Data Protection Memorandum

JENTIS GmbH

Verfasser/in	**Datum des Dokuments**
RA Peter Hense & RA Tilman Herbrich (CIPP/E)	*10 Februar 2023, v2.4*

Projekt

Datenschutzrechtliche Bewertung des „Essential Mode" der JENTIS Saas-Lösung

Executive Summary

Das vom EU-Datenschutzrecht und der Rechtsprechung vorgeschriebene Einwilligungserfordernis gilt für jeden Zugriff auf und jede Speicherung von Informationen aus den Endgeräten der Nutzer **(I.3.)**. In Anbetracht der BGH-Entscheidung „Cookie-Einwilligung II" **(I.1.)**, der gesetzlichen Regelung in § 25 TTDSG sowie aktuell angestoßener Untersuchungen von Aufsichtsbehörden und ersten Gerichtsurteilen ist das Einwilligungserfordernis beim Website-Tracking eine strikte Vorgabe.

Eine Ausnahme von diesem strikten Einwilligungserfordernis – „unbedingte Erforderlichkeit" ist in Art. 5 Abs. 3 S. 2 ePrivacy-RL geregelt **(II.1.).** Auch die Rechtsprechung und die derzeitige Auslegung des Wortlauts der Art. 5 Abs. 3 S. 1 ePrivacy-RL lässt darauf schließen, dass unter bestimmten Umständen die Berufung auf nachgelagerte Verarbeitungen beim Server-Side-Tracking ohne direkten Zugriff auf das Endgerät **(II.2.)** nicht unter dieses strenge Einwilligungserfordernis fällt. Wichtig ist, dass die Ausnahmen von der strikten Einwilligungspflicht nicht auf Third-Party-Dienste anwendbar sind.

In der Praxis ist die Umsetzung der Ausnahmen vom Einwilligungserfordernis aufgrund komplexer und schwer zu lösender Herausforderungen bei der Integration von Tracking-Anwendungen ohne eine langfristige und nachhaltige technische Lösung, die auch rechtskonform ist und wirksamen Datennutzung unterstützt, praktisch mit hohen Risiken verbunden **(II.3.)**.

JENTIS Data Capture Platform (DCP) bietet als Privacy Enhancing Technology eine langfristige Hilfestellung zur Sicherstellung der „Datenschutz"-Compliance in der Supply Chain und ermöglicht den Kunden flexible Konfigurationen der SaaS-Lösung, um der Volatilität der jeweiligen individuellen Risikolage von Unternehmen Rechnung zu tragen. Die JENTIS-Twin-Server Technologie **(III.1.)** ermöglicht die wirksame Verwendung von Website-Daten in beiden Situationen – bei expliziter Einwilligung des Nutzers (Tracking-Modus) und bei nicht vorhandener Einwilligung des Nutzers (als Fall-Back Lösung - JENTIS Essential Mode). Die Unternehmen können den „JENTIS Essential Mode" als Fallback-Lösung für das First-Party-Tracking so konfigurieren, dass die Anwendung der Ausnahmevorschriften vom Einwilligungserfordernis für den Endgerätezugriff konform und effektiv umgesetzt werden **(III.2.)**. Dadurch wird eine „Nutzungsanalyse" in einem reduzierten Umfang ohne Nutzerstimmung möglich, wenn der Nutzer das Cookie-Banner gar nicht anklickt oder keine Einwilligung erteilt. . Dies wird anhand einer Beispielkonfiguration für den JENTIS Essential Mode demonstriert **(III.2.c.aa.)**.

Die serverseitigen Übermittlungen der vom JENTIS-Server modifizierten (und bereinigten) Browser-Nutzer-Daten an Drittanbieter-Server können in Übereinstimmung mit Positionierungen von Aufsichtsbehörden als einwilligungsfreie nachgelagerte Verarbeitungsphase im konkreten Einzelfall auf überwiegende berechtigte Interessen gemäß Art. 6 Abs. 1 S. 1 lit. f) DSGVO gestützt werden **(III.3.)**. In Einklang mit der Ansicht der ENISA kann die Modifikation der Datenparameter als Privacy Enhancing Technology betrachtet und als wirksames Mittel der Pseudonymisierung eingesetzt werden.

Mithilfe von JENTIS können Unternehmen die datenschutzrechtlichen Vorgaben an das Tracking vollständig umsetzen und die Rechtsunsicherheiten beseitigen. Website-Betreiber können bei Nutzung von JENTIS

wirtschaftliche Vorteile ihrer jeweils eigenen First-Party-Daten nutzen, ohne ihre Daten oder die jeweilige unternehmerische Compliance durch unkontrollierte und intransparente Verarbeitung auf Seiten von Drittanbietern in rechtlicher Hinsicht zu gefährden **(IV.)**. Über die JENTIS-Technologie erhalten Unternehmen die vollständige Kontrolle beim Server-Side-Tracking zurück.

Inhaltsverzeichnis

Rechtliche Würdigung

I. Bestandsanalyse – Rechtliche Einordnung der Verarbeitung beim Website-Tracking

Die Implementierung von JavaScripts oder HTML-Elementen wie iFrames oder Image-Pixeln von Drittanbietern im Quellcode einer Website bedingt sowohl einen **Zugriff auf Endgeräteinformationen** als auch aufgrund des vom JavaScript initiierten https-Requests des Browsers des Nutzers (Client) eine **Übermittlung personenbezogener Daten** des Website-Besuchers. Nachfolgend werden die Website-Besucher auch als Nutzer oder User bezeichnet.

1. Einwilligung für Endgerätezugriff bei Tracking zu Analyse und Marketingzwecken

(1) Der BGH hat mit Urteil vom 28.05.2020[1] im Anschluss an die Vorabentscheidung durch den EuGH in der Rechtssache „Planet49" endgültig entschieden, dass für den **Einsatz von Cookies** (und ähnlichen Technologien), die nach Registrierung für ein Gewinnspiel auf dem Endgerät eines Nutzers gesetzt werden und eine **Auswertung des Nutzungsverhaltens** auf Websites von Werbepartnern und damit **interessenbasierte Werbung** ermöglichen, **im Grundsatz eine Einwilligung** vom Nutzer nach richtlinienkonformer Auslegung von § 15 Abs. 3 TMG (nunmehr § 25 TTDSG) am Maßstab von Art. 5 Abs. 3 S. 1 RL 2002/58/EG i. d. F. d. RL 2009/136/EG (ePrivacy-RL) **notwendig** ist.

Das Einwilligungserfordernis gilt nach dem Wortlaut der **Richtliniennorm** für jeden Zugriff auf und jede Speicherung von Informationen aus Endgeräten der Nutzer und **sperrt** nach Ansicht des BGH aufgrund der Kollisionsnorm gemäß Art. 95 DSGVO **für diesen Vorgang** die **Anwendung** anderer Regelungen der **DSGVO** als in Bezug auf die Einwilligung (Art. 4 Nr. 11, Art. 6 Abs. 1 S. 1 lit. a), Art. 7 DSGVO). Es ist nach übereinstimmender Ansicht des EuGH und BGH für das Vorliegen des Einwilligungserfordernis **unbeachtlich**, **ob** es sich bei den **Endgeräteinformationen** um **personenbezogene oder anonyme** Daten handelt.[2]

(2) Erste Gerichtsentscheidungen haben unter anderem den Einsatz von Google Analytics auf einer Website ohne Abfrage einer freiwilligen und informierten Einwilligung untersagt.[3]

(3) Es spielt für die Anwendbarkeit dieser Rechtsprechung nach Ansicht der europäischen Aufsichtsbehörden keine Rolle, ob der **Endgerätezugriff** und die **Speicherung** der Informationen auf Endgerät mittels Cookies oder **anderer Technologien** wie **Tracking-Pixel** erfolgt.[4] Vom Begriff des „Endgerätezugriffs" umfasst sind auch Zugriffe auf LocalStorage, Local Shared Objects sowie serverseitige Technologien wie die Nutzung von Browser-Fingerprinting-Technologien wie „Canvas Fingerprinting".[5]

2. Aktuelle Prüfungen von Aufsichtsbehörden und NGOs zur Rechtsdurchsetzung

(1) Für die **endgerätebezogene Speicherung** von und den endgerätebezogenen **Zugriff** auf User IDs und IP-Adressen mittels Cookies und ähnlichen Tracking-Methoden und der **Übermittlung personenbezogener**

[1] I ZR 7/16 – Cookie-Einwilligung II.
[2] Vgl. EuGH, Urt. v. 01.10.2019 – C-673/17, Rn. 70.
[3] Vgl. LG Rostock, Urt. v. 15.09.2020 – 3 O 762/19; LG Köln, Beschl. v. 29.10.2020 – 31 O 194/20 und Beschl. v. 13.04.2021 – 31 O 36/21; LG Frankfurt, Urt. v. 19.10.2021 – 3-06 O 24/21; LG München, Hinweisbeschluss v. 08.12.2021 – 33 O 14776/19.
[4] Vgl. DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 24; Europäische Datenschutzausschuss (EDSA) in seinen Leitlinien 8/2020 über die gezielte Ansprache von Nutzer:innen sozialer Medien, Version 2.0, Rn. 71 f.).
[5] LG Rostock, Urt. v. 15.09.2020 – 3 O 762/19; ICO, Guidance on the use of cookies and similar technologies, 2020; DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 7.

Daten z. B. beim Einsatz von Google Analytics auch an Google LLC in den USA ist nach Ansicht Datenschutzkonferenz (DSK) die **Abfrage einer Einwilligung** des Website-Besuchers zwingend erforderlich.[6] Konkret in Deutschland haben Prüfungen des Website-Trackings auf Seiten von Aufsichtsbehörden und NGOs in jüngerer Zeit spürbar zugenommen.

(2) Am 27.09.2021 hat der Europäische Datenschutzausschusses (EDPB) beschlossen, eine „Cookie-Banner Task Force" nach Art. 70 Abs. 1 lit. u) DSGVO einzurichten, um europaweit eine einheitliche Rechtsdurchsetzung zu fördern. Anlass hierfür ist nicht zuletzt die Aufrufaktion der NGO „Noyb" im Juli 2021 zur Einreichung von Nutzerbeschwerden gegen unzulässige Cookie-Banner-Gestaltungen in Bezug auf das Website-Tracking. Im August 2021 wurden allein durch Noyb nach eigenen Angaben 422 formelle Beschwerden bei den Aufsichtsbehörden eingereicht.

(3) Ebenso hat die Berliner Beauftragte für Datenschutz und Informationsfreiheit im August 2021 rund 50 Website-Betreiber mit deren rechtswidrigem Trackingpraktiken konfrontiert und Untersuchungen eingeleitet.

(4) Schließlich hat die Verbraucherzentrale Bundesverband e.V. (vzbv) im September 2021 ca. 100 Unternehmen wegen unzulässigem Tracking abgemahnt und angekündigt, im Fall des Untätigbleiben der Website-Betreiber gerichtlich vorzugehen.

3. Scheitern bisheriger Industrielösungen zum Website-Tracking

(1) Bisherige Branchenlösungen wie das Anbieten von „First-Party-Cookies" von Fremdanbietern („3rd party as 1st party") ändern nichts an den datenschutzrechtlichen Anforderungen an die Zulässigkeit von Tracking, wenn z.B. aufgrund der Bearbeitung von Domain Name System (DNS)-Einträgen Tracking-Ressourcen von Drittanbietern von der derselben Domäne ausgeliefert werden, von der die Website betrieben wird.[7] Mit anderen Worten: First-Party-Cookies können in gleicher Weise genutzt werden wie Third-Party-Cookies und ermöglichen z.B. ein „Cross-Site-Tracking".[8]

(2) Ebenso befreien Advertising-Technology-Lösungen wie Server-Side-Tracking über den Server Side Google Tag Manager (SSGTM) oder die Facebook Conversions API nicht von der Einhaltung der datenschutzrechtlichen Anforderungen, auch wenn die Informationen aus Endgeräten nicht über den Browser des Nutzers, sondern mittels einer Umleitung über ein serverseitiges API (Facebook) oder einen Server des Website-Betreibers auf der Google Cloud Platform oder via Docker Container auf eigenen Systemen (SSGTM) an die Drittanbieter gesendet werden.[9]

(3) Zuletzt sorgten Ankündigungen von Google im Frühjahr 2021, Third-Party-Cookies zu eliminieren, und stattdessen ein „Federated Learning of Cohorts (FLoC)" oder „FLEDGE" mit Streuverlusten anzubieten, für eine Kehrtwende der Industrie. Gleichwohl kritisiert die Information Commissioner Officer (ICO) diese Ansätze und verlangt von Verantwortlichen den Nachweis, dass diese Ansätze nicht zu einem vermehrten Fingerprinting führen, und Transparenz darüber, wie Google entsprechende GPS-Signale verarbeitet.[10]

---

[6] DSK, Beschluss vom 12. Mai 2020 – Hinweise zum Einsatz von Google-Analytics.
[7] Veale/Borgesius, AdTech and Real-Time Bidding under European Data Protection Law, 2021, S. 6.
[8] IPOL Study: JURI commitee, EU-Parlament, Regulating targeted and behavioural advertising in digital services, 2021, S. 44, Fn. 49.
[9] Vgl. etwa Papadogiannakis et al., User Tracking in the Post-cookie Era, 2021, S. 1 f.
[10] CNIL, Alternatives to third-party cookies, 23.11.2021; ICO, Data protection and privacy expectations for online advertising proposals, 2021, S. 24 f.

(4) Schließlich ist der Einsatz des Industriestandards Transparency and Consent Framework v2.0 (TCF v 2.0) des Branchenverbandes Interactive Advertising Bureau Europe (IAB Europe) zur Abfrage einer freiwilligen und informierten Einwilligungserklärung für Tracking-Dienste aktuell **Risiken** ausgesetzt.

Die **belgische Aufsichtsbehörde** (Autorité de protection des donnée - Gegevensbeschermingsautoriteit) hatte Anfang Februar 2022 in einem Bußgeldbescheid gegenüber IAB Europe in Höhe von EUR 250.000,00 entschieden, dass **Verarbeitungen** mittels des **TC-Consent-Strings gegen** verschiedene Pflichten aus der **DSGVO verstoßen**, insbesondere aufgrund der Komplexität der Verarbeitung nicht den Transparenzforderungen entsprächen und entsprechende Verarbeitungen deshalb rechtswidrig seien.[11] Das IAB Europe hat Klage gegen die Entscheidung der belgischen Behörde vor dem Market Court Brussel (Hof van beroep) eingereicht. Am 07.09.2022 wurde das Gerichtsverfahren aufgrund zweier Vorlagelagefragen des Market Courts zum Personenbezug des TC-Strings und der Verantwortlichkeit der IAB Europe für die Verarbeitung an den Europäischen Gerichtshof ausgesetzt.[12] Es bleibt das Vorabentscheidungsverfahren beim EuGH und die sich anschließende Fortführung des Verfahrens vor dem Market Court Brussel abzuwarten.

(5) Ohne Modifikation der Datenparameter und der beim Aufruf der Website erfolgenden Datenverarbeitung aufgrund der geladenen Tags von Drittanbietern, wie es z. B. durch den Einsatz der RudderStack bei entsprechender Konfiguration möglich ist (vgl. Pkt. II.), gilt das Einwilligungserfordernis aus § 25 Abs. 1 TTDSG für den Zugriff auf Endgeräteinformationen uneingeschränkt.

II. Rechtliche Unsicherheiten durch technologische Vielfalt beim Website-Tracking

Bisweilen sind in der Praxis Rechtsunsicherheiten in Bezug auf die datenschutzrechtlichen Anforderungen beim Website-Tracking aufgekommen. Die Rechtsunsicherheiten entstanden durch das gesetzgeberische Vakuum nach der BGH-Entscheidung „Cookie-Einwilligung II“, welches von Juristen und Marketern mit für sie günstigen Auffassungen befüllt wurde, die teils in diametralem Widerspruch zu bereits existenten gerichtlichen und behördlichen Entscheidungen standen.

Interpretationsspielraum wird in erster Linie bei der Frage gesehen, wann Cookies und ähnliche Tracking-Technologien unter das gesetzliche Kriterium „unbedingt erforderlich“ (Art. 5 Abs. 3 S. 2 ePrivacy-RL) fallen **(1.)** sowie welche weiteren rechtlichen Anknüpfungspunkte existieren, damit von einer Ausnahme vom Erfordernis einer informierten Einwilligung ausgegangen werden kann **(2.)** Aufgrund unzureichender Industrielösungen wächst das Bedürfnis nach langfristigen Strategien zur rechtskonformen und erfolgreichen Datennutzung **(3)**.

Dabei spielen Tracking-Proxy-Lösungen wie die JENTIS-Twin-Server-Technologie eine maßgebliche Rolle.

[11] Vgl. Veale/Nouwens/Santos, Anmerkung zum Bußgeldbescheid gegen IAB Europe, 2022; vgl. zur Kritik am TCF v2.0 im Allgemeinen Cèlestin Matte and others, ‘Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework’ (2020) S. 794; Midas Nouwens and others, ‘Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence’ (2020), S. 3 ff.; Nataliia Bielova and others, ‘Purposes in IAB Europe’s TCF: which legal basis and how are they used by advertisers?’ (2020) S. 4 f.; Michael Veale and Frederik Borgesius, ‘Adtech and Real-Time Bidding under European Data Protection Law’ (2021), S. 28.
[12] Market Court Brussel (Hof van beroep), Beschl. v. 07.09.2022.

1. Rechtsunsicherheit: Ausnahmen vom Einwilligungserfordernis für Endgerätezugriff

Von der Pflicht zur Abfrage einer Nutzereinwilligung für den Zugriff auf und der Speicherung von Informationen aus Endgeräten der Nutzer:innen beim Website-Tracking existieren in der Richtlinie zwei Ausnahmen, die auch in § 25 Abs. 2 TTDSG unverändert übernommen worden sind.[13]

a) Erforderlichkeit für Durchführung und Erleichterung elektronischer Kommunikation

Für die technisch zwingend veranlasste Übermittlung der IP-Adresse des Nutzers und weiterer Endgeräteinformationen wie z. B. Browser-Informationen bei HTTP basierten Anwendungen ist grundsätzlich der Ausnahmetatbestand in Art. 5 Abs. 3 S. 2 ePrivacy-RL einschlägig.

Danach bedarf es **keiner Einwilligung**, wenn eine **technische Speicherung** oder ein Zugriff auf Endgeräteinformationen zur **Durchführung** der **elektronischen Kommunikation** erfolgt. Voraussetzung ist jedoch, dass die Durchführung oder Erleichterung der elektronischen Kommunikation **alleiniger Zweck** der Verarbeitung ist.[14] Von dem Ausnahmetatbestand in Art. 5 Abs. 3 S. 2 ePrivacy-RL erfasst werden nach Ansicht des europäischen Datenschutzgremiums sowie einzelnen Aufsichtsbehörden:[15]

- die Fähigkeit, die Informationen über das Netzwerk zu leiten, insbesondere durch Identifizierung der Kommunikationsendpunkte,
- die Fähigkeit, Datenelemente in ihrer vorgesehenen Reihenfolge auszutauschen, insbesondere durch Nummerierung der Datenpakete sowie
- die Fähigkeit, Übertragungsfehler oder Datenverlust zu erkennen.

Die **Ausnahme** für die Durchführung oder Erleichterung der Kommunikation **umfasst** daher **auch Cookies**, die eine (oder mehrere) dieser Eigenschaften erfüllen, jedoch nur für den alleinigen Zweck der Übertragung oder Erleichterung; d. h. die Übertragung der Kommunikation muss ohne die Verwendung des Cookies unmöglich sein, damit die Ausnahme gilt.[16]

b) Unbedingte Erforderlichkeit zur Bereitstellung eines gewünschten Dienstes

(1) Die **zweite Ausnahme** in Art. 5 Abs. 3. S. 2 ePrivacy-RL – **Zugriff** auf Endgeräteinformationen ist **unbedingt erforderlich** („strictly necessary"), um einen vom Nutzer gewünschten Dienst der Informationsgesellschaft **bereitzustellen** – ist nach dem Urteil des BGH jedenfalls nicht für Zwecke der Werbung und Marktforschung einschlägig.[17] Nach Ansicht der Art. 29 Datenschutzgruppe[18] sind **drei wesentliche Voraussetzungen** zu erfüllen:

---

[13] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 19. Die Vorlagefragen zielenIst IAB Europe gemeinsam verantwortlich (Joint Controller) mit CMPs, Publisher und Vendoren? 2. Stellt der TC-String personenbezogene Daten dar?
[14] Art. 29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 3.
[15] Art. 29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 3 f., ICO, Guidance on the use of cookies and similar technologies, S 13.
[16] ICO, Guidance on the use of cookies and similar technologies, S. 13.
[17] BGH, Urt. v. 28.05.2020 – I ZR 7/16 – Cookie-Einwilligung II.
[18] Art. 29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 4.

1) Der Dienst wird ausdrücklich vom Nutzer angefordert: Der Nutzer hat eine positive Aktion durchgeführt, um einen Dienst mit einem klar definierten Umfang anzufordern.
2) Mit Dienst der Informationsgesellschaft ist in der Regel die Summe mehrerer Funktionalitäten gemeint, sprich die gesamte Website als solche. Die Art. 29 Datenschutz-Gruppe deutet aber auch an, dass die Ausnahmevorschrift auch für einzelne (Zusatz)Funktionalitäten gilt, die von dem Basisdienst „Website" bereitgestellt werden. Hierunter können im Einzelfall auch eine Interaktion mit einem Chatbot, Kartendienst sowie Streaming-Content fallen.[19] Cookies und ähnliche Technologien dürfen nach Ansicht der DSK z. B. für etwaige Zusatzfunktionen des Basisdienstes Website genutzt werden, wenn diese vom Nutzer angefordert werden, was beim bloßen Aufruf der Website noch nicht der Fall sei.[20]
3) Der Zugriff auf Endgeräteinformationen muss „unbedingt erforderlich" sein, um den Dienst – Website, App oder einzelne Funktionalitäten – bereitzustellen.

(2) Die **Belastbarkeit** dieser **Ausnahmevorschrift hängt** in erster Linie **vom** Grad der Restriktion der **Auslegung** des Begriffs der **Erforderlichkeit ab.** Einschränkend ist dabei jedoch zu berücksichtigen, dass die **Rechtsprechung** des **EuGH** prüft, ob **Beschränkungen** der Rechte auf Schutz personenbezogener Daten und die Achtung des Privatlebens bei der Verarbeitung personenbezogener Daten unbedingt erforderlich sind. Der EuGH[21] führte aus, dass

> *„[…] sich die Ausnahmen und Einschränkungen in Bezug auf den Schutz personenbezogener Daten sich auf das absolut Notwendige beschränken müssen […]."*

Außerdem hat der **EuGH** in der **Rechtssache „M5A-ScarA"[22]** anhand der Interessenabwägungsklausel (Art. 6 Abs. 1 S. 1 lit. f) DSGVO) ausgeführt, dass eine **Verarbeitung nur dann „erforderlich"** sei, wenn sie **nicht mit anderen Mitteln**, die **weniger stark** in die **Grundrechte** und Grundfreiheiten der betroffenen Personen, insbesondere die in den Art. 7 und 8 der EU-Grundrechte Charta verbürgten Rechte auf Achtung des Privatlebens und Schutz personenbezogener Daten, **eingreifen**, **vernünftigerweise** ebenso wirksam **erreicht werden kann.[23]** Außerdem sei die Voraussetzung der Erforderlichkeit der Datenverarbeitung gemeinsam mit dem sogenannten **Grundsatz der „Datenminimierung"** zu prüfen, der in Art. 6 Abs. 1 S. 1 lit. c) der RL 95/46 (nunmehr Art. 5 Abs. 1 lit. c) DSGVO) verankert sei und verlange, dass die personenbezogenen Daten

> *„[…] den Zwecken entsprechen, für die sie erhoben und/oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen […]."*

(3) Nach **Ansicht** der **DSK** gilt für die **Auslegung** des Begriffes **„unbedingt erforderlich"** Blick auf ErwGr. 66 ePrivacy-RL ein **restriktives Verständnis**. Für die unbedingte Erforderlichkeit könne deshalb **nicht** auf **wirtschaftliche Erwägungen** für die Realisierung eines Geschäftsmodells abgestellt werden.[24]

Strengere Anforderungen stellt die DSK an die Belastbarkeit der Ausnahmeregelung für die **Verwendung** von **Cookie-IDs** (Nutzer-IDs). Für derartige Speicherungen bestehe **nur** in **wenigen Fällen** eine unbedingte **Erforderlichkeit**, **da** viele **Funktionen**, die eine Speicherung oder einen Zugriff auf Endgeräteinformationen

[19] Zustimmend DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 20.
[20] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 23.
[21] EuGH, Urt. v. 04.05.2017 – C-13/16, Rn. 30 – Rigas.
[22] EuGH, Urt. v. 11.12.2019 – C-708/18, Rn. 48 – M5A-ScarA.
[23] Vgl. auch EuGH, Urt. v. 17.Juni.2021 – C-597/19, Rn. 110 m. w. N. – Telenet BVBA.
[24] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 22.

bedingen, **ohne** eine **Individualisierung erfolgen** können. Als **Negativbeispiel** führt die DSK z. B. die Nutzung einer **langfristig gespeicherten ID** für folgende Use Cases an:

- Protokollierung einer Einwilligung in einer Consent-Management-Plattform (CMP),
- Load-Balancing sowie
- Speichern von Einstellungen zur Sprache oder der Hintergrundfarbe.

Nicht ausgeschlossen ist nach Ansicht der DSK die **Anwendung der Ausnahmeregelungen** vom Einwilligungserfordernis bei der Nutzung ein und desselben **Cookies** für mehrere **unterschiedliche Zwecke**. Voraussetzung sei jedoch, dass für jeden einzelnen Zweck einer der Ausnahmen in § 25 Abs. 2 Nr. 2 TTDSG einschlägig sei.[25]

Nach Ansicht der **Datenschutzkonferenz** sind maßgebliche **Kriterien** für die Bestimmung des **von Nutzern** ausdrücklich **gewünschten Diensten**:[26]

- Granulare Festlegung, für welche Funktion des Telemediendienstes welcher konkrete Speicher- und Auslesevorgang von Informationen auf dem Endgerät erfolgt;
- Bestimmung, wessen primären Interessen diese Funktion dient: den eigenen Interessen der Anbieter, den Interessen der Nutzenden der Webseite, den Interessen des eingebundenen Drittdienstleisters oder den Interessen von Dritten.

Maßgebende **Kriterien** für die Bestimmung der **unbedingten Erforderlichkeit** seien:

- Zeitpunkt der Speicherung – Wann darf der Auslese- und Speichervorgang stattfinden?
- Inhalt der Informationen – Welche Informationen werden gespeichert und ausgelesen?
- Dauer der Speicherung der Informationen – Wie lange werden Informationen auf den Endgeräten gespeichert und für welchen Zeitraum können sie ausgelesen werden?
    - Der Zeitraum der Speicherung dürfe nur so lang gewählt werden, wie für die Umsetzung der granularen Funktion des Telemediendienstes erforderlich sei.
    - Grundsätzlich seien Session-Cookies eher erforderlich als langlebige Cookies.
- Auslesbarkeit der Informationen – Für wen sind Informationen vom Endgerät auslesbar und verwertbar?
    - Werden Informationen auf dem Endgerät der Nutzenden bei der Inanspruchnahme eines Telemediums gespeichert, müsse technisch sichergestellt werden, dass diese nachfolgend grundsätzlich nur von den Betreiber:innen der jeweiligen Webseite ausgelesen werden könnten.
    - Bei Third-Party-Cookies sei dies gerade nicht der Fall, so dass sichergestellt sein müsse, dass Drittdienstleister die ausgelesenen Informationen grundsätzlich ausschließlich für die von Nutzenden aufgerufenen Webseite verwendeten.

c) Zwischenfazit zum Nutzer-Tracking ohne Reduzierung der Datenparameter

Im Rahmen einer **Erforderlichkeitsprüfung** bezogen auf **das Third-Party-Tracking** für Nutzeranalysen wird man mit hinreichender Sicherheit zu dem Ergebnis gelangen, dass ohne Modifikation der Tracking-Parameter **keine unbedingte Erforderlichkeit** nach Art. 5 Abs. 3 S. 2 ePrivacy-RL vorliegen kann, da ein Third-Party-

[25] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 24.
[26] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 26 f.

Tracking stets den Kreis der Datenempfänger über den eigentlichen Diensteanbieter oder Vertragspartner hinaus erweitert, teils sogar in unkontrollierter Weise.

Solange eine vom Website-Betreiber selbst vorgenommene First-Party-Analyse ohne Einsatz von Drittanbietern möglich ist, wird man unter Berücksichtigung der genannten EuGH-Rechtsprechung und der Auffassung der DSK zum Website-Tracking nicht zur Erforderlichkeit für den Einsatz von Drittanbietern gelangen.[27]

2. Abgrenzung Endgerätezugriff, -Speicherung und nachgelagerte Verarbeitung

(1) Findet **kein direkter und unmittelbarer Zugriff oder Speicherung** der Informationen auf die **Endgeräteressourcen** eines Nutzers statt, etwa im Fall einer programmatischen Verarbeitungskette oder serverseitigen ex post Betrachtungen von aus technischen Gründen geschaffenen Logfiles, lässt sich in Übereinstimmung mit der **Ansicht des EuGH** und der **Aufsichtsbehörden** vertreten, dass die **Verarbeitung** von weitergeleiteten **Nutzungsdaten** (v. a. die IP-Adresse des Nutzers) zur Website-Analyse oder im Rahmen der Platzierung eines auf die individuellen Interessen eines Nutzers zugeschnittenes Werbemittels **nicht mehr von Art. 5 Abs. 3 S. 1 ePrivacy-RL erfasst** ist (kein Zugriff auf das Endgerät und keine Speicherung von Informationen aus Endgerät). Vielmehr stellt diese Verarbeitung eine dem Schutzbereich der ePrivacy-RL **nachgelagerte Verarbeitungsphase** dar.

Nachgelagerte Verarbeitungsphasen sind allein am **Maßstab der DSGVO** zu messen und ermöglichen eine flexiblere Handhabung. Gemeint sind im Nachgang der von dem Wortlaut in Art. 5 Abs. 3 S. 1 ePrivacy-RL erfassten Verarbeitungsphasen „Zugriff" und „Speicherung" stattfindende Verarbeitungsprozesse wie die Übermittlung oder Verwendung von Tracking-Daten.

(2) Der **EuGH** hat sich in der Entscheidung zum **One-Stop-Shop-Verfahren**[28] der Ansicht des EDPB angeschlossen, wonach der Anwendungsbereich der „special rule" in Art. 5 Abs. 3 ePrivacy-RL lediglich das Speichern und das Lesen von personenbezogenen Daten mittels Cookies erfasst. Die Regelung in Art. 5 Abs. 3 ePrivacy-RL gelte jedoch nicht für alle früheren Vorgänge und späteren Verarbeitungen der personenbezogenen Daten mittels entsprechender Technologien.

Der **EPDB** hat in seiner „Stellungnahme 5/2019 zum Zusammenspiel zwischen der e-Datenschutz-Richtlinie und der DSGVO" für den Fall des Targeting **klargestellt**, dass allein die **DSGVO für** die Beurteilung der **Rechtmäßigkeit** etwa der *„[…] Speicherung und Analyse von Daten über die Web-Browsing-Aktivitäten zum Zweck von Werbung auf Basis von Behavioural Targeting oder zu Sicherheitszwecken […]."* heranzuziehen ist.

In diesem Sinne hat bereits der **Conseil d'État** zu einem Bußgeldbescheid der CNIL gegen Google aufgrund einer mangelhaften Einwilligung für das Nutzer-Tracking den Standpunkt vertreten, dass der in der DSGVO enthaltene One-Stop-Shop Mechanismus für die Kontrolle und Sanktionierung der Vorgänge zum Zugriff auf oder zum Schreiben von Cookies im Endgerät von Nutzern nicht anwendbar sei, da diese in den Anwendungsbereich der ePrivacy-RL fallen.

(3) Schließlich wird im Gesetzesentwurf der Bundesregierung für das TTDSG ausdrücklich auf die **Anwendung der DSGVO für nachgelagerte Verarbeitungsphasen** hingewiesen.[29]

[27] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 27.
[28] EuGH, Urt. v. 15.06.2021 – C-645/19 – One-Stop-Shop, Rn. 74.
[29] BT-Drs. 19/27441, S. 38.

(4) Selbst wenn unter der Annahme, **Server-Side-Tracking sei stets eine** nachgelagerte Verarbeitungsphase ohne Endgerätezugriff und damit ausschließlich der Anwendungsbereich von Art. 6 Abs. 1 DSGVO eröffnet, ist ein Rückgriff auf Art. 6 Abs. 1 S. 1 lit. b) oder lit. f) DSGVO zumindest im Fall einer Nutzung von Third-Party-Tracking wie Google SSGTM nach einhelliger Auffassung europäischer Aufsichtsbehörden unzulässig.

Die Rechtsgrundlage nach **Art. 6 Abs. 1 S. 1 lit. b) DSGVO greift ins Leere**, weil die Verarbeitung zur Erfüllung eines Vertrages erforderlich sein müsste. Der Besuch einer Website mit E-Commerce-Angeboten oder redaktionellen Inhalten begründet bereits nicht einmal ein irgendwie geartetes Vertragsverhältnis, geschweige denn ist eine Anfertigung von Nutzungsprofilen oder Analyse des Nutzungsverhaltens zur Auslieferung von Inhalten, zum Versand von Waren oder zur Erbringung von Diensten ohne gesonderte und transparente Vereinbarung (z.B. Nutzerkonto) unbedingt erforderlich.

In den Leitlinien 2/2019 des EDPB wurde klargestellt, dass die Rechtsgrundlage aus Art. 6 Abs. 1 S. 1 lit. b) DSGVO zur Vertragsdurchführung nicht für Zwecke „service improvement", „online behavioural targeting" und „personalisation of content" herangezogen werden könne. Analyseverfahren oder Verarbeitungen zum Zwecke der personalisierten Werbung fallen demnach nicht unter diese Rechtsgrundlage. [30]

Vor dem Hintergrund der strengen EuGH-Rechtsprechung zur **dreistufigen Interessenabwägung** im Rahmen von **Art. 6 Abs. 1 S. 1 lit. f) DSGVO**[31] wird man auch überwiegende berechtigte Interessen bei einem Third-Party-Tracking ablehnen müssen.

> *„[…] Nach Art. 7 Buchst. f) der Richtlinie 95/46 ist die Verarbeitung personenbezogener Daten und drei kumulativen Voraussetzungen zulässig: berechtigtes Interesse, das von dem für die Verarbeitung Verantwortlichen oder von den Dritten wahrgenommen wird, denen die Daten übermittelt werden (1), Erforderlichkeit der Verarbeitung der personenbezogenen Daten zur Verwirklichung des berechtigten Interesses (2) und kein Überwiegen der Grundrechte und Grundfreiheiten der betroffenen Person (3) […]".*

Unter Berücksichtigung der EuGH-Rechtsprechung zur zweiten Stufe der Erforderlichkeit[32] und Auffassung der Datenschutzkonferenz zum Website-Tracking wird man ohne weitere Modifikation des Trackings nicht zur Erforderlichkeit für den Einsatz von Drittanbietern gelangen.[33]

(5) Aus diesem Grund bedarf es einer weiteren Reduzierung der verarbeiteten Datenparameter und damit der grundrechtlichen Eingriffstiefe, um Art. 6 Abs. 1 S. 1 lit. f) DSGVO belastbar anwenden zu können.

3. Fazit: Bedürfnis nach langfristigen Strategien für das Risikomanagement

Angesichts unzureichender Branchenlösungen für das Server-Side-Tracking (vgl. Pkt. I.1.) und fehlender Praktikabilität, die von Aufsichtsbehörden mitgeteilten Anforderungen an eine ausdrückliche Einwilligung für den Drittlandtransfer zu erfüllen, wächst das Bedürfnis nach langfristigen und nachhaltigen Strategien zur rechtskonformen und erfolgreichen Datennutzung von Drittanbietern mit globalen Infrastrukturen.

Eine Lösung für die Verflechtungen und Risiken im Bereich des Website-Tracking stellen Middleware-Konzepte wie die JENTIS SaaS-Lösung dar. **JENTIS** ermöglicht eine **flexible Konfiguration** der SaaS-Lösung, um der Volatilität der jeweiligen **individuellen Risikolage** von Unternehmen Rechnung zu tragen. Auf diesem Wege

[30] Zustimmend DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 30; Vorabentscheidungsverfahren anhängig beim EuGH, C-252/21.
[31] Vgl. EuGH, Urt. v. 17.Juni.2021 – C-597/19, Rn. 106 m. w. N. – M.I.C.M.
[32] Vgl. EuGH, Urt. v. 17.Juni.2021 – C-597/19, Rn. 110 m. w. N. – M.I.C.M.
[33] Vgl. DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 31 mit Verweis auf DSK, Orientierungshilfe für Anbieter von Telemedien, 2019, S. 13 sowie S. III Anhang I.

versetzt die JENTIS-Twin-Server Technologie Unternehmen beim Einsatz von Tracking-Technologien von Drittanbietern in die Lage, die rechtlichen **Anforderungen** in der **Supply Chain sicherzustellen**.

III. Wie JENTIS dabei hilft, rechtliche Risiken auszuräumen

(1) Die **JENTIS SaaS-Lösung** ermöglicht datenschutzkonformes **Server-Side-Tracking**. Dabei bietet JENTIS die Möglichkeit, Daten von der eigenen Website an JENTIS-Server zu übertragen und diese von dort aus an verschiedene andere Datenempfänger zu übermitteln und agiert in dieser Funktion selbst wie ein **technischer Vorfilter oder Proxy**.

Die Nutzerdaten werden zunächst unmittelbar als **First-Party-Daten** auf der Website erfasst. Die JENTIS SaaS-Lösung ermöglicht mithilfe eines **serverseitigen Taggings** eine reduzierende und substituierende Filterung von Datenströmen, bevor diese an Drittanbieter wie Google oder Facebook weitergeleitet werden. Dadurch erhält der Website-Betreiber als für die Verarbeitung Verantwortlicher die volle Kontrolle über die Daten beim Einsatz von Tracking-Anwendungen von Dritten.

(2) Die JENTIS SaaS-Lösung besteht aus folgenden zentralen **DCP-Komponenten**:

- JENTIS Tag Management,
- JENTIS Consent Management, und
- JENTIS Server Suite.

Alle **JENTIS-DCP Komponenten** werden **ausschließlich** in der **Europäische Union** (Österreich und Deutschland) betrieben.

(3) Für die Nutzung der JENTIS SaaS-Lösung ist sowohl ein DNS-Setup für die eigene Website als auch die Implementierung eines JavaScript Basis-Tracking-Codes von JENTIS im Quellcode der Website notwendig. Im Anschluss können über die JENTIS SaaS-Lösung First-Party-Daten von Website-Nutzern erhoben werden, ohne dass ein Zugriff durch Drittanbieter erfolgt.

Beim Einsatz der JENTIS Lösung werden vom Endgerät des Nutzers empfangene First-Party-Daten an den **JENTIS-Twin-Server** gestreamt, wo bei entsprechender Konfiguration alle **Third-Party-Komponenten entfernt** und so **ersetzt werden**, dass **weder** ein unmittelbarer **Endgerätezugriff noch** eine **unmittelbare Übermittlung** von Nutzerdaten wie der IP-Adresse und User-IDs im Rahmen einer unmittelbaren Serveranfrage des Browsers des Nutzers an Drittanbieter-Server erfolgt.

Aufgrund des Twin-Servers, der zwischen dem Endgerät des Nutzers und dem Drittanbieter steht, wird eine direkte Verbindung zwischen dem Browser des Nutzers und dem Drittanbieter von vornherein abgebrochen. Die Twin-Server-Technologie ermöglicht die Umwandlung von First-Party-Daten in modifizierte künstliche Daten (Twin-Daten), bevor diese an Server der Drittanbieter weitergegeben werden können. JENTIS Twin-Daten können als Originaldaten beibehalten oder als pseudonymisierte oder anonymisierte Daten konfiguriert werden.

Der Kunde erhält von JENTIS eindeutige Zugangsdaten, um das Interface von JENTIS nutzen zu können. In diesem kann der Kunde Einstellungen sowohl für den ausschließlich auf Servern gehosteten JENTIS Tag Manager als auch für den JENTIS DCP vornehmen.

(4) Durch JENTIS Lösung verfügt der Kunde über die Kontrolle, um zu entscheiden, welche Datenvariablen verarbeitet, entfernt, modifiziert und weitergeleitet werden sollen. Der Kunde hat eine

Auswahl von mehr als 400 Variablen. Die folgende Tabelle ist anhand von Beispielen zu entnehmen, wie der JENTIS-Kunde Datenparameter pseudonymisieren kann:

Datenparameter	Beschreibung
IP-Adresse	Diese muss aus technischen Gründen zwingend übertragen werden und wird dann am JENTIS-Server je nach Konfiguration entweder um das letzte Oktett gekürzt oder nach Abgleich mit einer Geo-Datenbank vollständig entfernt und durch einen künstlichen Wert ersetzt.
User-ID von JENTIS	Sie ist eine zufällig generierte Zahlenkombination und dient vor allem der Wiedererkennung des Website-Besuchers.
Kundenspezifische IDs	Dabei handelt es sich etwa um Order-IDs. Diese Daten werden von JENTIS nicht weiterverarbeitet, sondern als Zufallsprodukt neu erzeugt.
Client-IDs für externe Tools	Einige externe Tools benötigen selbst eine Client-ID, um Website-Besucher zu erkennen. Derartige Client-IDs werden am JENTIS-Server neu erzeugt und eine fiktive Client-ID an das externe Tool geschickt.
Browser Umgebungsdaten	Diese Daten werden im Browser des Website-Besuchers ausgelesen und an den JENTIS-Server geschickt. Dabei handelt es sich um statische Daten, die durch das Device des Website-Besuchers festgelegt sind.
Nutzer Aktionsdaten	Diese Daten werden im Browser des Website-Besuchers ausgelesen und an den JENTIS-Server geschickt. Dabei handelt es sich um Daten, welche die Aktionen des Website-Besuchers auf der Webseite beschreiben.
Zeitstempel (time stamp)	Es wird der time Stampe – aus der Serveranfrage des Browsers des Website-Besuchers bestehend aus Datum und Zeitangabe (UTC) an den JENTIS-Server gesendet.

Für die **Konfiguration** der **JENTIS-Twin-Server** sind lediglich die folgenden **vier Schritte** erforderlich:

- **Erstens** ist eine **Identifizierung** der Drittanbieter-Tags und jeweils abgefragten **Datenparameter** erforderlich.
- **Zweitens** erfolgt die Festlegung der risikobehafteten und zu modifizierenden (durch **Pseudonymisierung oder Anonymisierung)** Datenparameter.
- **Drittens** erfolgt die **Modifizierung** der festgelegten **Datenparameter** in der **JENTIS Suite**.
- **Viertens** sollte ein **Testen** der Modifizierung von Datenparameter **zur Qualitätssicherung** erfolgen.
- **Fünftens** kann nach erfolgreichem Test die JENTIS Lösung **live** geschaltet werden.

(5) Für die **rechtliche Beurteilung** der beschriebenen **Risiken und Rechtsunsicherheiten** (Pkt. II.) ergeben sich **zwei wesentliche Verarbeitungsschritte** in Bezug auf Nutzerdaten:

Zum einen der Endgerätezugriff, ausgelöst durch die Anfrage des Browsers des Nutzers an JENTIS Server zur Wiedererkennung eines Browsers des Nutzers über First-Party-Cookies durch Vergabe einer zufällig

generierten JENTIS User-ID für die vom Kunden festgelegten Use Cases. Die Laufzeit der JENTIS User-ID kann nach der Risikoaffinität der Kunden individuell sitzungsbezogenen oder persistent bis zu 24 Monate festgelegt werden.

Zum anderen die serverseitige Übermittlung der nach der Filterung bereinigten Tracking-Daten (Session ID, User ID, User Agent, demographische Standortdaten) an Server von Anbietern wie Google in Drittländern.

Auf Grundlage des skizzierten Funktionsprinzips der konfigurierten JENTIS DCP **(1.)** bei entsprechender Konfiguration Essential Mode kann auf die Abfrage einer Einwilligung verzichtet werden. Der First-Party-Endgerätezugriff lässt sich als „unbedingt notwendig" einstufen **(2.)** und die Datenübermittlung an Drittanbieter im Rahmen einzelner Use Cases aufgrund einer Modifizierung der Datenparameter der Browser-Session des Nutzers als wirksames Mittel der Pseudonymisierung auf die Rechtsgrundlage aus Art. 6 Abs. 1 S. 1 lit. f) DSGVO stützen **(3.)**.

1. Funktionsprinzip der konfigurierten JENTIS DCP

Folgende Funktionsprinzipien der JENTIS DCP können nur bei entsprechender Konfiguration durch Kunden ermöglicht werden:

(1) JENTIS fungiert als Middleware als eine Art Gatekeeper zwischen Browser des Website-Besuchers und Server von Drittanbietern. Damit besteht die Möglichkeit, alle gesammelten Daten vor dem Transfer an Drittanbieter DSGVO-konform zu durch Modifizierung zu pseudonymisieren (vgl. eingehend Pkt. III. 3 sowie die JENTIS Privacy Knowledge Base). Der Kunde bestimmt im JENTIS Tag Manager, welche Daten im Browser des Website-Besuchers ausgelesen und an JENTIS gesendet werden sollen. Auf Ebene der Datenparameter kann der Kunde festlegen, ob es sich bei den einzelnen Datenparametern um ein für den Drittlandtransfer relevantes Datum handelt.

Auf dieser Weise kann eine Parametrierung des Systems entlang der Vorgaben des jeweils anwendbaren Rechts in der Einsatzregion (GDPR [EU], PECR [UK], CCPA [CA], LGPD [BR], PIPL [CN] etc.) erreicht werden.

(2) Der Kunde bestimmt durch das Hinzufügen von "Trackern", welcher externe Drittanbieter Daten von JENTIS erhalten sollen. Dabei konfiguriert der Kunde jeden dieser Tracker so, dass klar bestimmt ist, welcher Datenparameter an den externen Drittanbieter übergeben werden soll. Bei jedem zu übergebenden Datenparameter, das als relevant eingestuft wurde, bestimmt der Kunde außerdem, ob vor der Weitergabe an den externen Anbieter eine Entfernung der Datenparameter, eine Pseudonymisierung durch Modifizierung der Datenparameter [vgl. hierzu Pkt. III. 2.] durchgeführt werden soll.

(3) Die detailgenaue Entfernung und Pseudonymisierung durch Modifizierung der Datenparameter ist möglich, weil die Browser-Session des Nutzers auf einem JENTIS Twin-Server 1:1 gespiegelt wird. So lassen sich individuell risikobehaftete Datenparameter nach Ansicht der jeweiligen zuständigen Aufsichtsbehörde nach dem Bedürfnis der Website-Betreiber die Risiken sinnvoll minimieren oder austauschen.

Die Rohdaten der Browser Session des Nutzers können vollständig gelöscht werden.

(4) In der JENTIS Server Suite findet im Data Backend eine Modifikation der Tracking-Daten dahingehend statt, dass z.B. die letzte Ziffer der IP-Adresse des Website-Besuchers, vor der Verarbeitung und der Weitergabe an die Drittanbieter gekürzt wird. Es ist als Option denkbar, vor Entfernung der IP-Adresse des Nutzers anhand einer auf dem Webserver hinterlegten Geo-Datenbank eine Zuordnung zu dem Land und der Stadt des Endgeräts, von dem die Anfrage gesendet wurde, einzufügen. Die IP-Adresse ist zur Standortermittlung

notwendig. Im Rahmen der Weiterverarbeitung werden sodann lediglich demographische Standort-Daten (Land/Stadt) an Dritte übermittelt, aber nicht die identifizierenden Bestandteile der IP-Adresse des Website-Besuchers.

Daten von Drittanbietern, wie z.B. Client-IDs oder User-IDs von Drittanbietern im Fall von Google Analytics, die eine eindeutige Zuordnung des Endgerätes ermöglichen, werden innerhalb der JENTIS Server Suite bei entsprechender Konfiguration pseudonymisiert und die neu generierten IDs als neuerzeugte fiktive Client-ID an den jeweiligen Drittanbieter gesendet. Dabei ist zu beachten, dass der Bezug von neu erzeugten IDs und der JENTIS-User-ID gespeichert wird. Auf diese Weise können User und Sessions von Kunden erkannt werden.

Ebenso werden bei entsprechender Konfiguration Datenparameter, die eine eindeutige Identifizierung der Nutzer ermöglichen, z.B. Order-IDs, von JENTIS nicht verarbeitet, sondern als Zufallsprodukt neu erzeugt.

(5) Die bereinigten Tracking-Daten, d. h. die modifizierten und ausgetauschten IDs der Drittanbieter nebst Informationen zum Nutzerverhalten (z. B. Events), werden vom JENTIS Server an den Drittanbieter-Server, z. B. Google Server übertragen. Es erfolgt weder eine Übertragung der von Google vergebenen Client-ID, die Kunden eigenen IDs noch der IP-Adresse des Nutzers.

(6) Mithilfe der von JENTIS erzeugten (eigenen) User-ID stellt nun der JENTIS Server und nicht der Client des Nutzers eine Anfrage an den Drittanbieter z. B. an Google zur Auslieferung des Analytics Scripts.

2. Bewertung der Endgerätezugriffe durch JENTIS-Server als „unbedingt erforderlich“

Die aufgrund der Serveranfrage des Browsers des Nutzers an den JENTIS Server erfolgte Auslieferung des First Party JavaScripts und des First-Party-Cookies von JENTIS bedingt bei Nutzung des JENTIS Tag Managers **(a)**, des JENTIS DCP **(b)** und der JENTIS Twin-Server-Technologie einen Zugriff auf Endgerätekapazitäten des Browsers des Nutzers **(c)**.

Bei der entsprechenden Konfiguration der JENTIS DCP, lässt sich dieser Vorgang als „unbedingt erforderlich“ nach Art. 5 Abs. 3 S. 2 ePrivacy-RL einstufen (vgl. III. 2. c.).

a) JENTIS Tag Manager

(1) Beim Aufruf der Website mit verbauten JENTIS Basis Tracking Code und eingerichteten DNS Record wird eine **https-Anfrage (Request) an JENTIS** gesendet. Aufgrund dieser Anfrage werden die **IP-Adresse des Nutzers** sowie System- und Browserinformationen an JENTIS **übermittelt**.

Für die bloße **Einbindung** eines **Tag-Managers** als „Container-Lösung“ muss noch **keine Einwilligung vom Nutzer** abgefragt werden, weil die Ausnahme vom Einwilligungserfordernis gemäß Art. 5 Abs. 3 S. 2, Var. 1 ePrivacy-RL herangezogen werden kann. Dies ergibt eine Anwendung der vom EDPB entwickelten Kriterien (vgl. Pkt. II. 1. a.). Denn für die lediglich technisch veranlasste Übermittlung der IP-Adresse des Nutzers und weiterer Endgeräteinformationen wie z. B. Browserinformationen ist grundsätzlich der Ausnahmetatbestand in Art. 5 Abs. 3 S. 2 RL einschlägig, soweit nicht ungefiltert weitere Nutzerdaten an Drittanbieter übermittelt werden.

(2) Die Nutzung des **JENTIS Tag Managers** erleichtert die elektronische Kommunikation, indem Informationen u.a. über Programmierschnittstellen an Drittanbieter übergeben werden. In dem Tag-Manager werden die jeweiligen Code-Snippets der Drittanbieter implementiert, ohne dass ein Website-Betreiber selbst den Quellcode der Website aufwändig ändern muss. Die Einbindung erfolgt stattdessen durch einen Container.

Dadurch bietet der Tag-Manager auch für Anwender ohne vertiefte IT-Kenntnisse die Möglichkeit, komplexe Drittanbieter-Tools auf der Website einzubetten. Außerdem erlaubt der JENTIS Tag-Manager, die Datenparameter der Nutzer in einer bestimmten Reihenfolge auszutauschen, insbesondere durch Ordnung und Systematisierung der Datenpakete.

b) JENTIS und Consent Manager

(1) Das **JENTIS DCP verbindet** sich im Browser zu **anderen** installierten **CMPs** wie z.B. User Centrics, um die Consent Informationen von dort zu erhalten und dann selbst danach die weitere Verarbeitung zu steuern. Der Einsatz des **JENTIS DCP** ermöglicht die Abfrage einer den datenschutzrechtlichen Anforderungen entsprechenden Einwilligung, z.B. für eine Nutzung von Drittanbietertools wie Google Analytics. Jedoch können Dienste zur Bereitstellung von Nutzerpräferenzen wie der **JENTIS DCP** ohne Abfrage einer Nutzereinwilligung zulässig sein.[34]

(2) Cookies und ähnliche Technologien dürfen nach auch Ansicht der DSK z. B. für etwaige Zusatzfunktionen des Basisdienstes Website genutzt werden, wenn diese vom Nutzer angefordert werden, was z.B. beim Einsatz von CMPs der Fall sei.[35] JENTIS DCP verarbeitet die Einwilligung von anderen CMP-Anbietern. Die Einbindung und Bereitstellung der Funktionen der CMPs durch JENTIS DCP ist in vertretbarer Weise **als in zulässiger Weise einwilligungsfrei** anzusehen.

(3) JENTIS verarbeitet bei der Anbindung des JENTIS DCP an eine andere installierte CMP **keine** langfristig in Cookies der CMP gespeicherte **User-IDs der CMP**.[36] Da JENTIS keinen Zugriff auf andere CMP-Cookies nehmen kann, die der Kunde in seine Website eingebunden hat, speichert JENTIS eine Consent-ID serverseitig zur Erfüllung der Protokollierungspflicht der Nutzer-Einwilligung nach Art. 7 Abs. 1 DSGVO und zur Erfüllung etwaiger Auskunftsersuchen von Betroffenen. Anders als in der DSK in ihrer Orientierungshilfe Telemedien argumentiert[37] hat der JENTIS als externer Dienstanbieter keine Möglichkeit die Nutzerpräferenzen für die Einstellungen in der CMP in einem Cookie zu speichern. Deshalb lässt sich die Verarbeitung der Consent ID als „unbedingt erforderlich“ nach Art. 5 Abs. 3 S. 2, Var. 2 ePrivacy-RL bzw. § 25 Abs. 2 Nr. 2 TTDSG einordnen.

c) JENTIS Essential Mode / Fall-Back-Lösung

Die JENTIS-Twin-Server Technologie ermöglicht die wirksame Verwendung von Website-Daten in beiden Situationen – bei expliziter Einwilligung des Nutzers (Tracking-Modus) und bei nicht vorhandener Einwilligung des Nutzers (als Fall-Back Lösung – JENTIS Essential Mode). Die Unternehmen können den „JENTIS Essential Mode“ als Fallback-Lösung für das First-Party-Tracking so konfigurieren, dass die Anwendung der Ausnahmevorschriften vom Einwilligungserfordernis für den Endgerätezugriff konform und effektiv umgesetzt werden. Dadurch wird eine „Nutzungsanalyse“ in einem reduzierten Umfang ohne Nutzerstimmung möglich, wenn der Nutzer das Cookie-Banner gar nicht anklickt oder keine Einwilligung erteilt. Dies wird anhand einer Beispielkonfiguration für den JENTIS Essential Mode demonstriert (**aa**) auf Grundlage der Anforderungen von Aufsichtsbehörden (**bb**).

[34] Art. 29-Datenschutzgruppe, WP 194, Stellungnahme 04/2012 zur Ausnahme von Cookies von der Einwilligungspflicht, S. 7 f., ICO, Guidance on the use of cookies and similar technologies, S 37.
[35] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 21.
[36] Vgl. dazu DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 26.
[37] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 26.

(1) Vorbehaltlich einer künftig anderslautenden Positionierung von Aufsichtsbehörden oder der Rechtsprechung ist die Anwendung der Ausnahmevorschrift vom Einwilligungserfordernis in Art. 5 Abs. 3 S. 2 ePrivacy-RL bzw. § 25 Abs. 2 Nr. 2 TTDSG bei der entsprechenden Konfiguration von JENTIS gewährleistet.

Durch die Verwendung von First-Party-Daten und die **Minimierung** der **Datenparameter auf** das technisch Notwendige bzw. das **unbedingt Erforderliche** kann der Kunde die Nutzerdaten im Essential Mode bzw. **als Fall-Back-Lösung** verfolgen, wenn der Nutzer seine Zustimmung nicht erteilt. Die Belastbarkeit der Ausnahmeregelung nach § 25 Abs. 2 Nr. 2 TTDSG für den notwendigen Zugriff auf das Endgerät in Form eines First-Party-Cookies setzt dabei voraus, dass der „**Essential Mode**" von **JENTIS** aktiviert wurde und in einer bestimmten Weise **konfiguriert** wird (vgl. Pkt. III. 2. c. aa.).

Im Ausgangspunkt steht der Anwendung der Ausnahmevorschriften nicht entgegen, dass das First-Party-Cookie von JENTIS **multifunktional** eingesetzt wird, weil es mehreren **unterschiedlichen Zwecken** dient.[38]

(2) Die aufgrund der Serveranfrage des Browsers des Nutzers an den JENTIS Server erfolgte **Auslieferung** des **First-Party-Cookies von JENTIS** bedingt einen Zugriff auf Endgerätekapazitäten des Browsers des Nutzers.

Die in der **Serverantwort** des JENTIS-Servers erfolgte **Speicherung** eines **First-Party-Cookies** nebst zufällig generierter **Client-ID dient** der Wiedererkennung des Endgeräts, um mithilfe eines serverseitigen Taggings eine **reduzierende** und **substituierende Filterung** von **Datenströmen** zu ermöglichen, bevor diese an Drittanbieter wie Google oder Facebook weitergeleitet werden. Dadurch wird der Verlust der Kontrolle beim Einsatz von Tracking-Anwendungen von vornherein verhindert und eine **rechtmäßige Datenverarbeitung** ermöglicht.

(3) Die durch die JENTIS Twin-Server-Technologie erfolgte **Reduzierung** und **Modifizierung** der **Datenparameter** für das Server Side Tracking, die im Zuge der Nutzerkommunikation mit der Website abgefragt werden (vgl. Pkt. III. 1.), **lässt sich** ebenfalls im Einklang mit der Auffassung des Europäischen Datenschutzbeauftragten (**EDPS**) in vertretbarer Weise **auf** die **Ausnahme vom Einwilligungserfordernis** gemäß Art. 5 Abs. 3 S. 2 Var. 2 ePrivacy-RL und § 25 Abs. 2 Nr. 2 TTDSG **stützen**.

Der **EDPS** hat ein „**Toolkit**" zur **Festlegung** für die **Beurteilung** der **„Erforderlichkeit"** von Maßnahmen in Übereinstimmung mit Art. 52 Abs. 1 GRCh veröffentlicht.[39]

> *„[…] Das Toolkit besteht aus dieser Einleitung, in der Inhalt und Zweck des Toolkits dargestellt werden, einer praktischen, in einzelne Schritte untergliederten **Checkliste für die Beurteilung der Erforderlichkeit** neuer Legislativmaßnahmen und einer **rechtlichen Analyse der Prüfung der Erforderlichkeit** der Verarbeitung personenbezogener Daten. […]"*

Diese **Kriterien** können nach Medieninformationen auch der Ansicht der Datenschutzorganisation „La Quadrature du Net" zufolge als **Orientierung** für die **Auslegung** des **Begriffs** der „**Erforderlichkeit**" nach der Art. 5 Abs. 3 S. 2 ePrivacy-RL **dienen**. Ebenso hat der **EDPB** in den „Leitlinien 2/2019" zur Auslegung des Begriffs der Erforderlichkeit **auf** das **Toolkit** des **EDPS** für den nicht-öffentlichen Bereich **Bezug genommen**.[40] Deshalb

[38] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 24.
[39] EDPS, Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit, 2017, S. 5.
[40] EDPB, Leitlinien 2/2019 für die Verarbeitung personenbezogener Daten gemäß Artikel 6 Absatz 1 Buchstabe b DSGVO im Zusammenhang mit der Erbringung von Online-Diensten für betroffene Personen, V2.0, S.9, Fn. 19.

wird auch in der **Fachliteratur** zutreffend vertreten, dass die Checkliste für die Bestimmung der „unbedingten Erforderlichkeit" in Art. 5 Abs. 3 S. 2 ePrivacy-RL und § 25 Abs. 2 Nr. 2 TTDSG verwendet werden kann.[41]

Vorbehaltlich künftiger Rechtsprechung und aufsichtsbehördlicher Positionierungen kann die **Methodik** eine Grundlage für die Aktivierung ausgewählter Funktionalitäten auf Websites bilden und der unter Pkt. II 1. b. **geschilderten Rechtsunsicherheit entgegenwirken**.

Laut EDPS impliziert die **Erforderlichkeit** das Erfordernis einer kombinierten, auf Fakten gestützten Bewertung der Wirksamkeit der Maßnahme mit Blick auf das angestrebte Ziel und auf die Frage, ob sie im Vergleich zu anderen Optionen für das Erreichen desselben Ziels weniger eingreifend ist. Die **Checkliste für die Beurteilung der Erforderlichkeit** besteht aus **vier** aufeinander folgenden **Schritten**. Jeder Schritt entspricht einer Reihe von Fragen, die die Beurteilung der Erforderlichkeit erleichtern.[42]

(4) Nachfolgend wird eine **beispielhafte Konfiguration** für den **Essential Mode** von **JENTIS** , die nach unserem Dafürhalten aufgrund der Anwendung des EDPS Necessity Toolkit zur Auslegung der Erforderlichkeit den Einsatz der Tracking-Proxy-Technologie in vertretbarer Weise als „**unbedingt erforderlich**" ohne Vorliegen einer Nutzereinwilligung rechtfertigen lässt.

aa) Beispielkonfiguration statistische Analyse des Nutzungsverhaltens auf Websites mit Google Analytics durch JENTIS DCP

- **Schritt 1 EDPS Necessity Toolkit:** Die für des EDPS Toolkits der Bestimmung der Erforderlichkeit des Endgerätezugriffs verlangte detaillierte faktische Darstellung des technischen Funktionsprinzips zur Bereinigung der Tracking-Daten von Drittanbieter-Diensten wie Google Analytics und Reduzierung der Nutzerdaten sowie Zweckfestlegung ist erfolgt (vgl. Pkt. III. 1).
- **Schritt 2 EDPS Necessity Toolkit**: Die für Schritt 2 des EDPS Toolkits erforderliche Beantwortung von Fragen zur Bestimmung der Tragweite der Eingriffsintensität der JENTIS DCP ist in Anbetracht der detaillierten Beschreibung der einzelne Datenverarbeitungsschritte ebenfalls erfolgt (vgl. Pkt. III. 1.).
- **Schritt 3 EDPS Necessity Toolkit:** Als Schritt 3 des EDPS Toolkits wurde als Use Cases das Ziel einer grundlegenden statistischen Analyse des Nutzungsverhaltens von Website identifiziert, um in Ausprägung der von Art. 16 Abs. 1 EU-Grundrechte-Charta gewährleisteten unternehmerischen Freiheit digitale Angebote zu optimieren, verbessern und dem Stand der Technik entsprechend weiterzuentwickeln. Art. 23 DSGVO enthält nach Ansicht des EDPS eine Auflistung von Zielen, aufgrund derer legitimerweise die Rechte natürlicher Personen und die Pflichten des Verantwortlichen eingeschränkt werden können. Hierzu zählt nach Art. 23 Abs. 1 lit. i) DSGVO auch der Schutz der Rechte und Freiheiten anderer Personen, sprich auch juristischer Personen und deren nach Art. 16 Abs. 1 GRCh zu berücksichtigenden unternehmerischen Freiheiten.
- **Schritt 4 EDPS Necessity Toolkit:** Gemäß Schritt 4 des EDPS Toolkits wurden bei der Prüfung der Erforderlichkeit spezifische Aspekte für die **nachfolgende Beispielkonfiguration** des **Essential Mode** von **JENTIS** berücksichtigt:
    - **Modifizierung der Client-ID von Google Analytics:**

[41] Hense, in: Taeger/Pohle, Computerrechts-Handbuch, 2022, 37. EL, Projektspezifischer Datenschutz, Rn. 112.
[42] EDPS, Beurteilung der Erforderlichkeit von Maßnahmen, die das Grundrecht auf Schutz personenbezogener Daten einschränken: Ein Toolkit, 2017, S. 10.

- Die Client-ID/User-ID von Google Analytics, die eine eindeutige Zuordnung des Endgerätes ermöglicht, muss vollständig modifiziert, d. h. durch eine fiktive Client-ID/User-ID ersetzt werden.
- Die JENTIS User-ID wird als First-Party-Cookie über die Domäne des Kunden im Browser des Nutzers gespeichert. Die Verarbeitung der selbst von JENTIS vergebenen User-ID stellt die einzige Referenz für die Wiedererkennung des Browsers des Nutzers dar.
- Nach Ansicht des BGH stellt eine in Cookies gespeicherte zufallsgenerierten Nummer (**Cookie ID**), die als **Endgeräteinformation** Registrierungsdaten des Nutzers zugeordnet ist, ein **Pseudonym** i. S. d. § 15 Abs. 3 TMG dar, wobei der BGH noch auf die Legaldefinition in § 3 Abs. 6a BDSG a.F. abstellte.[43]
- Die Speicherdauer der JENTIS Cookies sollte auf maximal 13 Monate eingestellt werden.
- Die nach Art. 4 Nr. 5 DSGVO erforderliche Einschränkung für eine wirksame Pseudonymisierung, dass die Zusatzinformationen separiert aufbewahrt werden und durch technisch-organisatorische Maßnahmen abgesichert sind, die gewährleisten, dass keine Zuweisung der Daten zu einer identifizierbaren Person erfolgt, wird gewährleistet. Unabhängig davon, ob die zusätzliche Information eine direkte Zuordnung oder eine Zuordnungsregel sein kann,[44] wird die technische und organisatorische Absicherung mittels einer **robusten Trennung** der System-Cluster **Serverinstanzen** im Rahmen eines **Server-Side-Tracking** von JENTIS gewährleistet.
- Die Verarbeitung durch die JENTIS Server erfolgt auf getrennten Dateninstanzen, auf dem ggf. Bestandsdaten von Nutzern (z. B. E-Commerce-Shop) gespeichert werden.

- **Kürzung der IP-Adresse:**
  - Die IP-Adresse des Nutzers wird auf Server von JENTIS um das letzte Oktett gekürzt; es findet keine Kommunikation des Browsers des Nutzers mit Google Servern statt. Im Fall einer **Teil-Unkenntlichmachung** der IP-Adressen durch Kürzung des letzten Oktetts nach Übermittlung der vollständigen IP-Adresse ist nach Ansicht der Rechtsprechung von einer **Pseudonymisierung** i. S. d. § 3 Abs. 6a BDSG a.F. auszugehen, wie eine rechtskräftige Entscheidung des LG Frankfurt zum Webanalysedienst „Piwik" zeigt.[45]
  - Dabei lehnte das Gericht die Einordnung der Kürzung der IP-Adresse als Mittel der Anonymisierung insbesondere deswegen ab, weil ein Website-Betreiber, der über Registrierungsdaten aus Nutzerkonten verfügt, jederzeit in Echtzeit eine Zuordnung zu Identifikationsmerkmalen vornehmen könnte.
- **Entfernung von Click-IDs in URLs:**
  - Sollte der Nutzer eine Kunden-Website über die Suchmaschine google.com aufrufen, sollte die Google Click ID als URL-Parameter („gclid") entfernt werden.
- **Modifizierung von kundenspezifischen IDs:**

[43] BGH, Urt. v. 28.05.2020 – I ZR 7/16 – Cookie Einwilligung II, Rn. 72; zustimmend in Bezug auf die DSGVO Menke, K&R 2020, 650, 652; Baumgartner/Hansch, ZD 2020, 435, 436.
[44] Schwartmann/Weiß, Entwurf für einen Code of Conduct zum Einsatz DSGVO konformer Pseudonymisierung, 2019, v1.0, S. 11.
[45] LG Frankfurt, Urt. v. 18.2.2014 – 3-10 O 86/12, Rn. 36; zustimmend Weidert/Klar, BB 2017, 1858, 1859.

- Ebenso werden Datenparameter, die eine eindeutige Identifizierung der Nutzer ermöglichen, z. B. Order-IDs oder Lead-IDs von JENTIS nicht verarbeitet, sondern als Zufallsprodukt neu erzeugt.
- Dabei wird eine zufällige UUID (Universally Unique Identifier, eine 128-Bit-Zahl) erzeugt.

- **Modifizierung des User Agent:**
  - Der User Agent wird gelöscht und durch einen neu erzeugten User Agent ersetzt.
- **Kein Fingerprinting:**
  - Es darf keine Kombination von Browser- und Geräteeinstellungen zur Identifizierung und Wiedererkennung von Nutzern erfolgen.
- **Zweckreduktion:**
  - Die Zwecke im Rahmen des Use Case „Analyse“ wurden darauf beschränkt, die Bewertung veröffentlichter Inhalte und der Nutzerfreundlichkeit der Webseite zu ermöglichen und die Wirksamkeit gestalterischen Entscheidung der Website zu bewerten oder zu verbessern.
  - Der Einsatz der Analyse sollte aus Kundensicht auf die Erstellung anonymer Statistiken beschränkt werden.
- **Keine Zusammenführung von IDs**
  - Die JENTIS User-ID wird nicht mit anderen Nutzerdaten wie einer CRM-ID oder Systemen mit Registrierungsdaten zusammengeführt.
- **Unschärfegrade bei Timestamps**
  - Sofern eine Re-Identifizierung eines Nutzers oder ein singling-out eines einzelnen Nutzers anhand des Timestamps einer Browser-Session möglich ist, können mithilfe der JENTIS-Twin-Server Technologie die Zeitangaben durch fiktive Werte (fiktive Zeitstempel) ersetzt werden.
  - Alternativ kann mithilfe der JENTIS-Twin-Server Technologie bei einem gleichzeitigen Mindestaufkommen im jeweils gemessenen Zeitabschnitt in einer homogenen Gruppe eine bloße Mindestunschärfe der Timestamps ausreichend sein. Von dem Erreichen eines homogenen Mindestaufkommens von Nutzern, sprich einer Gruppe von Nutzern, die dieselben Attribute teilen, hängt der Unschärfegrad der Timestamps (Cluster auf Stunden- oder Minutenbasis) im Einzelfall ab.

bb) Anforderungen der Aufsichtsbehörden

(1) Ungeachtet dessen gelangt man auch unter **Anwendung** der **Auslegungskriterien** der **DSK** für die „unbedingte Erforderlichkeit“ (vgl. Pkt. II. 1. b.) und der **CNIL** für den Einsatz von Tracking-Proxys zu **keinem anderen Ergebnis**.

(2) Die **strengen Anforderungen** der **DSK** an die Belastbarkeit der Ausnahmeregelung für die **Verwendung** von in Cookies gespeicherten **Nutzer-IDs** (Cookie-IDs) werden bei Zugrundelegung des Funktionsprinzips des Essential Mode von JENTIS erfüllt:

- Zunächst schließt die DSK die Belastbarkeit der Ausnahmeregelung in Art 5 Abs. 3 S. 2 ePrivacy-RL und § 25 Abs. 2 Nr. 2 TTDSG für die Reichweitenmessung und/oder Analyse von Website-Besucherzahlen per-se nicht aus.[46]
- Der Zeitpunkt der Speicherung des Session-Cookies und das Auslesen der Client-ID findet im Zuge der Auslieferung der Website nach Interaktion mit dem Cookie-Banner statt.
- Nach Maßgabe der vorstehenden Beispielkonfiguration des Essential Mode für Google Analytics werden sämtliche Identifikatoren mit Ausnahme der JENTIS-User-ID reduziert und modifiziert**.** Der First-Party-Cooke wird über die Domäne des Kunden im Browser des Nutzers gespeichert.
- Die Speicherdauer der First-Party-Cookies kann individuell je nach Risikoaffinität entweder wenige Minuten – einzelnen Besuche (Sitzungen) sind dann nicht mehr zusammenführbar – oder bis zu 24 Monate festgelegt werden. Nach Lesart der Orientierungshilfe der DSK stellt das Kriterium der Speicherdauer lediglich eines von mehreren Kriterien dar und ist allein nicht ausschlaggebend für die rechtliche Beurteilung der „unbedingten Erforderlichkeit".[47]
- Der Endgerätezugriff erfolgt ausschließlich durch die Server von JENTIS als Auftragsverarbeiter. Es erfolgt kein clientseitiger Endgerätezugriff durch Server von Google oder anderer Drittanbieter.
- Insbesondere wird bei entsprechender Konfiguration von JENTIS auch der Anforderung aus Art. 5 Abs. 3 S. 2 ePrivacy-RL bzw. § 25 Abs. 2 Nr. 2 TTDSG „vom Nutzer ausdrücklich gewünschten Telemediendienst" entsprochen. Denn im Einklang mit der Ansicht der DSK wird in erster Linie den Interessen der Nutzenden der Website Rechnung getragen. Dabei bleiben die Interessen der Drittanbieter aufgrund der Modifizierung von Datenparametern außer Betracht. Die Interessen der Betroffen wird durch folgende Gesichtspunkte gestärkt:
    - Verhinderung unmittelbarer Zugriffe von Drittanbietern auf Endgerät von Nutzer:innen;
    - Zugriffsbeschränkungen und Kontrolle über die Weitergabe der Daten an Drittanbieter und
    - Sicherstellung der Rechtskonformität.

(3) Schließlich erfüllt JENTIS bei entsprechender Konfiguration der ebenso die Anforderungen der französischen Aufsichtsbehörde (CNIL) an Proxy-Lösungen beim Einsatz von Tracking-Diensten, die soweit ersichtlich, als erste europäische Behörde den Einsatz von Proxy-Lösungen für den Einsatz von Google Analytics empfiehlt.

- keine Übermittlung der vollständigen IP-Adresse des Nutzers an Server von Tracking-Diensten.
- Die Client-IDs und Nutzer-IDs, die von Drittanbietern vergeben werden, werden durch den JENTIS-Server vollständig ersetzt.
- Die Browser- und Geräte-Informationen lassen nach Maßgabe der Beispielkonfiguration für Google Analytics aufgrund der gebildeten künstlichen Werte, insbesondere für den User Agent, keine Identifizierung durch die Drittanbieter zu. Auf diesem Wege kann ein Fingerprinting verhindert werden. Der Algorithmus, der die Ersetzung der Browser-Informationen vornimmt, gewährleistet ein ausreichendes Maß an Kollisionen (d. h. eine ausreichende Wahrscheinlichkeit, dass zwei verschiedene Kennungen nach der Modifizierung ein identisches Ergebnis liefern).

[46] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 22.
[47] DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 26 f.

- Referrer können gelöscht werden (Hinweis: bei Entfernung des Referrer leidet die Qualität der Analyse).
- Etwaige in den gesammelten URLs enthaltene Tracking-Parameter können individuell gelöscht oder ersetzt werden (z. B. die „UTM-Parameter", aber auch die URL-Parameter, die das interne Routing der Website ermöglichen).
- Die vom Tracking Proxy vergebene Client-ID zur Wiedererkennung des Browser-Nutzers oder deterministisch mitgeteilte IDs (CRM, eindeutige ID) lassen keine websiteübergreifende (Cross-Site) oder geräteübergreifende Erfassung (Cross-Device) des Nutzerverhaltens zu.
- Sämtliche Nutzerdaten, die eine Re-Identifizierung durch Tracking-Anbieter ermöglichen können, werden gelöscht.

cc) Zwischenergebnis

Zusammenfassend lässt sich festhalten, dass aufgrund folgender Gesichtspunkte die Ausnahmeregelung vom Einwilligungserfordernis gemäß Art. 5 Abs. 3 S. 2 Var. 2 ePrivacy-RL und § 25 Abs. 2 Nr. 2 TTDSG bei Nutzung des Essential Mode von JENTIS Anwendung findet:

- Verhinderung unmittelbarer Zugriffe von Drittanbietern auf Endgerät von Nutzer
- Vollständige Kontrolle über einzelne Datenpunkte
- Reduzierung oder Modifizierung von Datenpunkten
- Zugriffsbeschränkungen und Kontrolle über die Weitergabe der Daten an Drittanbieter
- Festlegung von Bedingungen für Datenweitergabe
- Sicherstellung der Rechtskonformität.

Die entsprechende Anwendung der JENTIS-Twin-Server Technologie führt zu einer weiteren Erschwerung der Zuordnung eines Browsers eines Endgerätes zu einem Nutzungsprofil als einzige Referenz für die spätere Wiedererkennung des Browsers und stellt daher eine **wirksame Maßnahme** dar, die im Rahmen eines First-Party-Endgerätezugriffs, den geringsten Eingriff in die Grundrechte aus Art. 7 und Art. 8 Abs. 1 EU-Grundrechte-Charta der Website-Besucher bedeutet.

Sofern eine Berufung auf die Ausnahmevorschrift in Art. 5 Abs. 3 S. 2 Privacy-RL bzw. § 25 Abs. 2 TTDSG möglich ist, bedarf es zwar keiner Einwilligung der Nutzer. Dennoch ist zwingend zu prüfen, ob für den jeweiligen Dienst die **Rechtsgrundlage aus Art. 6 Abs. 1 S. 1 lit. f) DSGVO** einschlägig ist. Für die notwendige **Dokumentation** der Interessenabwägung nach Art. 6 Abs. 1 S. 1 lit. f) DSGVO [EDPB, WP 260, Anhang] sollte **ein sog. LIA (Legitimate Interests Assessment)** nach Maßgabe der vom Kunde vorgenommenen Konfiguration der JENTIS DCP durchgeführt werden, um einen Nachweis für die erfolgte Interessenabwägung im Einzelfall erbringen zu können und die **Compliance** in der Supply Chain sicherzustellen. JENTIS stellt den Kunden für eine beispielhafte Konfiguration des Essential Modes ein Legitimate Interests Assessment zur Verfügung.

3. Bewertung der Übermittlungen neuerzeugter Client-IDs an Drittanbieter

(1) Als weitere Verarbeitungsvorgänge, die sich an den Endgerätezugriff durch JENTIS-Server anschließen, sind die serverseitigen Übermittlungen der bereinigten Tracking-Daten Server von Drittanbieter wie Google zu bewerten.

Es erfolgt weder eine Übertragung der von Google vergebenen Client-ID noch der IP-Adresse des Nutzers. Bei der Kommunikation des JENTIS-Servers von Drittanbietern wie Google werden ausschließlich die bereinigten Tracking-Daten – die neuerzeugte Client-ID, die IP-Adresse des Website-Servers, der modifizierte User Agent und die modifizierte Order-ID übermittelt (vgl. Pkt. III. 1.).

Die nach Modifizierung der Tracking-Parameter erfolgte Übermittlung an Drittanbieter wie Google lässt sich bei Durchführung eines **Legitimate Interests Assessment** für die kundenspezifischen Use Cases auf die Rechtsgrundlage in Art. 6 Abs. 1 S. 1 lit. f) DSGVO stützen.

(2) Die Bildung von **modifizierten und fiktiven Daten** nach dem **Zufallsprinzip** aus realen Rohdaten **entspricht** der Bildung von **Hash-Werten ,** soweit es um die **Einordnung der Modifizierung als** Maßnahme der **Pseudonymisierung** geht.

- Pseudonymisierung stellt eine geeignete Privacy Pattern im Rahmen von „Privacy by Design" dar[48] und kann bei „JENTIS" auf der Ebene der Verarbeitung und vor der Weitergabe an Drittanbietern angewendet werden. Nach Ansicht des BGH stellt bereits eine in Cookies gespeicherte zufallsgenerierten Nummer (Cookie ID), die als Endgeräteinformation Registrierungsdaten des Nutzers zugeordnet ist, ein Pseudonym i. S. d. § 15 Abs. 3 TMG dar, wobei der BGH noch auf die Legaldefinition in § 3 Abs. 6a BDSG a.F. abstellte.[49] Gleiches muss in der Konsequenz auch für andere Identifier wie Device IDs, IDFA, GAID und Universal IDs gelten.
- Die **ENISA** (European Union Agency for Cybersecurity) beschreibt künstlich generierte Daten („synthetische Daten") im Kontext des Datenschutzrechts als neuen Bereich der Datenverarbeitung, in dem Daten so aufbereitet werden, dass sie realen Daten (sowohl personenbezogenen als auch nicht-personenbezogenen) realistisch ähneln, sich aber nicht auf eine bestimmte identifizierte oder identifizierbare Person oder auf das „reale Ausmaß eines zu bewertenden Datenparameters" beziehen.[50] Dabei können synthetische Daten auch personenbezogene Daten darstellen, die jedoch so modifiziert werden, dass die Möglichkeit der Re-Identifizierung von Personen eingeschränkt wird.[51]
- Laut **ENISA** können solche „**modifizierte Daten**" als Technologie zur Verbesserung des Schutzes der Privatsphäre (**Privacy Enhancing Technology**) betrachtet werden und in diesem Sinne als Maßnahme der Pseudonymisierung eingesetzt werden.[52] Derartige Modifizierungen dienen nach Ansicht der **ENISA** in erster Linie der **Vertraulichkeit** der **Verarbeitung**,[53] die den Charakter „zusätzlicher Maßnahmen" in technischer und organisatorischer Hinsicht i .S. d. Art. 32 DSGVO aufweist.
- Im Fall der Use Cases beim Einsatz von JENTIS, z. B. bei der Website-Analyse, ist die Wiedererkennung des Nutzers über die **JENTIS User-ID** für Website-Betreiber möglich. Soweit mindestens die „Client-ID des Drittanbieters" sowie im Idealfall weitere **Tracking-Parameter** wie User Agent und etwaige -Kundenspezifische IDs nach entsprechender Konfiguration der JENTIS-DCP **durch künstliche Werte ersetzt, d.h. modifiziert** werden, weisen die übermittelten Datensätze aus Sicht des Empfängers keinen Personenbezug auf, weil die Zuordnungsregel über die JENTIS User-ID zu einem Endgerät ausschließlich bei JENTIS und Website-Betreibern liegt. Lediglich JENTIS als Auftragsverarbeiter und

[48] Vgl. BGH, Urt. v. 15.5.2018 – VI ZR 233/17 Rn. 26.
[49] BGH, Urt. v. 28.05.2020 – I ZR 7/16 – Cookie Einwilligung II, Rn. 72; zustimmend in Bezug auf DSGVO Menke, K&R 2020, 650, 652; Baumgartner/Hansch, ZD 2020, 435, 436.
[50] ENISA, Data Protection Engineering, 2022, S. 17.
[51] ENISA, Data Protection Engineering, 2022, S. 17.
[52] ENISA, Data Protection Engineering, 2022, S. 10.
[53] Vgl. ENISA, Data Protection Engineering, 2022, S. 17.

der Website-Betreiber, nicht aber Drittanbieter wie Google verfügen über die Zuordnungsregel – z. B. über die JENTIS User-ID – für die pseudonymen Tracking-Parameter. Es ist dann von einer **wirksamen Pseudonymisierung** nach Maßgabe von Art. 4 Nr. 5 DSGVO auszugehen.

- Die **Modifizierung realer Rohdaten** wie die von Drittanbietern vergebene Client-ID oder User ID ist **unter denselben Bedingungen** wie die **Bildung** von **Hashwerten** aus realen Rohdaten als Pseudonymisierung i. S. v. Art. 4 Nr. 5 DSGVO einzuordnen.[54] Solange die an der Stelle von Client-IDs und User-IDs verwendeten **künstlichen Werte irreversibel** sind, die **Kollisionsfreiheit** der aufbereiteten Datenparameter **sichergestellt** ist **und** die **IP-Adresse** des Nutzers **ersetzt** wurde, ist unter Berücksichtigung der einhelligen Beurteilung zu Hashwerten mangels entgegenstehender Stellunghamen oder Rechtsprechung von einer **DSGVO-konformen Pseudonymisierung** auszugehen.

(3) Die nach Art. 4 Nr. 5 DSGVO **erforderliche Einschränkung**, dass die **Zusatzinformationen separiert aufbewahrt** werden und durch technisch-organisatorische Maßnahmen abgesichert sind, die gewährleisten, dass keine Zuweisung der Daten zu einer identifizierbaren Person erfolgt, **wird** während der Kommunikation der unterschiedlichen Serverinstanzen **von JENTIS gewährleistet**. Unabhängig davon, ob die zusätzliche Information wie die JENTIS User-ID eine direkte Zuordnung oder eine Zuordnungsregel für die neuerzeugten Client IDs und Order IDs der Drittanbieter sein kann,[55] ist laut dem beschriebenen technischen Funktionsprinzip angesichts der Systemarchitektur von JENTIS eine robuste Trennung der Dateninstanzen gegeben, die eine Zuordnung für Drittanbieter ausschließen.

(4) Soweit ersichtlich, erhalten Drittanbieter wie Google bei den skizzierten Datenübermittlungen im Nachgang des Endgerätezugriffs lediglich eine von JENTIS **neuerzeugte Client-ID**, die nicht mit der von Google vergebenen Client ID oder User ID für Google Analytics übereinstimmt und deswegen **keine Zuordnung** der mitgelieferten Informationen **über das Nutzungsverhalten** von Website-Besuchern durch Google ermöglicht.

(5) Ebenso ist **kein Zugriff auf** die **JENTIS DCP** durch **Drittanbieter** wie Google auf Grundlage der zur Verfügung gestellten technischen Dokumentationen möglich. Es erfolgt **keine** direkte **Kommunikation** des **Browsers** des Nutzers **mit Drittanbietern**. Soweit ersichtlich, existiert zu der Frage, ob weiterhin von einem Personenbezug auszugehen ist, wenn lediglich ein Dritter über die Zuordnungsregel für die übermittelte pseudonyme Datensätze verfügt, jedoch keine rechtliche Möglichkeit für den Zugriff auf Identifizierungsmerkmale vorhanden ist, keine anderslautende als die Rechtsprechung des EuGH zum Personenbezug von IP-Adressen.[56]

(6) Im Einklang mit der Ansicht des EuGH[57] ist die Übermittlung der bereinigten Tracking-Daten als nachgelagerte Verarbeitungsphase einzuordnen, die dem Anwendungsbereich der DSGVO unterfällt (vgl. Pkt. II. 2.). Aufgrund der ergriffenen Schutzmaßnahmen – Entfernung der IP-Adresse, Zuordnung von neuerzeugten Werten für die Client-ID und Order-ID, für die Google keine Zuordnungsregel besitzt – lässt sich für die Übermittlung vorbehaltlich einer künftig anderslautenden Rechtsprechung die **Rechtsgrundlage** gemäß **Art. 6 Abs. 1 S. 1 lit. f) DSGVO** in vertretbarer Weise anwenden.

---

[54] Vgl. zum Hashing als valide Maßnahme zur Pseudonymisierung Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, S. 26; ENISA, Pseudonymisation techniques and best practices, 2019, S. 33; ENISA, Data Pseudonymisation: Advanced Techniques & Use Cases, 2021, S. 12; Artikel 29-Data Protection Working Party, WP 216, Opinion 05/2014 in Anonymisation Techniques, S. 20.
[55] Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, S. 11 f.
[56] Vgl. auch Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Rn. 12.
[57] EuGH, Urt. v. 15.06.2021 – C-645/19 – One-Stop-Shop, Rn. 74.

Dabei ist jedoch zwingend zu prüfen, ob die **Rechtsgrundlage aus Art. 6 Abs. 1 S. 1 lit. f) DSGVO** einschlägig ist. Für die notwendige **Dokumentation** der Interessenabwägung nach Art. 6 Abs.1 S. 1 lit. f) DSGVO[58] sollte **ein sog. LIA (Legitimate Interests Assessment)** durchgeführt werden, um einen Nachweis für die erfolgte Interessenabwägung erbringen zu können. JENTIS stellt den Kunden für eine beispielhafte Konfiguration des Essential Modes ein Legitimate Interests Assessment zur Verfügung.

IV. Zusammenfassung der Untersuchungsergebnisse

Im Ergebnis können bei Einsatz der **JENTIS SaaS-Lösung** für die Implementierung von Drittanbieter-Tracking-Tools wie Google Analytics bei entsprechender Konfiguration die beschriebenen **Rechtsunsicherheiten** (vgl. Pkt. II.) **ausgeräumt** werden.

Es bleibt festzuhalten: Mithilfe der JENTIS-Twin-Server Technologie lassen sich den lokal und **regional unterschiedlichen Ansichten** von Gerichten und Aufsichtsbehörden zur Nutzung von Tracking-Proxy-Lösungen zur Ermöglichung des rechtmäßigen Einsatzes von Tracking-Diensten sowie den individuellen Compliance-Vorgaben **im Einzelfall** vollumfänglich **Rechnung tragen**.

JENTIS ermöglicht mit der Server-Side-Tracking-Technologie eine **langfristige** und **nachhaltige Strategie**, **einerseits** um industrielle Herausforderungen im Zuge des 3rd-Party-Cookie phase-out zu meistern und **andererseits** um die Datenverarbeitung im Rahmen von Tracking-Anwendungen auf sichere Füße zu stellen. Aufgrund der individuellen Konfigurationsmöglichkeiten der JENTIS Server Suite sind Unternehmen auch **für künftig anderslautende Entscheidungen** von Aufsichtsbehörden **gewappnet** und können kurzfristig auf neue rechtliche Anforderungen reagieren.

Website-Betreiber können bei Nutzung von JENTIS **wirtschaftliche Vorteile** ihrer jeweils eigenen First-Party-Daten nutzen, **ohne** diese Daten oder die jeweilige unternehmerische **Compliance** durch **unkontrollierte** und **intransparente Verarbeitung** auf Seiten von Drittanbietern in rechtlicher Hinsicht zu **gefährden.**

V. Handlungsempfehlungen für Betrieb der JENTIS-DCP

Für den rechtskonformen Einsatz der JENTIS Saas-Lösung sind folgende Maßnahmen zu empfehlen:

- Evaluierung der Funktionsweise durch eine Software-Demo oder dieses Memorandum;
- Konfiguration der JENTIS n DCP durch Kunden;
- Notwendige **Dokumentation** der Interessenabwägung nach Art. 6 Abs.1 S. 1 lit. f) DSGVO[59] mittels **eines LIA (Legitimate Interests Assessment)**, zur Erfüllung der Rechenschafts- und Dokumentationspflichten für die erfolgte Interessenabwägung; JENTIS stellt den Kunden für eine beispielhafte Konfiguration des Essential Modes ein Legitimate Interests Assessment zur Verfügung.
- Transparente Informationen in den Datenschutzinformationen auf der Website;
- Opt-Out-Möglichkeiten für Nutzer durch automatisierte Systeme wie z. B. Opt-Out Links, auf die besonders in der Datenschutzerklärung oder der JENTIS CMP hingewiesen wird;
- Abschluss und Dokumentation Auftragsverarbeitungsvertrag mit JENTIS;

[58] EDPB, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260, rev.01, Anhang.
[59] EDPB, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260, rev.01, Anhang.

- Abschluss und Dokumentation der datenschutzrechtlichen Begleitvereinbarungen (Auftragsverarbeitungs-, Joint-Controller- oder Controller-2-Controller-Vereinbarung mit Drittanbietern).