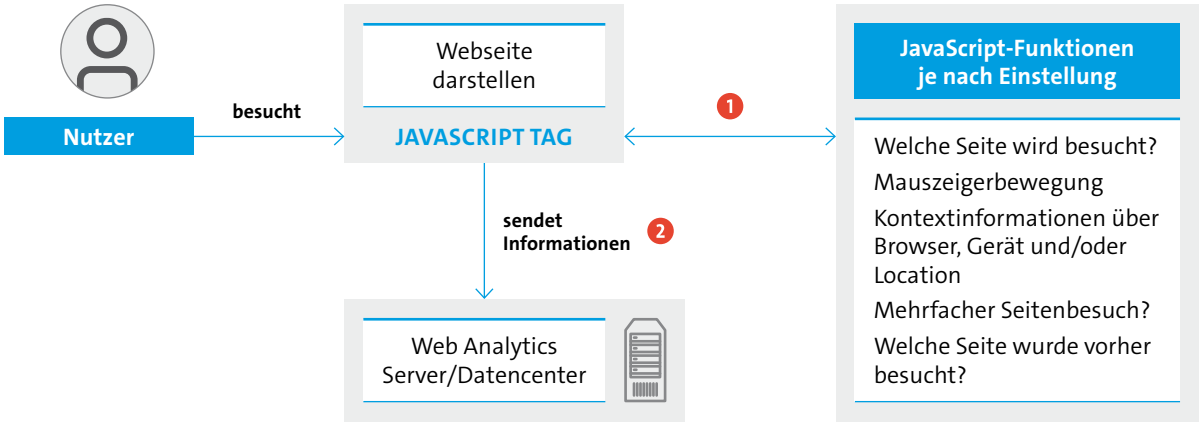

Abbildung 5: Implementierung des Pixel-basierten Tracking

Die Aufbereitung der Daten wird über webbasierte, grafische Anwendungen realisiert. Der wohl bekannteste Vertreter ist das kostenfrei verfügbare Google Analytics[4]. Zahlreiche weitere Anbieter sind im Markt aktiv, und unterscheiden sich vorrangig durch die nachfolgenden Analysemöglichkeiten der Daten. Das prinzipielle Vorgehen des Page Taggings unterscheidet sich nicht.

3.3 Methoden der Nutzeridentifikation

Wie oben bereits beschrieben, stellen die IP-Adressen meist keine ausreichende Möglichkeit der Nutzeridentifikation dar. Im Pixel-basierten Tracking hat sich vor allem der Einsatz von sog. Cookies und/oder Fingerprint zu einer besseren und zuverlässigen Nutzerwiedererkennung etabliert. Moderne Analytics-Lösungen unterstützen mehrere Methoden gleichzeitig. Werden z. B. die Cookies vom Nutzer abgelehnt, wird die Fingerprint-Methode als Fallback eingesetzt. Ist kein Fingerprint möglich, kann auf die IP-Adresse (mit den entsprechenden, oben bereits ausgeführten Nachteilen) zurückgegriffen werden.

4 ↗ https://de.wikipedia.org/wiki/Google_Analytics, zugegriffen am 06.09.2018.

Im Umfeld der mobilen Internetnutzung, die auf 3 Mrd. mobile Endgeräte geschätzt wird,[5] verfügt jedes Smartphone über eine eindeutige Geräte-ID, die oftmals eindeutig einem Nutzer zugeordnet werden kann.

Darüber hinaus ist eine Erfassung des Nutzers mithilfe seines Logins möglich – z. B. im passwortgeschützten Bereich eines Online-Shops oder Online-Bankings, mit Ausnahme der Fälle, wenn dasselbe Login von mehreren Personen (z. B. Familienmitgliedern) geteilt wird.

3.3.1 Einsatz von Cookies

Cookies sind kleine Textdateien, welche im Browser des Nutzers bzw. direkt auf dem Rechner abgespeichert und durch die aufgerufene Webseite gesetzt werden. Ist in der Webseite ein Pixel-basiertes Tracking implementiert, setzt es zusätzlich eigene Cookies. So wird zwischen den technisch erforderlichen Cookies der Webseite und den Tracking-Cookies (manchmal auch Marketing-Cookies genannt) unterschieden. Die Ersteren sind für den technischen Betrieb der Webseite notwendig, z. B. für die Speicherung der Artikel im Warenkorb eines Online-Shops. Die letzteren dienen der Erfassung der zusätzlichen Daten über das Nutzerverhalten. Sie enthalten in der Regel eine eindeutige Nutzer-ID, sowie weiterführende Informationen wie den Zeitstempel des allerersten Besuchs auf der Webseite, das aktuelle Besuchsdatum oder spezifische Schlüsselwerte, die für die spätere Analyse notwendig sind. Sie werden in Kombination mit der Webseiten-Domain abgelegt, sodass nur die Domain, die den Cookie gesetzt hat, diesen auch wieder auslesen kann.

Der Nutzer kann durch die Browser-Einstellungen die Nutzung der Cookies beeinflussen und diese z. B. komplett ablehnen. Das kann natürlich zur eingeschränkten Funktionalität der Webseite führen.

5 URL: ↗ https://de.statista.com/statistik/daten/studie/172505/umfrage/anzahl-der-personen-weltweit-die-mobil-das-internet-nutzen, zugegriffen am 06.09.2018.

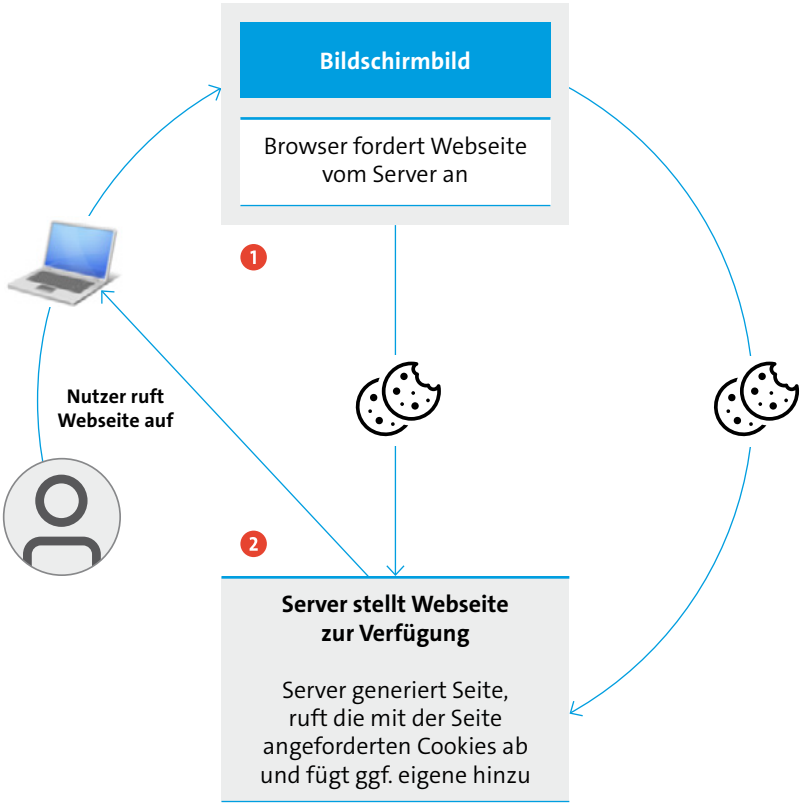

Abbildung 6: Das Lesen und Setzen von Cookies

Cookies nehmen eine wesentliche Rolle der Datenerhebung via Page Tagging ein, da sie dazu dienen, die Besucher mit einer hinreichenden Zuverlässigkeit wiederzuerkennen und die entsprechenden Datensätze zuzuordnen und zu verbinden. Wie bereits geschrieben ist die IP-Adresse dazu nicht zielführend anwendbar, da sie zu häufig beim Nutzer wechselt oder im B2B-Umfeld von mehreren Nutzern gleichzeitig verwendet wird. Mittels eines Cookies bzw. der im Cookie gespeicherten Nutzer-ID kann auch noch Wochen später eine Zuordnung stattfinden. Wird das Cookie vom Nutzer gelöscht, wird beim nächsten Besuch der Webseite ein neues Cookie mit einer neuen Nutzer-ID generiert. Eine Zusammenführung mit der alten Nutzer-ID ist dann ohne weiteres nicht mehr möglich.

Es werden vier verschiedene Arten von Cookies unterschieden.

Erforderliche Cookies

Erforderliche Cookies ermöglichen die Ausführung von spezifischen Funktionen einer Website und sind für einen ordnungsgemäßen und sicheren Betrieb erforderlich. Bspw. kann die Speicherung der Produkte im Warenkorb zur Übergabe an die Folgeseite im Cookie durchgeführt werden, sodass dieser auch beim (ggf. versehentlichen) Schließen des Browsers nicht verloren geht.

Bei einer Unterdrückung von erforderlichen Cookies können bestimmte Websitefunktionen nicht mehr ordnungsgemäß ausgeführt werden. Es sind entsprechend Einbußen bei der Nutzererfahrung zu befürchten.

Funktionale Cookies

Funktionale Cookies ermöglichen die Umsetzung von nutzerfreundlichen Websites, indem sie sich bspw. Nutzereingaben in Formularen, oder spezielle Anpassungen an das Design der Webseite durch den User merken und für den nächsten Besuch des Benutzers vorhalten. Somit erfolgt eine Verbesserung der Nutzererfahrung.

Statistische Cookies

Statistische Cookies werden zur Erfassung des Nutzerverhaltens auf der Website eingesetzt, bspw. für zahlreiche Anwendungen im Bereich Digital Analytics & Optimization. Dabei sammeln sie auf anonymisierter Basis diese Informationen über den Nutzer, welche Websites aufgerufen werden, ob Fehlermeldungen auftreten, und geben diese an die nachgelagerten Anwendungen weiter.

Marketing Cookies

Marketing Cookies werden angewendet, um das Surfverhalten des Benutzers auf den Websites zu verfolgen und zu beeinflussen. Dazu werden bspw. zielgerichtete Werbeanzeigen geschaltet, welche auf die Präferenzen des einzelnen Nutzers passen. Dies ist mit Marketing Cookies auch auf Partner-Webseiten möglich, bspw. durch sogenanntes Re-Targeting.

Ein Beispiel für die entsprechende Umsetzung der Cookie-Steuerung könnte zum Beispiel so aussehen wie in Abbildung 7.

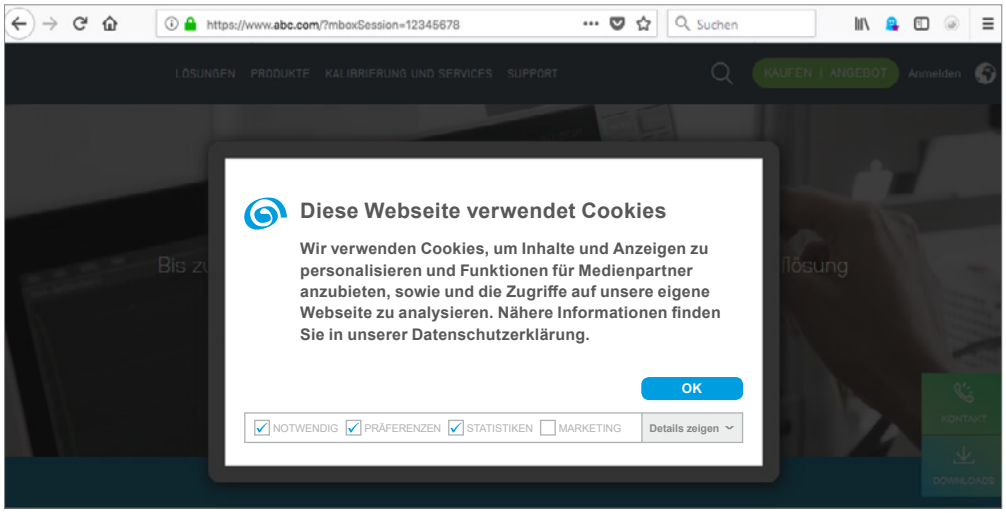

Abbildung 7: Beispielhafter Hinweis in einem Cookie-Banner auf die unterschiedlichen Cookie-Arten

3.3.2 Fingerprint-Verfahren

Obgleich das sogenannte Page Tagging die derzeit verbreitetste Methode der Datensammlung auf Webseiten ist, so ist es dennoch mit Problemen behaftet. Im Zuge des zunehmenden Datenschutzbedürfnisses der Nutzer wird von einer nicht unerheblichen Anzahl an Nutzern das Laden von Drittanbieter-Skripten, bspw. der benannten JavaScript-Messpixel für die Webanalyse, browserseitig unterbunden. Demzufolge kann keine Messung des Nutzungsverhaltens stattfinden. Zusätzlich unterbinden diese Maßnahmen auch den Einsatz von Cookies, und verhindern damit die Wiedererkennung der Nutzer.

Abbildung 8: Fingerprint-Verfahren

Eine Option, um dennoch die Besucher zweifelsfrei zuzuordnen, besteht im Einsatz eines sogenannten Fingerprint-Verfahrens. Dazu werden zahlreiche erkennbare Merkmale des Besuchers miteinander kombiniert und zu einem im hohen Maß eindeutigen Fingerabdruck zusammengeführt. Diese Merkmale sind:

- Genutzter Rechnertyp
- Installiertes Betriebssystem
- Bildschirmauflösung
- Version des Browsers
- Im Browser installierte Plug-Ins
- etc.

4 Anwendung von Digital Analytics & Optimization

Die im vorherigen Kapitel näher beschriebenen Methoden zur Datenerhebung werden in unterschiedlichen Zusammenhängen eingesetzt, um einen Beitrag zur Erkenntnisgewinnung abzuleiten. Hierzu werden je nach Zielsetzung auf den erhobenen Daten verschiedene analytische Verfahren angewendet und weitergehende Bearbeitungsschritte umgesetzt.

Sowohl bei der Analyse der erhobenen Daten als auch bei der Optimierung gibt es unterschiedliche Zielsetzungen, die wiederum abhängig von den involvierten Fachbereichen des jeweiligen Unternehmens sind.

Eine gute Verfügbarkeit und schnelle Ladezeiten einer Webseite sind eine wesentliche Voraussetzung, damit das digitale Angebot überhaupt genutzt werden kann. Durch die Identifikation von möglichen Verzögerungen im Seitenaufbau können zeitnah hardwaretechnische oder softwaretechnische Fehler festgestellt und somit mögliche Einschränkungen der Nutzung für den Anwender unterbunden werden.

Das frühzeitige Erkennen von Betrugsmustern bei Zahlungsvorgängen oder Zugriffen auf die Anwendung und Abwehren von solchen Zugriffen schützt Anwender vor Datenmissbrauch.

In den oben beschriebenen Szenarien spielt zunächst die Analyse der digitalen Nutzerinteraktionen eine wesentliche Rolle, damit auf der Grundlage eine Entscheidung zur Fehlerbehebung oder Optimierung des Nutzerverhaltens bzw. die des digitalen Angebots getroffen werden kann.

Im Folgenden werden einige Analysezielsetzungen exemplarisch beleuchtet.

4.1 Analytics

4.1.1 Besucherverhalten

Die Analyse des Besucherverhaltens dient dazu, zu verstehen, was das Verhalten der Besucher antreibt. Waren die dargestellten Inhalte nützlich für den Betrachter? Wurden die gewählten Prozesse – z. B. eine Registrierung oder ein Kauf – erfolgreich abgeschlossen?

Um das Besucherverhalten korrekt zu erheben und entsprechend messen und analysieren zu können, ist hierbei entscheidend, dass einzelne Besuche einem tatsächlichen Nutzer eindeutig zugeordnet werden können. Wesentlich ist hierbei nicht das Identifizieren des Individuums, sondern die Zuordnung mehrerer Besuche zur selben Browser-Client-Kombination (Client steht hier für z. B. PC, Notebook, Tablet oder Smartphone). Durch die Analyse ist ein besseres Verständnis des Besucherverhaltens möglich.

4.1.2 Präferenzen identifizieren

Die Identifikation von Präferenzen ermöglicht es, das inhaltliche Angebot oder Produktangebot auf die Bedürfnisse der Konsumenten besser auszurichten.

Hierzu werden zunächst der Abruf und die Verweildauer auf Artikel und Kategorieseiten im redaktionellen Kontext, aber auch auf Produktkategorie- und Produktseiten im Shopkontext erhoben und gemessen. Durch Sortierung der Kategorie- oder Detailabrufe nach Anzahl ist es so möglich, die am häufigsten in einem definierten Zeitraum abgerufenen Artikel zu identifizieren. Ebenso können die am stärksten besuchten Kategorien oder auch Produkte und Artikel mit hoher Verweildauer identifiziert werden.

Dies ermöglicht es, besonders attraktive Kategorien und Produkte zu identifizieren und Produkt- oder Content-Strategie für zukünftige Angebotsproduktion anzupassen. Gerade in diesem Zusammenhang ist es wesentlich, wiederholte Besuche desselben Besuchers auf einem Artikel von eindeutigen Einzelbesuchen unterscheiden zu können, um korrekte Ableitungen aus diesen Erhebungen und Messungen umzusetzen.

4.1.3 Segmentierung

Grundsätzlich ermöglicht Segmentierung im geschäftlichen Zusammenhang die Identifikation der wesentlichen Schlüsselfaktoren, die den Großteil des Geschäftsergebnisses beeinflussen. Man denke an Marktsegmente, die eine Gruppierung der potentiellen und bestehenden Kunden eines Unternehmens nach bestimmten Kriterien darstellen. Innerhalb eines solchen Marktsegments weisen die Kunden weitgehend gleiche Eigenschaften und Bedürfnisse auf.

Im Zusammenhang mit Digital Analytics ist hier die Identifikation und Charakterisierung der Kernzielgruppen zu verstehen, die einen wesentlichen Anteil am Erfolg der digitalen Kundenbeziehung des Unternehmens haben. Konkret kann dies bedeuten, dass 70 % der Einkäufe einer bestimmten Produktkategorie von Männern zwischen 30 und 39 Jahren mit Firefox-Browser auf Tablet-Geräten stattfinden. Diese Erkenntnisse können seitens des Anbieters für weitergehende Maßnahmen genutzt werden, Werbemaßnahmen können so z. B. zielgerichteter geplant und an die passenden Zielgruppen ausgerichtet werden.

4.1.4 Werbeerfolgsmessung

Bei der Werbeerfolgsmessung wird versucht, Besucher möglichst nahtlos den durchgeführten Werbemaßnahmen zuzuordnen. So ist es bereits von hoher Bedeutung, einen transparenten Überblick über die Herkunft der Besucher und die Beteiligung verschiedener kostenpflichtiger Werbemaßnahmen zu erhalten. Durch genaue Ableitung der Verteilung der Besucher nach Werbemaßnahmen und weitergehender Ableitung der Kosten der Akquise der Besucher wird die Kosten-Nutzen-Berechnung der eingesetzten Werbemittel ermöglicht (z. B. durch Ableitung der Kosten je Klick auf ein Werbemittel oder der Kosten einer Konvertierung eines Besuchers zum Käufer eines Produktes).

4.2 Optimization

Unter Digital Optimization im Sinne dieses Dokuments versteht man die sukzessive Verbesserung eines digitalen Angebots. Auf der einen Seite soll dadurch das Kundenerlebnis verbessert werden. Auf der anderen Seite soll es zu besserer Erreichung der Geschäftsziele beitragen. Hierbei ist von der Search Engine Optimization (kurz SEO – Verbesserung der Sichtbarkeit in den Suchmaschinen) zu unterscheiden. Diese Maßnahmen sind zwar als Teilbereiche notwendig, um eine ganzheitliche Optimierung der Webseite zu erreichen. Vorrangig wird aber im Rahmen der Digital Optimization die Verbesserung der Inhalte des digitalen Angebots selbst betrachtet.

Im Folgenden werden zwei wesentliche Maßnahmen der Optimierung beispielhaft dargelegt.

4.2.1 A/B-Testing

Das A/B-Testing steht beispielhaft für verschiedene Testverfahren, mit denen Inhalte eines digitalen Angebots iterativ optimiert werden, indem einzelne Elemente in einem definierten Zeitfenster gegen Varianten – Variante A gegen Variante B – ausgetauscht und getestet werden. Das Testen wird dadurch umgesetzt, dass für die gezeigten Varianten verschiedene Metriken wie Verweildauer, Klickzahl usw. erhoben werden und geprüft wird, welche der Varianten die besten Ergebnisse in den für den Test relevanten Metriken erreicht. Nach dem Test und der entsprechenden Identifikation der erfolgreichsten Variante wird typischerweise diese Variante als Basis verwendet und der Test mit weiteren Elementen fortgesetzt. Es werden Elemente wie Bildmaterial, Text, Überschriften, Schriftattributen, Buttonfarben- und Größen sowie Formularfelder im Testing betrachtet.

Im multivariaten Testing werden mehr als zwei Varianten eines Elements parallel getestet. Unterschiedliche Varianten bzw. Kombinationen von Varianten werden unterschiedlichen Nutzern in Echtzeit präsentiert. Damit der Nutzer nur mit einer Variante konfrontiert wird, soll er zuverlässig wiedererkannt werden können.

4.2.2 Retargeting

Mit Retargeting wird ein Verfahren bezeichnet, bei dem Besucher einer Webseite markiert – z. B. mithilfe eines Cookies – und während ihrer Onlineaktivitäten später erneut mit gezielter Werbung angesprochen werden. Hierbei wird ein Besucher bei der Datenerhebung auf der Webseite basierend auf seinem Verhalten verschiedenen Segmenten zugeordnet. Dies können einzelne Produkte oder Themenkategorien sein.

Verlässt der Anwender die besuchte Webseite wieder und setzt seine Internetaktivitäten anderweitig fort, wird ihm basierend auf den zugewiesenen Segmenten zielgerichtete Werbung angezeigt, wenn der Betreiber des vorab besuchten Portals sog. Retargeting-Kampagnen einsetzt. Die Retargeting-Kampagnen greifen dabei auf die im Cookie gespeicherte Nutzer-ID und ggf. weitere Informationen zurück. Durch Retargeting und Optimierung der Kampagnen ist es möglich, ehemalige Besucher auch außerhalb der eigenen Webseite wieder zurückzugewinnen und im Idealfall dazu zu bewegen, die vorab begonnenen Aktivitäten – wie Registrierung oder Kauf – abzuschließen.

5 Implikationen der ePrivacy Verordnung für Digital Analytics & Optimization

5.1 Einordnung ePrivacy Verordnung

5.1.1 Grundlegendes

Die ePrivacy Verordnung soll als Verordnung neben die DS-GVO treten und regelt den Sonderbereich der elektronischen Kommunikation. Das umfasst vor allem die Bereiche der digitalen Kommunikation (über Webseiten, E-Mails, OTT-Dienste) und Telekommunikation. Durch die steigende Bedeutung elektronischer Kommunikation wird die ePrivacy Verordnung einen großen Teil des Anwendungsbereichs der über Jahre hinweg ausverhandelten DS-GVO herausnehmen und hierzu Spezialregelungen treffen.

Ganz neu ist die Idee der Sonderregelungen im Bereich der elektronischen Kommunikation allerdings nicht. Die ePrivacy Richtlinie[6] aus dem Jahr 2002 trifft bereits Regelungen, vor allem für die Netzanbieter und zur Vertraulichkeit von Inhalten und Metadaten von Kommunikation. Die Richtlinie wurde 2009 geändert und trifft seitdem vor allem auch Regelungen zum Einsatz von Cookies, weswegen sie häufig als »Cookie-Richtlinie«[7] bezeichnet wird.

Anders als bei den bisherigen Regelungswerken handelt es sich bei der ePrivacy Verordnung um eine direkt wirkende EU-Verordnung, die anders als EU-Richtlinien in den Mitgliedstaaten zu unmittelbarer Wirkung gelangt. Die Mitgliedstaaten müssten also keine Umsetzungsregelungen treffen, sondern die ePrivacy Verordnung würde genau wie die DS-GVO direkte Anwendung genießen.

6 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation).

7 Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009 zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und -diensten, der Richtlinie 2002/58/EG über dieVerarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz.

5.1.2 Stand der ePrivacy Verordnung

Derzeit ist noch nicht absehbar, wann die ePrivacy Verordnung verabschiedet werden wird. Der ursprünglich von der EU-Kommission angedachte Zeitplan sah vor, dass die ePrivacy Verordnung zeitgleich mit der DS-GVO ab 25.05.2018 zur Anwendung gelangen sollte. Zum jetzigen Zeitpunkt (Stand September 2018) hat jedoch der Rat der Europäischen Union (Ministerrat) noch keine Verhandlungsposition für den Trilog gefunden[8], die Mitgliedstaaten sind derzeit dabei, ihre Stellungnahmen zu erarbeiten bzw. fortzuentwickeln. Die Verhandlungen werden sich voraussichtlich noch einige Zeit hinziehen. Da zudem dann noch der Trilog geführt werden muss und auch die ePrivacy Verordnung dringend eine Übergangsfrist von mindestens einem Jahr benötigt, ist der ursprüngliche Zeitplan, der Mai 2018 anvisierte, natürlich längst verstrichen und es ist auch fraglich, ob im Jahr 2019 die Änderungen wirksam werden. Da die Inhalte der ePrivacy Verordnung aber weitreichende Auswirkungen auf den kompletten DAO Bereich haben könnten, ist eine frühzeitige Analyse in jedem Fall angezeigt. Das vorliegende Faktenpapier soll zudem durch die technischen Erläuterungen auch noch zur Aufklärung beitragen und dadurch Folgen aufzeigen, die möglicherweise vom Gesetzgeber nicht erkannt wurden.

2016	2017	2018	2019 – ?
Die Kommission führte vom 12. April bis zum 5. Juli 2016 eine öffentliche Konsultation durch.	10. Januar 2017: Veröffentlichung Kommissionsvorschlag: ↗ https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A52017PC0010 26. Oktober 2017: Europaparlament beschließt EP-Entwurf zur ePrivacy Verordnung: ↗ http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A8-2017-0324&format=XML&language=EN Das Mandat wurde mit 318 (53 %) Stimmen bei 280 (47 %) Gegenstimmen sehr knapp angenommen. 17. November 2017: Sachstandsbericht der Estnischen Präsidentschaft 5. Dezember 2017: Estnische Präsidentschaft veröffentlicht aktualisierten Entwurf	25. Mai 2018: aktueller Sachstandsbericht zu den Verhandlungen im Rat zur ePrivacy VO: ↗ http://data.consilium.europa.eu/doc/document/ST-9079-2018-INIT/de/pdf 8. Juni 2018: Ministerrat zur ePrivacy Verordnung Regelmäßige Diskussionsstände in den aktuellen Ratsdokumenten, z. B. im März, April und Mai. → Noch offen: Allgemeine Ausrichtung des Rates in 2018?	Weiteres Voranschreiten der Verhandlungen zur Zeit offen, evtl. allgemeine Ausrichtung des Rates? Evtl. Trilogverhandlungen? → Mit Übergangsfrist von voraussichtlich mindestens einem Jahr ist es zur Zeit höchst unwahrscheinlich, dass die Regelungen der ePrivacy Verordnung noch im Jahr 2019 wirksam werden. Der früheste Zeitpunkt des Inkrafttretens könnte nach Abschluss der Trilogverhandlungen wohl im Frühjahr 2019 liegen. Mit der Übergangsfrist würden die Regelungen dann erst 2020 wirksam.

Abbildung 9: Übersicht zur Entstehung und weiterem Zeitplan der ePrivacy Verordnung (Stand September 2018)

8 ↗ http://www.consilium.europa.eu/media/35537/background_telecoms-june-2018-en.pdf, abgerufen am 11.09.2018.

5.2 Wesentliche Änderungen hinsichtlich Cookies/Web-Tracking

5.2.1 Rechtslage nach dem TMG

Im deutschen Recht gibt es zwar keine Regelung, die sich ausdrücklich auf das Setzen von Cookies bezieht, aber § 13 Abs. 1 Telemediengesetz (TMG) regelt bestimmte Informationspflichten der Diensteanbieter diesbezüglich. Das TMG wurde bisher auch noch nicht im Rahmen des 2. Datenschutzanpassungs- und Umsetzungsgesetztes (Datenschutzomnibus) geändert.[9] Darüber, welche Regelungen des TMG auch nach Geltungsbeginn der Datenschutzgrundverordnung am 25. Mai 2018 weitergelten, gibt es verschiedene Auffassungen. Die derzeitige gesetzliche Lage soll in diesem Kapitel dargestellt werden.

§ 13 Abs. 1 Satz 1 TMG regelt bisher:

Der Diensteanbieter hat den Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten sowie über die Verarbeitung seiner Daten in Staaten außerhalb des Anwendungsbereichs der Richtlinie 95/46/EG in allgemein verständlicher Form zu unterrichten, sofern eine solche Unterrichtung nicht bereits erfolgt ist.

Diensteanbieter sind daher verpflichtet, den Nutzer über die Verfahren zu informieren, mit denen personenbezogenen Daten erhoben und verwendet werden.

§ 13 Abs. 1 Satz 2 TMG regelt weiter:

Bei einem automatisierten Verfahren, das eine spätere Identifizierung des Nutzers ermöglicht und eine Erhebung oder Verwendung personenbezogener Daten vorbereitet, ist der Nutzer zu Beginn dieses Verfahrens zu unterrichten. Der Inhalt der Unterrichtung muss für den Nutzer jederzeit abrufbar sein.

Da Cookies ein solches automatisiertes Verfahren sind, besteht die Verpflichtung zur Vorab-Information. Neben dieser Regelung greifen aber auch die Vorschriften der §§ 12 Abs. 1 und 15 Abs. 1 Satz 1 TMG.

9 Das als Datenschutzomnibus bekannte Artikelgesetz, das mehr als 150 Fachgesetze enthält, wurde vom BMI koordiniert. Der entsprechende Gesetzesentwurf des BMI passierte am 05.09.2018 das Bundeskabinett und soll nach derzeitigem Zeitplan bis Ende des Jahres Bundestag und Bundesrat durchlaufen; der Gesetzesentwurf ist abrufbar unter ↗ https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2018/dsanpug.pdf?__blob=publicationFile&v=2, abgerufen am 11.09.2018.

Nach § 12 Abs.1 TMG gilt:

Der Diensteanbieter darf personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat.

Die Datenverarbeitung ist also nur dann erlaubt, wenn sie gesetzlich erlaubt ist oder eine Einwilligung des Nutzers vorliegt. Eine bedarfsgerechte und ausbalancierte Ausnahme hierzu findet sich aber in § 15 Abs. 3 Satz 1 TMG, wonach der Diensteanbieter

für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen darf, sofern der Nutzer dem nicht widerspricht.

Für weitere Details zu Pseudonymisierung, Anonymisierung und Verschlüsselung wird auf Kapitel 5.2.2 verwiesen.

Hier regelt das Gesetz also eindeutig eine Opt-Out Lösung, die aber zum Schutz der Nutzer und deren personenbezogene Daten auf wenige, sehr konkrete und aber für das Funktionieren von Webseiten und zur Monetarisierung von Online-Content notwendige Ausnahmen beschränkt ist.

Zusätzlich formuliert § 13 Abs 3. TMG:

Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

Ob die Regelungen des TMG seit dem 25.05.2018 von der DS-GVO vollständig verdrängt wurden, steht derzeit noch nicht abschließend fest. Die Datenschutzkonferenz (DSK) hat sich jedoch am 26.04.2018 in einem Positionspapier zum Verhältnis der DS-GVO und dem TMG geäußert. Die Bewertung der Rechtslage im Verhältnis der DS-GVO und dem TMG ist jedoch weder zutreffend noch hilfreich.[10] Weder ist nachvollziehbar, weshalb die Anwendung noch geltender TMG-Vorschriften völlig ausgeschlossen sein soll, noch erscheint die Fokussierung auf die Einwilligung für jegliche Art von Webtracking und Erstellung von Nutzerprofilen rechtlich und tatsächlich geboten. Es drängt sich der Eindruck auf, dass durch die Position ein von der DSK politisch gewünschtes Ergebnis der noch diskutierten ePrivacy Verordnung vorweggenommen werden soll.

10 Bitkom hatte sich seinerzeit zum Positionspapier auch positioniert: ↗ https://www.bitkom.org/Presse/Presseinformation/Bitkom-kritisiert-Position-der-Datenschutzkonferenz-zu-Webtracking.html und ↗ https://www.bitkom.org/noindex/Publikationen/2018/Positionspapiere/180511-Positionsbestimmung-der-Datenschutzkonferenz-vom-26-April-2018/Bitkom-Stellungnahme-Position-DSK-DSGVO-TMG.pdf, abgerufen am 11.09.2018.

5.2.2 Pseudonymisierung, Anonymisierung und Verschlüsselung: Ein Überblick

An dieser Stelle soll ein kurzer Überblick über die Begrifflichkeiten Pseudonymisierung, Anonymisierung und Verschlüsselung gegeben werden. Die Trennung der einzelnen Verfahren ist insbesondere im Hinblick auf die rechtliche Einordnung und die daraus resultierende Anwendbarkeit des Datenschutzrechts in Bezug auf die verschiedenen Verfahren von Bedeutung.

Pseudonymisierung

Die Datenschutzgrundverordnung definiert den Begriff Pseudonymisierung in Art. 4 Nr. 5. Darin heißt es:

Pseudonymisierung (ist) die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Auch Erwägungsgrund 26 der DS-GVO äußert sich zur Pseudonymisierung und gibt Aufschluss darüber, ob und wann auch pseudonymisierte Daten noch den für die Anwendbarkeit des Datenschutzrechts wichtigen Personenbezug aufweisen. Dort heißt es: *Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden. Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.*

Dass die Pseudonymisierung aber auch für die Erreichung von Datenschutz eingesetzt werden kann, stellt Art. 32 Abs. 1 lit. 1 DS-GVO klar, der in Bezug auf die Sicherheit der Verarbeitung die Pseudonymisierung als eine der technischen und organisatorischen Maßnahmen nennt.

11 Die Übersicht ist dem Bitkom Faktenpapier zu Blockchain & DS-GVO entnommen: ↗ https://www.bitkom.org/noindex/Publikationen/2018/Leitfaeden/Blockchain-und-Datenschutz/180502-Faktenpapier-Blockchain-und-Datenschutz.pdf, zugegriffen am 06.09.2018.

Und auch Art. 20 DS-GVO erwähnt die Pseudonymisierung explizit bei Datenschutz durch Technikgestaltung und datenschutzfreundlichen Voreinstellungen. Für die Frage, ob pseudonymisierte Daten personenbezogen sind gilt also im Ergebnis: Pseudonymisierte Daten sind noch immer personenbezogen (wenn sie es vor der Pseudonymisierung auch waren). Datenschutz muss daher beachtet werden.

Anonymisierung

Anonymisierte Daten sind solche Daten, die sich gerade nicht/nicht mehr auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Das zeigt sich ebenfalls an Erwägungsgrund 26:

Die Grundsätze des Datenschutzes sollten daher nicht für anonyme Informationen gelten, d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht mehr identifiziert werden kann.

Durch die Inbezugnahme des Satzes *»Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind«* wird auch hier deutlich, dass die Anonymisierung das Verändern der Daten dergestalt ist, dass sie nicht mehr oder nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (derart auch der frühere § 3 Abs. 6 BDSG: *Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.).*

Liegt also ein anonymisiertes Datum vor, gelten die Datenschutzgrundsätze nicht.

Verschlüsselung

Der Begriff Verschlüsselung wird in der DS-GVO nicht definiert, sondern lediglich an verschiedenen Stellen neben der Pseudonymisierung u. a. als eine technische und organisatorische Maßnahme genannt. Nach Simitis/Ernestus ist Verschlüsselung (Kryptographie) ein Querschnittsthema der Datensicherheit und dient dem Schutz der Informationen und der Organisation vor dem Zugriff unberechtigter Dritter. Kryptografie beschreibt die Technik, lesbare Informationen zu modifizieren, sodass diese nur mittels eines dazu geschaffenen Schlüssels wieder lesbar werden. Technisch beschreibt die Verschlüsselung/Kryptografie die Umwandlung von Informationen

mithilfe eines Verschlüsselungsverfahrens in eine nicht mehr zu interpretierende Zahlen- oder Zeichenfolge.[12] Dabei werden ein oder mehrere Schlüssel eingesetzt.

Wichtig: Entgegen verbreiteter Ansichten ändert die Verschlüsselung der Daten grds. nichts an deren Personenbezug. Solange derjenige, der die Daten verschlüsselt über den entsprechenden Schlüssel und damit die Mittel zu Re-Identifizierung des Nutzers verfügt, sind die verschlüsselten Daten personenbeziehbar und fallen daher unter den Begriff der personenbezogenen Daten.

5.2.3 Anwendbarkeit TMG

Der Gesetzgeber hat das deutsche TMG mit Blick auf die im Abstimmungsprozess befindliche ePrivacy Verordnung bewusst noch nicht angepasst. Auch im 2. Datenschutzanpassungs- und Umsetzungsgesetz (2. DSAnpUG), das am 05.09.2018 bereits das Kabinett passierte und mit dem zahlreiche Fachgesetze an die DS-GVO angepasst werden sollen, ist das TMG nicht enthalten (s. o.).

Die DS-GVO stellt in Art. 95 klar, dass sie natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste keine zusätzlichen Pflichten auferlegt, soweit sie den besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen.

In Absatz Nr. 3 ihres Positionspapiers geht die DSK zwar offenbar davon aus, dass es Teilvorschriften im TMG gibt, die in den Anwendungsbereich der Richtlinie 2002/58/EG fallen und damit deren Vorgaben umsetzen. Da ein Teil der Vorschriften nur dem Anwendungsbereich der Datenschutz-Richtlinie 95/46/EG und damit nun dem Anwendungsbereich der DS-GVO unterfallen, erklärt sie jedoch pauschal alle Vorschriften für unanwendbar. Offenbar hält sie eine Umsetzung der Richtlinie durch diese für nicht gegeben. Nach Meinung der Bundesregierung, die auch von der Kommission schriftlich bestätigt wurde,[13] ist dies jedoch nicht richtig. Die Vorschriften des 4. Abschnitts des TMG dienen eben auch der Umsetzung der ePrivacy-Richtlinie. Insbesondere § 15 Abs. 3 TMG, welcher Cookies betrifft, wurde von der Bundesregierung immer als ausreichende Umsetzung der Richtlinie 2002/58/EG angesehen. Unabhängig davon, dass diese Rechtsmeinung umstritten ist, kann dieser Wille des Gesetzgebers nicht einfach ignoriert werden.

12 Vergleiche Walter Ernestus, in: Simitis, Bundesdatenschutzgesetz, BDSG § 9 Technische und organisatorische Maßnahmen, 8. Auflage 2014, Rn. 166.

13 ↗ https://www.telemedicus.info/article/2716-EU-Kommission-Cookie-Richtlinie-ist-in-Deutschland-umgesetzt.html, abgerufen am 12.09.2018.

5.2.4 Pauschaler Ausschluss der Interessenabwägung im Einzelfall

In Abschnitt Nr. 9 des DSK Papiers wird postuliert, dass »jedenfalls beim Einsatz von Tracking-Mechanismen, die das Verhalten von betroffenen Personen im Internet nachvollziehbar machen und bei der Erstellung von Nutzerprofilen« die vorherige informierte Einwilligung des Nutzers per Erklärung oder sonstige eindeutige bestätigende Handlung eingeholt werden muss. Diese generelle Aussage ist weder vom TMG noch von der DS-GVO gedeckt. Die DSK unterscheidet in Ziff. 9 ihres Positionspapiers nicht danach, ob ein Cookie einmalig oder dauerhaft (»persistent«) verwendet wird, sondern behandelt sämtliche dort benannte Tracking-Mechanismen und Nutzerprofile unterschiedslos, was der Interessenlage nicht gerecht wird und unserer Ansicht nach im Rahmen einer Interessenabwägung zu berücksichtigen wäre. Sie setzt sich damit in Widerspruch zu den Aussagen der Art. 29-Gruppe in ihrem WP 194, Abschnitt 2.3.

Auch der EuGH hat in seinem Urteil Breyer (Urteil des EuGH in der Rechtssache C-582/14 Breyer vs. Bundesrepublik Deutschland, Rn. 62) dazu entschieden, dass eine mitgliedstaatliche Norm, die kategorisch und ganz allgemein die Verarbeitung von Nutzungsdaten ausschließt bzw. einem Einwilligungsvorbehalt unterstellt, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen, europarechtswidrig ist. Dies gilt auch für eine entsprechende aufsichtsbehördliche Auslegung. Die DSK unterscheidet in Ziff. 9 ihres Positionspapiers ferner nicht danach, ob es sich um Nutzungsprofile unter Verwendung von Pseudonymen handelt und missachtet damit die gesetzgeberische Wertung in § 15 Abs. 3 TMG welche weiterhin gültig ist.

Im Rahmen einer differenzierteren Positionsbestimmung sollte außerdem eine Unterscheidung beim Einsatz von sogenannten First Party Cookies und Third Party Cookies erfolgen. Hierbei sollte sich an den in der Industrie etablierten Konzepten und Begrifflichkeiten orientiert werden. Dies insbesondere, soweit eine etwaige Zulässigkeit pauschal anhand der Einordnung als First oder Third Party Cookie erfolgen sollte.

Vertiefung: Technischer Hintergrund

Technischer Hintergrund

First Party Cookies sind stets mit der gleichen Domain verknüpft, auf der z. B. ein Tag (also z. B. Programmcode zum Durchführen von Websitetracking) aufgerufen und ausgeführt wird. D. h. die Website B kann Informationen, die in einem First Party Cookie der Website A gespeichert wurden, nicht nutzen. Third Party Cookies kommen regelmäßig beim webseiten-übergreifenden Einsatz von Online-Werbemaßnahmen zum Einsatz.

First Party Cookies werden allerdings nicht nur vom Webseitenbetreiber gesetzt, sondern sie können z. B. auch von einem vom Webseitenanbieter auf seiner Webseite integrierten Dritten (z. B. einem Web-Tracking Anbieter) gesetzt und genutzt werden. Der Einsatz von solchen Anbietern erfolgt in der Regel weisungsgebunden im Rahmen eines Auftragsverarbeitungs-verhältnisses. Ein von einem Webseiten-Tracking Anbieter im Auftrag des Webseitenanbieters ausgelesener First-Party Cookie wird durch den beauftragten Zugriff des Auftragnehmers nicht zum Third-Party Cookie.

Schwächen / Risiken der Abgrenzung nach First und Third Party Cookie

Bei der Verwendung dieser Begrifflichkeiten ist also darauf zu achten, dass sich dadurch nicht die dahinterstehenden Verantwortlichkeiten ableiten lassen. Ein originär Verantwortlicher (Betreiber eines Dienstes) kann sich ggf. aus technisch-organisatorischen Gründen dazu entscheiden, einen eigenen Cookie in der technischen Ausgestaltung eines Third Party Cookies auszuliefern. Zugleich kann der Cookie eines nicht-originär Verantwortlichen, also eines beauf-tragten Drittanbieters, als First Party Cookie ausgeliefert werden. Hierzu bedarf es zwar grundsätzlich der Kooperation des originär Verantwortlichen, doch würde dies an der letzt-lichen Legitimation der (Auftrags-)Verarbeitung durch den nicht-originär Verantwortlichen nichts ändern.

Ebenfalls ist durch die technische Ausgestaltung nicht ersichtlich, ob und inwieweit der originär-Verantwortliche und der nicht-originär Verantwortliche weitergehende Maßnahmen, z. B. eine Auftragsvereinbarung, geschlossen haben oder nicht.

5.3 Neuregelung durch die ePrivacy Verordnung

Die ePrivacy Verordnung trifft vor allem im Bereich des Webseiten-Trackings einige neue Regelungen. Sie geht dabei zum einen über die Anforderungen der DS-GVO und zum anderen auch über die bisherigen Regelungen der ePrivacy Richtlinie (2009) hinaus.

Folgende Bereiche sind hier von besonderer Relevanz:

1. Der Einsatz von Cookies darf ohne ausdrückliche Einwilligung nur noch erfolgen, wenn sie »unbedingt nötig« oder »zwingend technisch notwendig« sind um einen Dienst zu erbringen (siehe Art. 8 Abs.1 a, 2 der Fassung des Parlaments).

2. Der Einsatz von sogenannten Zugangssperrren wie »Cookie-Walls« wird in der ePrivacy Verordnung abgelehnt. Die Einwilligung darf nicht zur Bedingung für den Service (Webseitenangebot) gemacht werden. Es sollen von Anbietern stets alternative Möglichkeiten der Nutzung angeboten werden, die nicht abhängig gemacht werden von Datennutzung und entsprechender Freigabe der Nutzer (Art. 8).

3. Regelung zur Browserschranke in Artikel 10, die bisher vorsieht, dass der Nutzer bei der Erstinstallation Voreinstellungen zum Tracking treffen muss.

4. Zeitliche Befristung der Einwilligung wird diskutiert. Außerdem muss die Einwilligung jederzeit widerrufen werden können.

5. Reichweitenmessung im Web steht auf der Kippe.

Auf diese Folgen soll in den nachfolgenden Abschnitten eingegangen werden.

5.4 Abweichung der ePrivacy Verordnung von der DS-GVO

Anders als bisher soll es künftig für alle Nutzungen der Verarbeitungs- und Speicherfunktionen im Endgerät einer ausdrücklichen Einwilligung bedürfen, wenn personenbezogene Daten verarbeitet werden sollen. Das würde weite Teile des Webseiten-Trackings betreffen. Die Privilegierung für pseudonymes Tracking ist in dem Verordnungsentwurf nicht mehr vorgesehen. Anders als die DS-GVO erlaubt die ePrivacy Verordnung auch keine Datenverarbeitung auf der Grundlage berechtigter Interessen. Die Erlaubnistatbestände sind also deutlich restriktiver und schränken auch die unter der DS-GVO erlaubten Verarbeitungstätigkeiten stark ein.

Die ePrivacy Verordnung erlaubt bis auf wenige, eingeschränkte Ausnahmen also im Grundsatz nur noch solche Cookies und Endgerät-Speicherungen, die für den Betrieb des angebotenen Dienstes unbedingt nötig sind.

Von besonderer Bedeutung für die Diskussion rund um Tracking sind Art. 8 und 10 der ePrivacy Verordnung, die in den folgenden Abschnitten näher untersucht werden.

5.4.1 Artikel 8 der ePrivacy Verordnung

Art. 8 stellt strenge Anforderungen an alle Speicherungen oder Zugriffe von Informationen, die auf den Endgeräten der Nutzer gespeichert sind. Art. 8 besagt im Wesentlichen in der derzeitigen Fassung nach den Änderungsvorschlägen des Parlaments:

Artikel 8

(1) Jede vom jeweiligen Nutzer nicht selbst vorgenommene Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer, auch über deren Software und Hardware, ist untersagt, außer sie erfolgt aus folgenden Gründen:

a) sie ist für den alleinigen Zweck der Durchführung eines elektronischen Kommunikationsvorgangs über ein elektronisches Kommunikationsnetz unbedingt nötig oder

b) der Nutzer hat seine ausdrückliche Einwilligung gegeben oder

c) sie ist für die Bereitstellung eines vom Nutzer ausdrücklich angeforderten Dienstes der Informationsgesellschaft technisch zwingend nötig oder

d) sie ist für die Messung der Reichweite des vom Nutzer angeforderten Dienstes der Informationsgesellschaft technisch nötig, […]

da) sie ist nötig, um Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität der Endeinrichtungen des Endnutzers zu wahren, und zwar durch Aktualisierungen und für den hierfür erforderlichen Zeitraum, […]

db) sie ist im Rahmen von Arbeitsverhältnissen für die Erfüllung einer von einem Arbeitnehmer wahrzunehmenden Aufgabe technisch zwingend nötig, sofern

i) der Arbeitgeber die Endeinrichtung bereitstellt bzw. deren Nutzer ist,

ii) der Arbeitnehmer der Nutzer der Endeinrichtung ist und

iii) sie überdies nicht der Überwachung des Arbeitnehmers dient.

(1a) Unabhängig davon, ob es sich um einen vergüteten Dienst handelt, darf keinem Nutzer der Zugang zu einem Dienst oder einem Funktionselement der Informationsgesellschaft mit der Begründung verweigert werden, er habe seine Einwilligung in die Verarbeitung personenbezogener

Daten bzw. in die zur Bereitstellung dieses Dienstes oder dieses Funktionselements nicht erforderliche Nutzung von Verarbeitungs- oder Speicherkapazitäten seiner Endeinrichtung nach Artikel 8 Absatz 1 Buchstabe b nicht gegeben.

[...][14]

Der Wortlaut des Art. 8 verdeutlicht ein weiteres Problem der ePrivacy Verordnung: Die Regelungen sind nicht aufeinander abgestimmt und das System aus Verbot, Ausnahme und Rückausnahme unübersichtlich und unstimmig. Liest man z. B. Art. 8 Abs. 1 lit. d des Verordnungsentwurfs isoliert, entsteht der Eindruck, die Reichweitenmessung wäre nach wie vor privilegiert, da hierfür keine ausdrückliche Einwilligung eingeholt werden muss:

Jede vom jeweiligen Nutzer nicht selbst vorgenommene Nutzung der Verarbeitungs- und Speicherfunktionen von Endeinrichtungen und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer, auch über deren Software und Hardware, ist untersagt, außer sie ist für die Messung der Reichweite des vom Nutzer angeforderten Dienstes der Informationsgesellschaft technisch nötig, sofern diese Messung vom Betreiber oder in seinem Namen oder von einer unabhängigen Webanalyse Agentur durchgeführt wird, die im öffentlichen Interesse – auch für wissenschaftliche Zwecke – tätig ist, sofern die Daten aggregiert sind und der Nutzer die Möglichkeit hat, der Nutzung zu widersprechen, und sofern personenbezogene Daten keinem Dritten zugänglich gemacht und die Grundrechte des Nutzers durch diese Messung nicht beeinträchtigt werden, und falls eine Publikumsmessung im Namen eines Betreibers von Diensten der Informationsgesellschaft durchgeführt wird, dürfen die erhobenen Daten nur von diesem Betreiber verarbeitet werden und müssen getrennt von den Daten aufbewahrt werden, die bei Publikumsmessungen erhoben wurden, die im Namen anderer Betreiber durchgeführt werden [...]

Fraglich bleibt aber dabei, ob Dienstleister wie die AGOF oder die IVW weiterhin Reichweite messen dürfen, da Art. 8 Abs. 1 lit. d den Anwendungsbereich auf solche Betreiber oder Agenturen beschränkt, die im öffentlichen Interesse – auch für wissenschaftliche Zwecke – tätig ist. Hier trifft der Verordnungsentwurf keine klare Regelung, sodass eine Rechtsunsicherheit verbleibt. Marktforschung wie bisher stünde damit nicht mehr auf einer festen Grundlage, Anbieter und Agenturen müssten im Zweifelsfall auf Auslegungshilfen der Aufsichtsbehörden warten oder in Rechtsstreitigkeiten eine Entscheidung für den jeweiligen Einzelfall abwarten.

Hinsichtlich des Art. 8 wird zurzeit (Stand September 2018) im Rat der Europäischen Union diskutiert, dass es für Contentanbieter, deren Geschäftsmodell kostenfrei ist und über Marketingmaßnahmen monetarisiert wird, zulässig sein sollte, die Nutzung des Dienstes an die Einwilligung des Nutzers zu knüpfen, mit der er der Datennutzung im Rahmen von Analyse- und Trackingtools zustimmt. Dies könnte eine Lösung für kostenfreie Geschäftsmodelle darstellen,

14 Der vollständige Gesetzestext ist zu finden unter: ↗ http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0324+0+DOC+XML+V0//DE#title1, abgerufen am 11.09.2018.

die andernfalls unter den strengen Regeln der ePrivacy Verordnung mangels Monetarisierungsmöglichkeit wohl nicht weiter bestehen könnten. Die Verhandlungen zu diesem Aspekt sind aber noch nicht abgeschlossen.

5.4.2 Artikel 10 der ePrivacy Verordnung

Ein weiteres Problem zeigt sich, wenn Art. 10 des Verordnungsentwurfs betrachtet wird. Die Legalausnahme (wie rechtsunklar sie auch sein mag), wird durch den Art. 10 nämlich vollständig konterkariert. In Art. 10 sieht der Verordnungsentwurf vor (Kommissions-Entwurf mit Änderungen durch das EU-Parlament):

Artikel 10

Bereitzustellende Informationen und Einstellungsmöglichkeiten zur Privatsphäre

(1) In Verkehr gebrachte Software, die elektronische Kommunikation ermöglicht, darunter auch das Abrufen und Darstellen von Informationen aus dem Internet, muss

a) in der Voreinstellung aktivierte Einstellungen zum Schutz der Privatsphäre aufweisen, durch die verhindert wird, dass andere Parteien außer zu den in Artikel 8 Absatz 1 Buchstaben a und c genannten Zwecken Informationen an die Endeinrichtung eines Nutzers übermitteln, dort speichern oder bereits dort gespeicherte oder von dort erhobene Informationen verarbeiten,

b) nach der Installation den Nutzer informieren und ihm die Möglichkeit bieten, die nach Buchstabe a festgelegten Einstellungen zum Schutz der Privatsphäre zu ändern oder zu bestätigen, indem er aufgefordert wird, in eine Einstellung einzuwilligen, und indem ihm die Möglichkeit geboten wird, zu verhindern, dass andere Parteien zu de in Artikel 8 Absatz 1 Buchstaben a,c, d und da genannten Zwecken Informationen verarbeiten, die an die Endeinrichtung übermitteln werden, bereits dort gespeichert sind oder von dort erhoben werden,

c) dem Nutzer die Möglichkeit bieten, nach der Installation der Software mittels Einstellungen eine ausdrückliche Einwilligung zu geben.

(1-1) Vor der ersten Verwendung der Verwendung der Software muss der Nutzer von der Software über die Privatsphäreeinstellungen und die je nach dem aufgerufenen Dienste der Informationsgesellschaft verfügbaren detaillierten Einstellungsoptionen informiert werden. Bei der Verwendung der Software müssen die Einstellungen leicht zugänglich und so gestaltet sein, dass die Nutzer in der Lage sind, eine fundierte Entscheidung zu treffen.

[...][15]

15 Der vollständige Test des Artikels 10 in der Fassung des Europäischen Parlaments ist hier zu finden: ↗ http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0324+0+DOC+XML+V0//DE#title1, abgerufen am 11.09.2018.

Art. 10 sieht also vor, dass die Browserhersteller bei der Installation eine Default-Einstellung vorsehen, die es untersagt, dass Dritte Informationen in der Endeinrichtung eines Endnutzers speichern oder bereits in der Endeinrichtung gespeicherte Informationen verarbeiten. Das blockt aus technischer Sicht viele First und Third Party Trackingmechanismen und würde damit auch die Tätigkeit zur Reichweitenmessung betreffen. Cookies wären, unabhängig davon, ob sie für den Seitenaufbau, die Seitenfunktionen erforderlich sind, ebenfalls blockiert. Die meisten der gängigen Tracking-Mechanismen würde damit nicht mehr funktionieren, die Webseitenfunktionen zum großen Teil dadurch gestört werden.

Der Browser kann zudem nicht evaluieren, ob z. B. ein Cookie notwendig ist, um die Funktionsweisen einer Webseite aufrecht zu erhalten, oder ob es sich um ein zusätzliches Cookie handelt (z. B. eines das für Marketingzwecke eingesetzt wird). Lehnt der Nutzer die Cookies im Browser grundsätzlich ab, kann es zum fehlerhaften Verhalten der Webseite führen – vgl. Abbildung 10.

Da verschiedene Webseiten auf die Browsereinstellungen unterschiedlich reagieren können und die Fehlermeldung, falls sie angezeigt wird, nicht immer selbsterklärend ist, führt es zur Irritation des Nutzers. Er weiß am Ende des Tages nicht, wie er die jeweilige Webseite und seinen Browser konfigurieren muss, um den gewünschten Grad des Datenschutzes zu erreichen. Vielmehr ist er nicht in der Lage für unterschiedliche Webseiten dedizierte Datenschutzprofile zu pflegen. Seine negative Erfahrung mit den Online-Angeboten kann unter anderem negativen Einfluss auf das Online-Geschäftsmodell im europäischen Wirtschaftsraum haben.

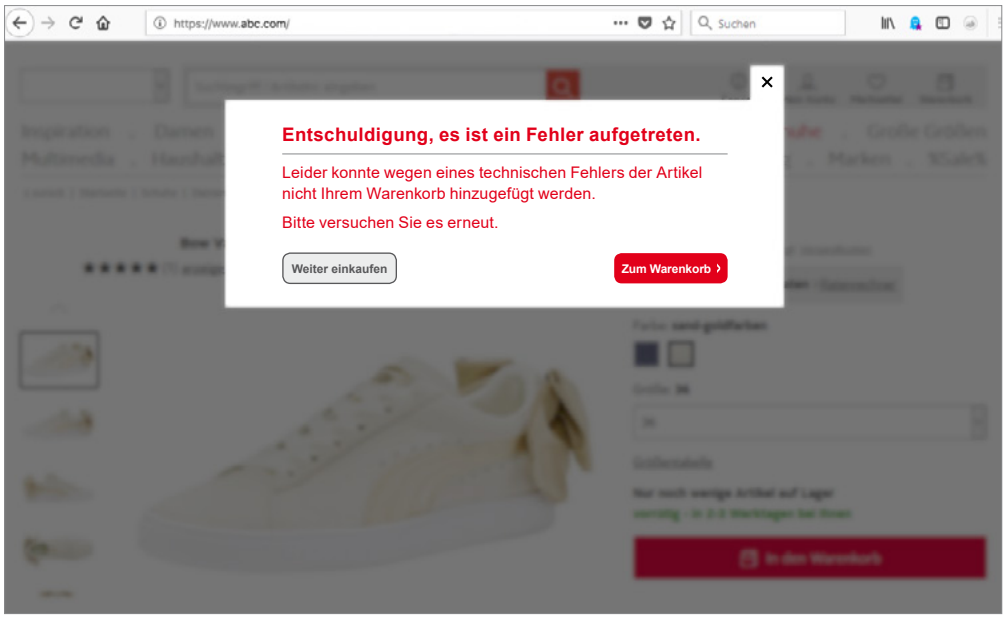

Abbildung 10: Beispielhafte Fehlermeldung aufgrund abgelehnter funktionaler Cookies

Die Auswirkungen der Einschränkung der Cookie-Nutzung ist in Kapitel 6 beschrieben. Für eine technische Beschreibung der einzelnen Cookie-Arten siehe Kapitel 3.3.1.

Hinzu kommt, dass die Vorschrift des Art. 10 dennoch ihr Ziel verfehlt, da ein vollumfänglicher Schutz vor Tracking mit der Regelung gar nicht erreicht wird. So würden z. B. Fingerprinting-Verfahren weiterhin zum Tracken des Nutzers eingesetzt werden können, da die Browserschranke diese Verfahren nicht blockieren würde.

Daran ändert wohl auch die Regelung des Art. 10 Abs. 1 lit. b nichts, der die Möglichkeit der Festlegung von Einstellungen durch den Nutzer vorsieht, da eine informierte Entscheidung der Nutzer hier nicht erwartet werden kann und der ganz überwiegende Teil der Nutzer an der negativen Voreinstellung keine Änderung vornehmen wird. Eine Einräumung einer Einwilligung auf dieser Ebene ist daher nicht zu erweitern, sodass auch die Reichweitenmessung weiterhin ausgeschlossen bliebe.

Ausnahmeregelungen hier technisch zu implementieren ist nicht oder nur unter derart hohem Aufwand für die Browserhersteller möglich, dass mit einer Lösung auf technischer Ebene nicht zu rechnen ist. Durch die Regelung wird der Browser zudem datenschutzrechtlich in die Stellung des Verantwortlichen gebracht, die er aber in Bezug auf Trackingmaßnahmen, die auf der Ebene der Contentanbieter (Seitenbetreiber) gesetzt werden, gar nicht hat. Dies macht auch ein Blick in Art. 25 Abs. 1 und 2 der DS-GVO deutlich, der bei den Privacy by Design Grundsätzen stets den Verantwortlichen adressiert. Art. 4 Nr. 7 DS-GVO definiert dabei den Verantwortlichen wie folgt:

»Verantwortlicher [ist] die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.«

Da der Browser weder über die Zwecke noch die Mittel der Verarbeitung auf der Ebene der Webseiten entscheidet, sondern nur den Zugang zu diesen ermöglicht, kann er nicht als Verantwortlicher betrachtet werden und ist daher auch kein tauglicher Adressat für Privacy by Design Vorschriften, die die Webseitenbetreiber betreffen.

Browserhersteller dürfen daher auch nicht dafür verantwortlich gemacht werden, welche Datenverarbeitungen auf den Webseiten, die über ihren Browser erreichbar sind, ermöglicht oder nicht ermöglicht werden. Diese Systemwidrigkeit ist dringend aufzulösen.

An der Regelung des Art. 10 wird zudem ein weiteres Problem des Verordnungsentwurfs deutlich: die Einwilligungseinholung über die jeweilige Webseite liefe ebenfalls ins Leere, wenn die Voreinstellungen im Browser das Setzen des Cookies o. ä. technisch verhindern.

Anpassungen der Art. 8 und 10 sind daher dringend geboten um zum einen die Systematik des Datenschutzes aufrecht zu erhalten und zum anderen legitime Geschäftsmodelle nicht ohne Not und über Gebühr zu strapazieren oder sogar zu verhindern. Die Zielerreichung der Vorschriften muss ebenfalls noch einmal gründlich untersucht werden. Es besteht ansonsten die Gefahr, dass die Regelungen massive Auswirkungen auf Darstellbarkeit und Monetarisierbarkeit von Webseiten haben, ohne dass letztlich das gewollte Ziel erreicht wird: Stärkung der Nutzersouveränität und des Datenschutzes bei gleichzeitiger Aufrechterhaltung der Web-Landschaft und Vielfalt. Hierfür bedürfte es abgestimmter und ausbalancierter Regelungen. Und für Nutzersouveränität wird es am Ende mehr brauchen als ein ständiges Einwilligen auf Webseiten.

6 Praktische Auswirkungen auf die Nutzererfahrung und auf Geschäftsprozesse und mögliche Wettbewerbseinschränkungen

Mit der DS-GVO wurden bereits EU-weit einheitliche strenge datenschutzrechtliche Vorschriften für alle Sektoren festgelegt, die ein flächendeckend hohes Datenschutzniveau garantieren. Der Gesetzentwurf der EU Kommission zur e-Privacy Verordnung und die sogar noch restriktivere Fassung des Europäischen Parlaments wird voraussichtlich die im langjährigen und mühsamen Prozess gefundene Balance zwischen dem Schutz der Privatsphäre und neuen Technologien wieder zerschlagen, indem in weiten Bereichen Datenverarbeitungen, die unter der DS-GVO zulässig wären, entweder unter den Vorbehalt einer strengeren Form der Einwilligung gestellt oder gänzlich untersagt werden. Die Wettbewerbsfähigkeit der Wirtschaft in Europa wird damit über viele Wirtschaftszweige hinweg bedroht.[16]

Vor allem die Anforderungen des Art. 8 verbieten viele Verarbeitungen zu pauschal und undifferenziert. Art. 8 Abs. 1 verbietet jede vom Endnutzer nicht selbst vorgenommene Nutzung der Verarbeitungs- und Speicherfunktion und jede Erhebung von Informationen aus Endeinrichtungen der Endnutzer. Ausnahmen sind nur in sehr engen Fällen vorgesehen. Nicht jede Nutzung von Verarbeitungs- und Speicherfunktion ist aber grundsätzlich schlecht oder ein einschneidender Eingriff in die Privatsphäre des Nutzers. Das gesamte System der ePrivacy Verordnung ist aber darauf ausgerichtet, die Verarbeitungen im Endgerät als ein Ausspähen des Nutzers zu klassifizieren. Das zeigt sich zum Beispiel auch im Erwägungsgrund 20, in dem keine Unterscheidung zwischen nützlichen bzw. notwendigen Cookies und z. B. Marketing- Cookies gemacht werden. Vielmehr werden dort »Spyware und Webbugs« neben anderen Cookie-Technologien als »Verfolgungstechniken« deklariert.

Die oben dargestellten Restriktionen der ePrivacy Verordnung werden auch auf verschiedensten Ebenen der Webseitenfunktionen Auswirkungen haben. Dies lässt sich gut erkennen, wenn man die verschiedenen Cookie-Arten nebeneinander betrachtet. Wie bereits in Kapitel 3.3.1 dargestellt, lässt sich zwischen erforderlichen, funktionalen, statistischen und Marketing-Cookies unterscheiden. Weder die derzeitige aufsichtsbehördliche Auffassung zur DS-GVO und dem TMG, noch die ePrivacy Verordnung beachten die entsprechenden technischen Besonderheiten

16 Siehe auch die Studie des wik, die davon ausgeht, dass in Deutschland von einer Reduktion des gesamten digitalen Werbebudgets von etwa einem Drittel auszugehen ist und mittel- bis langfristig sogar zu erwarten ist, dass die Werbebudgets in geschlossene Systeme wandern und alternativ Bezahlschrankensysteme etabliert werden. Die Studie ist abrufbar unter: ↗ https://www.wik.org/index.php?id=938&L=0&id=938, aufgerufen am 11.09.2018.

und Differenzierungen. Für ein funktionierendes Web-Ökosystem ist es aber von größter Relevanz, dass Funktionalitäten und technische Gegebenheiten korrekt in Regulierungsvorhaben und Auslegungen der Behörden berücksichtigt werden. Anderenfalls werden die Auswirkungen gravierende Folgen haben:

Bei einer Unterdrückung von erforderlichen Cookies können bestimmte Webseitenfunktionen nicht mehr ordnungsgemäß ausgeführt werden. Es sind entsprechend Einbußen bei der Nutzererfahrung zu befürchten – vgl. Abbildung 9. Auch ein Fehlen bzw. Blockieren funktionaler Cookies wirkt sich aus, da diese zwar nicht zwangsläufig für den Betrieb und die Nutzung einer Webseite erforderlich sind, jedoch eine gute Nutzererfahrung ermöglichen und demnach als Bestandteil moderner Webauftritte empfehlenswert sind. Zahlreiche Anwendungen im Bereich DAO basieren zudem auf der Arbeit von statistischen Cookies und sind daher für die beständige Optimierung von Webauftritten erforderlich. Marketing Cookies, die sicher im Fokus der ePrivacy Verordnung standen, sind ebenfalls zwar für die Funktion einer Webseite nicht zwingend erforderlich, aber ein essentieller Bestandteil der Technologien im Online-Advertising. Ohne entsprechende Cookies gehen dieser Branche Informationen über den Nutzer verloren. Eine gezielte Werbeansprache wird somit schwierig bis unmöglich, eine kompetitive Monetarisierung kostenfreier Webangebote steht damit ebenfalls vor dem Aus. Mit entsprechenden Mitteln wie einer Pseudonymisierung und einer ausbalanciertes, datenschutzwahrenden gesetzlichen Regelung könnte aber auch hier das Datenschutzniveau hochgehalten werden. Dies erfordert aber Anpassungen des derzeit diskutierten Verordnungstextes.

Die technische Nutzung der Verarbeitung und Speicherfunktion sowie die Erhebung von Informationen aus Endeinrichtungen können sich zudem in vielen Fällen auch positiv auf den Endnutzer auswirken: Cookies werden beispielsweise als technisches Mittel eingesetzt, um Werbung effizienter einzusetzen. Durch den sogenannten Frequency Cap (dt. Deckelung der Frequenz) wird beispielsweise die Häufigkeit einer Werbeeinblendung für einen Nutzer reguliert (z. B. maximal 10-mal angezeigt, dann wird einanderes Werbemittel benutzt). Auch muss derjenige, der die Werbung selbst schaltet zu Abrechnungszwecken mit dem Vermarkter wissen, wie viele Besucher die Werbung gesehen haben. Eine angemessene Abwägung, um die gegenseitigen Interessen zu wahren, könnte auch dabei stattfinden. Die Datenschutzgrundverordnung sieht zum Beispiel solche Abwägungen vor.

Wichtig für die Nutzererfahrung und das Funktionieren des Webs ist vor allem auch, dass ein alleiniges Abstellen auf die Einwilligung als Grundlage der Datenverarbeitung nicht praktikabel ist. Wird nur noch auf die Einwilligung abgestellt, wird zugleich auch die Nutzung von pseudonymisierten Daten weder berücksichtig, noch privilegiert (wie dies momentan unter § 15 Abs. 3 TMG der Fall ist). Auch Tatbestände aus der DS-GVO, wie das berechtigte Interesse, sollen keine Anwendung finden. Gerade in der digitalen Welt, in der laufend neue Anwendungen und Geschäftsmodelle entstehen, sind flexiblere Regelungen dringend erforderlich.

Darüber hinaus ist auch die Nutzersicht zwingend zu berücksichtigen. Denn unklare und zu komplexe Datenschutzanforderungen an den Webseitenbetreiber führen zu entsprechenden undurchsichtigen Implementierungen auf der Webseite. Der Normalverbraucher ist zudem nicht in der Lage, zwischen den Einstellungen auf einer Webseite und denen direkt im Browser zu unterscheiden. Wie sich diese Einstellungen gegenseitig beeinflussen und ob er tatsächlich den gewünschten Datenschutz hat, weiß er dann nicht mehr. Diese negative Nutzererfahrung vor dem Hintergrund der momentan vorherrschenden hohen Standards der Benutzerfreundlichkeit ist eine weitere mögliche Ursache der negativen Entwicklungen im europäischen Wirtschaftsraum. Das komplette Gegenteil der angedachten Datenschutzmaßnahmen könnte eintreten, wenn der verzweifelte Nutzer alle Datenschutzmechanismen abschaltet und ignoriert, um die Online-Dienste wie gewohnt nutzen zu können.

Auswirkungen wird auch haben, dass bisher gängige und etablierte Verfahren nicht mehr zulässig sein werden. So sollen bisher übliche Verfahren nur dann erlaubt sein, wenn der Anbieter sie selbst durchführt (Art. 8 Abs.2 i. V. m. Art. 10). In den meisten Fällen wird aber bereits die Reichweitenmessung und insbesondere weitergehende Webanalytics von Dritten angeboten.
So ist bspw. das sogenannte Third-Party-Webanalytics das weit überwiegend genutzte Verfahren. Wird in Zukunft die Webanalyse nur noch dann als zulässig erachtet, wenn der Anbieter sie selbst vornimmt, steht also ein gesamtes Geschäftsmodell auf der Kippe. Damit müsste der weit überwiegende Teil der europäischen Wirtschaft seine Verfahren beim Bereitstellen von Webseiten und Internetdiensten umstellen. Während finanzstarke Unternehmen das erforderliche Know-How, die Technik und die personellen Ressourcen hierfür möglicherweise in ihren eigenen Häusern aufbauen können, werden viele kleine und mittelständische Unternehmen nicht in der Lage sein dies zu tun und daher auf die Analyse ihrer Webangebote verzichten müssen und mithin im Wettbewerb abgehängt.

Bitkom vertritt mehr als 2.600 Unternehmen der digitalen Wirtschaft, davon gut 1.800 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 400 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom