White Paper:

Tracking und Consent Layer mit DSGVO und Unwirksamkeit des Privacy Shield

LÖWENSTARK®
ONLINE MARKETING

Hartmut Deiwick, Geschäftsführer der Löwenstark Digital Group und der Löwenstark Online-Marketing GmbH

Seit 2018 baut Deiwick gemeinsam mit dem Inhaber der Löwenstark, Marian Wurm, die Unternehmensgruppe weiter auf. Er ist primär für die Dienstleistungsqualität der mehr als 100 Online-Marketing-Kollegen der Löwenstark zuständig, zunächst als COO dann als Geschäftsführer.

Hartmut Deiwick ist seit mittlerweile 15 Jahren im Digitalgeschäft aktiv. Seine ersten Erfahrungen mit dem E-Commerce machte Deiwick seit 2006 als Controller und kaufmännischer Leiter in der Versandapotheke APONEO. Hier baute er gemeinsam mit dem Inhaber die Versandapotheke auf und bereitete das Unternehmenswachstum inklusive Investorensuche für die weitere Entwicklung vor.

Als Geschäftsführer der PharmaHera Service GmbH, dem ausgegründeten Apothekendienstleister von APONEO, vollzog er mit englischen Investoren die weitere Professionalisierung des Unternehmens.

Das Thema „Aufbau“ verfolgt Deiwick bereits seit 2001. Vor seiner Karriere im Digitalgeschäft war er als Stadtplaner in Berlin aktiv und unter anderem an Einkaufszentren in Berlin planerisch beteiligt. Hier entwickelte er sein Interesse am Thema Handel.

Berlin, 02.08.2020

Inhalt

1. Einleitung

Die digitale Welt ist im stetigen Wandel. Neue Möglichkeiten und Herausforderungen bestimmen seit jeher das Digitalgeschäft und führen zu katalytischen Entwicklungen – sei es wie aktuell aufgrund neuartiger Viren mit ihren Begleiterscheinungen und Konsequenzen oder aufgrund regulatorischer Eingriffe der Judikative der EU und Deutschlands.

Die am 25. Mai 2018 in Kraft getretene EU-Datenschutz-Grundverordnung (DSGVO) ist den meisten mittlerweile ein Begriff, die Auswirkungen werden aber größtenteils noch ignoriert oder die Anforderungen nur teilweise umgesetzt. Etwas mehr Umsetzungsdynamik hat sich mit dem EuGH-Urteil vom 01. Oktober 2019 und dem BGH-Urteil vom 28. Mai 2020 in Sachen „Planet49“ ergeben. Die deutlichste und sichtbarste Auswirkung ist hier die Zunahme von Cookie-Bannern und mehr oder weniger konfigurierbaren Consent Layern.

Kaum haben sich die Werbetreibenden auf diese „neuen“ Umstände eingestellt, erschwert die nächste bahnbrechende Entscheidung des EuGH die erprobten Workflows der Digitalunternehmen. Mit der Entscheidung „Schrems II“ ist das sog. "Privacy Shield-Abkommen" für ungültig erklärt worden und damit die in der Praxis gängige Rechtsgrundlage für die Übermittlung personenbezogener Daten zwischen der EU und den USA von einem auf den anderen Tag weggefallen.

Was haben die DSGVO und Schrems II gemeinsam? Sie ändern unsere Datenlage im Online-Marketing fundamental und damit unsere Praxis der Umsatz- und Kostenoptimierung. Dafür werden andere Skills zur Auswertung relevanter. Wer sich jetzt am besten auf diese neuen Gegebenheiten einstellt, wird einen entscheidenden Wettbewerbsvorteil besitzen.

Dieses White Paper zeigt Ihnen die Konsequenzen bei nicht datenschutzkonformen Handlungen und vor allem die besten Lösungen innerhalb des Performance Marketings zur aktuellen Regulierung auf. Hierzu greifen wir auf öffentliche Diskussionsbeiträge und Best Practices unserer Kunden zurück – natürlich anonymisiert. Das White Paper ist explizit keine Rechtsberatung und kann eine individuelle Rechtsberatung nicht ersetzen. Hierzu sollten Sie einen Fachanwalt konsultieren.

2. Rechtliche Ausgangslage

2.1. DSGVO

Die DSGVO wird in Marketingkreisen meistens negativ bewertet. Tatsächlich handelt es sich aber bei der DSGVO um die größte europäische Initiative zum Datenschutz seit Jahrzehnten. Durch sie werden die europäischen Bürger in die Lage versetzt, den Umgang mit den eigenen personenbezogenen Daten zu steuern und zu kontrollieren. Aus Sicht des Datenschutzes hat Europa eine globale Vorreiterrolle eingenommen.[1]

Nunmehr muss jeder für die Datenverarbeitung Verantwortliche einer Organisation Aufzeichnungen über die Aktivitäten zur Verarbeitung personenbezogener Daten führen und diese kontrollieren. Dazu gehören persönliche Daten, die innerhalb der Organisation, aber auch von

[1] https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/datenpolitik/datenschutz-eu/datenschutz-eu-node.html

Dritten – sogenannten „Datenverarbeitern“, mit denen zwingend ein Auftragsdatenverarbeitungsvertrag (ADV-Vertrag) abzuschließen ist, - verarbeitet werden. [2]

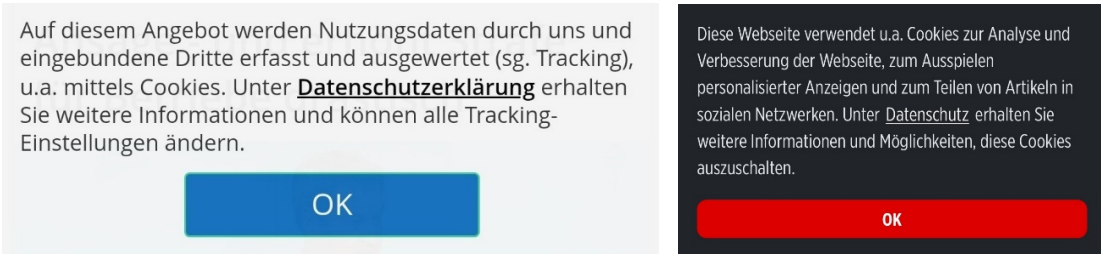
Neben den innerbetrieblichen Prozessveränderungen und Dokumentationen zum Umgang mit personenbezogenen Daten ist für die Digitalunternehmen insbesondere der Umgang mit den Nutzerprofilen von Webseiten-Besuchern von entscheidender Bedeutung. Aufgrund des bereits erwähnten Grundsatzurteils „Planet49“ des EuGH ist für den Einsatz von Cookies zwingend die vorherige ausdrückliche Einwilligung des Nutzers über einen konformen Cookie-Consent-Layer einzuholen.

Es sind aber nicht alle Cookies betroffen. Weiter ohne Einwilligung erlaubt sind so genannte First Party Cookies, die in der Regel vom Websitebetreiber auf dessen Seite der User unterwegs ist, stammen. Das sind z.B.:

- Warenkorb-Cookies
- Cookies für Logins
- Cookies, die eine Länder- oder Sprachauswahl betreffen
- Cookies, die Consent Tools für die Cookie-Einwilligung setzen.

Third Party Cookies hingegen werden von Werbetreibenden genutzt, die über ihre Werbeschaltungen auf anderen Seiten mit den Cookies Nutzerinformationen sammeln. Es handelt sich dabei um Datensätze, die im Browser des Nutzers hinterlegt werden, wenn er eine Seite mit der Werbung besucht. Besucht er erneut eine Seite mit Werbung des gleichen Anbieters, wird er wiedererkannt. Third Party Cookies bedürfen der Zustimmung des Users.

In der allgemeinen Praxis nutzen viele Internetseiten gleichwohl weiterhin Cookiebanner, die beim Weitersurfen eine Zustimmung unterstellen. Diese sind rechtlich unwirksam. Zahlreiche, auch bekannte Internetseiten haben diese Anforderung noch nicht rechtskonform umgesetzt.[3]



Negativ-Beispiele für Cookie-Banner – häufig verwendet von Medienunternehmen

Mit seinem finalen Urteil vom 28. Mai 2020 ist der BGH, der Einschätzung des EuGH vom Vorjahr in Bezug auf den Fall Planet49 gefolgt. Danach ist die aktive und freie Einwilligung des Nutzers unbedingt erforderlich, bevor nicht-notwendige Cookies auf einer Website platziert werden. Vorab angekreuzte Auswahlkästchen werden im BGH-Urteil ebenso als gesetzwidrig eingestuft.[4]

[2] https://www.datenschutz-grundverordnung.eu/grundverordnung/art-28-ds-gvo/
[3] Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, 28. Tätigkeitsbericht, 17.6.2020, S. 32.
[4] https://www.bundesgerichtshof.de/SharedDocs/Pressemitteilungen/DE/2020/2020067.html

ABER: Bei dem Gerichtsurteil ging es nicht um Cookies an sich, sondern um die rechtskonforme Speicherung personenbezogener Daten. Das bedeutet, dass auch andere Trackingverfahren, die personenbezogene Daten speichern, einer aktiven Bestätigung des Users über einen Consent Layer bedürfen.

2.2. Schrems II / Unwirksamkeit des Privacy Shield

Der EuGH fällte am 16. Juli 2020 ein Urteil in dem als Schrems II bekannten Fall (benannt nach dem österreichischen Rechtsanwalt und Datenschutzaktivisten Maximilian Schrems), in dem der Privacy-Shield-Beschluss 2016/1250 für unwirksam erklärt wird. Diese geschah, weil die weitgehenden Eingriffsbefugnisse der US-Geheimdienstbehörden, insbesondere vor dem Hintergrund fehlender Überprüfungs- und Rechtsschutzmöglichkeiten, für EU-Bürger ein dem EU-Datenschutzrecht gleichwertiges Niveau ausschließen. Damit ist ein legaler Datentransfer in die USA gegenwärtig nicht möglich.

Die sogenannten Standardvertragsklauseln, die europäische Unternehmen mit Anbietern in Drittländern abschließen können, um das europäische Datenschutzniveau auch in den Drittländern zu wahren, erklärt der EuGH dagegen unter bestimmten Bedingungen für grundsätzlich zulässig. Er betont in diesem Zusammenhang jedoch, dass sowohl die europäischen Datenexporteure als auch die Datenimporteure in Drittländern verpflichtet sind, vor der ersten Datenübermittlung zu prüfen, ob im Drittland staatliche Zugriffsmöglichkeiten auf die Daten bestehen, die über das nach europäischem Recht Zulässige hinausgehen. Bestehen solche Zugriffsrechte, können auch die Standardvertragsklauseln den Datenexport nicht rechtfertigen. Bereits ins Drittland übermittelte Daten müssen zurückgeholt werden. Anders als bisher verbreitet vertreten, genügt also der reine Abschluss von Standardvertragsklauseln nicht, um Datenexporte in die USA zu ermöglichen.[5]

Datenschutz ist in Deutschland Ländersache, das heißt jedes Bundesland hat eine eigene Aufsichtsbehörde mit einem zuständigen Landesdatenschutzbeauftragten. Aber die Aussage der Berliner Beauftragten für Datenschutz und Informationsfreiheit, Maja Smoltczyk, sind richtungsweisend. Sie forderte in einer Pressemitteilung am 17. Juli 2020 sämtliche ihrer Aufsicht unterliegenden Verantwortlichen auf, die Entscheidung des EuGH zu beachten. D.h.: Verantwortliche, die – insbesondere bei der Nutzung von Cloud-Diensten – personenbezogene Daten in die USA übermitteln, sind nun angehalten, umgehend[6] zu Dienstleistern in der Europäischen Union oder in einem Land mit angemessenem Datenschutzniveau zu wechseln.

Fazit: Das bedeutet aber auch, dass das am häufigsten angewandte Webanalysetool Google Analytics aufgrund der Nutzung personenbezogener

[5] https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/pressemitteilungen/2020/20200717-PM-Nach_SchremsII_Digitale_Eigenstaendigkeit.pdf

[6] https://edpb.europa.eu/our-work-tools/our-documents/other/frequently-asked-questions-judgment-court-justice-european-union_de

Daten nicht mehr zulässig ist und die Verwendung von der Datenschutzbehörde ab sofort mit einem Bußgeld belegt werden kann.

2.3. Rechtliche Konsequenzen bei datenschutzrechtlichen Verstößen

In der Regel werden Datenschutzbehörden aktiv, wenn Beschwerden von Betroffenen vorliegen oder allgemeine Kontrollaktionen im Rahmen der aufsichtsbehördlichen Überwachungsaufgaben anstehen.

2.3.1. Verfahrensablauf

Bei Beschwerden eröffnet die Behörde nach Eingang der Beschwerde im Regelfall ein Verwaltungsverfahren. Dies dient zunächst dazu, den Sachverhalt genau zu ergründen. In einem ersten Schreiben teilt die Behörde dem aus datenschutzrechtlicher Sicht für die Verarbeitung der personenbezogenen Daten Verantwortlichen den Gegenstand der Beschwerde mit und gibt ihm im Rahmen einer Anhörung Gelegenheit, hierzu innerhalb einer Frist von zwei bis vier Wochen, Stellung zu nehmen. Reagiert der Verantwortliche nicht oder nur unzureichend, ergeht gegen ihn ein förmlicher Bescheid, in dem er verpflichtet wird, der Behörde die notwendigen Auskünfte zu erteilen. Spätestens jetzt sollte der Verantwortliche innerhalb der ihm gesetzten Frist (meist 14 Tage ab Zustellung des Bescheides) reagieren. Tut er dies nicht, wird die Behörde die Festsetzung eines Zwangsgeldes androhen. Verweigert der Verantwortliche danach immer noch die Mitwirkung, setzt die Behörde ein Zwangsgeld fest, das gegebenenfalls im Wege des Zwangsvollstreckungsverfahrens beigetrieben wird. Die Höhe des Zwangsgeldes beträgt mindestens 10 und höchstens 50.000€. Dass Zwangsmittel kann so oft und so lange angewendet werden, bis die Verpflichtung vollständig erfüllt ist. Zudem besteht die Möglichkeit, Ersatzzwangshaft beim zuständigen Verwaltungsgericht zu beantragen, wenn das festgesetzte Zwangsgeld uneinbringlich sein sollte.

Grundsätzlich bestimmt die Behörde Art und Umfang der Sachverhaltsermittlungen nach pflichtgemäßem Ermessen. Hat der Verantwortliche alle erforderlichen Informationen erteilt und ist die Behörde der Ansicht, dass ein Verstoß gegen datenschutzrechtliche Bestimmungen vorliegt, kann diese gemäß Art. 58 Abs. 2 DSGVO entsprechende Abhilfemaßnahmen - Warnungen, Verwarnungen, Anweisungen und Anordnungen, Geldbußen, Widerruf von Zertifizierungen - ergreifen. Auch in diesem Verfahrensabschnitt wird vor dem Erlass eines verbindlichen Bescheids dem Verantwortlichen Gelegenheit gegeben, zu der beabsichtigten Abhilfemaßnahme Stellung zu nehmen. Die angeordnete Maßnahme kann ebenfalls mittels Zwangsgeldes durchgesetzt werden. In schwerwiegenden Fällen leitet die Behörde ein Bußgeldverfahren ein.

2.3.2. Sanktionen

Bei Verstößen gegen die Rechte der betroffenen Personen gemäß Art. 21 Abs. 2, 3 DSGVO werden nach Art. 83 Abs. 5 lit. b DSGVO im Einklang mit Art. 83 Abs. 2 DSGVO Geldbußen von bis zu 20.000.000 € oder im Fall eines Unternehmens von bis zu 4% seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt - je nachdem, welcher der Beträge höher ist. Bei der Festsetzung der Geldbuße haben die Aufsichtsbehörden gemäß Art. 83 Abs. 1 DSGVO sicherzustellen, dass die Verhängung von Geldbußen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist. Der vom Verordnungsgeber vorgesehene hohe Bußgeldrahmen dient dem Ziel einer einheitlichen und konsequenten Durchsetzung der Vorschriften der DSGVO in der gesamten EU.

2.3.3. Bußgeldkonzept

Die DSK hat ein Konzept zur Zumessung von Geldbußen bei Verstößen gegen die DSGVO durch Unternehmen verabschiedet. Ziel des Konzepts ist eine einheitliche, transparente und nachvollziehbare Anwendung der gesetzlichen Vorgaben der DSGVO zur Bußgeldzumessung durch die deutschen Aufsichtsbehörden.

Die konkrete Bußgeldzumessung erfolgt laut Bußgeldkonzept in fünf Schritten: Zunächst wird das betroffene Unternehmen einer Größenklasse zugeordnet (1.), danach wird der mittlere Jahresumsatz der jeweiligen Untergruppe der Größenklasse bestimmt (2.), dann ein wirtschaftlicher Grundwert ermittelt (3.), dieser Grundwert mittels eines von der Schwere der Tatumstände abhängigen Faktors multipliziert (4.) und abschließend der unter 4. ermittelte Wert anhand täterbezogener und sonstiger noch nicht berücksichtigter Umstände angepasst (5.).

2.3.4. Beispiele für Bußgelder

N26 Bank GmbH
Die Online-Bank der N26 Bank GmbH führte unrechtmäßig eine sog. „schwarze Liste“ ehemaliger Kundinnen und Kunden. Es gab ein Bußgeld in Höhe von 50.000 EUR.

Delivery Hero Germany GmbH
Die Daten von Kundinnen und Kunden des Lieferdienstes der Delivery Hero Germany GmbH wurden über viele Jahre gespeichert, selbst wenn diese jahrelang nicht mehr bestellt hatten. Es wurden insgesamt Bußgelder von 195.307 EUR erteilt. Die Mehrzahl der Fälle betraf die Nichtbeachtung der Betroffenenrechte wie das Recht auf Auskunft über die Verarbeitung der eigenen Daten, das Recht auf Löschung der Daten sowie das Recht auf Widerspruch.

Kolibri Image
5.000 EUR wegen fehlendem Auftragsverarbeitungsvertrag.

Knuddels
20.000 EUR wegen unverschlüsselter Kundendaten auf dem Server[7]

[7] https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank.php

3. Konformes Tracking nach DSGVO und Schrems II

Wer rechtssicher weiter Marketingtools verwenden und dafür tracken möchte, muss sich zwei Metathemen vor Augen führen: zum einen muss ein datenschutzkonformer Consent Layer auf der Seite aktiv sein, unabhängig wie die personenbezogenen Daten technisch erhoben werden und zum anderen und noch gravierender, müssen sich alle Webseitenbetreiber von ihren amerikanischen Lösungen trennen, sofern diese personenbezogene Daten von europäischen Bürgern auf amerikanische Server weiterleiten.

Aus diesem Grund werden im folgenden Abschnitt Alternativen zu Google Analytics aufgezeigt und zudem Trackings von Marketinglösungen unter die Lupe genommen, insbesondere in Hinblick auf ihre Serverlösungen. Zudem nehme ich Bezug auf meinen Artikel in der t3n, in dem ich alternative cookieless Trackingmöglichkeiten aufgezeigt habe.[8] Allerdings vor den aktuellen Entwicklungen.

3.1. Trackinganbieter für Webanalysetools

Wie bereits beschrieben, haben sich durch die DSGVO und vor allem Schrems II neue Anforderungen an die Unternehmen ergeben. Gleichzeitig besteht weiter das Erfordernis die eigene Webseite zu optimieren. Google Analytics (GA) war aufgrund der Kostenfreiheit ein probates Mittel für Website-Betreiber und es bietet tatsächlich Unmengen an Funktionen zur Erfassung von Besucherzahlen, Aufenthaltsdauer, Absprungrate, Ursprungsland, verwendeter Software und vieles mehr.

Gleichzeitig war Google Analytics auch immer ein Tool, das aufgrund seiner Usability, aber vor allem auch aufgrund der dahinterliegenden Strategie von Google kritisch zu sehen war. Denn natürlich war die Nutzung nicht kostenlos. Die Nutzer haben kontinuierlich mit den Daten ihrer Kunden bezahlt.

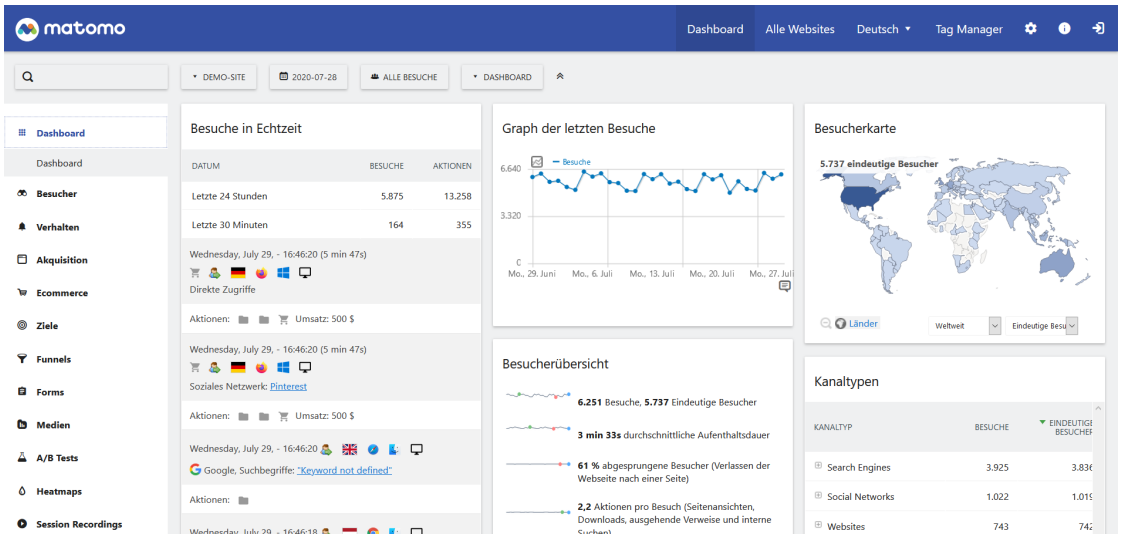
In der Folge werden drei alternative und vor allem rechtskonforme Webanalyse-Tools vorgestellt. Es handelt sich um Matomo als Tool, das am zweithäufigsten Anwendung in Deutschland findet[9] sowie um etracker und Open Web Analytics. Diese werden bereits zum Teil von den Kunden der Löwenstark Online-Marketing GmbH verwendet bzw. die Einführung wird gerade vollzogen. Es gibt viele weitere Lösungen. Es besteht hier kein Anspruch auf Vollständigkeit. Anhand der näher betrachteten Lösungen sollen grundsätzliche Erfordernisse beleuchtet werden.[10]

3.1.1. Matomo

Die Open-Source-Lösung Matomo, früher bekannt als Piwik, ist nach Google Analytics das meistgenutzte Analyse-Tool in Deutschland. Nutzer haben die Möglichkeit, sämtliche Daten auf eigenen Servern zu speichern. So greifen also nur die Seitenbetreiber auf die erhobenen Daten zu. Matomo stellt umfangreiche Informationen in Echtzeit bereit und lässt

[8] https://t3n.de/news/cookieless-tracking-zukommt-1232500/
[9] https://trends.builtwith.com/analytics/audience-measurement/country/Germany
[10] https://t3n.de/news/google-analytics-alternativen-511230/

Seitenbetreiber jede Customer-Journey bis auf die Personenebene nachvollziehen. Die Dashboards lassen sich zudem per Drag-&-Drop an die eigenen Vorlieben anpassen.[11]



Das Matomo Dashboard ähnelt in Design und Struktur Google Analytics [12]

Die Datenqualität ist zudem besser als bei Google Analytics, da Matomo im Gegensatz zu anderen Web-Analyse-Diensten nicht von AdBlockern blockiert oder gestört wird, da das Tool die Privatsphäre der Besucher respektiert. Dies führt zu exakteren und realistischeren Analysedaten. Gleichzeitig wird Referrer-Spam durch eine ständig erweiterte Blacklist herausgefiltert, die von einem Matomo-Team und der Community gemeinsam gepflegt wird. So wird verhindert, dass Spammer die Analysedaten verfälschen.

Datenschutzseitig empfiehlt sich eine Umkonfigurierung der Lösung. Zum einen sollte mittels PrivacyManager-Plugin die IP-Anonymisierung eingestellt werden, da sonst Matomo die IP-Adresse des Nutzers speichert und es sich hierbei um personenbezogene Daten handelt. Zum anderen muss vom Verwender des Web-Analyse-Tools entschieden werden, ob Cookies Verwendung finden sollen oder cookieless getrackt wird. Bei beiden Optionen muss nach aktueller Rechtsauffassung ein Consent Layer die Zustimmung des Nutzers erfragen, da auch bei der Cookieless-Variante über Device-Fingerprinting personenbezogene Daten erfasst werden.[13]

Ein Argument für das Webanalysetool Matomo ist der Preis. Da Matomo selbst eine Open-Source-Lösung ist, ist die selbstgehostete Version (Matomo OnPremise) von Matomo Analytics kostenlos. Diese Version kann ganz normal heruntergeladen werden und auf dem eigenen Webserver installiert werden. Kosten entstehen hier nur beim eigenen Webhoster oder wenn bestimmte Plugins zur verbesserten Zahlensicht gekauft werden, wobei die Preise sehr moderat sind.[14]

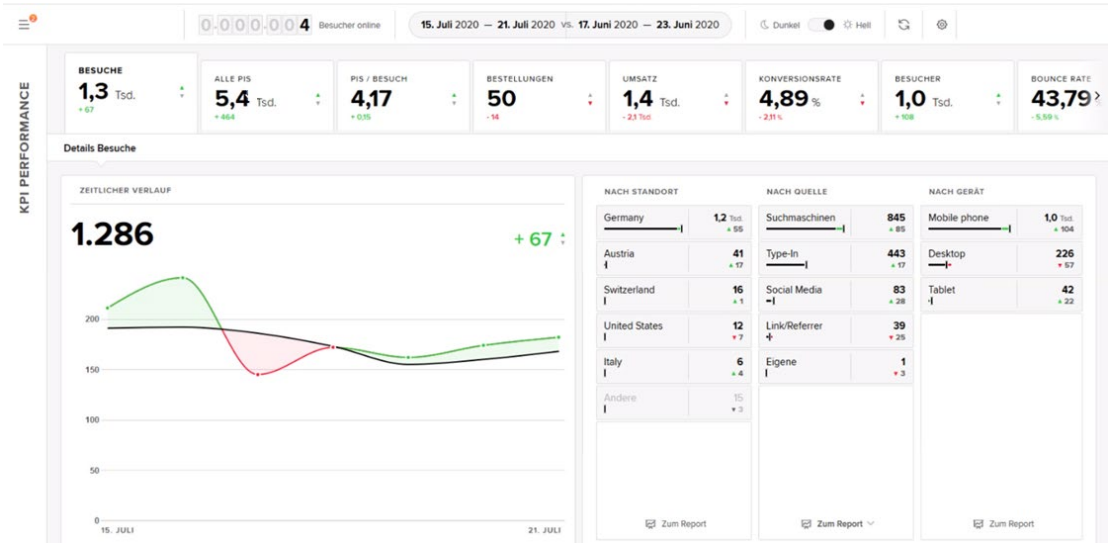
Das eigene Hosting stellt außerdem sicher, dass der Verwender seine ggf. erhobenen personenbezogenen Daten kontrolliert auf europäischen Servern sichert.

[11] https://matomo.org/features/
[12] https://demo.matomo.org/
[13] https://www.it-recht-kanzlei.de/matomo-richtig-verwenden-dsgvo.html
[14] https://plugins.matomo.org/premium

Fazit: Matomo besticht mit der Vielzahl an Auswertungsmöglichkeiten, seiner gegenüber Google Analytics besseren Datenqualität, ist in der Basisversion kostenfrei und wird gleichzeitig stetig weiterentwickelt. Darüber hinaus ist Matomo auch nach der Unwirksamkeit des Privacy Shields rechtskonform.

3.1.2. etracker

Etracker ist je nach Quelle das dritt- oder vierthäufigst angewendete Webanalyse-Tool in Deutschland. Das Tool ist kostenpflichtig, wobei die Firma aufgrund der aktuellen Rechtsprechung die Pro Version bis zum 31.8. für 12 Monate kostenlos im Angebot hat, um damit den Kundenstamm in der aktuell günstigen Lage auszubauen.[15]



Das etracker Dashboard ist klar strukturiert und erlaubt umgehend einen Überblick über relevante KPI

Der Anbieter wirbt offensiv mit „Web-Analyse ohne Opt-In Pflicht“. Dabei bezieht sich das Unternehmen auf die Tatsache, dass in der Standard-Konfiguration von etracker weder Cookies gesetzt noch der Local Storage genutzt wird. Somit kann nach Ansicht des Unternehmens komplett auf Cookie-Hinweise und Einwilligungs-Dialoge verzichtet werden, sofern keine weiteren nicht erforderlichen Cookies zum Einsatz kommen. Auch als Fall-Back-Option ist etracker Analytics Cookieless sehr hilfreich, da ein Session-Tracking auch ohne Einwilligung bzw. bei Cookie-Ablehnung ermöglicht wird. Richtigerweise verweist etracker insgesamt darauf, dass es sich um eine eigene Rechtseinschätzung handelt. Argumentiert wird damit, dass weder eine „Speicherung von Informationen“ noch ein „Zugriff auf Informationen, die bereits im Endgerät eines Teilnehmers oder Nutzers gespeichert sind“ im Sinne von Art. 5 Abs. 3 der Richtlinie 2002/58 („Cookie-Richtlinie“) stattfindet. Es ist zumindest Vorsicht geboten.[16]

Etracker Analytics bietet seinen Nutzern verschiedene Möglichkeiten des Web-Controllings und Targetings. Zu den Basic-Funktionen gehören Live-Tracking, Klickpfad-Analyse und die Auswertung von Nutzerstatistiken. Der darüber hinaus gehende Funktionsumfang ist vom

[15] https://www.etracker.com/pricing/
[16] https://www.etracker.com/session-tracking-einwilligungsfrei/

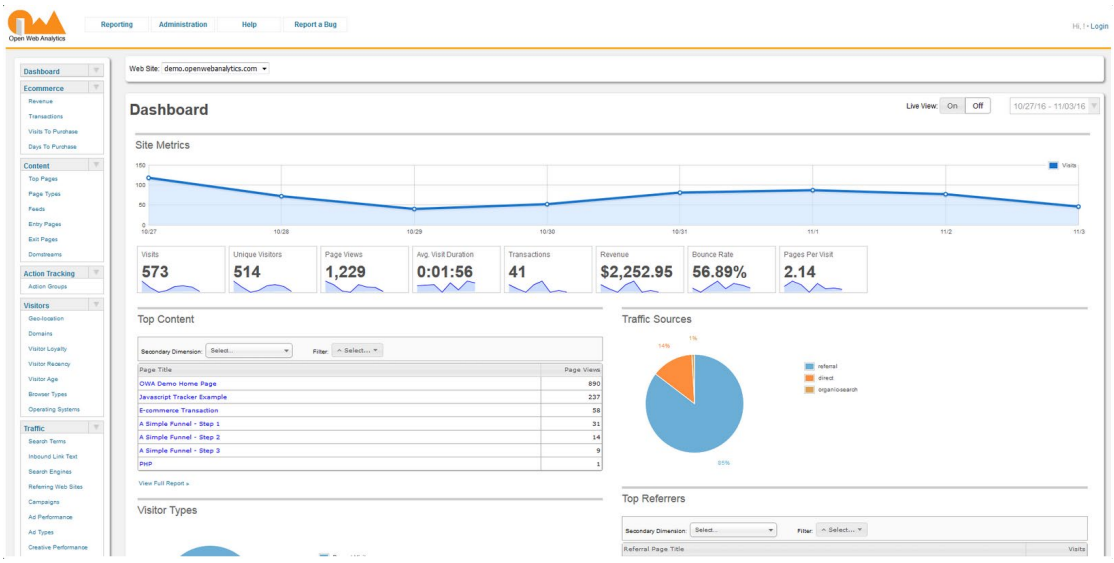
gewählten Paket abhängig. Die größeren Pakete bieten Zusatzfeatures wie UX Analytics, App Analytics und den Zugriff auf die Rohdaten. Zudem gibt es praktische Funktionen wie Maustracking oder eine Zufriedenheitsanalyse, die man bei anderen Tools nicht findet.

Das Preismodell ist insbesondere für Webseiten mit hohem Aufkommen teurer als Matomo. Abgerechnet wird nach Tracking Requests (Touchpoints), das meint Page Impressionen, Events und Weiterleitungsklicks ohne nachfolgende Page Impressionen.

Fazit: Insgesamt ist etracker ein bewährtes Webanalysetool mit zahlreichen Features, das darüber hinaus sehr vorbildlich mit deutschen Serverstandorten agiert. Die Kosten sind dabei auf jeden Fall höher als bei Matomo, dafür muss aber weniger Energie in die Konfiguration investiert werden.

3.1.3. Open Web Analytics

Eine weitere Open-Source-Lösung stellt Open Web Analytics dar. Bei Open Web Analytics bekommt man schnell das Gefühl, man würde mit Google Analytics arbeiten. Viele bereits von Google Analytics bekannte Funktionen sind hier ebenfalls vertreten, wie z.B. das Geo-Tracking. Das Tool ist kostenlos. Für die Anzahl der Datensätze gibt es keine Limits. Gleiches gilt auch für die Anzahl der getrackten Webseiten.



Wer das Dashboard wie bei Google Analytics wünscht, ist bei Open Web Analytics richtig

Interessant sind die Heatmap-Funktion und die Eye-Tracking-Methode. Zudem kann man E-Commerce-Ziele definieren und spezielle Statistiken zur Benutzung, der Site-Conversion und zu benutzerdefinierten Ereignissen abrufen.

Da Open Web Analytics als Open-Source-Lösung ebenfalls auf eigenen Servern betrieben wird, haben Seitenbetreiber auch hier die volle Kontrolle über ihre Daten, da diese nicht bei Drittanbietern gespeichert werden.[17]

Was die Performance der Anwendung betrifft, ist Matomo allerdings die bessere Google-Analytics-Alternative. Weitere Nachteile sind klar die unzuverlässigen Fortschritte der Weiterentwicklung. Updates gibt es nur selten und unregelmäßig.

Fazit: Kostenlose Open-Source-Lösung, die rechtskonform ist und viele Features aufweist, allerdings in der Weiterentwicklung hinter dem Konkurrenten Matomo hinterherhinkt.

3.2. Marketing Trackings und Social Plugins

Um es deutlich zu sagen: Inzwischen ist es ganz klar vorherrschende Rechtsauffassung, dass durch das entscheidende Argument des EuGH: "fehlende Kontroll- und Rechtsschutzmöglichkeiten hinsichtlich der erheblichen Zu- und Eingriffsmöglichkeiten der US-Sicherheitsdienste" auch die Standardvertragsklauseln keine wirksame Rechtsgrundlage für den Datentransfer in die USA darstellen.

Grundsätzlich ist daher aktuell jede Übertragung personenbezogener Daten in die USA als unzulässig anzusehen. Das betrifft neben Tracking Tools auch sämtliche Social Plugins und Nutzung von Youtube-/Vimeo- Videos, Webfonts von Google und Adobe, ReCapcha und Google Maps.

Fazit: Anwender amerikanischer Tools, die personenbezogene Daten erheben und auf amerikanischen Server transferieren, müssen entweder die Risiken von möglichen Bußgeldern in Kauf nehmen oder eine Alternative zum bislang genutzten Tool evaluieren.

3.2.1. Marketingautomatisierung/ E-Mail-Marketingtools

Mit dem Urteil ist die Nutzung von US-Tools wie Mailchimp, Hubspot, Active Campaign und Co. ab sofort mit noch größeren Risiken behaftet. Der amerikanische Anbieter für Marketingautomatisierung MailChimp beruft sich jetzt auf EU-Standardvertragsklauseln. Dieses verbietet sich wie unter „2.2 Schrems II / Unwirksamkeit des Privacy Shield“ belegt wird. Es ist daher dringend geboten, sofort auf eine datenschutzkonforme Lösung wie zum Beispiel XQueue umzusteigen.

3.2.2. Affiliate Cookies

Bei Affiliate Marketing-Cookies muss beachtet werden, ob es sich um klassische oder Remarketing-Cookies handelt. Mit Verwendung von klassischen Affiliate Cookies besteht ein berech-

[17] https://t3n.de/news/google-analytics-alternativen-511230/

tigtes Interesse des Webseitenbetreibers nach Art. 6 Abs. 1 DSGVO (Remarketing ausgeschlossen). Daher ist lt. Bundesverband Digitale Wirtschaft (BVDW) keine explizite Zustimmung durch den Nutzer notwendig und die Cookies können als essenziell angesehen werden.

Darüber hinaus stellt der BVDW fest, dass die schlichte Zuordnung (Attribution) von Transaktionen (z.B. Kauf im Onlineshop) als Ergebnis von Vertriebsmaßnahmen zur Vermarktung selbst bei Verwendung von Cookies nicht in den Regelungsbereich des § 15 Abs. 3 fällt, da hier keine Nutzungsprofile erstellt werden. Die Attribution – auch unter Verwendung von Cookies – kann weiterhin durch berechtigtes Interesse i.S.d Art. 6. Abs. 1 lit. f DSGVO gerechtfertigt sein. Beim Setzen von Cookies zur Zuordnung von Transaktionen, wie beispielsweise im Bereich des Affiliate-Marketings, handelt es sich um eine technische Lösung unter Nutzung von pseudonymen Daten, die allein dazu dienen diese Vertriebsmaßnahmen erfolgsgerecht abrechnen zu können. Die Attribution ist erforderlich zur Sicherstellung der Finanzierung von Inhalten, die vom Nutzer im Internet aktiv angefragt werden.[18]

3.2.3. Social Plugins

Konnte man sich vor Schrems II mit der Zwei-Klick-Variante oder den Shariff-Buttons rechtlich absichern, ist aktuell von einer grundsätzlichen Unzulässigkeit auszugehen. Die Reaktionen der Datenschutzbehörden in ihren Pressemitteilungen lassen auch nicht die Vermutung aufkommen, dass es hier eine Möglichkeit der Zulässigkeit gibt.

4. Best Practice Consent-Layer

Wie die Ausführungen auf den vorigen Seiten zeigen, ist ein Consent-Layer bereits jetzt ein Muss und gehört quasi zur „Datenschutzhygiene“ eines jeden Webseitenbetreibers - genauso wie aussagekräftige und vor allem korrekte Datenschutzerklärungen. Das bedeutet, dass wir uns die optimale Variante eines Consent-Layers aussuchen müssen, da wir ihn aufgrund der diversen Trackings zu Marketingzwecken in den meisten Fällen gar nicht umgehen können.

Ein sehr gutes Beispiel für optimierte Consent-Layer bieten die deutschen Versandapotheken. Sie stehen zum einen in einem starken Wettbewerb und sind daher immer auf der Suche nach Optimierungen und Wettbewerbsvorteilen. Zum anderen sind sie im E-Commerce die am stärksten datenschutzrechtlich geforderte Branche, da sie auch über die in Art. 9 DSGVO besonders geschützten Gesundheitsdaten ihrer Kunden verfügen und damit in besonderem Maße im Fokus der Aufsichtsbehörden stehen.

4.1. Grundlagen zu Consent-Layern

Um die Einwilligungserfordernisse auf Webseiten rechtskonform umzusetzen, bietet sich eine Consent Management Plattform (CMP) an, die das Transparency & Consent Framework (TCF) in der Version 2 des IAB Europe[19] unterstützt. Es gibt hier diverse Anbieter wie unter anderem Usercentrics, Consentmanager oder Cookiebot.

[18] https://www.bvdw.org/themen/publikationen/detail/artikel/datenschutzkonformes-affiliate-marketing/

[19] https://iabeurope.eu/transparency-consent-framework/

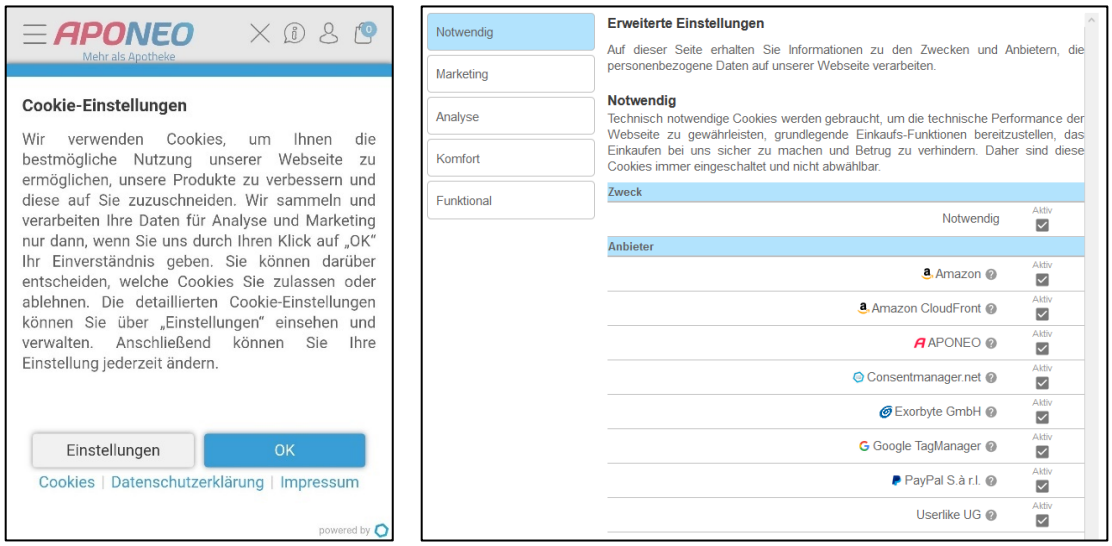
Eine wirksame Zustimmung muss immer eine frei gegebene, spezifische, informierte und unmissverständliche Angabe der Wünsche des Nutzers sein, d.h. eine klare und bestätigende Handlung des Nutzers.

Die Richtlinien des European Data Protection Boards (EDPB-Guidelines) stellen u.a. klar, dass das Scrollen oder fortgesetzte Browsen auf einer Website keine gültige Zustimmung darstellt und dass Cookie-Banner keine vorgekreuzten Kontrollkästchen haben dürfen.

Auch sogenannte Cookie Walls (erzwungene Zustimmung) werden als nicht konform eingestuft. Dabei handelt es sich um eine Möglichkeit für Websites, Benutzern den Zugriff zu verweigern, wenn sie nicht mit allen auf dieser Website vorhandenen Cookies und Trackern einverstanden sind. Es ist eine Art Barriere, die den Benutzer in eine "take it or leave it"-Situation bringt, in der er sich entweder für Marketing-Cookies und ähnliche Tracking-Technologien entscheiden muss, anderenfalls wird ihm der Zugang zur Website und deren Dienste verweigert. Auch Cookie Walls werden von den EDPB-Guidelines ausdrücklich ausgeschlossen und sind somit abmahnfähig.[20]

4.2. Positivbeispiele

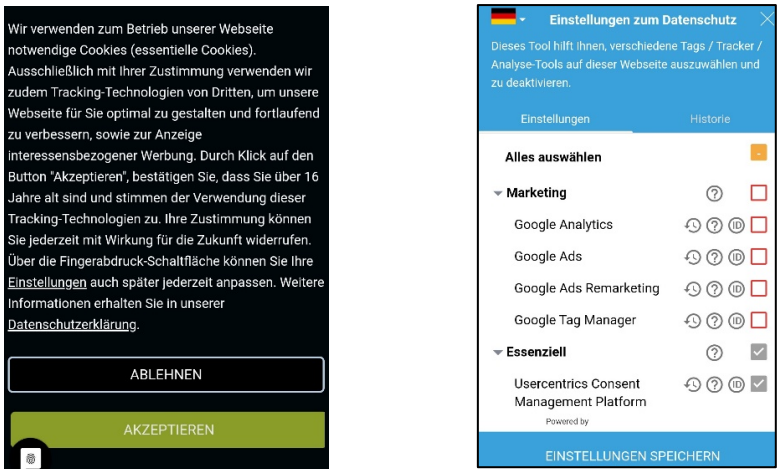
Die Consent-Layer der großen Versandapotheken weisen eine Annahmequote von 85-90% auf. Dafür bedienen sie sich eines Einstiegsfensters, das mit dem OK-Button die Cookies annimmt und bei potenziellem Ablehnungswunsch den Button „Einstellungen“ anbietet. Alleine diese Einstiegsseite macht den Erfolg in Relation zu anderen Consent-Layer-Designs aus.



Ob APONEO oder DocMorris – die großen Versandapotheken haben einen rechtskonformen Consent-Layer mit der höchsten Annahmequote

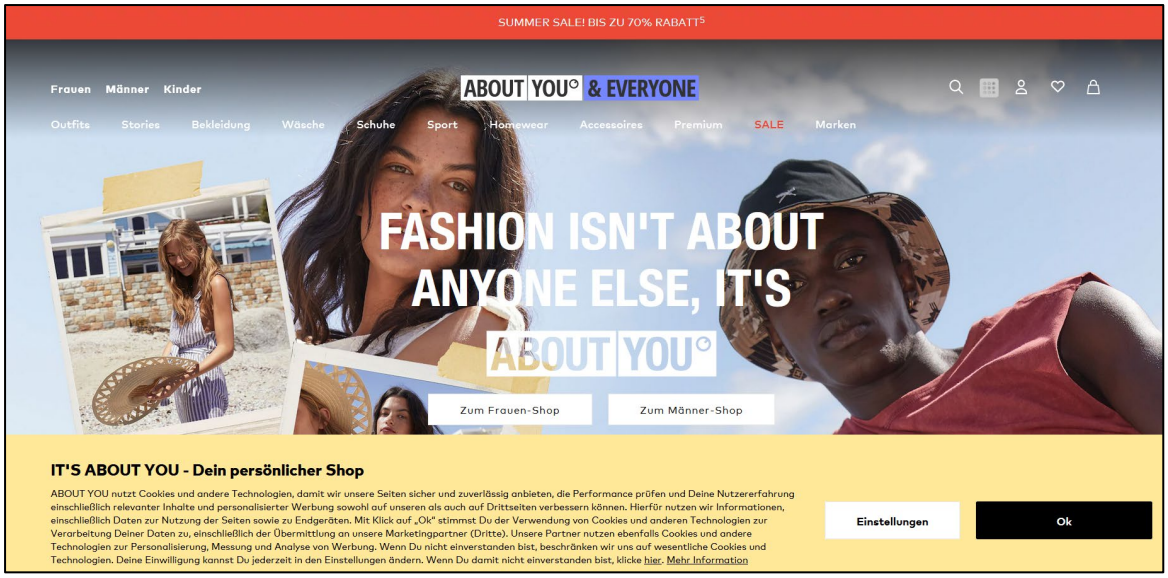
Consent-Layer, die offensiv die Ablehnung der Cookies anbieten, erreichen maximal eine Annahmequote von 75%. Die Range geht hier aber in Abhängigkeit der Neubesucher bis zu lediglich 50%. Hier wird die Zahlenbasis dünn – insbesondere, wenn es um die Steuerung von Google Ads geht.

[20] https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_de



Rechtskonform, aber von der Gestaltung lädt es zum Ablehnen ein und führt zu einer niedrigen Annahmequote

Ebenfalls entscheidend für den Erfolg einer Consent-Layer-Lösung ist vor allem in der Desktop-Ansicht die Positionierung des Banners. Best Practice ist hier ganz klar ein Ein-Drittel-banner, der die Nutzung der Seite erschwert und damit den Kunden subtil in die Nutzung des Consent-layers drängt.



Gute Lösung von About you – die Marke und der Shop sind deutlich zu erklären, den Banner wird der Besucher zur besseren Nutzung der Seite trotzdem klicken um die volle Convenience der Seite zu erleben

Sehr unglücklich sind Lösungen, die die gesamte Seite abdecken und im schlimmsten Fall nicht einmal die gesuchte Marke des Seiteninhabers erkennen lassen. Hier wird Umsatz verspielt. Dieser verlorene Umsatz ist zudem nicht direkt zu messen, da die Besucher vor der Nutzung des Consent-Layers die Seite wieder verlassen und ein Tracking nicht stattfinden durfte. Den „realen" Umsatzverlust kann man sich z.B. in der SEA nur über die Verhältniszahl von Klicks zu Sitzungen errechnen. Hier wird der Quotient nach der Umstellung zwangsläufig geringer und damit der verlorene Umsatz sichtbar.

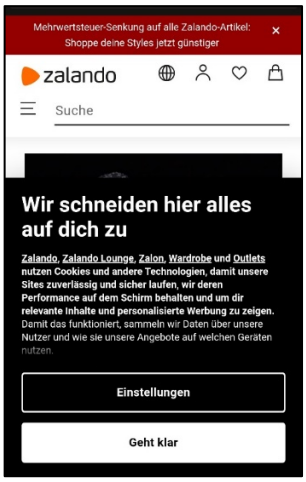
Ein bislang nicht ausgeschöpftes Potential bietet die Incentivierung von Cookie-Annahmen über Gutscheine wie bei der Newsletteranmeldung. Hier wird sich in der Zukunft zeigen, wie

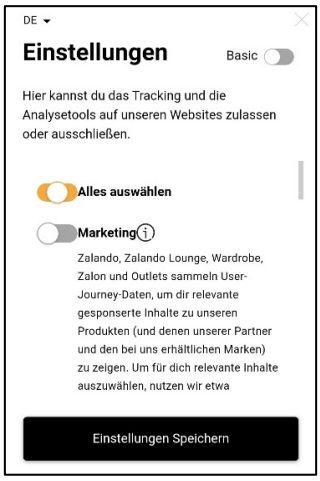
die Unternehmen die Zahlenwelt fördern und welche zusätzlichen Maßnahmen zur Steigerung der Annahmequote sich durchsetzen.

4.3. Negativbeispiele

Der Consent-Layer von Zalando entspricht z.B. auf dem ersten Blick dem Best Practice-Ansatz. Bei genauerer Betrachtung sieht man in den Einstellungen pauschale Auswahlmöglichkeiten für Marketing, Personalisierung und Funktional ohne differenzierte Wahlmöglichkeit auf Cooki-Ebene. Dies ist unzulässig.

Nach Ansicht von EuGH, BGH und der Datenschutzkonferenz ist für jedes Tracking-Tool eine genaue Information über Sinn und Zweck, Art und Umfang der Datenspeicherung und ggf. deren Weitergabe an Dritte, sowie Rechte wie Widerruf der Einwilligung usw. erforderlich und außerdem in jede Nutzung einzeln einzuwilligen. Hinzu kommt bei dem Beispiel Zalando, dass jedenfalls zum Zeitpunkt des Seitenaufrufes bereits vor Erteilung der Zustimmung vier Tracker (u.a. G A) aktiv waren.





Wenn beispielsweise die sehr engagierte Berliner Beauftragte für den Datenschutz auf diese Consent-Lösung einen Blick wirft, könnte auf Webseitenbetreiber, die keine Möglichkeit anbieten, einzelne Cookies auszuwählen, einiger Ärger zukommen.

Der normale Verfahrensweg ist, dass der Verantwortliche in einem umfangreichen Fragenkatalog aufgefordert wird, zur Art und Weise der Einholung der Einwilligungen Stellung zu nehmen:

- Nachweis der ausführlichen Informationserteilung über sämtliche Tools
- differenzierte Einwilligungen
- Nachweis Auftragsverarbeitungsverträge
- Nachweis, dass die Voraussetzung der EU-Standardklauseln bei Übertragung an Drittanbieter vor der Übertragung sorgfältig geprüft und dokumentiert wurden
- Vorlage Verarbeitungsverzeichnis

Da ein Nachweis datenschutzkonformen Vorgehens wohl kaum gelingen wird und die Aktivierung der Tracker vor Erteilung leicht nachzuweisen ist, würde neben dem Verbot der Datenübertragung in die USA ein Rekord-Bußgeld verhängt werden, dessen Höhe abhängig vom Jahresumsatz ist.

5. Maßnahmen zur Umsatz- und Kostenoptimierung bei eingeschränktem Tracking

Um der sich verschlechternden Zahlenlage durch Consent Layer und fehlende Trackingmöglichkeiten aufgrund von Schremms II zu begegnen, müssen neben den bereits genannten Optimierungen weitere Maßnahmen getroffen werden. Die Stärke des Online-Marketings war immer die stabile und aussagkräftige Datenlage und diese gilt es möglichst zu erhalten.

5.1. Loginphase vorziehen und arbeiten mit Micro Conversions

Je früher der Nutzer sich auf einer Seite registriert und anmeldet, umso besser für die Seitenanalyse. In der Registrierung und im Login Bereich der Webseite angekommen, wird eine Wiedererkennung über den Account des Nutzers möglich. Somit wird auch das Nutzerverhalten auf der Webseite transparent und kann über die Nutzer ID nachverfolgt werden. Marketing Aktivitäten können nun gezielt und individuell pro Nutzer ausgerichtet werden, um z.B. Transaktionen im Shop zu steigern. Bestandskunden können über ein cookiebasiertes Autologin angemeldet werden. Schwieriger verhält es sich mit neuen Besuchern, die zu einer Registrierung bewegt werden müssten. Hier wird man als Webseitenbetreiber wieder mit Incentivierungen oder mit funktionalen Nachteilen bei einer Nicht-Registrierung arbeiten müssen.

Da sich viele Besucher trotzdem nicht registrieren werden, bedarf es auch anderer Wege. Eine Option stellt hier die Micro Conversion dar. Micro Conversions können jeder Klick und jede Eingabe sein, die ein künftiger Kunde tätigt, sofern sie gemessen werden. Hierbei wird zwischen Prozess Meilensteinen und sekundären Aktionen unterschieden.

- Prozessmeilensteine sind alle Interaktionen, die den Kunden näher an die Macro Conversion bringen (Customer Journey). Im eCommerce wären das alle Seiten, die der Kunde vor dem Abschluss der Bestellung besucht
- Sekundäre Aktionen sind Interaktionen des Nutzers die nicht primär zielführend sind und somit nicht der Macro Conversion unterliegen. Beispiele hierfür wären: Eine Bewertung zu einem Artikel zu hinterlassen, ein Video anzusehen, einen Blog Post zu lesen und weitere. Grundsätzlich kann man sagen, dass sekundäre Micro Conversions das Interesse an der Seite bekunden.[21]

Es müssen dann gar nicht mehr einzelne Nutzer verfolgt werden, sondern es werden Erkenntnisse aus der reinen Datenmenge der Mirco Conversions gewonnen. Zwischen den einzelnen Customer Journey Phasen können dann die individuellen Conversionrates berechnet werden.

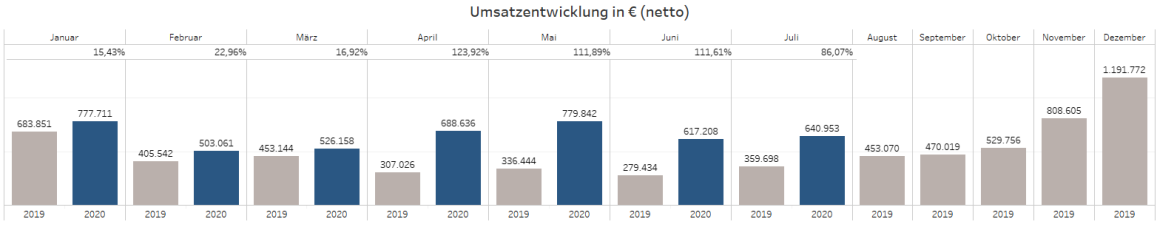
5.2. Data Analytics - Hochrechnungen mit Backendzahlen und historischen Werten

Webanalysetools waren allein nie aussagekräftig, zumindest wenn es um die genutzten Marketingkanäle und den Gesamtüberblick ging. Aus diesem Grund musste der ganzheitlich operierende Marketer immer schon alle Tools mit ihren KPI verknüpfen, ob manuell, über Datenbanklösungen oder Tools.

Ein gern begangener Fehler ist auch immer wieder der unterlassene Blick in die Zahlen der Warenwirtschaftssysteme. Nur hier gibt es die umsatzseitige Wahrheit und schon so mancher

[21] https://onlinemarketing.de/lexikon/definition-micro-conversion

Verantwortliche hat sich schon über die gravierenden Unterschiede gewundert. Durch den Consent-Layer und die nicht mehr zulässigen Marketing-Trackings wird der Gap zwischen Web- und Backendzahlen noch größer.



Entwicklung der Online-Marketing Kanäle März - Juli 2020

	März				April				Mai				Juni				Juli			
	Umsatz €	% VJ	Kosten	KUR	Umsatz €	% VJ	Kosten	KUR	Umsatz €	% VJ	Kosten	KUR	Umsatz €	% VJ	Kosten	KUR	Umsatz €	% VJ	Kosten	KUR
Direct	52.594	31,86%			67.924	96,41%			77.082	113,19%			61.904	84,23%			66.391	67,58%		
SEO	83.017	20,56%			107.215	72,67%			121.669	95,35%			97.711	131,60%			104.795	103,70%		
Google	315.123	10,32%	23.819	7,56%	416.090	156,94%	23.476	5,64%	470.551	143,28%	22.942	4,88%	368.819	126,18%	15.199	4,12%	374.557	70,58%	14.847	3,96%
Email	5.320	17,11%			6.871	16,10%			7.797	39,00%			6.262	115,25%			6.716	7,59%		
Social	16.450	19,37%	1.278	7,77%	21.245	104,88%	1.313	6,18%	24.109	239,53%	2.015	8,36%	19.362	308,25%	1.950	10,07%	20.766	129,40%	2.016	9,71%
Affiliate	53.653	32,73%	4.966	9,26%	69.291	115,69%	6.183	8,92%	78.633	146,69%	7.655	9,74%	63.150	91,80%	5.715	9,05%	67.728	100,63%	6.763	9,99%
Gesamt	**526.158**	**16,11%**	**30.063**	**5,71%**	**688.636**	**124,29%**	**30.972**	**4,50%**	**779.842**	**131,79%**	**32.612**	**4,18%**	**617.208**	**120,88%**	**22.864**	**3,70%**	**640.953**	**78,19%**	**23.625**	**3,69%**

Königsdisziplin Zahlenverständnis - als Steuerungsgrundlage unverzichtbar und Grundlage für weitreichende Entscheidungen zur Budgetoptimierung

Umso wichtiger sind Gesamtzahlenverständnis, Hilfsrechnungen mittels Micro Conversions oder historische Werte oder Branchenkenntnisse. Diese müssen je nach Zahlenlage zu einem Gesamtbild zusammengefügt und auf die Backendzahlen umgelegt werden.

6. Fazit

Unternehmer müssen ständig eigenständig über den richtigen Kurs in schwierigen Zeiten entscheiden. Aktuell müssen Webseitenbetreiber abwägen, ob sie rechtskonform oder unternehmerisch handeln wollen. Wobei bei nicht rechtskonformer Herangehensweise auch schnell ein wirtschaftliches Thema in Form von Bußgeldern entstehen kann.

Wer also rechtlich absolut sichergehen und jedes Risiko von Abmahnungen oder Bußgeldern vermeiden will, muss Dienste, die auf das Privacy Shield setzen, abschalten, auf die Nutzung verzichten und alternative Dienste nutzen, die ihre Datenverarbeitung in der EU durchführen.

Die eigene unternehmerische Entscheidung kann aber auch dahingehend getroffen werden, solche Dienste, die zum Datentransfer in die USA auf das Privacy Shield gesetzt haben, weiterzuverwenden. Abmahnungen und Bußgelder sind dabei sehr wahrscheinlich. Blickt man auf eine ähnliche, ältere Entscheidung des EuGH zum Safe Harbour-Abkommen, dem Vorgänger des Privacy Shields, kam es dort in der direkten Folgezeit zu keinen Reaktionen der Behörden, obwohl für knapp sechs Monate eine rechtliche Grundlage für den Datenaustausch gefehlt hat. Die politische Lage spricht diesmal allerdings gegen eine schnelle Lösung und damit auch gegen ein Stillhalten der Datenschutzbehörden. Von der derzeitigen US-Regierung ist nicht zu erwarten, dass sie Entgegenkommen zeigt und EU-Bürgern ein höheres Rechtsschutzniveau eröffnet als dies gegenwärtig der Fall ist. Es bleibt also abzuwarten, ob und wann die Behörden das seit dem 16. Juli geltende Recht durchsetzen.

Während man beim Thema Privacy Shield noch abwägen kann, ist ein rechtskonformer Consent Layer aber auf jeden Fall jetzt schon zwingend umzusetzen. Aus diesem Grund sind die Optimierungen - wie dargestellt - ein Muss und bereiten neben weiteren Maßnahmen den entscheidenden Punkt vor:

Entscheidend wird zukünftig sein, dass über unternehmensindividuell angepasste Datenanalysen und -modelle ein vollständiger Überblick über die Kundenentwicklung und Marketingausgaben hergestellt wird und kontinuierlich zuverlässige Aussagen getroffen werden können. Wer hier seine Daten am besten im Griff hat, wird im Wettbewerb reüssieren.