

## Darstellung der Tätigkeit mit Bezug auf den Datenschutz

Die targeting360 GmbH setzt für ihre Kunden Retargeting- und Display-Kampagnen um.

Hierzu verarbeitet targeting360 im Auftrag personenbezogene Daten. Sie technisch-organisatorische Maßnahmen, um das in Art. 32 DSGVO geforderte Schutzniveau für diese personenbezogenen Daten zu gewährleisten.

### 1. Allgemeines

#### a) Personenbezogene Daten per Definition

Obwohl die targeting360 keinen direkten Rückschluss auf die natürliche Person ziehen kann, sind die von uns anhand der pseudonymen User-ID ("Online-Kennung") erhobenen Daten gemäß Definition der DSGVO als personenbezogen zu betrachten. Sämtliche Daten sind bei targeting360 maximal der jeweiligen User-ID zugeordnet. Diese Daten dienen u.a. zur passenden Wiederansprache der User mit den entsprechenden Produkten und Werbemitteln.

Für die Aufzeichnungen der Statistiken verwendet targeting360 nur abgeleitete (anonyme) Daten ohne Personenbezug. Die Speicherung der IP erfolgt bei targeting360 grundsätzlich nur anonymisiert durch Verkürzung.

#### b) Wie werden die Daten verwendet

Grundsätzlich werden die Daten zur gezielten Ansprache der User für den jeweiligen Advertiser mit Retargeting-Werbemitteln verwendet, wobei entsprechend auch der Inhalt der Werbemittel durch passende Produktauswahl an den User angepasst ist.

#### c) Wie lange werden die Daten gespeichert

Die im Rahmen der DSGVO als personenbezogenen Daten zu betrachtenden Daten werden lediglich über einen Zeitraum von maximal 90 Tagen ab Zeitpunkt der Erhebung gespeichert. Unabhängig davon speichert targeting360 anonyme Daten über einen längeren Zeitraum (Statistiken, Anzahl Sales etc.)

#### d) In welchem Land werden die Daten gespeichert

Sämtliche Daten werden nur auf Servern in Deutschland gespeichert, in verschiedenen Rechenzentren des Sub-Dienstleisters Hetzner Online GmbH des technischen Dienstleiters NEORY. Zwischen diesen Beiden besteht ein entsprechender ADV-Vertrag, innerhalb dessen auch die entsprechenden technischen und organisatorischen Maßnahmen geregelt sind, die von diesen Gesellschaften gewählt wurden, um ein angemessenes Schutzniveau für personenbezogene Daten zu gewährleisten. Es sei darauf hingewiesen, dass die NEORY nur die technische Infrastruktur stellt, sie hat keinerlei Zugriff auf die Daten selber. Das komplette Server-Setup (inkl. Einrichten des Betriebssystems mit entsprechenden User-Accounts) erfolgt

durch die NEORY als technischen Dienstleister. Dem Sub-Dienstleister sind User-Accounts und Passwörter nicht bekannt.

e) Welche Daten werden an targeting360 übermittelt

Explizit übermittelt werden die jeweiligen Parameter der Pixel zu denen die Seitenart/typ, die Produkt-IDs sowie die Kategorie-IDs gehören. Bei Verwendung der Search-Retargeting-Pixel ist hier auch der übergebene Searchterm zu beachten.

Grundsätzlich gilt bei diesen Daten aber, dass diese explizit vom Advertiser übergeben werden. Die übergebenen Daten werden mit dem Zeitpunkt aufgezeichnet und der anonymen User-ID zugeordnet. Durch Bereitstellung eines Produktfeeds durch den Advertiser, welcher im targeting360 System importiert wird, ist durch die Produkt-ID auch eine konkrete Rückführung auf das betrachtete Produkt möglich.

Des Weiteren erfolgt systemimmanent sowohl beim Aufruf der Retargeting-Pixel als auch bei der Ausspielung der Werbemittel, bedingt durch den Aufbau des im Internet verwendeten TCP/IP-Protokolls auch die Übermittlung der IP an targeting360. Diese wird von targeting360 gekürzt und gehasht gespeichert und genutzt um mittels sogenannter Geo-Datenbanken daraus folgende „grobe“ Informationen abzuleiten:

Herkunftsland/Region/Bundesland/Stadt

Internetzugangsprovider

Zugangsgeschwindigkeit (gruppiert in vier Gruppen: Cable/DSL, Dialup, Cellular, Corporate)

Der Abgleich erfolgt über Datenbanken die von Maxmind (<https://www.maxmind.com/de/home>) zur Verfügung gestellt werden. Diese werden vom technischen Dienstleister NEORY in regelmäßigen Abständen heruntergeladen, so dass diese lokal vorliegen. Der Abgleich der IP-Adressen erfolgt dann lokal, es findet keine Übermittlung der IP-Adressen an Maxmind z.B. durch Webservices oder ähnliches statt.

Des Weiteren übermitteln Browser in der Standard-Einstellung automatisch und „ungefragt“ bei jedem Aufruf einen sogenannten User-Agent-String mit. Dieser User-Agent-String enthält Informationen über den verwendeten Browser inkl. Version, ggf. des verwendeten Betriebssystems sowie bei mobilen Geräten unter Umständen auch Hinweise auf das entsprechende Device. Dies wertet targeting360 ebenfalls aus, und erzeugt daraus folgende anonyme Informationen:

Browser-Art (Firefox, Chrome, etc.) inkl. Version

Betriebssystem (z.B: Windows 10, Windows 7, iOS, Android 6.0, Linux etc.)

Device (Desktop, Android Phone, iPhone, Android Tablet, iPad, Symbian, Blackberry, Windows Phone)

Des Weiteren übermitteln Browser in der Standard-Einstellung automatisch die präferierte Sprache mit. Diese Information speichert targeting360 ebenfalls um in multilingualen Ländern eine sprachspezifische Ansprache zu ermöglichen.

Des Weiteren übermitteln Browser den sogenannten HTTP-Referrer, die URL der Seite innerhalb dessen der Retargeting-Pixel/das Werbemittel verbaut war, sowie Bildschirmauflösung, Größe des Browserfensters und ggf. Position des Werbemittels innerhalb der Seite. Diese speichert targeting360 ebenfalls zur Qualitätssicherung und Fehlerkontrolle ab.

## 2. Tracking

### a) Welche Cookies setzt targeting360

Cookie-Name	Cookie-Wert	Zweck
{\$datapoolId}_uid	max 32 Zeichen alphanumerisch	Enthält die Unique-User-ID für den jeweiligen Daten-Pool (siehe unten). Die Laufzeit dieses Cookies ist 90 Tage und wird bei jedem Zugriff erneuert.
{\$datapoolId}_optout	nicht gesetzt oder "1"	Falls sich der User explizit gegen die Nutzung und Erhebung seiner personenbezogenen Daten ausgesprochen hat, wird dieser Cookie gesetzt und mit 1 befüllt. In diesem Zuge erfolgt dann auch eine Löschung sämtlicher personenbezogenen Daten sowie Löschung des {\$datapoolId}_uid Cookies. Die Laufzeit ist bis Ende des Jahres 2099 datiert.
{\$datapoolId}_optin	nicht gesetzt oder "1" sowie weitere OptIn-Informationen	Enthält die Informationen, falls ein expliziter OptIn erfolgt ist, mit der Info, dass dieser erfolgt ist und ggf. weiteren Informationen (z.B. Timestamp, Consent-Quelle etc.). Die Laufzeit dieses Cookies ist 90 Tage und wird bei jedem Zugriff erneuert.

{\$datapoolId} ist eine eindeutige 14-stellige alphanumerische Kennung des Data-Pools

Je nach verwendeter DSP der targeting360 können noch mehr Cookies der einzelnen DSP gesetzt werden. Diese sind individuell und zum jetzigen Zeitpunkt nicht aufführbar.

Zwischen den DSP's und targeting360 besteht ein entsprechender ADV-Vertrag. Dieser beinhaltet auch die

entsprechenden technischen und organisatorischen Maßnahmen, die gewählt wurden, um eine der DSGVO entsprechende Schutzstufe für personenbezogene Daten zu gewährleisten.

b) Welche Pixelaufrufe erfolgen

Technologie / Beispielaufruf

targeting360(NEORY) /

<https://ad.ad-srv.net/retarget?a=XXXXX&version=1>

Adform /

<https://track.adform.net/Serving/TrackPoint/?pm=XXXXXXXX&ADFPageName=XXXXX...>

Adition /

<https://ad13.adfarm1.adition.com/tagging?type=image&network=XXXX...>

Google DoubleClick Bid Manager /

<https://XXXXXXXXX.fl.s.doubleclick.net/activityi;src=XXXXXXXXX;type=invmedia;cat=XXXXXXXXXXXXX...>

MediaMath /

[https://pixel.mathtag.com/event/js?mt\\_id=XXXXXX&mt\\_adid=XXXXX...](https://pixel.mathtag.com/event/js?mt_id=XXXXXX&mt_adid=XXXXX...)

### 3. Technische und organisatorische Maßnahmen im Überblick

#### a) Organisationskontrolle

Jeder Mitarbeiter ist auf das Datengeheimnis verpflichtet und hat dafür Sorge zu tragen, dass personenbezogene Daten außenstehenden Dritten nicht zugänglich werden. Des Weiteren dürfen keine Daten an Mitarbeiter übermittelt werden, die für diese keine Berechtigung besitzen.

Der externe Datenschutzbeauftragte nimmt in unregelmäßigen Abständen unangekündigte Kontrollen vor und schult Mitarbeiter in datenschutzrechtlichen Fragen.

#### b) Zugangskontrolle

Eine spezielle Zugangskontrolle in den Räumen der targeting360 findet nicht statt.

Auf den Rechnern der targeting360 werden keine personenbezogenen Daten natürlicher Personen gespeichert. Der Zugriff auf Rechner und die Software mit der personenbezogene Daten verarbeitet werden, sind Passwort-geschützt und nur dem jeweiligen Mitarbeiter bekannt.

#### c) Zugriffs- und Speicherkontrolle

Entsprechend ergreift targeting360 technische und organisatorische Maßnahmen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Jeder Advertiser der targeting360 erhält auf Verlangen einen oder mehrere eigene Logins. Hinter diesen

Logins werden nur Statistiken des jeweiligen Advertisers gespeichert. Jeder Advertiser kann aufgrund der Administrations-Rechte und Datenbank-Strukturen nur auf Datensätze zugreifen, die seinem Login zugeordnet sind. Ohne diesen Login ist ein Einloggen in die Adserver-Technologie nicht möglich. Die gleichen Authentifizierungs-Mechanismen finden zudem auch in der Schnittstellen-Technologie (API) Anwendung.

Die Systeme sind so konfiguriert, dass ein regulärer Zugriff mit administrativen Rechten nur für Techniker der NEORY aus gesicherten Netzsegmenten möglich ist. Der Zugriff geschieht über kryptographisch stark gesicherte (SSH, HTTPS) Wege.

Berechtigungen für Abteilungsfreigaben, beispielsweise auf Fileservern, können nur vom technischen Dienstleister NEORY vergeben werden. Für Freigaben und Zugriffe auf Arbeitsplatzrechner ist grundsätzlich der jeweilige Mitarbeiter verantwortlich.

#### d) Auftragskontrolle

Die targeting360 ergreift technische und organisatorische Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

Alle Weisungen des Auftraggebers zum Umgang mit personenbezogenen Daten werden dokumentiert und an zentraler Stelle für die mit der Datenverarbeitung befassten Mitarbeiter der targeting360 hinterlegt.

Der Datenschutzbeauftragte des Auftraggebers hat das jederzeitige Recht, die Umsetzung seiner Weisungen bei der targeting360 zu kontrollieren.

#### e) Verfügbarkeitskontrolle

Die targeting360 ergreift technische und organisatorische Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

targeting360 unternimmt erhebliche Anstrengungen in Zusammenarbeit mit seinem technischen Dienstleister NEORY, um eine ständige Verfügbarkeit der Daten sicherzustellen.

#### f) Schutz vor Viren

Auf sämtlichen im Unternehmen eingesetzten Windows-Rechnern werden Virens Scanner eingesetzt.