Leistungsmessung im Affiliate Marketing

Ein Kompendium
Juni 2022

www.bvdw.org

Leistungsmessung im Affiliate Marketing

Ein Kompendium

Juni 2022

Einleitung – Tracking für eine faire Verteilung der Erlöse

Tracking ist die Basis für die Wirtschaftlichkeit von mehr als 100.000 aktiven Publishern und deren Webseiten in Deutschland. Influencer, Medien, Blogger oder die Betreiber von Hobby-Sites refinanzieren ihre Arbeit häufig über die Bewerbung von Affiliate-Programmen. Es liefert die Basis für einen fairen Anteil an den Verkaufserlösen und ist somit die Grundlage für die Vielfalt des Internets im deutschsprachigen Raum. Ein funktionierendes Tracking und damit die Leistungsmessung ist die Basis für ein erfolgreiches Affiliate- und Performance-Marketing. Es gewährleistet die Zuordnung von Erfolgen wie Klicks, Registrierungen (Leads) oder Einkäufen (Sales) auf einzelne Online-Marketing-Kanäle oder Publisher bzw. deren Werbeflächen mit dem Ziel der erfolgsorientierten Messung und erfolgsbasierten Vergütung.

Mit Tracking sind **keine** Targeting-Mechanismen gemeint, wie sie bspw. beim Retargeting Anwendung finden. Es dient **nicht** der Verfolgung eines Nutzers über verschiedene Websites hinweg, um ihm personalisierte Werbung anzeigen zu können oder um ein weitreichendes Nutzerprofil zur Vorhersage des Verhaltens und der Interessen für Werbezwecke zu erstellen.

Aktuell unterliegen die technischen und rechtlichen Rahmenbedingungen des Trackings zahlreichen Änderungen. In vielen Fällen sind Anpassungen notwendig, um auch in Zukunft die korrekte Messung der Werbeleistung im Online-Marketing gewährleisten und so eine sinnvolle Steuerung der Ausgaben erzielen zu können.

Die hier vorgestellten technischen Prozesse und Verfahren wurden streng nach den aktuell geltenden Gesetzgebungen und Urteilen ausgewählt, wobei auch erst zukünftig in Kraft tretende Gesetze und Regelungen berücksichtigt wurden. Insbesondere sind hier die seit 2018 geltende Datenschutz-Grundverordnung (DSGVO), das Urteil zu Planet49 sowie das am 01. Dezember 2021 in Kraft getretene „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien“ – kurz TTDSG – berücksichtigt. Eine rechtliche Einordnung oder Bewertung findet in diesem Kompendium nicht statt. Diese wurde bereits in einem gesonderten Leitfaden erarbeitet: „Rechtliche Grundlagen der Attribution im Affiliate-Marketing unter TTDSG und DSGVO“. Da die in diesem Kompendium beschriebenen technischen Prozesse und Verfahren in einem Gesamtkontext mit dem jeweiligen Shopsystem und den verwendeten Affiliate- und Tracking-Systemen stehen, bedarf es ggf. einer rechtlichen Individualprüfung.

Einige der in diesem Kompendium beschriebenen technischen Prozesse und Verfahren erfordern das Einverständnis für die Erhebung und Verarbeitung von personenbezogenen Daten oder das Schreiben oder Lesen von Informationen auf dem Endgerät des Endverbrauchers. In vielen Fällen werden diese Einverständniserklärungen durch Consent-Management-Plattformen, kurz CMPs, erhoben, verarbeitet und weitergegeben. In diesem Dokument wird auf das Zusammenspiel dieser Systeme mit den Trackingverfahren eingegangen, jedoch nicht auf die rechtlichen Voraussetzungen von Consent-Verfahren.

Dem Anstieg der Anforderungen an den Datenschutz im Digital-Marketing folgen auch die Browserhersteller, teilweise sogar im vorauseilendem Gehorsam, und bieten dem User unterschiedliche automatisierte Schutzmechanismen sowie manuelle Einstellmöglichkeiten. Apples Safari ITP, ETP von Firefox, Samesite oder auch die von Google angekündigte vollständige Unterbindung von Drittanbieter-Cookies (Third Party Cookie) gehören dazu. Einige dieser Funktionen haben direkten Einfluss auf das Tracking und gehen dabei teilweise über die gesetzlichen Anforderungen hinaus. Darum werden hier Prozesse und Verfahren beschrieben, um mit diesen Entwicklungen Schritt zu halten.

Dieses Kompendium richtet sich an Marketer, Techniker und Datenschützer aller Player der gesamten Affiliate- und Performance-Branche. Es bietet einen Überblick über aktuelle sowie zu erwartende Entwicklungen und gibt klare Handlungsempfehlungen für Tracking-Prozesse und -Verfahren. Darüber hinaus wird auf klassische Fehler und Missverständnisse hingewiesen sowie Best Practices im Hinblick auf Consent-Management, Datenschutz und Tracking aufgezeigt.

Berlin, im Juni 2022

Grundlagen und Bausteine – die Technik im Hintergrund

Speicherverfahren

Zur Leistungsmessung müssen beim Klick des Users auf das jeweilige Werbemittel grundlegende Daten vom Affiliate-System erhoben und gespeichert werden, so dass eine Zuordnung der späteren Transaktion auf den Online-Marketing-Kanal, den Publisher oder dessen Werbefläche möglich ist.

Für die korrekte Zuordnung müssen diese Daten zum Zeitpunkt der Transaktion (Lead, Sale, Basket) verfügbar sein oder dem System vom Shop oder von dessen Trackingweiche übermittelt werden. Anhand dieser Informationen ermittelt das System den Online-Marketing-Kanal, den Publisher und die Werbefläche, welche die Werbeleistung erbracht hat, und verknüpft diese Information mit der Transaktion für eine spätere Auswertung oder Vergütung.

Für die Speicherung und Weitergabe an den Advertiser beim Klick eines Users auf ein Werbemittel gibt es zwei grundlegende Möglichkeiten: Die Daten werden entweder in einer Click-ID zusammengefasst oder in mehreren einzelnen Parametern übergeben.

Daten

Während des Trackingprozesses werden unterschiedliche Informationen zu verschiedenen Zwecken erhoben und verarbeitet. Die folgende Tabelle gibt einen Überblick über die gängigsten Parameter. Abhängig vom Anwendungsfall können weitere Daten benötigt werden.

Parameter	Beschreibung	Ort	Zweck
Click-ID/ Action-ID	Eindeutige ID des Klicks; wird vom System erzeugt (Primärschlüssel)	Klick	Attribution
View-ID	Alternative zur Click-ID beim Post-View-Tracking (Primärschlüssel)	View	Attribution
Session-ID	eindeutige ID der Session, dient der Verknüpfung des Klicks und mit der Session nach Einverständnis	Klick	Attribution (verfällt, wenn kein Einverständnis gegeben wird)
Campaign-ID / Kampagnen-ID / Advertiser-ID	Eindeutige Identifikation der Kampagne, des Partnerprogramms	Klick / Transaktion	Attribution
Projekt-ID / Partner-ID / Publisher-ID	Identifikation des Partners oder Kanals	Klick	Attribution
Sub-IDs	Ergänzende ID, welche vom Publisher genutzt wird, um seine Kanäle oder auch User zu identifizieren, z.B. für Cash-back-Programme oder Meta-Netzwerke	Klick	Attribution für bestimmte Publisher-Modelle
Timestamp	Zeit, in der der Klick oder die Transaktion stattgefunden hat	Klick / Transaktion	Attribution
Produkt- und Warenkorbdaten	Art und Wert der Bestellung	Transaktion	Attribution und Berechnung der Provision
Fingerprint-Daten	Diverse Informationen zu Device und Browser	Klick	Attribution optional bei Finger-print-Tracking
Advertising-ID	Eindeutige Device-ID bei Mobile-SDKs	Klick	Attribution optional bei Mobile- oder Cross-Device-Tracking
Browser-ID	Unique ID des Browsers, falls Cross Device	Klick	erweiterte Attribution
Consent-Daten	Informationen zum Einverständnis des Nutzers	Klick / Transaktion	Daten- und Nutzerschutz
Referrer	URL der vorherigen Seite	Klick	Betrugserkennung
IP-Adresse	Eindeutige ID des Nutzer-Gerätes, welche auf das Länderkürzel reduziert wird. Hierüber kann nachträglich keine Benutzerkennung mehr stattfinden.	Klick	Betrugserkennung
Browser	Browsername und Version	Klick	Qualitätssicherung
Device	Gerät und Betriebssystem	Klick	Qualitätssicherung
Ad-ID / Werbemittel-ID	Art und Größe des Werbemittels	Klick	Analyse
Deeplink	URL der Zielseite	Klick	Analyse

Click-ID (Primärschlüssel)

Bei jedem Klick eines Users auf ein Werbemittel wird vom Affiliate-System eine eindeutige ID erstellt. Diese identifiziert u.a. den jeweiligen Werbekanal, den Publisher und die Werbefläche. Detailinformationen zum Klick werden in der Datenbank des Affiliate-Systems gespeichert und der ID zugeordnet. Die ID kann über verschiedene Methoden gespeichert oder an den Shop des Advertisers übergeben werden. Erfolgt im Anschluss des Klicks eine Transaktion, so wird diese der ID zugeordnet und der Werbekanal, der Publisher sowie die Werbefläche können in der Attribution berücksichtigt werden.

Direkte Weitergabe der Werte (gehasht/ ungehasht)

Alternativ zur Click-ID können die für die Attribution notwendigen Informationen auch vollständig an den Advertiser übergeben werden. Dies kann gehasht oder ungehasht erfolgen. Ungehasht sollten die Daten dabei nur im grundlegendsten Fall einer reinen Weitergabe von Werbeflächen-ID, Programm-ID und Werbemittel-ID verarbeitet werden.

Conversion-Daten

Von einer Conversion oder auch Transaktion spricht man, wenn das provisionsauslösende Ereignis eingetreten ist, z.B. eine Online-Anmeldung abgeschlossen oder eine Bestellung getätigt wurde. Um auf dieser Basis den Publisher vergüten zu können, müssen Informationen zur Transaktion übermittelt werden.

Hierbei wird zwischen drei Arten unterschieden:

1. **Lead**
   Unter einem Lead versteht man die Transaktion eines potenziellen Kunden oder Interessenten. Dies kann eine Registrierung, ein Vertragsabschluss, eine Anmeldung zum Newsletter, ein Download oder eine Installation sein. Im Finanzwesen ist ein Lead das erste Ausfüllen eines Antrages. Hier wird oft ein zweistufiges Lead-Sale-Modell eingesetzt, in dessen Verlauf ggf. auch zwei Provisionen generiert werden können.

2. **Sale**
   Ein Sale ist ein Einkauf oder eine Bestellung. Vergütet wird dieser entweder über einen fixen Betrag, vergleichbar mit einem Lead-Modell, oder auf prozentualer Basis des Netto-Warenkorb-Wertes.

3. **Basket Sale**
   Bestellt der User mehrere Produkte innerhalb eines Warenkorbes, können die Art und Höhe der Provision für die einzelnen Produkte voneinander abweichen (z.B. Bekleidung = 10%, Elektronik = 5%). Um die einzelnen Werte berechnen zu können, wird beim Basket-Tracking jedes Einzelprodukt separat ans Netzwerk übergeben.

Je nach Art der Conversion (Lead / Sale / Basket) werden weitere Daten an das Netzwerk übermittelt:

- Zeitpunkt der Conversion
- Warenkorbdaten
  (Order-ID, Preis, Währung, Warengruppe, Provisionsgruppe, Produktinfos)
- Kundenart zur möglichen Differenzierung zwischen Bestands- und Neukunden
- Vouchercodes (siehe Vouchercode-Tracking)
- User Hash (siehe Cross-Device-Tracking)

Consent-Daten

Um das Einverständnis des Users zur Erhebung und Speicherung von personenbezogenen Daten – im Rahmen der DSGVO oder im Fall der Speicherung von Informationen auf dem Device des Users unter Beachtung des TTDSG – verarbeiten und anderen Parteien zur Verfügung stellen zu können, müssen diverse Daten erhoben werden. Hierzu gehören z.B. Zeitpunkt und Ort des Einverständnisses, der Zweck der erlaubten oder untersagten Verarbeitung sowie die konkrete Erlaubnis oder Untersagung der Speicherung von Cookies o.Ä. Die Erhebung dieser Informationen erfolgt in der Regel durch eine Consent-Management-Plattform (CMP). Die Übergabe der Informationen kann einzeln oder unter Verwendung eines Consent-Strings (siehe Kapitel: TCF-String-Protokoll) erfolgen.

Speicherarten

Für das Speichern gibt es sowohl persistente als auch nicht persistente Lösungswege. Persistent ist ein Lösungsweg dann, wenn die Informationen nach vollständiger Beendigung und Wiederaufnahme einer neuen Browser-Session hinaus weiterhin verfügbar sind. Da im Tracking die Persistenz eine wichtige Rolle spielt, werden im Folgenden die gängigsten Methoden des persistenten Speicherns kurz erläutert.

Cookie

Die bisher gängigste Methode für das persistente Speichern sind http-Cookies. Beim Klick auf ein Werbebanner werden diese beim User gespeichert und auf der Bestellabschlussseite ausgelesen. Beim Setzen und Auslesen eines Cookies spielen folgende Eigenschaften eine tragende Rolle, da Browser-Regulierungen Cookies mit bestimmten Eigenschaften blockieren bzw. deren Laufzeiten ändern können (siehe Anhang: Kapitel Browser-Regulierungen):

- **First-Party vs. Third-Party**
  Das First-Party-Cookie wird entweder vom Advertiser-System selbst oder über eine Subdomain des Advertisers, die auf ein anderes System, wie z.B das Affiliate-Netzwerk routet, gesetzt. Die Top-Level-Domain, über die das Cookie gesetzt wurde, gleicht also der Top-Level-Domain der Landingpage des Shops, auf welcher sich der User nach dem Klick auf ein Werbemittel befindet. Von Third Party wird gesprochen, wenn sich die Top-Level-Domain von Cookie und Shop unterscheiden. In dem Fall wurde das Cookie nicht vom Shop, sondern über ein anderes System wie beispielsweise das Affiliate-Netzwerk gesetzt.

  Beispiel First-Party:
  Cookie-Domain: https://tracking.shop.de
  Shop-Domain: https://www.shop.de

  Beispiel Third-Party:
  Cookie-Domain: https://tracking.netzwerk.com
  Shop-Domain: https://www.shop.de

- **JavaScript (clientseitig gesetzt) vs. HTTP-Header-Cookie (serverseitig gesetzt).**
  (siehe Anhang: Kapitel Browser-Beschränkungen, s. Safari)

- **„HTTP only“ Flag**
  (Cookie kann nicht clientseitig gelesen werden)

- **Secure vs. Non Secure Flag**
  (siehe Anhang: Kapitel Browser-Beschränkungen, s. Google Chrome)

- **SameSite Flag**
  (siehe Anhang: Kapitel Browser-Beschränkungen, s. Google Chrome)

Je nachdem, welche Eigenschaften das Cookie am Ende besitzen soll, kann es beim Klick entweder während oder nach dem Redirect auf die Landingpage gesetzt werden. Third-Party-Cookies können beispielsweise in einem Zwischen-Redirect auf das Netzwerksystem gesetzt werden. First-Party-Cookies werden in den meisten Fällen nach dem Redirect gesetzt. Die Landingpage-URL erhält GET-Parameter mit den Tracking-Informationen, welche entweder clientseitig über JavaScript ausgelesen und im Cookie gespeichert (dies kann z.B. über das Master-Tag des Netzwerks geregelt werden) oder serverseitig vom Advertiser-System selbst verarbeitet werden. CNAME- oder A-Record-Routings vom Advertiser zum Netzwerk ermöglichen es, dass auch das Netzwerk serverseitige First-Party-Cookies auf die Advertiser-Domain setzen kann. Dies ist sowohl als Zwischen-Redirect als auch auf der Advertiser-Seite nach dem Redirect möglich. (Siehe Anhang: Kapitel Codebeispiele, Es wird ein einfaches PHP-Script-Beispiel beschrieben, das zeigt, wie ein serverseitiges First-Party-Cookie gesetzt werden kann.)

Hat das Cookie kein Ablaufdatum gespeichert, handelt es sich um ein nicht persistentes Session-Cookie. Es wird nach vollständiger Beendigung der aktuellen Browser-Session (i. d. R. Schließen des Browserfensters) gelöscht.

Local Storage

Statt in einem Cookie können die benötigten Daten auch im Local Storage des Browsers abgelegt werden. Auf diesen lässt sich nur via JavaScript zugreifen, weshalb die Speicherung nach dem Redirect auf der Advertiser-Seite stattfinden muss. Das Auslesen auf der Checkout-Seite findet ebenfalls via JavaScript statt. Laufzeiten können dem Local Storage nicht mitgegeben werden. Um ein im Netzwerk hinterlegtes Ablaufdatum einzuhalten, kann jedoch ein zweiter Eintrag im Local Storage mit einem Timestamp angelegt werden. Analog zum Cookie wird auch die Speicherung im Local Storage durch Browser-Regulierungen eingeschränkt.

Browser-Cache

Der Browser-Cache dient üblicherweise Performance-Zwecken. Fragt der Browser eine Ressource des Webservers an, wird diese vom Server zurückgesendet. Der Browser kann die Ressource anschließend im Cache ablegen und muss sie bei wiederholten Aufrufen nicht erneut vom Webserver abrufen. Der Browser-Cache lässt sich jedoch auch für das Tracking nutzen. Ein Beispiel hierfür ist das ETag-Tracking (siehe Kapitel: Trackingverfahren).

Nicht persistent lassen sich die benötigten Daten in der Session speichern, indem sie beispielsweise als URL-Parameter auf der Landingpage weitergegeben werden.

Übertragungsarten

Eine Conversion kann auf zwei grundsätzlichen Wegen an das Netzwerk übermittelt werden: vom Device des Users (clientseitig) oder vom Server des Shops (serverseitig).

Clientseitig

Der Conversion-Code des Netzwerks ist direkt in den Quellcode der Abschlussseite eingebunden. Der Aufruf erfolgt so immer in Echtzeit. Die direkte Einbindung ermöglicht es dem Netzwerk, auf Cookies und den Local Storage zurückzugreifen, hat aber den Nachteil, dass die Aufrufe beispielsweise durch Adblocker oder Browser-Einschränkungen unterbunden werden können.

- JavaScript
  Ein JavaScript-Schnipsel oder eine externe Scriptquelle des Netzwerks ist in der Abschlussseite eingebaut. Das Script greift dann auf eine oder mehrere Methoden zurück, um die Conversion an das Netzwerk zu senden.

- Pixel
  Ein HTML-Image-Tag ist direkt als „Pixel“ in den Quellcode der Abschlussseite eingebunden. Meist dient diese Art der Einbindung als Fallback, um auch dann tracken zu können, wenn Browser oder Server den Aufruf von externen Script-URLs blockieren oder ein Endnutzer die Nutzung von JavaScript deaktiviert hat. Da die Einbindung unabhängig von JavaScript erfolgt, muss der Aufruf bei Consent-Managern oder Trackingweichen separat berücksichtigt werden.

Serverseitig

Die Conversion wird in Echtzeit oder zeitverzögert direkt vom Server des entsprechenden Advertisers an das Netzwerk gesendet. Browserseitige Einschränkungen werden somit komplett umgangen. Die Einbindung per Server-to-Server-Aufruf hat den Vorteil, dass sie unabhängig von Browser oder Endgerät funktioniert. Der Advertiser sendet dabei die für die Zuordnung benötigten Daten, so dass ein Aufruf sowohl synchron als auch asynchron möglich ist. Die Übermittlung erfolgt entweder über einen HTTP-Request (Pixel) oder an eine API des Netzwerks (siehe Kapitel: Welche Daten werden beim Klick gespeichert?).

Consent-Verfahren und -Übergaben

Das am 01. Dezember 2021 in Kraft getretene „Gesetz zur Regelung des Datenschutzes und des Schutzes der Privatsphäre in der Telekommunikation und bei Telemedien (TTDSG)“ verlangt unter anderem die Einwilligung durch einen Nutzer, wenn eine Speicherung von Informationen auf dessen Endgerät oder der Zugriff auf Informationen, die bereits im Endgerät gespeichert sind, erfolgt.

Durch das Zusammenspiel von Publisher, Advertiser und Netzwerk im Affiliate-Marketing stellt sich die Herausforderung, an welcher Stelle die Einwilligung durch den User erfolgen muss, um die notwendige Erfolgsmessung gewährleisten zu können. Im Gegensatz zu dem Regelfall, bei dem die Einwilligung mit dem Setzen eines Cookies durch den Verwender erfolgt, ist grundsätzlich auch die Einholung der Einwilligung durch einen Dritten möglich. Dabei muss gewährleistet sein, dass der Verwender die Informationen zur Einwilligung durch den User erhält.

Im Folgenden werden die für das Affiliate-Marketing wichtigen Szenarien beschrieben. Zudem wird aufgezeigt, an welcher Stelle der Consent eingeholt werden muss.

Weitere Informationen zu den „Best Practice Consent-Abfrage“ sind im Paper „Einwilligungsmanagement – Consent-Management in der Praxis“ der Arbeitsgruppe Consent Management im BVDW-Ressort Data Economy zu finden:

https://www.bvdw.org/der-bvdw/news/detail/artikel/bvdw-veroeffentlicht-leitfaden-zum-einwilligungsmanagement/

Der Publisher holt den Consent für das Netzwerk ein

Die Einwilligung für das Setzen eines Cookies durch das jeweilige Affiliate-Netzwerk erfolgt hier bereits bei dem Besuch der Website eines Publishers. Die Einwilligung kann an dieser Stelle über dessen CMP stattfinden. Dabei muss sichergestellt sein, dass die Informationen über die Einwilligung durch ein Consent-Signal an das Affiliate-Netzwerk weitergegeben werden. Ob der Affiliate-Publisher zur Einholung des Consents verpflichtet ist, muss individuell auf Basis der entsprechenden Vertragsbedingungen durch das Affiliate-Netzwerk (Publisher-AGB) geprüft werden.

Der Advertiser holt den Consent für das Netzwerk und für sich selbst ein

Es sind mehrere Szenarien möglich, die das Einholen des Consents durch den Advertiser für sich selbst oder für das jeweilige Affiliate-Netzwerk erfordern. Wird im Redirect durch das Netzwerk kein Cookie abgelegt, sondern lediglich eine Click-ID als GET-Parameter angehängt, welche im Online-Shop des Advertisers gespeichert werden muss, bedarf es der Abfrage einer Einwilligung durch den Advertiser für ein eigenes Cookie. Wird ein Skript des Affiliate-Netzwerks geladen, das Informationen aus dem Endgerät des Nutzers ausliest oder ein Cookie schreibt, muss ebenfalls der Consent über die CMP des Advertisers abgefragt werden. In diesem Fall erfolgt wiederholt die Einholung des Consents durch einen Dritten, wobei die Übergabe der Einwilligung des Nutzers an das Affiliate-Netzwerk sichergestellt sein muss.

Ausnahmen in Bezug auf die Abfrage der Einwilligung im Kontext Affiliate-Marketing ergeben sich bei einzelnen Publisher-Modellen wie bspw. Cashback und Loyalty (siehe Kapitel: Sonderfälle).

Consent-Übergaben

Die Informationen über den Umfang des Consents, den der User gegeben hat, bezeichnet man als Consent-Signal. Hier wird festgehalten, wann der User welchen Zwecken der Datenverarbeitung zugestimmt hat bzw. wofür eine Ablehnung erfolgte. Das Consent-Signal wird von der Consent-Management-Plattform an alle beteiligten Parteien weitergegeben. Hierüber kann der jeweilige Partner auslesen, welche Art der Einwilligung er vom User erhalten hat, und etwaige Restriktionen entsprechend berücksichtigen.

Die Signale können auf unterschiedliche Weise übergeben werden. Entscheidend ist jedoch, dass alle Beteiligten die Informationen richtig lesen und interpretieren können.

Das TCF-String-Protokoll im Kontext des TCF 2.0 des IAB Europe

Bei der Signalübergabe über das TCF-String-Protokoll auf Basis des TCF 2.0 des Interactive Advertising Bureaus EUROPE (IAB) wird ein standardisierter Consent-String generiert und an jede Routine in der Trackingkette angefügt, damit alle Vendoren innerhalb dieser Kette die Datenschutzeinstellungen des Nutzers berücksichtigen können. Der Consent-String ist eine gehashte Aneinanderreihung sämtlicher Einstellungen des Users, bestehend aus den Freigaben definierter Zwecke (Purposes) und den freigegebenen Vendoren. Alle am TCF teilnehmenden Vendoren müssen sich vorab registrieren lassen.

Um das TCF-Protokoll als Vendor für das eigene Consent Management verwenden zu können, in den Einstellungen der CMPs aufgeführt zu werden, die Signale zu erhalten und diese interpretieren zu können, ist es notwendig, sich beim IAB Europe über folgenden Link zu registrieren: https://iabeurope.eu/join-the-tcf/ Eine Registrierung als Vendor ist aktuell mit jährlichen Kosten von 1.500 EUR verbunden.

Seitenbetreiber, die über TCF nur den Consent für Drittdienstleister einholen, müssen nicht registriert sein. In diesem Fall genügt es, eine CMP zu nutzen, welche für TCF zertifiziert ist. Das TCF-2.0-Protokoll ist unter Publishern mittlerweile zu einem Standard avanciert und kommt insbesondere bei Display-Publishern zum Einsatz, um den Consent an unterschiedliche Vendoren wie Adserver, DSP, Affiliate-Netzwerke oder Trackinglösungen weiterzugeben. Hierzu werden drei GET-Parameter verwendet, die die Erlaubnis des Schreibens oder Auslesens von Cookies und anderen Speichermethoden steuern, indem sie an die URLs der Tracking-Routinen angefügt werden:

gdpr=0/1

Dieser GET-Parameter steuert, ob ein User der DSGVO unterliegt. Ist dieser Parameter gleich 1, so muss der Consent-String zwingend interpretiert werden.

gdpr_pd=0/1

Dieser teils optionale Parameter steuert, ob persönliche Daten im Sinne der DSGVO übertragen werden.

gdpr_consent=CONSENT_STRING

Dieser Parameter ist eine encodete Zeichenkette, welche entschlüsselt ein JSON-Objekt darstellt. In dieser Zeichenkette lassen sich die einzelnen Purposes und der Status der Erlaubnis durch den User sowie die erlaubten Vendoren in Form von Vendor-IDs ablesen.

Beispielstring (encodiert)

COvFyGBOvFyGBAbAAAENAPCAAOAAAAAAAAAAAEEUACCKAAA.IFoEUQQgAIQwgIwQABAEAAAAOIAACAIAAAAQAIAgEAACEAAAAAgAQBAAAAAAAGBAAgAAAAAAFAAECAAAgAAQARAEQAAAAAJAAIAAgAAAYQEAAAQmAgBC3ZAYzUw

Beispielstring (decodiert)

Der Beispielstring kann hier decodiert werden: https://www.consentstringdecoder.com
Nach dem Decoding dieses Strings zeigt sich, dass die Purposes 1-3 alle erlaubt wurden. Zu erkennen sind außerdem die einzelnen Vendor-IDs, die Cookies für die genannten Purposes setzen dürfen.

Ein Beispiel:

Die Vendor-ID 123 benötigt die Erlaubnis für die Purposes 1, 4 und 7 (Informationen auf einem Gerät speichern und/oder abrufen, personalisierte Anzeigen und Anzeigenmessung). Daher darf dieser Vendor ein Cookie nur dann zu diesem Zweck ausgeben oder auslesen, wenn die Purposes 1, 4 und 7 im dekodierten TCF-String unter „purposeConsents“ auf „true“ stehen und wenn er unter „vendorConsents“ mit „true“ aufgeführt ist.

Ist eine der beiden Voraussetzungen nicht gegeben, darf der Vendor mit der ID 123 keinerlei Cookies oder ähnliche Technologien nutzen, um auf dem Rechner des Endnutzers zu schreiben. Ein Tracking ist unter diesen Umständen also nicht erlaubt.

Für das TCF-2.0-Protokoll existieren einige Standard-Programmbibliotheken zum Decodieren des TCF-Strings, welcher als GET-Parameter an jeden Vendor in der Tracking-Kette angefügt wird. Es folgen einige Beispiele:

- **PHP / composer:** https://packagist.org/packages/dynata/iabtcf
- **Node / npm:** https://www.npmjs.com/package/@iabtcf/core
- **Java:** https://github.com/InteractiveAdvertisingBureau/iabtcf-java
- **Python:** https://github.com/gguridi/iab-tcf

Eine Einbindung der TCF-Signalübergabe sowie -Interpretation ist daher nicht mit viel Aufwand verbunden, muss aber gründlich getestet werden.

Eine weniger technische Beschreibung des TCF 2.0 gibt es hier: https://iabeurope.eu/tcf-2-0/

Eine genaue Erläuterung des – sich stets weiterentwickelnden – TCF-2.0-Protokolls kann bei Github abgerufen werden: https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework

Die generelle Erläuterung seitens des IAB zum TCF ist hier zu finden:
https://iabeurope.eu/iab-europe-transparency-consent-framework-policies/

NonTCF

Grundsätzlich ist es auch möglich, die Signalweitergabe ohne das Standardverfahren TCF anzustoßen. Diese ist dann allerdings nicht standardisiert und muss von Publisher und Affiliate-System im Vorfeld abgestimmt werden.

Die Weitergabe an das Affiliate-Netzwerk kann beispielsweise mit abgestimmten Zeichenketten via Data Layer oder GET-Parameter erfolgen.

Beispiel Awin:

GET-Parameter:
„&cons=[0/1]“

Awin Advertiser Master Tag Data Layer:
„AWIN.Tracking.AdvertiserConsent = [false/true]“

Beispiel communicationAds (Advertiser & Publisher):
&ca_cnt=0/1

Beispiel retailAds (Advertiser & Publisher):
&ra_cnt=0/1

Beispiel lead-alliance (Advertiser & Publisher).
„&cons=0/1 (oder 2 für cashback-loyalty Publisher)“

Beispiel easy Marketing (Advertiser, Publisher und Trackingweichen)
„&consent=1“, „&cons=1“ oder „&co=1“

Trackingverfahren und Prozesse

Affiliate-Marketing ist People-Business – diese Beschreibung des Performance-Marketing-Kanals wird gerne auf Konferenzen und in Fachartikeln verwendet. Der Aussage liegt das besondere Zusammenspiel der bereits dargestellten Parteien Publisher und Advertiser sowie deren Agenturen und Netzwerken zugrunde. Vernachlässigt wird dabei jedoch die Bedeutung der Erfolgsmessung für den Kanal Affiliate-Marketing. Diese ist ebenfalls ein essenzieller Bestandteil, denn sie ermöglicht es, Interaktionen des Nutzers mit dem Online-Shop des Advertisers messbar zu machen. Im Folgenden werden unterschiedliche Verfahren vorgestellt, die übergreifend als Affiliate-Marketing-Tracking definiert werden.

Mit dem Tracking im Affiliate-Marketing zwingend verbunden ist die Zuordnung der Werbeleistung bzw. die „Wertung“ der einzelnen Touchpoints. An dieser Stelle sprechen wir von einer Attribution, die beispielsweise die Zuordnung einer Werbeleistung zu einem Werbekanal oder zu einem Affiliate-Publisher innerhalb eines Partnerprogramms ermöglicht. Vor allem in der heutigen Zeit, in der Kaufentscheidungen online immer komplexer und durch zahlreiche Touchpoints beeinflusst werden, zeigt sich die enorme Bedeutung einer vorher definierten Attributionslogik. Technisch umgesetzt wird diese Logik zumeist mit einer sogenannten Trackingweiche.

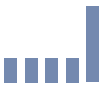
Alle im Folgenden dargestellten Affiliate-Tracking-Verfahren sowie die korrekte Attribution entsprechen dabei immer unserem Anspruch des sogenannten Data-light-Ansatzes (Datensparsamkeit). Dabei liegt der Fokus auf der Erhebung bzw. Verarbeitung nur derjenigen Daten, die unbedingt erforderlich sind, um abschließend die Attribution im Affiliate-Marketing technisch ermöglichen zu können.

Attribution

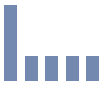
Der Zweck des Trackings ist die Zuordnung (Attribution) der Werbeleistung zu einer vom User durchgeführten Transaktion. Ein Attributionsmodell basiert auf einer Regel, einer Gruppe von Regeln oder einem datengetriebenen Algorithmus. Über diese Faktoren wird beispielsweise festgelegt, in welchem Umfang den verschiedenen Touchpoints in Conversion-Pfaden Conversions zugeordnet werden. Es gibt hier zwei grundlegende Modelle: regelbasierte Modelle und datengetriebene Modelle. In beiden Fällen kann Single- oder Multi-Attribution angewendet werden.

Regelbasierte Attributionsmodelle (statisch)

Bei regelbasierten Attributionsmodellen wird der Beitrag zu einer Conversion mithilfe fester Regeln ermittelt – unabhängig von Conversion-Typ und Nutzerverhalten.



Last Click:
Die Conversion wird dem letzten Klick zugeordnet.
Hierbei handelt es sich um die gängigste Attributionsmethode.



First Click:
Die Conversion wird dem ersten Klick zugeordnet.

Linear:
Der Beitrag der Conversion wird allen Klicks der Customer Journey gleichmäßig zugeordnet.

Zeitverlauf:
Je kürzer ein Klick vor der Conversion erfolgt, desto höher wird sein Beitrag zur Conversion eingestuft.

Positionsbasiert:
Die Conversion wird jeweils zu 40 % dem ersten und letzten Klick zugeordnet.
Die verbleibenden 20 % werden auf die anderen Klicks entlang des Pfads verteilt.

Datengetriebene Attribution (dynamisch)

Bei der dynamischen Attribution wird der Wert der Conversion basierend auf den erfassten Daten für jeden Conversion-Typ verteilt. Anders als bei den zuvor beschriebenen Modellen wird hier der Wert jedes Klicks anhand verschiedener Daten berechnet. Zugrundeliegende Faktoren sind beispielsweise die Reihenfolge der Klicks, die Zeit zwischen den Klicks, Produkte und Wertigkeiten sowie Nutzer- oder Kunden-Typ.

Jedes datengetriebene Modell wird an den jeweiligen Werbetreibenden und Conversion-Typ angepasst.

Single-Attribution

Einem Klick wird die Transaktion vollständig zugewiesen (z. B. Last Click oder First Click).

Multi-Attribution

Mehrere Klicks erhalten einen Anteil der Conversion (z. B. linear, nach Zeitverlauf oder positionsbasiert).

Sonderformen der Attribution

Im Affiliate-Marketing werden – neben den oben genannten „klassischen" – auch regelbasierte Attributionsformen auf dem jeweiligen Geschäftsmodell des Publishers angewendet. Hierbei wird dem User eine bestimmte Funktion zur Verfügung gestellt, die von ihm als Teil eines Dienstes des Anbieters ausdrücklich gewünscht wird.

- **Basket Freeze, beispielsweise für Gutschein-Publisher**
  Hat der User bereits Artikel in den Warenkorb gelegt, stellt jedoch im Warenkorb-Prozess fest, dass er die Möglichkeit hätte, einen Gutschein einzulösen, könnte es sein, dass er den Bestellvorgang kurzfristig unterbricht, um im Netz nach einem passenden Gutschein zu suchen. Arbeitet der Advertiser mit entsprechenden Gutschein- oder Deal-Seiten zusammen und wird der User fündig, könnte ein weiterer Klick erzeugt werden, der die spätere Transaktion auf den jeweiligen Publisher attribuiert, welcher aber faktisch keine oder nur eine geringe Werbeleistung erbracht hat. Um dies zu vermeiden, kann ein sogenannter Basket Freeze eingesetzt werden, der die Attribution stoppt, sobald der User Produkte in den Warenkorb gelegt hat.

- **Harte Attribution für Cashback- und Loyalty-Programme**
  Nutzer, die über ein Cashback- oder Loyalty-Programm in einen Shop gelangen, erwarten eine entsprechende Vergütung in Form einer Gutschrift oder eines Bonus, beispielsweise über ein Punktesystem. Erfolgt jedoch aufgrund zusätzlicher oder nachgelagerter Klicks eine Attribution auf andere Kanäle oder Publisher, müsste der User unter Umständen auf die Gutschrift oder die Bonuspunkte verzichten. Um dies zu vermeiden, kann die Attribution bei einem Klick von einem der Cashback- oder Loyalty-Partner so geregelt sein, dass sie zu 100 % dem besagten Kanal oder Publisher zugeordnet wird. Rechtlich besitzen diese Publishermodelle im Tracking eine Sonderstellung. Weitere Informationen hierzu finden Sie im Leitfaden „Orientierungshilfe: Rechtliche Grundlagen der Attribution im Affiliate Marketing unter TTDSG und DSGVO", Seite 14:
  https://www.bvdw.org/veroeffentlichungen/publikationen/detail/artikel/orientierungshilfe-rechtliche-grundlagen-der-attribution-im-affiliate-marketing-unter-ttdsg-und-dsg/

Click-ID-Tracking, Parameter-Tracking oder auch Session-Tracking

Beim Click-ID-Tracking generiert das Tracking des Netzwerks oder der Trackingweiche eine ID. Diese ID referenziert entweder auf Klickdaten in der Datenbank des Trackinganbieters oder beinhaltet direkt eine verschlüsselte Kombination mehrerer Parameter, die dazu ausreichen, auf den Klick und somit auf die Partnerschaft zu referenzieren. Für ein funktionierendes Performance-Tracking ist es unumgänglich, die ID nach einer Transaktion über das Conversion-Tracking inklusive der Informationen zu der Transaktion an das Netzwerk zurückzugeben. Diese ID muss vom Online-Shop des Advertisers gespeichert werden. Dies erfolgt entweder über ein First-Party-Cookie im Browser oder über den Advertiser. Die ID ist eine in der Regel nicht profilbildende, vom User losgelöste Zeichenfolge, welche ausschließlich Informationen über den Klick oder die Session wiedergeben kann. Ob die ID vom Client oder von einem Server des Advertisers zurück an das Netzwerk übermittelt wird, ist für die Technologie zunächst irrelevant. Beides ist möglich.

Container Tag

Der Begriff Container Tag – oder kurz: Container – steht bei der Verwaltung von Webseiten für wenige Zeilen JavaScript, die auf allen Seiten vorhanden sein müssen, um Funktionen, Skripte und weitere Container nachladen zu können. Dies hat den Vorteil, dass nach dem einmaligen Einbau durch einen Programmierer darauffolgende Änderungen dynamisch übernommen werden. Darunter fallen unter anderem Funktions-Updates des Anbieters oder die Auslieferung zusätzlicher Tags, Pixel oder Skripte. Als Beispiele für Container sind Tag-Manager, Tracking-Weichen, Netzwerk-Container oder Consent-Management-Container zu nennen.

In vielen Fällen existiert ein Webinterface, in dem sich Einstellungen, Regeln und Skripte verwalten lassen.

Container können darüber hinaus auch in einer Kaskade angelegt sein, also Elemente nachladen, die ihrerseits wieder Elemente nachladen.

Ein Beispiel: Der Google Tag Manager lädt einen Netzwerk-Container, der dann wiederum das Pixel eines Publishers lädt.

Im Affiliate-Marketing werden Container beispielsweise von Netzwerken oder Tracking-Weichen-Anbietern zur Verfügung gestellt.

Diese laden dann die für das Conversion-Tracking nötigen Funktionen, etwa für das Schreiben von Cookies oder die Übermittlung einer Conversion und deren Parameter.

Netzwerk-Container kommen auch bei der Auslieferung von Targeting-Skripten im Namen von Publishern zum Einsatz. Dies erleichtert dem Advertiser das Setup, wenn er die Absicht hat, mit einem zusätzlichen Targeting-Publisher zusammenzuarbeiten.

Landingpage-Tracking

Bei diesem Trackingverfahren wird auf der Landingpage ein Trackingcode implementiert, der die Traffic-Quelle identifiziert. Hierzu ist es notwendig, die Traffic-Quelle in der Landingpage-URL per GET-Parameter zu übergeben. Die Werte dieser GET-Parameter sind eindeutig und lassen sich einem Kanal oder einem Publisher direkt zuordnen. Des Weiteren können über die Parameter weitere Daten wie beispielsweise die Sub-ID übergeben werden, die im Tracking bei Bedarf wieder verwendet werden.

Diese Parameterübergabe, auch Link-Decoration genannt, wird mittlerweile von einigen Browsern für einzelne als „Cross Site Tracker for user [profile] tracking“ eingestufte Domains verhindert. Zudem ist der Browser technisch limitiert, was das Tracking an dieser Stelle erschwert. Trackinganbieter lösen das Problem durch stetige Weiterentwicklungen ihrer Tracking-Container.

Server-to-Server-Tracking

Das Server-to-Server-Tracking basiert in der Regel auf dem Click-ID-Tracking. Dabei wird die vom Netzwerk übermittelte Click-ID in einem First-Party-Cookie oder in der Session im Shop des Advertisers gespeichert und beim Checkout via API-Call, inklusive der für die Transaktion notwendigen Informationen, analog des clientseitigen Trackings an das Netzwerk übermittelt. Der daraus resultierende Vorteil ist, dass die Übermittlung der Bestell- und Klick-Informationen nicht mehr von den möglicherweise gegebenen Einschränkungen des Client-Browsers abhängig ist. Darüber hinaus kann bei einer asynchronen Implementierung gewährleistet werden, dass sich die Informationen beim Fehlschlagen der Übertragung (z. B. durch Ausfall einer der beiden Seiten) nachträglich erneut übermitteln lassen.

Wichtig: Ein serverseitiges Tracking ersetzt keine Datenspeicherung via Cookies oder anderer Technologien. Die ID muss meist auch beim serverseitigen Tracking gespeichert werden und unterliegt somit ebenso den Regeln des Consent-Managements.

Paralleles Tracking

Mit Hilfe dieser Trackingtechnologie ist es möglich, beim Klick des Publishers auf die Advertiser-Seite auf den Netzwerk-Redirect zu verzichten. Bei AWINs „Bounceless Tracking“ und vergleichbaren Technologien wird über ein Skript im sogenannten Publisher-Master-Tag der Redirect über die Click-URL entfernt und durch einen via Link-Decoration mit einer Click-ID versehenen Direktlink auf den Advertiser ersetzt. Auf diese Weise wird der User nicht mehr über einen Netzwerk-Link geleitet (Bounce, Redirect), sondern direkt auf die Advertiser-Seite. Parallel sendet der Browser im Hintergrund die Klick-Parameter über die Funktionen „Ping“ und „Beacon“ an das Netzwerk.

Diese Methode wird auch von Google für „Google Parallel Tracking“ zur Performancemessung angewandt.

Da diese Parallelfunktionen keine Cookies schreiben können, stehen sie bei den Browser-Herstellern nicht in der Profiling-Kritik, sondern werden für statistische Anwendungen sogar empfohlen.

Postview-Tracking

Die gängigsten Methoden, um die Werbewirksamkeit von Marketing-Kanälen oder Publishern zu bewerten, basieren auf den Klicks der User auf die Werbemittel der Advertiser.

In einigen Fällen ist es notwendig, den View, also die Betrachtung der Werbefläche, in die Attribution einzubeziehen. Hierzu wird bereits bei der Werbeeinblendung ein Cookie des Tracking-Systems (Affiliate-System sowie Trackingweiche, wenn vorhanden) gesetzt.

Besucht der User die Seiten des Advertisers zu einem späteren Zeitpunkt, wird er anhand des Cookies wiedererkannt und der View wird in der Attribution bewertet. View-Cookies besitzen in der Regel untergeordnete Wertigkeit, darüber hinaus ist ihre Haltbarkeit geringer und sie überschreiben in der Regel keine Click-Cookies.

Das Postview-Tracking beruht in der Regel auf den bereits stark eingeschränkten Third-Party-Cookies. Es existiert noch keine branchenweit etablierte und annähernd zuverlässige Nachfolgemethode für die Performance-basierte Attribution von Views.

App-Tracking

Da eine App bei iOS oder Android keinen Zugriff auf die Cookies des Browsers oder anderer Apps hat, ist es notwendig, auf ID-Tracking zu setzen. Hierbei muss die Click-ID vom Browser in die App übertragen werden. Um dies zu gewährleisten, kommen komplexe Tracking-Methoden zum Einsatz, da die Betriebssysteme nur rudimentär oder gar nicht in der Lage sind, die IDs in die Apps zu übertragen. Häufig erfolgt die Übertragung dieser Click-ID durch ein unbemerktes, schnelles Öffnen des Browsers über die App und den Redirect auf ein sogenanntes App-Callback. Die Click-ID wird dann einmalig in die App übertragen und dort für immer gespeichert. Im Falle eines Events (Install, Lead, Conversion oder andere Aktionen in der App) wird dann in der Regel ein Tracking-Callback zu einer App-Tracking-Software ausgeführt, der im Stile einer Trackingweiche das Event serverseitig an weitere Instanzen wie Affiliate-Netzwerke und andere Marketing-Kanäle verteilt. Firebase unterstützt diese Methodik ebenfalls. Bei Android kann das Tracking auch über das App-Tracking von Google Analytics ausgeführt werden.

Da dieses Verfahren sehr komplex ist und Änderungen an den Apps notwendig sind, die dann durch komplexe Review-Verfahren von den App-Stores genehmigt werden müssen, gibt es spezialisierte Tracking-SDK-Anbieter wie adjust.io, Appsflyer usw. Es empfiehlt sich, auf ein einheitliches Verfahren für alle relevanten Devices und somit auf einen etablierten Tracking-SDK-Anbieter (MMP) zu setzen, dessen SDK, ähnlich einem Container, nur einmalig integriert werden muss.

Cross-Device-Tracking

Um das Tracking über mehrere Geräte hinweg zu gewährleisten, kommt das Cross-Device-Tracking zum Einsatz. Hierbei wird beispielsweise der stationäre Rechner des Nutzers mit dessen Smartphone verknüpft. Dies erfolgt zumeist über IDs, welche sich von Device zu Device nicht ändern.

Ein klassisches Beispiel für ein Cross-Device-Kriterium ist eine Login-E-Mail-Adresse, die auf mehreren Devices genutzt wird. Die Login-ID oder -Mailadresse wird dabei zunächst am stationären Rechner gehasht, dann bei einem Klick an den Trackingcode übergeben und schlussendlich vom Tracking in einer Datenbank gespeichert. Sobald der User nun über ein Mobilgerät mit der gleichen gehashten ID eine Conversion auslöst, kann die Tracker-Datenbank beide Touchpoints demselben (aber keinem bestimmten) Benutzer zuordnen und die Sessions miteinander verknüpfen. Der Klick am stationären Rechner kann dann mit der Conversion am mobilen Gerät verbunden werden.

Die Nutzung pseudonymisierter Nutzer-IDs für solche Zwecke muss in der Regel in den AGB des Webseitenbetreibers aufgeführt werden. Auch dieses Tracking benötigt Cookies, so dass möglicherweise der Consent eingeholt werden muss.

Dieses Verfahren gilt es in allen von einem Advertiser verwendeten Trackinginstanzen (z. B. Trackingweiche und Affiliate-Netzwerk) zu gewährleisten, um ein erfolgreiches Tracking implementieren zu können.

Cookieless Tracking

Cookieless Tracking ist ein Oberbegriff über Technologien, welche vollkommen ohne das Setzen von Cookies oder ähnliche Methoden funktionieren. Dies lässt sich über eine Kombination aus Click-ID- und Server-to-Server-Tracking oder beispielsweise über Vouchercode-Tracking (siehe unten) realisieren.

Vouchercode-Tracking

Wenn ausschließlich über Vouchercodes getrackt werden soll, benötigt das Affiliate-System eine Liste an Vouchercodes inklusive einer Zuordnung zu den nutzenden Publishern. Im Falle einer Gutscheineinlösung wird dieser Vouchercode im Conversion-Tracking mittels Trackingcode übergeben. Das Netzwerk verknüpft den übermittelten Vouchercode dann im Hintergrund mit dem Publisher, um diesem die Conversion zuzuschreiben. So kann beim Checkout und bei der erfolgreichen Übermittlung des Vouchercodes über diese Liste attribuiert werden.

Fingerprint-Tracking

Unter Fingerprint-Tracking oder Fingerprinting versteht man eine Technologie, mit deren Hilfe so viele Informationen wie möglich über den Browser zu einem Fingerprint „vermischt" werden. Dabei werden Teile der IP-Adresse und des Nutzer-Agents sowie Daten aus den JavaScript-Objekten der Browser zu einem annähernd einzigartigen Fingerabdruck zusammengeführt. Da Daten zur Verwendung kommen, die sich vom Klick bis zur Conversion nicht ändern, kann dieser Browser anhand seines Fingerprints wiedererkannt werden. Ungenaue Fingerprints könnten jedoch dann entstehen, wenn beispielsweise zwei identisch konfigurierte Nutzer-Agents über die gleiche IP-Adresse surfen. Ein Beispiel aus der Praxis wäre ein Büro mit identisch konfigurierten Endgeräten. Darüber hinaus ändert sich der Fingerprint beispielsweise bei der Verwendung des Nutzer-Agents durch Versionsupdates, so dass sich das Fingerprint-Tracking nur für kurze Zeitspannen (Stunden bis Tage) nutzen lässt. Das Fingerprint-Tracking erreicht eine Genauigkeit von 90 %, d. h. über 90 % von ansonsten nicht trackbaren Conversions werden korrekt zugeordnet.

Auch Fingerprint-Tracking unterliegt dem Consent!

ETag-Tracking

Beim ETag-Tracking wird ein weiterer Header (ETag, Entity Tag) vom Webserver ausgeliefert und vom Browser gespeichert – jedoch nicht als Cookie oder als Local Storage, sondern im Cache des Browsers selbst. Ruft ein User eine Seite auf, hat der Tracking-Anbieter die Möglichkeit, für den User einen ETag-Header mit einer eindeutigen ID zu setzen. Schließt ein User seinen Browser und öffnet die Seite, beispielsweise mit neuer IP, wieder, wird die Seite aus dem Cache geladen und weist weiterhin den ETag mit derselben ID auf. Sobald der User die Seite ohne Cache aufruft (z.B. durch Leeren des Caches oder unter Verwendung eines Cache-Busters), wird der ETag verworfen und es können keine Rückschlüsse mehr auf die User-Session geführt werden. Da das Caching jedoch stark von Browseranbietern und Benutzereinstellungen abhängt, handelt es sich bestenfalls um eine unterstützende Trackingmethode.

Sonderfälle

Ohne Consent und Cookie innerhalb der Session

Eine Session beschreibt eine Reihe von Ereignissen, ohne dass der User zwischendurch das Browserfenster schließt. Innerhalb einer Session können Daten durch Weitergabe von URL-Parametern von Shopseite zu Shopseite vorgehalten werden, ohne auf dem Endgerät gespeichert werden zu müssen. Wendet man diese Verfahren für eine Click-ID, Publisher-ID oder Ähnliches an, ist ein Conversion-Tracking innerhalb derselben Session ohne Speicherung von Daten auf dem Gerät des Endnutzers möglich.

Abhängig von den für die eindeutige Kennung verwendeten Daten und der individuellen Auslegung der relevanten Gesetze kann es der Fall sein, dass dieses Tracking keinen Consent benötigt. Das Tracking und Zuordnen von Transaktionen über eine Session hinaus ist jedoch ohne Einverständnis des Nutzers nicht mehr erlaubt, da Daten gespeichert werden müssen. Weitere Informationen hierzu finden Sie im BVDW-Leitfaden „Orientierungshilfe: Rechtliche Grundlagen der Attribution im Affiliate Marketing unter TTDSG und DSGVO“.

Cashback-Loyalty-Ausnahme

Ausnahmen zur Einholung des Consents werden ebenfalls im TTDSG definiert. Dort ist unter anderem festgehalten, dass ein ausdrücklich gewünschter Telemediendienst durch den User keine Einwilligung erfordert. Dieser Anforderung werden im Rahmen des Affiliate-Marketings insbesondere die Publisher-Modelle Cashback und Loyalty gerecht. Die Publisher-Modelle schaffen Kaufanreize über eine Bonifikation in Form von Cashback- oder Bonuspunkten. Mit der Teilnahme drückt der User aktiv den Wunsch aus, nach Kaufabschluss einen Bonus zu erhalten, und nimmt hin, dass für die Zuordnung der Transaktion ein technisch erforderliches Cookie gesetzt werden muss. Insofern könnte an dieser Stelle von der Einwilligungspflicht zur Verwendung von Cookies abgesehen werden. Weitere Informationen hierzu finden Sie im BVDW-Leitfaden „Orientierungshilfe: Rechtliche Grundlagen der Attribution im Affiliate Marketing unter TTDSG und DSGVO“:

https://www.bvdw.org/veroeffentlichungen/publikationen/detail/artikel/orientierungshilfe-rechtliche-grundlagen-der-attribution-im-affiliate-marketing-unter-ttdsg-und-dsg/

Mindestanforderungen an ein Idealsetup aus technischer Sicht

Das Minimalsetup bezieht sich auf den Standardfall im Affiliate-Marketing, nämlich eine Journey von Klick zu Bestellabschluss, und hat als Ziel, eine möglichst vollständige Erfassung von vergütungsfähigen Sales und Leads zu garantieren, die den Publishern die Vergütung sicherstellt, den Advertisern das notwendige Vertrauen gibt und vor allen Dingen den Anforderungen und Herausforderungen des Datenschutzes gerecht wird. Ein möglichst zuverlässiges Tracking minimiert außerdem zeitaufwendige Beschwerden und Nachbuchungsanfragen bei einigen Publishermodellen.

Die hier ausgewählten Trackingmethoden ergeben sich aufgrund verschiedener technischer Einschränkungen aktueller Browser (siehe Anhang „Browserbeschränkungen im Detail“) und werden für ein reibungsloses Tracking in Kombination benötigt. Die folgenden Anforderungen sind deshalb als Mindestanforderung zu sehen:

First-Party-Tracking

Notwendig für ein reibungsloses Tracking ist der Einsatz von First-Party-Cookies und ähnlichen Techniken der Speicherung wie Local Storage. Third-Party-Technologien können aufgrund der bereits bestehenden technischen Einschränkungen in mehreren Browsern nicht mehr für Tracking empfohlen werden, sie werden allenfalls als Ergänzung empfohlen.

First-Party-Tracking bezeichnet das Speichern der trackingrelevanten ID beim Advertiser, welche zumeist durch einen Parameter an die Landingpage des Shops übergeben wird. Diese ID muss durch den Advertiser oder durch vom Affiliate-Dienstleister bereitgestellte Routinen First Party gespeichert werden. Das kann im Cookie, in der Sessiondatenbank, im Local Storage oder mittels anderen Technologien geschehen. Diese ID muss im Falle eines Leads oder eines Sales im Conversion-Trackingcode serverseitig und/oder clientseitig wieder angegeben werden.

Serverseitiges Tracking

Serverseitiges Tracking vermindert Verluste durch clientseitige Plugins, Tools, individuelle Einstellungen, Timeouts im Browser, Skriptfehler auf der Webseite und Security-Policy-Konfigurationsfehler auf dem Webserver. Als Empfehlung gilt, das serverseitige Tracking neben dem clientseitigen Tracking zu implementieren, um die technischen Verluste so gering wie möglich zu halten. Das serverseitige Tracking ist lediglich ein Aufruf einer API oder Tracking-URL im Hintergrund und somit einfach zu implementieren.

Zusammenfassung zur Mindestanforderung

Nur die Kombination zweier Trackingmethoden kann alle marktrelevanten Browser abdecken und bietet gleichzeitig Redundanz als Absicherung gegen technische Ausfälle. Die Fokusgruppe kommt zu dem Schluss, aufgrund obiger Vorgaben den Einbau je einer server- und einer clientseitigen Trackingmethode zu empfehlen. Die Affiliate-Netzwerke unterstützen hier mit einfachen Methodiken, so dass der Einbau einfach vonstattengeht. Die Speicherung der Klickdaten muss für beide mit Hilfe von möglichst voneinander unabhängigen First-Party-Cookies erfolgen, d. h. Cookies in der Domain des Shops. Die serverseitige Trackingmethode sollte ein First-Party-Cookie mit dem Flag „httponly“ oder eine alternative Safari-kompatible Methode verwenden, um das bestmögliche browserkonforme Tracking zu ermöglichen (siehe Anhang: Browser-Beschränkungen).Diese Anforderung wird erfüllt, sobald ein Anbieter eine eigene Trackingmethode mit First-Party-Cookies anbietet und zusätzlich serverseitiges Tracking ermöglicht.

Ausblick – so wird die faire Verteilung künftig gesichert

Das Blockieren der Third-Party-Cookies unter Privacy-Aspekten wird durch die Browser fortgeführt. Nach den Blocking-Maßnahmen in Apple Safari (ITP) sowie Mozilla Firefox (ETP) plant nun auch das Chromium-Projekt (u. a. Google Chrome und Microsoft Edge) das Blockieren von Third-Party-Cookies. Aus diesen Gründen werden von Browser- und Ad-Tech-Anbietern derzeit Alternativlösungen entwickelt, die in allererster Linie eine datenschutzkonforme Leistungsmessung sowie ein im Browser stattfindendes Targeting ermöglichen. Hierzu sind bereits jetzt vielversprechende Technologien in der Entwicklung, die laut den Anbietern sowohl den Datenschutz als auch die Industrieinteressen vollumfänglich berücksichtigen. Die wichtigsten Entwicklungen stellen wir hier vor.

Conversion Measurement API von Google

Um die Attribution eines Views oder eines Klicks zu einer Bestellung weiterhin zu ermöglichen, entwickelt das Konsortium derzeit die Conversion Measurement API. Mit einem HTML-Attribut an einem A-Tag wird es künftig möglich sein, in einem späteren Conversion-Event den Lead oder Sale im Browser zu speichern. Zeitgleich wird ein anonymes Zählpixel ohne Cookies vom Client an das Affiliate-System übergeben. Somit wird der Sale anonym im Netzwerk registriert, die Attribution zum Publisher allerdings im Browser gespeichert. In einem vom Browser festgelegten, zufälligen Intervall wird asynchron und anonym der sogenannte Conversion-Report an das Netzwerk geschickt. In diesem steht, verknüpft mit der Bestellnummer, der Quell-Publisher. Somit lässt sich die Attribution ohne Cookies und vollständig anonym durchführen. Heute unverzichtbare Warenkorbdaten wie Artikelinformationen, genauer Preis, Order-ID, Zeitpunkt des Einkaufs oder Warengruppe blieben jedoch in der Version des momentanen Entwurfs auf der Strecke.

Demo: https://peacock-demo-283822.nw.r.appspot.com/

Datenschutzkonforme Targeting-Technologien

Um das Targeting eines Nutzers für Display-Affiliate-Modelle künftig anonym und im Browser gestalten zu können, werden derzeit mehrere Technologien entwickelt, die im Browser ausgeführt werden und durch die ein Datenaustausch zu Drittparteien nicht mehr notwendig ist. Beispielsweise befindet sich eine Browser-Technologie namens „Topics“ in der Entwicklung, die das Targeting der User im Browser ermöglicht. Andere Technologien wie FLEDGE, die es ermöglichen sollen, bei Display-Publishern datenschutzkonform zu agieren, sind ebenso in der Entwicklung bzw. Erforschung. Hier lassen sich die Interessen des Nutzers im Browser erheben und speichern, um zielgerichtet Werbung ausspielen zu können. Die Browser übernehmen dann die Aufgabe der DSPs, die über Third-Party-Routinen bisher ein Profil des Nutzers auf einem Server erstellt haben. Solch eine Profilerstellung fällt in diesem Fall weg.

Konkret werden die Interessen eines Nutzers mittels einer Browser-API über JavaScript gesetzt. Sobald ein Interesse aus einem der oben genannten Systeme, z. B. über den Besuch einer Seite mit Affinität zu diesem Interesse, definiert werden kann, wird ein JavaScript-Befehl ausgeführt, um den User mit diesem Interesse im Browser und ohne Datenaustausch mit Dritten zu flaggen.

Mit der Einführung dieser Technologien werden keine Informationen mehr zu den Interessen des Nutzers auf den Servern der DSPs gespeichert. Auf diese Weise entfällt die Profilerstellung bei Drittanbietern, was den Datenschutz der User erhöht, da die Speicherung im Browser in einer anonymen Datenbank erfolgt, auf die ausschließlich der User Zugriff hat.

Dokumentation: https://github.com/WICG/floc, https://github.com/WICG/turtledove/blob/main/FLEDGE.md

Mit PARAKEET ist derzeit eine weitere vielversprechende, von Microsoft eingereichte Erweiterung der Browser im Gespräch, die ein datenschutzkonformes Benutzertracking ermöglicht. Über dieses eingereichte WICG-Proposal wäre es möglich, Retargeting, Lookalike-Targeting, In-Market-Targeting oder auch Contextual-Targeting durchzuführen.

Auch bei PARAKEET werden die Interessen und Retargeting-Marker im Browser des Nutzers gespeichert und Teile des Real-Time-Biddings in den Browser verlagert. Das hat zur Folge, dass diese Informationen nicht mehr in Third-Party-Systemen zu speichern sind, was den Datenschutz erhöht. Allein der Browser – und somit der User – besitzt die Kontrolle über die Daten und ist damit in der Lage zu steuern, wem er diese zur Verfügung stellt.

Technisch wird bei PARAKEET durch die Publisher-Website ein Bid-Request über JavaScript generiert. Der Browser sendet dann einen anonymisierten Bid-Request mit den Interessen des Nutzers, jedoch ohne Cookies oder Verwendung anderer Technologien, an die Ad Networks, bestehend aus SSP und DSP. Wie es auch beim aktuellen Mechanismus der Fall ist, geben diese in Echtzeit ein Gebot für den Bannerplatz ab. Anders als derzeit registriert dann jedoch der Browser, welches Gebot das höchste ist, und entscheidet somit auch, welcher Banner ausgeliefert wird.

PARAKEET gehört zu den vielversprechendsten Entwürfen, um Display-Publishern die Ausspielung weiterhin zu ermöglichen.

Dokumentation: https://github.com/WICG/privacy-preserving-ads/blob/main/Parakeet.md

Login-IDs

Als eine weitere Möglichkeit, den Wegfall von Third-Party-Cookies sowohl im Tracking als auch im Targeting zu kompensieren, dürften Login-IDs ebenfalls eine Rolle spielen.

Hierbei dient ein Identifier des Nutzers (in vielen Fällen die E-Mail-Adresse) als zentraler Login, der webseitenübergreifend genutzt werden kann. Die Einstellungen, die die Verarbeitung der Nutzerdaten betreffen, werden dabei zentral im Profil des Logins festgelegt und können dann von allen teilnehmenden Partnern genutzt werden. Somit lässt sich eine Erkennung des Nutzers bei allen Websites gewährleisten, bei denen der Login aktiv ist.

Aktuell sind diverse Anbieter mit derartigen Lösungen am Markt aktiv oder arbeiten an einer Umsetzung. Hier lohnt es sich, ein Auge auf die Entwicklungen zu haben – vor allem, weil davon auszugehen ist, dass es nicht „die eine" Lösung geben wird. Ein Zusammenspiel aus verschiedenen Anbietern dürfte vermutlich die sinnvollste Lösung sein, um eine bestmögliche Erkennung des Nutzers und damit die Gewährleistung des Trackings im Affiliate-Marketing zu ermöglichen. Ob dies auch eine Lösung für Publisher ohne Nutzerlogin sein kann – also abseits von News- und Informationsportalen –, ist noch fraglich.

Autorenverzeichnis

Armin Auber
Software Engineer, Lead-Alliance GmbH

Thomas Becker
Senior Technical Solutions Engineer, Awin AG

Cristian Bobocel
Senior Integration Manager, Webgains GmbH

Uwe Falke
Teamleiter Affiliate Marketing, diva-e Excellence Value GmbH,
stv. Vorsitzender der Fokusgruppe Affiliate Marketing im BVDW

Ralf Fischer
Gründer und Geschäftsführer, verticalAds Group GmbH

Marc Heß
Marc Heß, Senior Analytics & Tracking Specialist, wysiwyg* software design gmbh
(vormalig bei Artefact Germany GmbH)

André Koegler
Vorsitzender der Fokusgruppe Affiliate Marketing im BVDW

Mustafa Korkmaz
Software Engineer, Artefact Germany GmbH

Benedikt Schimmel
Head of Media Buying, Oliro GmbH

Daniel Steinweg
Head of IT-Operations, easy Marketing GmbH

Julian Weiß
Teamleiter Affiliate Marketing, xpose360 GmbH

Markus Wigbels
Gründer und Geschäftsführer, easy Marketing GmbH

Anhang

Browserbeschränkungen im Detail

Um den User vor unerwünschten Tracking- und Targeting-Verfahren zu schützen, wurden bereits vor vielen Jahren technische Funktionen zum Steuern und Blockieren dieser Verfahren in die Browser implementiert. Zunächst begann man damit, Drittanbietercookies zeitlich einzuschränken. Schon bald wurden diese Einschränkungen jedoch sukzessive weiter ausgebaut. Während die ersten Schritte nur eine zeitweise oder explizit vom User zu setzende Beschränkung darstellten, wurden diese Beschränkungen weiter verschärft und sind mittlerweile Standard. Welche Browser welche Beschränkungen aufweisen, wird im Folgenden näher beschrieben:

Google Chrome

Chrome behandelt seit Februar 2020 Cookies, deren SameSite Flag beim Setzen nicht explizit deklariert wurde. als SameSite=Lax. Mit dieser Eigenschaft kann ein Cookie nicht mehr im Third-Party-Kontext ausgelesen werden. Um dennoch ein Third-Party-Tracking zu ermöglichen, ist es obligatorisch, das SameSite Flag für jeden gesetzten Cookie explizit mit „none" zu deklarieren. Die auf diese Weise geflaggten Cookies müssen auch die Secure-Eigenschaft beinhalten. Dies beschränkt Third-Party-Cookie-Tracking auf https-Seiten. Das Drittanbieter-Tracking ist auf Chrome somit transparenter und lässt sich anhand von Cookie-Eigenschaften besser nachvollziehen.

Ursprünglich plante Google die standardmäßige Blockierung von Third-Party-Cookies im Chrome Browser ab 2022, jedoch wurde bereits eine Fristverlängerung bis mindestens 2023 angekündigt. Das Ende von Third-Party-Cookies ist jedoch fest beschlossen.

Weitere Infos gibt es unter:
https://blog.chromium.org/2020/02/samesite-cookie-changes-in-february.htm
https://www.chromium.org/updates/same-site

Apple Safari

Seit 2013 gibt es in Apples Safari-Browser Browserbeschränkungen, die das Third-Party-Tracking sowie seit 2017 Teile des First-Party-Trackings einschränken. Cookies, die von Third-Party-Anbietern gesetzt wurden, werden inzwischen komplett geblockt.

Ebenso geblockt werden Local-Storage-Einträge, die von Drittanbieter-Scripts gesetzt wurden. Auf diese Weise schränkt man ein Third-Party-Tracking in Apples Browser auf den mobilen Geräten sowie den Macs nicht nur ein – man verhindert es. Das betrifft derweil nicht nur die Safari-Browser, sondern mobil auch sämtliche Apps und alle anderen Browser, die auf einem iDevice installiert sind.

Es empfiehlt sich aufgrund der Einschränkungen durch ITP und der großen Marktmacht der Apple-Geräte, das Tracking auf ein modernes First-Party-Tracking umzustellen, wie es im Idealsetup in diesem Whitepaper beschrieben ist. Andernfalls ist das Tracking über Apple-Geräte nicht mehr möglich.

- First-Party-Cookies, gesetzt durch den HTTP-Header (Server), sind unbeschränkt.
- First-Party-Cookies, gesetzt durch JavaScript, werden nach 7 Tagen gelöscht.
- First-Party-Cookies, gesetzt durch JavaScript, werden nach 24 Stunden gelöscht, wenn der lokale Algorithmus (Häufigkeit, Redirects) eine Domain als Tracker identifiziert.

Die Einschränkungen im Detail:

ITP 2.1 https://webkit.org/blog/8613/intelligent-tracking-prevention-2-1/

ITP 2.2 Intelligent Tracking Prevention 2.2 | WebKit

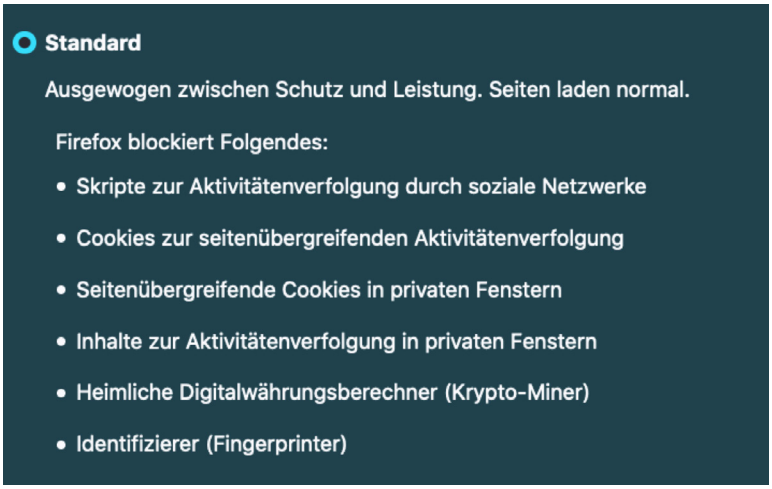
ITP 2.3 (Intelligent Tracking Prevention 2.3 | WebKit

ITP 2.4 Preventing Tracking Prevention Tracking | WebKit

Mozilla Firefox

Mit ETP (Enhanced Tracking Protection) ging Firefox bereits Mitte 2019 einen ersten Schritt in Richtung Blockieren von Cookies und schuf damit eine neue Dimension: Während zuvor das Blockieren von (potenziellen) Tracking-Cookies nur in privaten Sitzungen aktiv war, setzte ETP dies nun in der Standardinstallation um. Mittels Community-gepflegter „Trackerlisten" wurden Third-Party-Cookies von Domains geblockt, die als potenzielle Tracker gemeldet wurden.

Ein Jahr später hatte man die Maßnahme mit ETP 2.0 verschärft. Nun werden alle Cookies von gelisteten „Trackern" nach 24 Stunden geblockt, und zwar ergänzend zu ETP 1.0 nun auch während einer Redirect-Chain. Einzige Ausnahme bilden Domains direkt besuchter Webseiten – jedoch lediglich für 45 Tage.



Weitere Infos:

ETP https://blog.mozilla.org/press-de/2019/09/03/firefox-69-blockiert-standardmaessig-tracking-cookies-von-drittanbietern-und-cryptomining/

ETP 2.0 https://blog.mozilla.org/press-de/2020/08/04/firefox-fuehrt-verbesserten-tracking-schutz-2-0-ein-tracker-werden-standardmaessig-umgeleitet/

Microsoft Edge (Chromium Engine seit 2020)

Die „Tracking Prevention“ beruht, wie bei Firefox, auf einer Ausschlussliste bekannter Tracker des Community-gepflegten Anbieters disconnect.me. Das Lesen von Third-Party-Cookies für Domains aus der Blocklist ist gesperrt. Ausnahmen gelten für Cookies regelmäßig direkt besuchter Seiten, wie es bei Safari der Fall ist.

Opera

Seit Oktober 2019 stellt Opera seinen Tracker-Blocker im Easy-Setup-Menü zur Verfügung. Anhand einer Liste, die auf der Easyprivacy Tracking Protection List basiert, werden Tracker erkannt und gegebenenfalls blockiert. Der User kann einsehen, welche Aufrufe beim Besuchen einer Website blockiert wurden.

Tracker-Blocker https://blogs.opera.com/germany/2019/10/opera-browser-64-wird-dank-neuen-datenschutz-funktionen-fast-20-schneller

Codebeispiele

Setzen eines First Party-Http-Only-Secure-Cookies in PHP

```
//Aufruf: https://tracking.shop.net/setCookie.php?clickID=12345678
$ccname = 'clickID';
$clickID = $_GET[$ccname];
$cookieRuntime = 720 //in Stunden.. kann auch als url parameter übergeben werden
$cookieDomain = „shop.net“ //falls Wildcard Cookie auf Shopdomain
$options = ['expires' => time()+60*60*$cookieRuntime,
 'path' => '/',
 'domain' => $cookieDomain,
 'secure' => true,
 'httponly' => true, ];
 //sameSite Parameter kann leer gelassen werden, da sowieso 1st party Kontext
setcookie($ccname,$clickID,$options);
```

Auslesen des Cookies und anschließender Server2Server-Call in PHP

```
$clickcookiename = 'clickID';
$clickcookie = $_COOKIE[$clickcookiename] ?? „„;
//------------S2S call----------------------------
$url = „https://networkurl/networkconversion.php?clickID=„.$clickcookie;
$ch = curl_init($url);
 curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);
 curl_setopt($ch, CURLOPT_HEADER, 0);
 $data = curl_exec($ch);
 curl_close($ch);
```

Weitere Quellen

Cookie:
https://www.ionos.de/digitalguide/hosting/hosting-technik/was-sind-cookies/

First-Party vs. Third-Party:
https://piwikpro.de/blog/was-ist-der-unterschied-zwischen-first-party-cookies-und-third-party-cookies/

client- vs. serverseitig (HttpOnly Flag):
https://www.onlinesolutionsgroup.de/blog/glossar/c/cookie-set-without-httponly-flag/

Session-Cookie:
https://www.datenschutz.org/session-cookie/

SameSite-Attribut + Chrome-Änderung:
https://www.e-dialog.at/blog/webanalyse/alles-zur-chrome-samesite-cookie-aenderung/

Local Storage:
https://developer.mozilla.org/de/docs/Web/API/Window/localStorage

Weiterführende Whitepaper

BVDW: Leitfaden „Einwilligungsmanagement - Consent-Management in der Praxis
https://www.bvdw.org/veroeffentlichungen/publikationen/detail/artikel/leitfaden-einwilligungsmanagement-consent-management-in-der-praxis/

BVDW: Orientierungshilfe: Rechtliche Grundlagen der Attribution im Affiliate Marketing unter TTDSG und DSGVO
https://www.bvdw.org/veroeffentlichungen/publikationen/detail/artikel/orientierungshilfe-rechtliche-grundlagen-der-attribution-im-affiliate-marketing-unter-ttdsg-und-dsg/

BVDW: Durch Browser-Updates: Empfehlung zur Anpassung bestehender Tracking-Methoden
https://www.bvdw.org/der-bvdw/news/detail/artikel/durch-browser-updates-empfehlung-zur-anpassung-bestehender-tracking-methoden/

BVDW: Datenschutzkonformes Affiliate-Marketing – eine rechtliche Einordnung
https://www.bvdw.org/der-bvdw/news/detail/artikel/datenschutzkonformes-affiliate-marketing-1/

Easy-Marketing: Rechtssicheres Tracking im Affiliate-Marketing
https://easy-m.de/rechtssicheres-tracking-im-affiliate-marketing

Bundesverband Digitale Wirtschaft (BVDW) e.V.

Der Bundesverband Digitale Wirtschaft (BVDW) e.V. ist die Interessenvertretung für Unternehmen, die digitale Geschäftsmodelle betreiben oder deren Wertschöpfung auf dem Einsatz digitaler Technologien beruht. Als Impulsgeber, Wegweiser und Beschleuniger digitaler Geschäftsmodelle vertritt der BVDW die Interessen der digitalen Wirtschaft gegenüber Politik und Gesellschaft und setzt sich für die Schaffung von Markttransparenz und innovationsfreundlichen Rahmenbedingungen ein. Sein Netzwerk von Experten liefert mit Zahlen, Daten und Fakten Orientierung zu einem zentralen Zukunftsfeld. Neben der DMEXCO und dem Deutschen Digital Award richtet der BVDW eine Vielzahl von Fachveranstaltungen aus. Mit Mitgliedern aus verschiedensten Branchen ist der BVDW die Stimme der Digitalen Wirtschaft.

Fokusgruppe Affilliate Marketing

In der Fokusgruppe Affiliate Marketing im BVDW arbeiten Performance-Marketing-Agenturen, Technologie-Anbieter, öffentliche Netzwerke, Advertiser und Publisher zusammen.

Was tun wir

Austausch: Die Fokusgruppe Affiliate Marketing dient als Informations- und Austauschplattform für alle Marktteilnehmer – hier werden relevante und aktuelle Themen diskutiert.

Aufklärungs- und Öffentlichkeitsarbeit: Das Verständnis und die Wahrnehmung für Affiliate Marketing stärken. Hierzu treten wir auf „Non-Affiliate"-Veranstaltungen auf und positionieren uns in entsprechenden Fachmedien. Damit wird die gemeinsame Stimme der Fokusgruppe noch stärker in den Vordergrund rücken.

Standardisierung: Setzen von Standards innerhalb des Affiliate-Marketing-Kanals mit Hilfe von Selbstverpflichtungen, Zertifizierungen, Schulungen und Ausbildungsmöglichkeiten.

Mission Statement

Ein MUSS für jeden Online-Marketing-Mix
Das performancebasierte Abrechnungsmodell des Affiliate Marketings ist wichtiger denn je und hat insbesondere während der Corona-Pandemie dank seiner Plan- und Skalierbarkeit in erheblichem Maße an Bedeutung hinzugewonnen.

Schon seit jeher gekennzeichnet durch Innovationen, Vielfältigkeit sowie Flexibilität ist das Affiliate Marketing als attraktiver und gewinnbringender Online-Vertriebskanal bestens für die Zukunft gerüstet.

Höchste Priorität liegt dabei für die Branche auf datenschutzrechtlichen Rahmenbedingungen wie DSGVO über TTDSG bis hin zur ePrivacy-Verordnung sowie auf browsertechnischen Einschränkungen wie ITP, ETP und Googles Sandbox.

Der Grundgedanke der Mitgliedsunternehmen dieser Fokusgruppe basiert auf Fairness und dem Ziel, die Branche durch das Zusammenwirken von Advertisern, Publishern und Netzwerken weiterzuentwickeln und zu stärken.

Beteiligen auch Sie sich und gestalten Sie gemeinsam mit uns die Zukunft des Affiliate Marketings!

www.bvdw.org

Impressum

Leistungsmessung im Affiliate Marketing – Ein Kompendium

Erscheinungsort und -datum	Berlin, Juni 2022
Herausgeber	Bundesverband Digitale Wirtschaft (BVDW) e.V. Schumannstraße 2, 10117 Berlin, +49 30 2062186 - 0, info@bvdw.org, www.bvdw.org
Geschäftsführer	Sven Bornemann
Präsident	Dirk Freytag
Vizepräsidenten	Thomas Duhr, Anke Herbener, Corinna Hohenleitner, Dr. Moritz Holzgraefe, Alexander Kiock, Julian Simons
Kontakt	franke@bvdw.org
Vereinsregisternummer	Vereinsregister Düsseldorf VR 8358
Rechtshinweise	Alle in dieser Veröffentlichung enthaltenen Angaben und Informationen wurden vom Bundesverband Digitale Wirtschaft (BVDW) e.V. sorgfältig recherchiert und geprüft. Diese Informationen sind ein Service des Verbandes. Für Richtigkeit, Vollständigkeit und Aktualität können weder der Bundesverband Digitale Wirtschaft (BVDW) e.V. noch die an der Erstellung und Veröffentlichung dieses Werkes beteiligten Unternehmen die Haftung übernehmen. Die Inhalte dieser Veröffentlichung und / oder Verweise auf Inhalte Dritter sind urheberrechtlich geschützt. Jegliche Vervielfältigung von Informationen oder Daten, insbesondere die Verwendung von Texten, Textteilen, Bildmaterial oder sonstigen Inhalten, bedarf der vorherigen Zustimmung durch den Bundesverband Digitale Wirtschaft (BVDW) e.V. bzw. die Rechteinhaber (Dritte).
Ausgabe	Erstausgabe
Titelmotiv	© iStock /Genestro