Memorandum

JENTIS GmbH

SPIRIT LEGAL®

Verfasser/in	**Datum des Dokuments**
RA Tilman Herbrich (CIPP/E)	*22.05.2023, v0.99*

Projekt:

Datenschutzrechtliche Bewertung des ID Pooling als Datenschutzmaßnahme (Basiskonzept Synthetischer User)

Executive Summary

Aus der Betrachtung des **Basiskonzepts „Synthetische User“**[1] folgt, dass das ID Pooling als autonome Funktion der JENTIS Data Capture Platform ("DCP") eine signifikante Qualitätssteigerung der Daten ermöglicht und im Kontext der Privacy eine Maßnahme zum Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen im Sinne des Artikels 25 der DSGVO[2] darstellen kann.

Das ID Pooling ist mit Einwilligung der Nutzer und bei aktiviertem JENTIS Essential Mode[3] (ohne Einwilligung durch synthetische User) technisch durchführbar. In Kombination mit dem JENTIS Essential Mode als Fallback-Lösung kann das ID Pooling auf die Ausnahmevorschrift vom Einwilligungserfordernis für den Endgerätezugriff (z. B. § 25 Abs. 2 TTDSG) im Einklang mit aufsichtsbehördlichen Positionen gestützt werden.

Im Hinblick auf internationale Datenübermittlungen stellt das **ID Pooling** als wirksame Maßnahme der **Pseudonymisierung** im Vorfeld der Übermittlung von Gruppen-IDs eine **„zusätzliche Maßnahme“** i. S. d. **EuGH**-Entscheidung „Schrems II“[4] dar.

In dem spezifischen Use Case von Google Ads[5] bietet das ID Pooling eine praktikable und nachhaltige Lösung, um Conversions rechtskonform zu messen. Sollten Website-Besucher über eine Google Ads-Anzeige auf die Website gelangen und in dem Consent-Tool keine Einwilligung für Google Ads erteilen, **ermöglicht** JENTIS mit der Bildung von Nutzer-Clustern, einer Segmentierung auf Gruppenebene und einem ID Pooling eine **Conversion-Messung** für eine bestimmte Eigenschaft des Gruppen-Segments **ohne** Abfrage einer **Einwilligung.**

Beurteilungsgrundlage

1. Zusammenfassung von Nutzern in Gruppen (Clustering) und Segmentierung

(1) Um den qualitativen Mehrwert von Online-Daten zu schaffen und Erkenntnisse aus dem Nutzerverhalten zu erhalten, ist es üblich, dass Website-Betreiber und Werbenetzwerk-Anbieter gegenseitig eine bekannte User-ID austauschen, um einen User im Werbenetzwerk zu identifizieren und diesen dort mit gezielten Botschaften anzusprechen.

[1] Basiskonzept “Erstellung von synthetischen Usern als Folge der kombinierten Verarbeitung von eingewilligten und unbedingt erforderlichen Daten im Sinne der ePrivacy und der DSGVO zum Zweck von Online Marketing.”, JENTIS GmbH, April 2023 (siehe Anhang).
[2] Data protection by design and by default, Art. 25, DSGVO
[3] Informationen zum JENTIS Essential Mode siehe hier.
[4] EuGH, 16.7.2020 – C-311/18 – Schrems II.
[5] Siehe z.B. LG Köln zum Einsatz von Google Ads.

(2) Die Übermittlung der personalisierten IDs an Drittanbieter in Drittländer ohne angemessenes Schutzniveau, wie z. B. die Übermittlung der Google-Click-ID (GCID) oder Google Client-ID, verstößt nach Ansicht von Aufsichtsbehörden und der Rechtsprechung ohne Implementierung von „Additional Measures" durch den Website- und App-Betreiber gegen die Anforderungen an einen wirksamen Drittlandtransfer nach Art. 44 ff. DSGVO.

(3) Im Sonderfall des **Conversion-Tracking** durch **Google Ads,** erfolgt als Lösung für eine DSGVO-konforme Drittlandübermittlung in einem **ersten Schritt** unter Verwendung der **JENTIS DCP** für Nutzer aus einer Ads-Kampagne ein **Clustering**, d. h. eine Zusammenfassung der Nutzer in eine Gruppe. Dabei werden Nutzer mit ähnlichen Eigenschaften – z. B. männlich, zwischen 30 und 40 und vielleicht mit Interesse an Golf – zu dieser Gruppe zusammengefasst (**Segmentierung**). Die Mindestgröße einer Gruppe besteht aus 100 Nutzern. Bei diesem Vorgang werden gleichzeitig sämtliche Google IDs – Client-ID oder Click-ID – zu einem sog. Pool zusammengefasst und der Bezug zum Nutzer aufgelöst. Als Ergebnis des Clustering und der Segmentierung besteht lediglich ein Segment von Nutzern und ein Pool von IDs.

2. Conversion-Messung auf Gruppenebene

(1) Führt ein Nutzer eine Conversion durch (z.B. Anmeldung zum Newsletter oder Erreichen der Kaufbestätigungsseite), wird mithilfe der JENTIS DCP eine zufällige ID aus dem dazugehörigen Pool als Gruppen-ID verwendet, um an Drittanbieter (z. B. Google) lediglich die Information zu übergeben, dass für einen Nutzer aus dem Segment eine Conversion erfolgt ist. Für diesen gesamten Pool an Nutzern wird dabei lediglich eine Gruppen-ID vergeben, die zufällig aus den vorhandenen Drittanbieter-IDs ausgewählt wird.

(2) Vor Übergabe der Gruppen-ID an einen Drittanbieter erfolgt eine Gegenprüfung, dass es sich nicht um die Original-ID des Nutzers aus der Gruppe handelt. Nach Übergabe kann der Drittanbieter die erfolgte Conversion lediglich einer Gruppen-ID mit einem bestimmten Segment als Eigenschaft zuordnen. Ein Herausgreifen eines Nutzers aus der Gruppe (sog. „singling-out") ist für den Drittanbieter dann nicht mehr möglich.

3. Synthetische Usern und ID Pooling

Durch die Verwendung von ID-Pooling mit synthetischen Usern können Online-Marketing-Maßnahmen ohne individuelle Identifizierung durchgeführt werden. Dieser Ansatz ermöglicht Kampagnen- und Werbe-Lernprozesse bei Google, ohne auf personenbezogene Daten angewiesen zu sein.

Rechtliche Würdigung

1. Urteil des LG Köln zum Einsatz von Google Ads

(1) Laut einem aktuellen **Urteil** des **LG Köln**[6] erfüllt der Einsatz von **Google Ads nicht** die **Anforderungen** an einen **wirksamen Drittlandtransfer** in die USA nach Maßgabe der EuGH-Entscheidung „Schrems II".[7] Nach Ansicht des LG Köln erfüllen die Standardvertragsklauseln von Google „Google Ads Data Processing Terms" nicht die Anforderungen an das EuGH-Urteil „Schrems II" für die Anwendung von Art. 46 Abs. 2 lit. c) DSGVO an einen rechtmäßigen Drittlandtransfer. Insbesondere stelle die Kürzung von IP-Adressen keine "Additional Measure" i. S. d. EuGH-Urteil „Schrems II" dar.

[6] LG Köln, Urt. v. 23.03.2023 (33 O 376/22).
[7] EuGH, 16.7.2020 – C-311/18 – Schrems II.

(2) Außerdem stellt das LG Köln **hohe Anforderungen** an die **Abfrage** einer **ausdrücklichen Einwilligung** für den **Drittlandtransfer** nach Art. 49 Abs. 1 lit. a) DSGVO. So reiche ein Hinweis auf dem 1st Layer eines Cookie-Banners nicht aus, dass die Einwilligung für Cookies auch die Einwilligung in Drittländer ohne angemessenes Schutzniveau wie die USA erfasst (Art. 49.1 DSGVO). Zur Erfüllung der „besonderen Informiertheit" der Einwilligung müssten Nutzer u. a. darüber informiert werden, an welche Drittländer und Empfänger die Nutzerdaten übermittelt werden. Eine solche Auflistung des jeweiligen Drittlandes, in welches die Daten übermittelt werden, sowie aller über 60 Unterauftragnehmer für Google Analytics als Empfänger ist aufgrund des Umfangs praktisch nicht zu handhaben. Google behält sich z. B. in Ziff. 10.1 Datenverarbeitungsbedingungen für Google Ads vor, personenbezogene Daten in jedem Land zu verarbeiten, in dem Google oder Unterauftragnehmer Einrichtungen vorhalten.

(3) Als Folge der Entscheidung des LG Köln Urteils existiert aktuell **keine praktikable Möglichkeit**, **Google Ads ohne** Einsatz einer **Privacy Enhancing Technologie** datenschutzkonform **einzusetzen**.

2. Datenschutzrechtliche Einordnung des ID Pooling

(1) Der im JENTIS Basiskonzept beschriebene Vorgang des ID Pooling[8] ist als **Privacy Enhancing Technologie** einzustufen.[9] Aufgrund der Auflösung des Bezugs zu einem bestimmten Nutzer und bloßen Zuordnung zu einer Gruppen-ID für ein bestimmtes Segment und der Sicherstellung, dass nicht die ursprüngliche von Google einem Nutzer zugeordnete ID verwendet wird, ist der Vorgang „**ID Pooling**" lediglich als **Pseudonymisierung** i. S. d. Art. 4 Nr. 5 DSGVO einzustufen.

(2) Sofern eine Re-Identifizierung eines Nutzers oder ein singling-out eines einzelnen Nutzers anhand des Timestamps einer Browser-Session möglich sein sollte, werden mithilfe der JENTIS DCP die Zeitangaben durch synthetisierte Werte (fiktive Zeitstempel) ersetzt.

In Bezug auf den konkreten Anwendungsfall von Google Ads und Conversion Tracking ist zu beachten, dass die Nutzung weiterer URL-Parameter wie Produkt-IDs oder UTM-Parameter wie „utm_source", "utm_campaign" und „utm_network" nichts an dieser Auslegung ändert. Im Fall der Nutzung dieser URL-Parameter ist kein unmittelbares Google Ads Conversion Tracking mehr möglich, sondern lediglich eine Zuordnung der Conversions zu Google als Quelle, zu dem Werbekanal Google Ads, zu einer bestimmten Google Ads Kampagne sowie zu einem Produkt. Die Mindestgröße für das Datensegment einer Google Ads Kampagne beträgt im Google Displaynetzwerk 100 aktive Nutzer innerhalb der letzten 30 Tage und im Google Suchnetzwerk 1000 aktive Nutzer innerhalb der letzten 30 Tage.

(3) Für Drittanbieter wie Google besteht aufgrund des ID Pooling **keine Zuordnungsmöglichkeit** durch **eigene IDs**, weil Drittanbieter nach Übergabe der Gruppen-ID zu keinem Zeitpunkt mehr einen clientseitigen Zugriff auf das Endgerät des Nutzers besitzen.

Die juristische Bewertung steht im Einklang mit einer aktuellen und fachlich einschlägigen Rechtsprechung des **Gerichts der Europäischen Union** zum fehlenden Personenbezug von IP-Adressen für Empfänger, die keine rechtlichen Möglichkeiten zur Re-Identifizierung eines Nutzers haben.[10]

---

[8] Basiskonzept "Erstellung von synthetischen Usern als Folge der kombinierten Verarbeitung von eingewilligten und unbedingt erforderlichen Daten im Sinne der ePrivacy und der DSGVO zum Zweck von Online Marketing.", JENTIS GmbH, April 2023.
[9] Vgl. für Begriffsbestimmung ENISA, Data Protection Engineering, 2022, S. 9.
[10] EuG, Urt. v. 26.04.2023 – T-557/20, Rn. 101 ff.

In diesem Sinne hatte bereits das **Handelsgerichts des Kantons Zürich** zum Schutz des Persönlichkeitsrechts nach Art. 28 des ZGB (Schweiz) entschieden, wonach eine Pseudonymisierung für den Empfänger, der die pseudonymisierten Datensätze keiner bestimmten Person zuordnen kann, als Anonymisierung zu werten ist.[11]

3. Datenschutzrechtliche Beurteilung des ID Pooling

(1) Der im JENTIS Basiskonzept beschriebene Vorgang der Segmentierung von Nutzern auf Gruppenebene sowie zum ID Pooling ist als robuste Maßnahme der Pseudonymisierung i. S. d. Art. 4 Nr. 5 DSGVO einzuordnen.

(2) Für den Vorgang der Segmentierung und des IP Pooling erfolgt **kein erneuter unmittelbarer Zugriff** auf **oder unmittelbare Speicherung** der Informationen in **Endgeräteressourcen** von Nutzern. Deshalb unterfällt der Vorgang als nachgelagerte Verarbeitungsphase im Einklang mit der **EuGH-**Entscheidung zum **One-Stop-Shop-Verfahren,**[12] der **Gesetzesbegründung** zum TTDSG[13] und der Ansicht des **EDPB**[14] ausschließlich den Regelungen der DSGVO.

(3) Das ID Pooling wurde unabhängig davon, ob Nutzer eine Einwilligung erteilt haben oder mithilfe des JENTIS Essential Mode (mit Synthetische User) die Ausnahmeregelung in § 25 Abs. 2 TTDSG belastet wird, designt, um das **Konzept von „Privacy by design und by default"** nach Maßgabe von Art. 25 Abs. 1 und Abs. 2 DSGVO umsetzen zu können. Im Zuge der **Entwicklung** des „ID Pooling wurden **Privacy Design Strategies** als Leitlinien **berücksichtigt** und dadurch die Umsetzung des Konzepts von Privacy by Design als Privacy Enhancing Technology ermöglicht.[15]

Hierzu wurden datenorientierte Strategien wie „minimieren", „verbergen", „separieren" und „abstrahieren" sowie prozessorientierte Strategien wie „informieren", „kontrollieren", „durchsetzen" und „demonstrieren" umgesetzt.[16] Auf Grundlage dieser Privacy Design Strategien können die vom EDPB geforderten Zielvorgaben bei Nutzung des ID Pooling vollständig umgesetzt werden. Erreicht werden soll dies durch **„geeignete technische und organisatorische Maßnahmen"** und „notwendige Garantien" (Art. 25 Abs. 1 DSGVO), was nach Ansicht der **EDPB** jegliche Mittel erfassen kann, wie den **Einsatz fortschrittlicher technischer Lösungen**, aber auch die grundlegende Schulung von Mitarbeitern. Notwendig ist dabei, dass die Maßnahmen und Garantien dazu dienen können, alle **Datenschutzgrundsätze aus Art. 5** und Erwägungsgrund 39 DSGVO wirksam **umzusetzen**.[17]

(4) Den **EDPB** Empfehlungen folgend müssen für eine wirksame Pseudonymisierung als „zusätzliche Maßnahme" i. S. d. EuGH-Entscheidung „Schrems II"[18] bei Nutzung von Cloud-Diensten – wie etwa dem Server Side Google Tag Manager – **entsprechende Verfahren** zur **Pseudonymisierung im Vorfeld der Übermittlung** an den Drittanbieter angewendet werden.[19] Eine wie von Google im Verfahren angegebene **Transportverschlüsselung** oder **„Data-at-rest"-Verschlüsselung** stellen für sich noch keine „zusätzlichen

[11] Vgl. HGer ZH, Urt. v. 04.05.2021 – HG190107-O.
[12] EuGH, Urt. v. 15.06.2021 – C-645/19 – One-Stop-Shop, Rn. 74.
[13] BT-Drs. 19/27441, S. 38.
[14] EDPB, Stellungnahme 5/2019 zum Zusammenspiel zwischen der eg-Datenschutz-Richtlinie und der DSGVO S. 23.
[15] Vgl. ENISA, Data Protection Engineering, 2022, S. 6 f.
[16] Vgl. Agencia Espanola Proteccion Datos (AEPD), A Guide to Privacy by Design 2019, S. 23 f.
[17] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default v2.0, Rn. 61. Zu den in Art. 5 DSGVO festgelegten Datenschutzgrundsätzen zählen Rechtmäßigkeit, Transparenz, Zweckbindung. Verarbeitung nach Treu und Glauben, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie die Rechenschaftspflicht.
[18] EuGH, 16.7.2020 – C-311/18 – Schrems II.
[19] EDPB Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, Rn. 94 f.

Maßnahmen“ dar, die ein im Wesentlichen gleichwertiges Schutzniveau gewährleisten. Deshalb ist nach Ansicht der Norwegischen Datenschutzbehörde auch die bei Google Analytics 4 automatische Kürzung der IP-Adressen auf Servern in der EU, bevor die Daten auf Servern von Analytics erfasst werden, nicht ausreichend, um die Anforderungen des EDPB an „zusätzliche Maßnahmen“ zu erfüllen.[20]

(5) Aufgrund der vorgenommenen Pseudonymisierung lässt sich für die Übermittlung der zufällig ausgewählten Gruppen-ID an Drittanbieter beim Server-Side-Tracking die **Rechtsgrundlage** gemäß **Art. 6 Abs. 1 S. 1 lit. f) DSGVO** in vertretbarer Weise anwenden. Soweit Nutzerdaten ohne Einwilligung im reduziertem Umfang als technisch notwendiger Vorgang erfasst wurden, ist die Verarbeitung nicht persistent. Entsprechende Rohdaten werden nach Gegenprüfung zur Sicherstellung, dass keine ursprüngliche von Google einem Nutzer zugewiesene ID an Google übermittelt wird, vollständig gelöscht.

(6) Für die notwendige **Dokumentation** der Interessenabwägung nach Art. 6 Abs.1 S. 1 lit. f) DSGVO[21] sollte **ein sog. LIA (Legitimate Interests Assessment)** durchgeführt werden, um einen Nachweis für die erfolgte Interessenabwägung erbringen zu können.

(7) Für die **rechtskonforme Nutzung** der ID Pooling Funktion sind **folgende Maßnahmen** zu **empfehlen**:

- Konfiguration der JENTIS DCP durch Kunden;
- Durchführung der LIA (Legitimate Interests Assessment);
- Transparente Informationen in den Datenschutzinformationen auf der Website;
- Abschluss und Dokumentation Auftragsverarbeitungsvertrag mit JENTIS.

[20] Vgl. PM der Norwegian DPA vom 01.03.2023.
[21] EDPB, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260, rev.01, Anhang.