Data Protection Memorandum

JENTIS GmbH

SPIRIT LEGAL®

Verfasser/in	Datum des Dokuments
RA Peter Hense & RA Tilman Herbrich (CIPP/E)	*11. Juni 2022, v2.1*

Projekt

Bewertung der JENTIS Saas-Lösung zur Umsetzung der Anforderungen aus dem EuGH-Urteil „Schrems II“

Executive Summary

Bisherige Industrielösungen wie Server-Side-Tracking zur Ermöglichung eines qualitativen Website-Tracking trotz zunehmender Verbreitung von AdBlockern und Tracking Prevention Systemen ändern nichts an den strengen Anforderungen für die Übermittlung personenbezogener Daten in Drittländer wie die USA ohne angemessenes Schutzniveau i. S. d. EuGH-Rechtsprechung in der Rechtssache „Schrems II“ **(I.1.)**. Die Drittlandproblematik hat sich aufgrund einhelliger europaweiter Entscheidungen von Aufsichtsbehörden zu Google Analytics und ersten Rechtsprechungstendenzen seit Anfang 2022 erheblich verschärft **(I.2.).** Bei Nutzung des Server Side Google Tag Manager kommt hinzu, dass der gesamte Tech Stack des Unternehmens in der Google Cloud Platform eingebettet wird und damit auch für unkritische Tracking-Dienste mit reiner EU-Infrastruktur ein Verlust der Kontrolle über den Zugriff auf Nutzerdaten einhergeht. Auch wenn der Server Side Google Tag Manager nicht in der Google Cloud, gehostet wird, ist dieses Problem nicht gelöst.

Aufgrund komplexer und schwer zu lösender Herausforderungen bei der Integration von Tracking-Anwendungen und unzureichender Branchenlösungen wächst das Bedürfnis nach langfristigen und nachhaltigen Strategien zur rechtskonformen und wirksamen Datennutzung **(I.3.).** JENTIS bietet als Privacy Enhancing Technology eine langfristige Hilfestellung zur Sicherstellung der „Schrems II“-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.

Bisweilen sind in der Praxis eine Reihe erheblicher Rechtsunsicherheiten in Bezug auf die Drittlandthematik beim Website-Tracking aufgekommen: Angefangen bei den nicht praktikablen Anforderungen an die Abfrage einer Einwilligung für die Übermittlung in ein Drittland ohne angemessenes Schutzniveau über eine Consent-Management-Platform **(I.1.)** über die Auslegung, was unter „zusätzlichen Maßnahmen“ zur Absicherung von Drittlandtransfers nach Maßgabe der neuen Standardvertragsklauseln der EU-Kommission zu verstehen ist **(II.2./II.3.)**, bis hin zum Umgang mit der Ankündigung des geplanten „Trans Atlantic Data Privacy Framework“ als Nachfolgeabkommen für das vom EuGH für unwirksam erklärte EU-US Privacy Shield **(II.4.)**.

Auf Grundlage des skizzierten Funktionsprinzips der JENTIS Systeme **(III.1.)** lässt sich die „Schrems II“-Compliance in der Supply Chain beim Einsatz von Drittanbietern wie Google für das Website-Tracking **(III.3.)** mittels einer Synthetisierung der Datenparameter der Browser-Session des Nutzers als wirksames Mittel der Pseudonymisierung nach Maßgabe der Empfehlungen des EDPB sicherstellen **(III.2.)**. Im Einklang mit der Ansicht des EDPS können „synthetische Daten“ als Privacy Enhancing Technology betrachtet und als

„zusätzliche Maßnahme“ bei Datenübertragungen außerhalb der Europäischen Union eingesetzt werden. Ein Singling-Out oder eine Re-identifizierung einzelner Nutzer ist bei Synthetisierung der Identifier auf JENTIS-Systemen innerhalb der Europäischen Union im Drittland für Tracking-Anbieter nicht mehr möglich. JENTIS kann deshalb die „Schrems II“-Anforderungen an internationale Datentransfers 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.)**. Mithilfe der 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 Tracking Diensten, z. B. für Google Analytics 4.0 „gtag.js" 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 an Server von Drittanbietern wie Google in den USA [vgl. EuGH, Urt. v. 29.07.2019 – C-40/17, Rn. 26 – Fashion ID].

Der rechtliche Rahmen für internationale Datentransfers wird maßgebend von Entwicklungen in der Industrie, Gerichtsentscheidungen und im jeweiligen Zuständigkeitsbereich von Auditierungen durch Aufsichtsbehörden geprägt. Die Übermittlung personenbezogener Daten wie IP-Adressen [vgl. EuGH, Urt. v. 19.10.2016 – C-582/14, Rn. 47 – Breyer] und Client- und User-IDs [vgl. BGH, Urt. v. 28.05.2022 – I ZR 7/16 – Cookie-Einwilligung II, Rn. 72] in die USA als Drittland ohne angemessenes Schutzniveau i. S. d. Kapitel 5 DSGVO wird durch die Entwicklung von einem Client-Side-Tracking hin zu einem reinen Server-Side-Tracking nicht vermieden **(1.)**. Die Anforderungen an die Rechtmäßigkeit von internationalen Datentransfers haben sich aufgrund einhelliger europaweiter Entscheidungen von Aufsichtsbehörden zu Google Analytics und ersten Gerichtsurteilen seit Anfang 2022 erheblich verschärft **(2.).**

1. Entwicklungen in der Industrie

(1) Seit 2017 ist zu beobachten, dass jenseits von **Ad-Blockern** gängige Browser-Anbieter wie Safari und Firefox per Voreinstellung **Tracking-Blockadesysteme** „ITP" (Intelligent Tracking Prevention v2.3) des Browsers „Safari" oder „ETP" (Enhanced Tracking Prevention) verwenden, die ein Third- und teilweise ein First-Party-Tracking zu Analyse- und Werbezwecken von vornherein verhindern. Diese technischen Entwicklungen in der Browserlandschaft haben negative Konsequenzen für die Auswertung des Nutzungsverhaltens:

- bekannte Trackingskripte werden blockiert und nicht ausgeführt,
- Third- und wesentliche First-Party-Cookies werden per Default blockiert,
- die Laufzeit auch von First-Party-Cookies und die Nutzung der Endgerätekapazität „LocalStrorage" wird eingeschränkt (7 Tage bis zu 24 Std.),
- Marketing-Attributionen können nicht mehr durchgehend erfolgen,
- die Customer Journey kann nur für kurze Zeiträume von 1-7 Tage nachvollzogen werden,
- mangels belastbarer Daten wird eine gezielte Optimierung von Marketing-Kampagnen erschwert.

(2) Bisherige Lösungsansätze wie Server-Side-Tracking, etwa über den Server Side Google Tag Manager (SSGTM) oder die Facebook Conversions API zur Umgehung von Ad-Blockern und Tracking befreien nicht von der Einhaltung der datenschutzrechtlichen Anforderungen. Im Gegenteil, die Aufsichtsbehörde in Baden-Württemberg (**„LfDi BaWü"**) stellt in den „FAQ zu Cookies und Tracking" (S. 16) klar: Auch beim **Server-Side-Tracking** müssen sowohl die Anforderungen aus dem **TTDSG** als auch der **DSGVO** eingehalten werden.

(3) **Rechtlicher Anknüpfungspunkt** für die Anwendung des TTDSG ist der **Zugriff auf Informationen aus** einer vom Browser gestellten **Serveranfrage** aufgrund der Implementierung von JavaScripts im Quellcode oder der Website [LG München, Hinweisbeschluss v. 08.12.2021 – 33 O 14776/19]. Laut „LfDi BaWü" handelt sich beim Server-Side-Tracking neben dem Endgerätezugriff bei der Übermittlung personenbezogener Daten um eine Verarbeitung nach Art. 4 Nr. 2 DSGVO.

(4) Zwar werden 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 [vgl. etwa Papadogiannakis et al., User Tracking in the Post-cookie Era, 2021, S. 1 f.]. Bei Nutzung des **SSGTM** kommt **verschärfend** hinzu, dass der gesamte **Tech Stack** des Unternehmens in der Google Cloud Platform eingebettet wird und damit auch für unkritische Tracking-Dienste mit reiner EU-Infrastruktur ein **Verlust der Kontrolle** über den Zugriff einhergeht.

(5) **Privacy Enhancing Technologies** wie der **JENTIS Tag Manager** und die **JENTIS Server Suite** (vgl. Pkt. III.), ermöglichen eine Modifikation der Datenparameter der beim Aufruf einer Website stattfindenden Datenverarbeitung aufgrund der geladenen Tags von Drittanbieter und **können** mittels Privacy by Design einen **rechtskonformen Einsatz** in der Supply Chain **sicherstellen**.

2. Aktuelle Rechtslage zu Datenübermittlungen in Drittländer ohne angemessenes Schutzniveau

a) Anforderungen an die Übermittlung von Nutzerdaten in Drittländer

(1) Für Datenübermittlungen an Drittanbieter wie Google mit Sitz in einem Drittland außerhalb der EU/des EWR, für die die EU-Kommission keinen Angemessenheitsbeschluss nach Art. 45 Abs. 1 DSGVO erlassen hat, ist eine alternative **Rechtfertigung** für den **Drittlandtransfer** notwendig.

(2) Als **Rechtfertigung** für die Datenübermittlung an die Google LLC in den USA ohne angemessenes Schutzniveau im Fall der Nutzung von z. B. Google Analytics [vgl. Datenschutzkonferenz (**„DSK"**), Beschluss vom 12.05.2020 – Hinweise zum Einsatz von Google-Analytics], verbleibt im Nachgang der EuGH-Rechtsprechung [EuGH, 16.7.2020 – C-311/18 – Schrems II] praktisch nur die **Vereinbarung** von **Standardvertragsklauseln** (Standard Contractual Clauses, **„SCC"**).

(3) In dem **Urteil des EuGH** vom 16.7.2020 wurde nicht nur das EU-US-Privacy-Shield für ungültig erklärt, sondern – je nach der rechtlichen Lage im Zielland – für einen rechtlich zulässigen Drittlandtransfer auf Grundlage der Standardvertragsklauseln weitere Maßnahmen oder Garantien gefordert [EuGH, 16.7.2020 – C-311/18 – Schrems II]. Damit ist nicht nur das EU-US-Privacy-Shield als Rechtsgrundlage für den Datentransfer in die USA weggefallen. Auch jeder Datentransfer und Datenzugriff durch US-Unternehmen, der sich auf Standardvertragsklauseln gemäß Art. 46 Abs. 2 lit. c) DSGVO stützt, erfordert **zusätzliche** technische und organisatorische **Maßnahmen („Supplementary Measures")** zum Schutz vor dem Zugriff von US-Behörden sowie zur Gewährleistung eines effektiven Rechtsschutzes für Betroffene gegen unberechtigte Zugriffe.

b) Aktuelle Prüfungen von Aufsichtsbehörden und NGOs zur Rechtsdurchsetzung

(1) Die **Österreichische Behörde** hat mit Teilbescheid vom 22.12.2021 und Teilbescheid vom 22.04.2022 entschieden, dass für den Drittlandtransfer beim Einsatz von Google Analytics, die von Google in den SCC mitgeteilten technischen und organisatorischen Maßnahmen, wie die Kürzung der IP-Adresse nach Übermittlung in die USA nicht ausreichen, um die Anforderungen der EuGH-Rechtsprechung zu erfüllen. Vor allem seien die von Google in den SCC „Google Ads Data Processing Terms" (u.a. Google Analytics) in Annex II und Ziff. 8 und 9 angeführten Beschreibungen – etwa zur Kürzung der IP-Adresse nach Übermittlung –unzureichend und entsprächen nicht den vom EDPB definierten Zusatzmaßnahmen für Drittlandtransfers.

(2) Dieser Ansicht haben sich inzwischen die Aufsichtsbehörde in Baden-Württemberg (**„LfDi BaWü"**), die CNIL, (Frankreich) die Autoriteit Persoonsgegevens (Niederlande) sowie die Datatilsynet aus Norwegen und Dänemark angeschlossen. Zuvor hat bereits der EDPS festgestellt, dass der Einsatz von Google Analytics auf Websites des Europäischen Parlaments aufgrund unzureichender „Zusatzmaßnahmen" unzulässig ist. Die CNIL hat im Juni 2022 in ihren „FAQs zu Google Analytics" klargestellt, dass es nicht möglich ist, Google Analytics so zu konfigurieren, dass keine Daten in Länder außerhalb der EU übertragen werden.

(3) Hintergrund der aufsichtsbehördlichen Verfahren und Sanktionen waren die von der NGO „NOYB" in ganz Europa eingereichten 101 Beschwerden wegen der unrechtmäßigen Nutzung von Google Analytics und Facebook Connect durch große Unternehmen.

(4) Laut Ziff. 7 der Nutzungsbedingungen Google Analytics sind Website-Betreiber voll für die Einhaltung aller Datenschutzgesetze verantwortlich, einschließlich des Kapitel 5 der DSGVO. Im Fall einer Inanspruchnahme von Google wegen unzulässigen Drittlandübermittlungen, lässt sich Google eine **umfassende Haftungsfreistellung** in Ziff. 8 der Nutzungsbedingungen einräumen. Auch in dem von Google zu internationalen Datentransfers veröffentlichen Whitepapers im November 2021 weist **Google** darauf hin, dass die Ausführungen **keine Rechtsberatung** darstellen und Kunden von Google Analytics die rechtlichen **Risiken eigenständig** zu **bewerten** haben.

c) Aktuelle Rechtsprechung zu unzulässigen Drittlandübermittlungen

(1) Die **Risikolage** für Datenübermittlungen in die USA bei Nutzung von Google Analytics wird durch erste Gerichtsentscheidungen **verschärft**.

So hat das **LG München** (Urt. v. 20.01.2022 – 3 O 17493/20) in einer aktuellen Entscheidung zur Einbindung von Google Fonts in einer Website über APIs bereits aufgrund der **Übermittlung der IP-Adresse** eines Nutzers beim Aufruf einer Website an Server der Google LLC in den USA dem Betroffenen sowohl einen **Unterlassungs**- als auch **Schadenersatzanspruch** in Höhe von 100,00 EUR zugesprochen. Zur Begründung führte das LG München für die Verletzung des allgemeinen Persönlichkeitsrechts an, dass Nutzerdaten durch die Google LLC unkontrolliert verarbeitet werden und die USA nach der Rechtsprechung des EuGH kein angemessenes Schutzniveau aufweist.

(2) Zuvor hatte bereits das **VG Wiesbaden** (Beschl. v. 01.12.2021 – 6 L 738/21.WI) entschieden, dass bei dem Einsatz der Consent Management Platform (**„CMP"**) „Cookiebot" auf einer Website eine

unzulässige **Übermittlung von IP-Adressen** in die USA stattfinde und der Drittlandtransfer nicht gerechtfertigt sei. Die **Entscheidung** im einstweiligen Verfügungsverfahren wurden im Wesentlichen aufgrund von Verfahrensanforderungen im Einstweiligen Rechtsschutz derweil **vom VGH Kassel** (Beschl. v. 17.01.2022 – 10 B 2486/21) im Beschwerdeverfahren **aufgehoben** worden. Eine abschließende Klärung könne lediglich in einem Hauptsacheverfahren erfolgen.

(3) Der Council of State in Belgien hat schließlich am 06.05.2022 (case no: 253.677) entschieden, dass eine Entscheidung zur Auswahl eines US-amerikanischen Auftragnehmers im Rahmen eines öffentlichen Ausschreibungsverfahrens durch den Staatsrat mit der Begründung auszusetzten sei, da die Behörde nicht ausreichend geprüft habe, ob der Auftragnehmer die Anforderungen der Datenschutz-Grundverordnung erfülle, insbesondere die Bestimmungen zur Übermittlung und Weiterverarbeitung durch ein anderes Unternehmen, Smart Analytics, mit Sitz in Russland.

(4) Nach der Kenntnis der Verfasser sind weitere Gerichtsverfahren im Zusammenhang mit Drittlandübermittlung anhängig, weshalb auch künftig mit einer weiteren Rechtsdurchsetzung zu rechnen ist.

3. Fazit: Bedürfnis nach langfristigen Strategien für das Risikomanagement

(1) **Bereits kurz**- und **mittelfristig** bestehen spürbare **Risiken** bei Nutzung von Tracking-Diensten aufgrund der Einbindung von Drittanbieter, die globale Infrastrukturen wie Cloud-Services nutzen.

(2) **Website-Betreiber** benötigen **alternative Lösungsansätze**, die eine Modifikation der Datenverarbeitung beim Tracking ermöglichen. Der LfDI BaWü deutet in den „FAQ zu Cookies und Tracking“ (S. 16) an, dass derartige **Middleware-Lösungen**, die sich zwischen Kommunikation des Endgeräts, Webserver und Server von Drittanbietern schalten, einen **rechtskonformen Einsatz** beim **Server-Side-Tracking** ermöglichen können.

(3) **JENTIS bietet** als Privacy Enhancing Technology eine **langfristige** Hilfestellung zur Sicherstellung von Privacy by Design und ermöglicht den Kunden **flexible Konfigurationen** der SaaS-Lösung, **um** der Volatilität der jeweiligen **individuellen Risikolage** von Unternehmen **Rechnung** zu **tragen**.

II. Rechtliche Unsicherheiten durch technologische Vielfalt beim Website-Tracking

Bisweilen sind in der Praxis erhebliche Rechtsunsicherheiten in Bezug auf die datenschutzrechtlichen Anforderungen beim Website-Tracking aufgekommen. Die Rechtsunsicherheiten betreffen in erster Linie die Frage, **(1.)** welche Anforderungen an die Abfrage einer Einwilligung für die Übermittlung in ein Drittland ohne angemessenes Schutzniveau über eine Consent-Management-Platform zu stellen sind und **(2.)** was unter „zusätzlichen Maßnahmen“ zur Absicherung von Drittlandtransfers aufgrund der Nutzung von cloudbasierten Anwendungen für die Realisierung von Server-Side-Tracking-Mechanismen nach Maßgabe der neuen Standardvertragsklauseln der EU-Kommission zu verstehen ist.

Jüngere Entscheidungen der Aufsichtsbehörden zu Google Analytics belegen die hohen Anforderungen an die rechtskonforme Gestaltung von Standardvertragsklauseln, insbesondere mit Blick auf die Bewertung der in den Anlagen der SCC bezeichneten „zusätzlichen Maßnahmen“ **(3.)**.

Schließlich ist die am 25.03.2022 verkündete Einigung zwischen US-Präsident Biden und Präsidentin der EU-Kommission Ursula von der Leyen auf ein neuen „Trans Atlantic Data Privacy Framework" (**„TADPF"**) als Nachfolgeabkommen für das vom EuGH für unwirksam erklärte EU-US Privacy Shield derzeit erheblichen Rechtsunsicherheiten ausgesetzt **(4.)**.

1. Rechtsunsicherheit Einwilligung für Drittlandtransfer: Ist eine praktikable Umsetzung möglich?

Bereits die Nutzung von Consent-Management-Plattformen, die auf Cloud-Lösungen z. B. von AWS, Microsoft Azure oder Google als Infrastruktur aufbauen, kann die Compliance mit den Vorgaben aus dem EuGH-Urteil „Schrems II" von vornherein verhindern, wie der Fall vor dem **VG Wiesbaden** (Beschl. v. 01.12.2021 – 6 L 738/21.WI, nicht rechtskräftig) angedeutet hat. Selbst wenn man eine CMP ohne jedwedes Drittlandrisiko in Anspruch nimmt, ist die Abfrage einer Einwilligung für den Drittlandtransfer aufgrund von Tracking-Diensten wie Google Analytics mit **kaum überwindbaren praktischen Hürden** verbunden.

Als Ausnahme für einen Drittlandtransfer ist die Umsetzung einer ausdrücklichen Einwilligung gemäß Art. 49 Abs. 1 S. 1 lit. a) DSGVO mit **erheblicher Komplexität und Risiken** verbunden. Zum einen lehnen Aufsichtsbehörden die rechtliche Zulässigkeit einer Einwilligung für die Übermittlung an Tracking-Dienste in Drittländern ab. Zum anderen ist die Erfüllung der Informationspflichten in Bezug auf Empfänger und sämtliche Drittländer im Rahmen der Abfrage einer Einwilligung in einer CMP mit **kaum überwindbaren praktischen Hürden** [vgl. JENTIS Blog, Mit rechtlichen Unsicherheiten beim Website-Tracking umgehen.] verbunden:

(1) Bei der Prüfung, welche Verarbeitungen von Art. 49 Abs. 1 S. 1 lit. a) DSGVO erfasst sind, ist ein **vorsichtiger Maßstab** anzuwenden. Der **Europäische Datenschutzausschuss** (**„EDPB"**) fordert eine **vorherige Unterrichtung** über die konkreten bestehenden Risiken, die aus dem fehlenden Schutzniveau im Drittland herrühren. Abstrakte Hinweise auf eine fehlende Angemessenheit im Drittland seien nicht ausreichend [vgl. EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 vom 25.5.2018, S. 9 f.]. So muss hervorgehoben werden, **welche** möglichen **Risiken** sich für die betroffenen Personen aus der Tatsache ergeben, dass das **Drittland kein** angemessenes **Schutzniveau** bietet und dass keine geeigneten Garantien vorliegen.

Außerdem sei die „**umfassende Angabe**" von **Empfängern** im Drittland **und** das **jeweilige Drittland** genau zu bezeichnen. Werden diese Informationen nicht zur Verfügung gestellt, kommt die Ausnahmeregelung daher nicht zur Anwendung [vgl. EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 vom 25.5.2018, S. 9].

(2) Nach Ansicht der **Datenschutzkonferenz** kann der **Einsatz** von **Tracking-Tools** zur Nachverfolgung des Nutzerverhaltens grundsätzlich **nicht** auf Grundlage einer **Einwilligung** nach Art. 49 Abs. 1 S. 1 lit. a) DSGVO gestützt werden [DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, S. 32]. Umfang und Regelmäßigkeit solcher Transfers widersprächen regelmäßig dem Charakter des Art. 49 DSGVO als Ausnahmevorschrift und den **Anforderungen** aus **Art. 44 S. 2 DSGVO** [vgl. hierzu auch EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 vom 25.5.2018, S. 9; vgl. auch CNIL, „FAQs zu Google Analytics", Juni 2022].

(3) In der **praktischen Umsetzung** wird man z. B. beim Einsatz von Google Analytics **regelmäßig** daran **scheitern**, die umfangreichen **Informationspflichten** des EDPB in einem Consent-Layer transparent **abbilden** zu können, um eine akzeptable Consent-Rate zu erzielen. Denn die Auflistung des jeweiligen Drittlandes, in welches die Daten übermittelt werden, sowie aller über 50 Unterauftragnehmer für den Google Analytics als Empfänger ist aufgrund des Umfangs rechtssicher kaum praktisch handzuhaben. 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.

Im Fall von Google Analytics müssten Website-Besucher **in** einer **CMP** jeweils für das **Drittland** über **fehlende** Betroffenenrechten, Beschwerdemöglichkeiten bei Aufsichtsbehörden und fehlende Datenverarbeitungsgrundsätzen **informieren**. Die **Hinweise** müssten für **jedes Drittland** ohne angemessenes Schutzniveau wie **Taiwan**, **Philippinen**, **Brasilien**, **Mexiko**, **Malaysia** und **Indien** erteilt werden [vgl. z. B. zu Indien Studie im Auftrag des EDPB, Government access to data in third countries, 2021]. Lediglich für Drittländer wie Japan und Argentinien bestehen Angemessenheitsbeschlüsse der EU-Kommission nach Art. 45 DSGVO.

(4) **Fazit:** Selbst beim consent-based Marketing durch Nutzung von CMP-Lösungen lässt sich die Drittlandproblematik bei Nutzung von Google-Diensten nicht sinnvoll überwinden. Eine den Anforderungen der Aufsichtsbehörden entsprechende Konfiguration einer CMP ist derzeit mangels Rechtsprechung mit **kaum überwindbaren praktischen Hürden** verbunden.

2. Rechtsunsicherheit Drittlandtransfer: Was sind „zusätzliche Maßnahmen“?

(1) Als **Rechtfertigung für den Datentransfer** in unsichere Drittländer**,** z. B. in die USA, verbleibt im Nachgang der EuGH-Rechtsprechung [EuGH, 16.7.2020 – C-311/18 – Schrems II] praktisch nur die Vereinbarung von Standardvertragsklauseln. Jeder Datentransfer und Datenzugriff durch US-Unternehmen, der sich auf Standardvertragsklauseln gemäß Art. 46 Abs. 2 lit. c) DSGVO stützt, erfordert **zusätzliche** technische und organisatorische **Maßnahmen („Supplementary Measures“)** zum Schutz vor dem Zugriff von US-Behörden sowie zur Gewährleistung eines effektiven Rechtsschutzes für Betroffene gegen unberechtigte Zugriffe.

(2) So muss der Datenexporteur – also jede Stelle wie Website-Betreiber, die personenbezogene Daten in den Machtbereich des Drittlandes übermittelt, einschließlich der Datentransfers von in Europa ansässigen Konzerngesellschaften mit US-amerikanischem Mutterkonzern – künftig zuerst prüfen, ob die Verpflichtungen im Drittland eingehalten werden können und ein angemessenes Schutzniveau gewährleistet ist. Sollte dies – wie in den USA insbesondere durch den Anwendungsbereich von Section 702 FISA und E.O. 12333 und die Zugriffsberechtigungen der Sicherheitsbehörden – nicht der Fall sein, müssen konkrete kompensatorische Maßnahmen ergriffen werden, die sicherstellen, dass das Schutzniveau wirklich eingehalten wird [Heckmann, Datenschutzkonforme Nutzung von Cloud-Lösungen aus unsicheren Drittländern, Wissenschaftliches Gutachten, 2021, S. 15; Heinzke, GRUR-Prax 2020, 436].

(3) Selbst mittels einer **Standortwahl** von **Servern** in **Europa** lässt sich die **Drittlandthematik nicht** von vornherein **vermeiden**. Nach dem Gutachten im Auftrag der DSK zum aktuellen Stand des US-Überwachungsrechts und der Überwachungsbefugnisse unterfallen US-amerikanische Anbieter elektronischer Kommunikationsdienste dem US-Überwachungsgesetz 50 U.S. Code § 1881a (Section 702 FISA), selbst wenn sie die Daten außerhalb der USA, nämlich innerhalb der EU, speichern. Ebenso könnte bei Nutzung von Cloud-Ressourcen von US-Unternehmen, wie beim Server Side Google Tag Manager im Rahmen des CLOUD Acts bei der Speicherung der Daten auf Servern innerhalb der EU der US-Anbieter zur Herausgabe der Daten verpflichtet werden [Heckmann, Datenschutzkonforme Nutzung von Cloud-Lösungen aus unsicheren Drittländern, Wissenschaftliches Gutachten, 2021, S. 16; Paal/Kumkar, MMR 2020, 733].

(4) Nach Ziff. 14 der SCC ist eine Pflicht zur Durchführung und Dokumentation eines „**Transfer Impact Assessments**" vorgesehen, in dem eine Analyse und Mitigation für Risiken eines Zugriffs von Sicherheitsbehörden auf Grundlage von „zusätzlichen Maßnahmen" als zusätzliche vertragliche, technische und organisatorische Maßnahmen zu erfolgen hat.

Welche „**zusätzlichen Maßnahmen**" zu ergreifen sind, ist anhand der vom **EDPB** am 18.06.2021 im Nachgang zu den neuen SCC der EU-Kommission veröffentlichten „Recommendations 01/2020 on measures [...]" in der Version 2.0 zu evaluieren. Ohne Dokumentation von zusätzlichen Maßnahmen zur Riskmitigation wird die Anwendung der SCC von Aufsichtsbehörden nicht akzeptiert. Als **Zusatzmaßnahmen** können z. B. die **Anonymisierung** oder fortgeschrittene **Pseudonymisierung** von Daten sowie weitgehende **Verschlüsselungstechnologien** fallen, wenn sichergestellt ist, dass die Empfänger im Drittland keinen Zugriff auf die Zuordnungsregel für die pseudonymisierten Daten i. S. d. Art. 4 Nr. 5 DSGVO oder die zu verarbeitenden Daten erhalten [Paal/Kumkar, MMR 2020, 733].

(5) **Fazit:** Es ist in Bezug auf den Einsatz von Tracking-Diensten im Einzelfall zu evaluieren, wie eine valide Pseudonymisierung im Vorfeld der Übermittlung von Nutzerdaten an Google im Einzelfall erfolgen kann, um die „Schrems II"-Compliance zu gewährleisten.

3. Rechtsunsicherheit Google & Co.: Reichen „zusätzliche Maßnahmen" in SCC aus?

Die europäischen **Aufsichtsbehörden** stellen an **„zusätzliche Maßnahmen" in SCC** beim nicht modifizierten Einsatz von Tracking-Diensten von US-Anbietern (vgl. bereits Punkt I.2.b.) **strenge Anforderungen**:

(1) Im Kern erachten die **Aufsichtsbehörden** europaweit die von Google in den SCC „Google Ads Data Processing Terms" (u.a. Google Analytics) in Annex II und Ziff. 8 und 9 angeführten „zusätzliche Maßnahmen" – etwa zur Kürzung der IP-Adresse nach Übermittlung durch Google – als unzureichend, sodass die Anforderungen an die „Schrems II"-Rechtsprechung nicht erfüllt werden.

(2) Die **Österreichische Behörde** hatte in ihrem Teilbescheid vom 22.12.2021 darauf verwiesen, dass eindeutige Online-Kennungen wie IP-Adressen und einzigartige Kennungen wie Cookie-IDs (bei Google Client ID und User ID) als Ausgangspunkt für die Überwachung durch Nachrichtendienste verwendet werden. Es könne nicht ausgeschlossen werden, dass Nachrichtendienste bereits zuvor

Informationen gesammelt haben, mit deren Hilfe Daten aus Serveranfragen auf einzelne Nutzer rückführbar sind.

Dass die **NSA** als US-Sicherheitsbehörde auf **Cookies**, insbesondere von Google Analytics, zur Überwachung des Internetverkehrs **zugreift**, wurde bereits 2013 in Medienberichten nach den Snowden-Enthüllungen hinreichend dargelegt.

(3) Dieser Ansicht haben sich inzwischen die Aufsichtsbehörde in Baden-Württemberg, die CNIL, (Frankreich), die Autoriteit Persoonsgegevens (Niederlande) sowie die Datatilsynet aus Norwegen und Dänemark angeschlossen.

Zuvor hat bereits der EDPS festgestellt, dass der Einsatz von **Google Analytics** auf Websites des Europäischen Parlaments aufgrund der **unzureichenden Umsetzung** von „**zusätzlichen Maßnahmen**" von Google gegen die Anforderungen an Drittlandübermittlungen nach Art. 44 ff. DSGVO verstößt.

Die CNIL hatte explizit klargestellt, dass UUIDs (Universally Unique Identifier) wie Cookie-IDs keine pseudonymen Daten darstellen, sondern den Zweck haben, einen Nutzer zu identifizieren. Ähnlich hatte die DSK bereits die Annahme einer Pseudonymisierung (Art. 4 Nr. 5 DSGVO) bei Nutzung von Werbe-IDs, Cookie-IDs oder Unique-User-IDs abgelehnt [DSK, Orientierungshilfe Telemedien, 2019, S. 15].

(4) Die CNIL hat in ihren „FAQs zu Google Analytics" aus dem Juni 2022 explizit hervorgehoben, dass für den Einsatz von Google Analytics der bloße Abschluss der bereitgestellten Standardvertragsklauseln nicht ausreichend sei, um die Anforderungen aus Art. 46 Abs. 2 lit. c) DSGVO zu erfüllen. Ebenso sei es nicht möglich, Google Analytics in einer Weise zu konfigurieren, dass keine Daten in Länder außerhalb der EU übermittelt werden.

Deshalb müssten Website-Betreiber selbst zusätzliche Maßnahmen i. S. d. der „Schrems II"-Rechtsprechung ergreifen, um den Einsatz von Google Analytics zu legitimieren. Zusätzliche Maßnahmen wie eine valide Pseudonymisierung vor Übermittlung der Nutzerdaten an Google können nach Ansicht der CNIL durch Tracking-Proxy-Lösungen wie die JENTIS-Twin-Server Technologie (vgl. Pkt. III.) erreicht werden.

(5) Den **EDPB** Empfehlungen folgend müssen für eine wirksame Pseudonymisierung als „zusätzliche Maßnahme" i. S. d. EuGH-Entscheidung „Schrems II" bei Nutzung von Cloud-Diensten – wie etwa der Server Side Google Tag Manager, **entsprechende Verfahren** zur **Pseudonymisierung im Vorfeld der Übermittlung** an den Drittanbieter angewendet werden [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.]. Eine wie von Google im Verfahren angegebene **Transportverschlüsselung** oder **„Data-at-rest"-Verschlüsselung** stellen für sich noch keine „zusätzlichen Maßnahmen" dar, die ein im Wesentlichen gleichwertiges Schutzniveau gewährleisten. Deshalb dürfte 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 sein, um die Anforderungen des EDPB an „zusätzliche Maßnahmen" zu erfüllen.

Selbst wenn man wie die österreichische Behörde in ihrem Teilbescheid vom 22.04.2022 einen risikobasierten Ansatz im Kapitel 5 der DSGVO vollständig ablehnt, ist bei Erfüllung dieser vom EDPB vorgegeben Maßnahmen ein rechtskonformer Einsatz von Tracking-Diensten möglich.

(6) **Fazit:** Im Fall von **Tracking-Diensten** wie Google Analytics, gleich ob als Client-Side- oder Server-Side-Tracking-Lösung, ist es **notwendig**, bereits im **Vorfeld** der **Übermittlung** die **Datenparameter** für das **Tracking** – IP-Adresse, User Agent, Client-ID, User ID und ggf. Order IDs – einer **validen Pseudonymisierung** zu unterziehen, damit die Anforderungen aus dem EuGH-Urteil „Schrems II" vollständig umgesetzt werden können.

Die **JENTIS-Lösung ermöglicht** mittels **Modifizierung/Synthetisierung** der verarbeiteten Datenparameter die Umsetzung einer **wirksamen Pseudonymisierung**, um die Anforderungen an „zusätzliche Maßnahmen" belastbar dokumentieren zu können.

4. Rechtsunsicherheit TADPF: Wird es einen neuen Angemessenheitsbeschluss für die USA geben?

Schließlich ist die am 25.03.2022 verkündete Einigung zwischen US-Präsident Biden und Präsidentin der EU-Kommission Ursula von der Leyen auf ein neues „Trans Atlantic Data Privacy Framework" (**„TADPF"**) als Nachfolgeabkommen für das vom EuGH für unwirksam erklärte EU-US Privacy Shield derzeit erheblichen Rechtsunsicherheiten ausgesetzt.

(1) Bislang ist noch kein ausverhandelter Text des Abkommens als Grundlage für eine etwaige Executive Order in den USA und einen etwaigen Angemessenheitsbeschluss der EU-Kommission nach Art. 45 DSGVO existent. In einer Antwort der EU-Kommission auf eine Anfrage des EU-Parlaments vom 11.05.2022 wurde mitgeteilt, dass die Einzelheiten noch ausgearbeitet und diese noch in Rechtstexte umgesetzt werden müssten.

(2) Erst auf dieser Grundlage könne die EU-Kommission einen **Entwurf** für einen **neuen Angemessenheitsbeschluss** für die USA vorschlagen und das entsprechende Annahmeverfahren einleiten. Das Annahmeverfahren beinhaltet die **Einholung einer Stellungnahme** des **EDPB** und ein positives **Votum** der **Mitgliedstaaten** im sog. Komitologieverfahren. Das **Europäische Parlament** hat dabei ein **Kontrollrecht** über Angemessenheits-Entscheidungen der EU-Kommission als Durchführungsrechtsakt i. S. d. Art. 291 AUEV. Erst dann, wenn diese Verfahren im Rahmen von Durchführungsrechtsakten abgeschlossen sind, kann die Kommission einen neuen Angemessenheitsbeschluss nach Art. 45 DSGVO erlassen.

(3) Dabei ist zur berücksichtigen, dass ein etwaiger Angemessenheitsbeschluss der EU-Kommission keinen Freibrief für die Datenübermittlung in die USA erteilt. Wie beim Vorgängerabkommen dem EU-US Privacy Shield wird eine **Selbstzertifizierung von US-Unternehmen** bei der US-Regierung erforderlich sein, d. h. ist eine Prüfung erforderlich, ob eine aktive Zertifizierung für den jeweiligen Datenempfänger auch tatsächlich vorliegt.

(4) Ungeachtet dessen ist mit folgenden **drei** bislang **nicht** von den Verhandlungspartnern **thematisierte Risiken** umzugehen:

Erstens stellt sich Frage wie mit Unterauftragsverarbeitern, im Fall von Google Analytics über 50 Unterauftragnehmer, als Empfänger der Daten in Drittländern ohne angemessenes Schutzniveau wie **Taiwan**, **Philippinen**, **Brasilien**, **Mexiko**, **Malaysia** und **Indien** umzugehen ist. Für diese Drittländer existiert kein Angemessenheitsbeschluss der EU-Kommission.

Zweitens ist noch ungewiss, ob die Entscheidung des Supreme Court vom 04.03.2022 in Sachen „FBI ./. Fazaga" Auswirkungen auf die aktuellen Verhandlungen zwischen der EU und der USA haben werden. Denn der im TADPF angedachte **„Independent Data Protection Review Court" könnte durch** die höchstrichterliche **Entscheidung** vom Supreme Court aufgrund der Aufrechterhaltung des „state secret privilege", wonach wichtige Informationen zu den Überwachungsmaßnahmen betroffenen Personen nicht offen gelegt werden müssen, **in Frage gestellt werden** [vgl. Lejeune, Trans-Atlantic Data Privacy Framework trotz U.S. Supreme Court Entscheidung in FBI v. Fazaga?, 31.03.2022].

Drittens weist der Hessische Datenschutzbeauftragte zu Recht auf den Umstand hin, dass nach Art. 44 S. 2 DSGVO alle Bestimmungen des Kapitel 5 DSGVO in Weise anzuwenden sind, dass das Schutzniveau der DSGVO nicht untergraben wird [Roßnagel, ZD 2022, 305 f.]. Daraus folgt, dass der TADPF und ein etwaig darauf gestützter Angemessenheitsbeschluss für die USA in tatsächlicher Hinsicht ein der DSGVO gleichwertiges Schutzniveau sicherstellen muss. Hierfür wird die Einrichtung eines „Independent Data Protection Review Court" und die Zusicherung von Zugriffsbeschränkungen auf Seiten der US-Sicherheitsbehörden und Nachrichtendienste allein nicht unbedingt ausreichend sein. Vor diesem Hintergrund empfiehlt der Hessische Datenschutzbeauftragte die Entwicklung und Gestaltung von Techniksystemen sowie einer an den Vorgaben der „Schrems II"-Rechtsprechung orientierten Datenschutzberatung [Roßnagel, ZD 2022, 306].

5. 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 versetzt die JENTIS SaaS-Lösung Unternehmen beim Einsatz von Tracking-Technologien von Drittanbietern in die Lage, die **„Schrems II"-Compliance** in der Supply Chain **sicherzustellen**.

III. Wie JENTIS dabei hilft, rechtliche Risiken auszuräumen

(1) Die **JENTIS SaaS-Lösung** ermöglicht ein **hybrides Tracking** in einer Kombination aus clientseitigem und serverseitigem Tracking. JENTIS bietet 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**.

Dabei werden Nutzerdaten 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 wird der Verlust der Kontrolle beim Einsatz von Tracking-Anwendungen von vornherein verhindert.

Die JENTIS SaaS-Lösung umfasst unabhängig davon eine **eigenständige CMP-Lösung**, die auf Grundlage einer Nutzerzustimmung nach Maßgabe der datenschutzrechtlichen Anforderungen eine Weitergabe von Tracking-Daten an AdTech-Anbieter ermöglicht.

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

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

Alle **JENTIS-Systeme** werden in **Österreich** auf Servern der A1 Telekom Austria **gehostet**. Ein Drittlandrisiko wie bei gängigen Cloud-Diensten wird von vornherein vermieden.

(3) Für die Nutzung der JENTIS SaaS-Lösung ist sowohl ein DNS-Setup auf der eigenen 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 im Quellcode der Website implementierte Third-Party-Tags wie JavaScripte, iFrames und Image-Pixel derart modifiziert, 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 der JENTIS Middleware wird eine direkte Verbindung zwischen dem Browser des Nutzers und der Drittanbieter von vornherein vermieden.

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

(4) Im Einzelnen werden je nach Konfiguration des Administrators folgende Datenkategorien verarbeitet:

Datenparameter	**Beschreibung**

IP-Adresse	Diese muss aus technischen Gründen zwingend übertragen werden und wird dann am JENTIS-Server anonymisiert weiterverarbeitet.
User-ID von JENTIS	Sie ist eine zufällig generierte Zahlenkombination und dient vor allem der Wiedererkennung des 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 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 Besuchers ausgelesen und an den JENTIS-Server geschickt. Dabei handelt es sich um statische Daten, die durch das Device des Besuchers festgelegt sind.
Benutzer Aktionsdaten	Diese Daten werden im Browser des Besuchers ausgelesen und an den JENTIS-Server geschickt. Dabei handelt es sich um Daten, welche die Aktionen des Besuchers auf der Webseite beschreiben.

(5) Für die **rechtliche Beurteilung** der beschriebenen **Risiken und Rechtsunsicherheiten** (Pkt. II.) ergeben sich auf Grundlage des in den technischen Dokumentationen von JENTIS dargelegten Funktionsprinzips **zwei wesentliche Verarbeitungsschritte** in Bezug auf Nutzerdaten:

Erstens der Endgerätezugriff, ausgelöst durch die Anfrage des Browsers des Nutzers an JENTIS Server zur Wiederkennung eines Browsers des Nutzers über First-Party-Cookies durch Vergabe einer zufällig generierten JENTIS User-ID für die festlegten Use Cases. Die Laufzeit der JENTIS kann nach der Risikoaffinität der Kunden sitzungsbezogenen oder persistent bis zu 24 Monate festgelegt werden.

- An dieser Stelle wirkt sich die Drittlandthematik nicht aus. Alle JENTIS-Systeme werden auf Servern der A1 Telekom Austria gehostet.
- Für die Frage, unter welchen Voraussetzungen JENTIS im „Private Mode“ als „technisch notwendig“ ohne Einwilligung der Nutzer eingesetzt werden kann, ist Gegenstand einer separaten Begutachtung.

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

- Angesichts der Übermittlung von „bereinigten Tracking-Daten“ können die Anforderungen von Art. 44 ff. DSGVO im Einklang mit aufsichtsbehördlichen Positionierungen wie nachfolgend dargelegt erfüllt werden.

Auf Grundlage des skizzierten Funktionsprinzips der konfigurierten JENTIS Systeme **(1.)** lässt sich die „Schrems II“-Compliance in der Supply Chain **(3.)** mittels einer Synthetisierung der Datenparameter der Browser-Session des Nutzers als wirksames Mittel der Pseudonymisierung **(2.)** sicherstellen.

1. Funktionsprinzip der konfigurierten JENTIS Systeme

(1) JENTIS fungiert als Middleware als eine Art Gatekeeper zwischen Browser und Server von Drittanbietern. Damit besteht die Möglichkeit, alle gesammelten Daten vor dem Transfer an Drittanbieter DSGVO-konform zu pseudonymisieren (vgl. Pkt. III. 2.).

(2) Der Administrator bestimmt im JENTIS Tag Manager, welche Daten im Browser des Besuchers ausgelesen und an JENTIS gesendet werden sollen. Auf Ebene der Datenparameter kann der Administrator 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.

(3) Der Administrator bestimmt durch das Hinzufügen von “Trackern”, welcher externe Drittanbieter Daten von JENTIS erhalten sollen. Dabei konfiguriert der Administrator 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 Administrator außerdem, ob vor der Weitergabe an den externen Anbieter eine Entfernung der Datenparameter oder eine Synthetisierung der Datenparameter [vgl. hierzu Pkt. III. 2.] durchgeführt werden soll.

Die detailgenaue Entfernung oder Synthetisierung 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 minimiert 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 IP-Adresse des Website-Besuchers vor der Weitergabe an die Drittanbieter vollständig entfernt 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 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 nicht verarbeitet und als synthetisch erzeugte fiktive Client-ID an den jeweiligen Drittanbieter gesendet.

Ebenso werden 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 synthetisierten und ausgetauschten IDs der Drittanbieter sowie die demographischen Standort-Daten (Land/Stadt) 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 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.

(7) Die Verarbeitung von Nutzerdaten beim Website-Tracking unter Einbindung der JENTIS-Lösung ermöglicht den Kunden, je nach Use Case, JENTIS Systeme so zu konfigurieren, dass ein Betreten von rechtlich festem Boden möglich ist, ohne den unter Pkt. II geschilderten Rechtsunsicherheiten ausgesetzt zu sein. Die vom EDPB geforderte wirksame Pseudonymisierung vor Übermittlung an Drittanbieter [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.] kann in JENTIS Systemen eine Synthetisierung relevanter Datenparameter umgesetzt werden.

2. Bewertung der Übermittlungen synthetisch erzeugter Client-IDs an Drittanbieter

(1) Als für den Drittlandtransfer relevanten Verarbeitungsvorgang, der sich an den Endgerätezugriff durch JENTIS anschließt, ist die serverseitige Übermittlung der bereinigten Tracking-Daten (synthetisch erzeugte Client-ID und Order-ID sowie Eventdaten) an Drittanbieter wie z. B. Google zu bewerten.

(2) Es erfolgt weder eine Übertragung der von Google vergebenen Client-ID noch der IP-Adresse des Nutzers. Bei der Kommunikation des Web-Server mit JENTIS-Servern und anschließend mit den Google-Servern werden je nach Konfiguration der JENTS-Systeme bereinigte Tracking-Daten – die synthetisch erzeugte Client-ID, die IP-Adresse des Web-Servers, der synthetisierte User Agent und die synthetisierte Order-ID – übermittelt (vgl. Pkt. I. 1.).

(3) Die Bildung von **synthetischen Daten** aus Rohdaten lässt sich als **„zusätzliche Maßnahme“** zur Absicherung des Drittlandtransfers i. S. d. „Schrems II“-Rechtsprechung einordnen.

- Die **ENISA** (European Union Agency for Cybersecurity) beschreibt „**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 [vgl. ENISA, Data Protection Engineering, 2022, S. 17].

- Laut **EDPS** können „**synthetische Daten**" als Technologie zur Verbesserung des Schutzes der Privatsphäre (**Privacy Enhancing Technology**) betrachtet werden und in diesem Sinne als „**zusätzliche Maßnahme"** bei **Datenübertragungen außerhalb** der **Europäischen Union** oder innerhalb von Organisationen, die keine Identifizierung einer bestimmten Person benötigen, eingesetzt werden.
- Die Synthetisierung dient nach Ansicht der **ENISA** in erster Linie der **Vertraulichkeit** der **Verarbeitung** [vgl. ENISA, Data Protection Engineering, 2022, S. 17], die den Charakter „zusätzlicher Maßnahmen" in technischer und organisatorischer Hinsicht i.S.d. Art. 32 DSGVO aufweist.
- Es verbietet sich eine pauschale **rechtliche Einordnung** von synthetischen Daten. Soweit das Risiko der Re-identifizierung nicht ausgeschlossen werden kann, weil synthetische Daten mit realen Daten vermengt werden, sind synthetische Daten **nicht als anonyme Daten** einzuordnen [EDPS, Synthetic data: what use cases as a privacy enhancing technology, 2021, S. 3]. Auch die ENISA schließt die Annahme einer Anonymisierung im Fall der Vermischung von realen Daten und synthetischen Daten aus [vgl. ENISA, Data Protection Engineering, 2022, S. 18].
- Im Fall der Use Cases beim Einsatz von JENTIS, z. B. bei der Website-Analyse, ist die Wiederkennung 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 Order-IDs nach entsprechender Konfiguration der JENTIS-Systeme **synthetisiert** werden, weisen die übermittelte Datensatz 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 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 CNIL hat jüngst in ihren „FAQs zu Google Analytics vom 07.06.2022" explizit Proxy-Lösungen, wie sie von JENTIS mit der Twin-Server Technologie bereitgestellt werden, als rechtmäßiges Instrument zur Lösung für das „Schrems II"-Problem hervorgehoben. Dabei müssten Proxy-Lösungen folgende Voraussetzung erfüllen:
    - Keine Übermittlung der IP-Adresse des Nutzers. Sollte der Proxy-Server den Standort durch vorherigen Abgleich mit einer Geo-IP-Datenbank abgeglichen haben, muss die Angabe so beschaffen sein, dass keine Re-Identifizierung möglich ist.

- Der Algorithmus, der die Ersetzung vornimmt, sollte ein ausreichendes Maß an Kollisionen gewährleisten (d. h. eine ausreichende Wahrscheinlichkeit, dass zwei verschiedene Kennungen nach dem Hashing ein identisches Ergebnis liefern und das Ergebnis des Hashings für dieselbe Kennung nicht immer dasselbe ist).
- Referer müssen gelöscht werden.
- In den gesammelten URLs enthaltenen Parameter müssen gelöscht werden (z. B. die Click-IDs und URL-Parameter, die das interne Routing der Website ermöglichen);
- Informationen, die zur Erstellung eines Fingerprintings beitragen können, wie z. B. "User-Agents", müssen neu verarbeitet werden, um die seltensten Konfigurationen zu entfernen, die zu einer erneuten Identifizierung führen können.
- Keine Sammlung von Identifikatoren zwischen mehreren digitalen Angeboten (Cross-Site) oder aus eigenen Kundensystemen (z. B. CRM-ID);
- Löschung aller anderen Rohdaten, die zu einer Re-Identifizierung führen können.

- Mithilfe von JENTIS können alle Voraussetzungen der CNIL an Proxy-Server erfüllt werden. Denn die Synthetisierung von Nutzer Daten entspricht wie sogleich beschrieben der Bildung von Hash-Werten wie sie die CNIL vorschlägt.

(4) Die Bildung von **synthetischen Daten** aus realen Rohdaten **entspricht** der Bildung von **Hash-Werten**, soweit es um die **Einordnung der Synthetisierung als** Maßnahme der **Pseudonymisierung** geht.

- Pseudonymisierung stellt eine geeignete Privacy Pattern im Rahmen von „Privacy by Design" dar [vgl. BGH, Urt. v. 15.5.2018 – VI ZR 233/17 Rn. 26] und kann bei „JENTIS" bereits auf Rohdatenebene 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 [BGH, Urt. v. 28.05.2020 – I ZR 7/16 – Cookie Einwilligung II; zustimmend in Bezug auf DSGVO Menke, K&R 2020, 650, 652; Baumgartner/Hansch, ZD 2020, 435, 436]. Gleiches muss in der Konsequenz auch für andere Identifier wie Device IDs, IDFA, GAID und Universal IDs gelten.
- Außerdem wird die Anwendung von **Hashing-Verfahren** auf Klardaten von Nutzern von europäischen Behörden [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; EDPS/AEPD, Introduction to the Hash Function as a personal data Pseudonymisation technique, 2019, S. 21] und der Kommentierung als **Pseudonymisierung i. S. d. Art. 4 Nr. 5 DSGVO** angesehen [Stentzel/Jergl, in: Gierschmann/Schlender/Stentzel/Veil, DSGVO, Art. 4 Nr. 5 Rn. 6; Arning/Rothkegel, in: Taeger/Gabel, DSGVO/BDSG, 3. Aufl., Art. 4 Rn. 144]. Mittels einer ausreichenden Hashfunktion werden Eingabedaten auf Grundlage eines Algorithmus in einen Schlüsseltext (Hashwert) transformiert, der jedenfalls nicht mit verhältnismäßigem Aufwand reversibel ist

und bei denselben Eingabedaten stets derselbe ist [vgl. 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].

- Die Anwendung von **Hashfunktionen** im Kontext der **Erstellung von Zielgruppen** stellt auch nach Einschätzung der „Fokusgruppe Datenschutz" des Bundesministeriums des Innern, eine Pseudonymisierung i. S. d. Art. 4 Nr. 5 DSGVO dar [Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, S. 26].
- Die Bildung von **Hashwerten** aus **Rohdaten** wie die **E-Mail-Adresse**, **Telefonnummer** [vgl. hierzu ENISA, Pseudonymisation techniques and best practices, 2019, S. 33] und **Bürgernummern** [vgl. hierzu Artikel 29-Data Protection Working Party, WP 216, Opinion 05/2014 in Anonymisation Techniques, S. 20] zur Erstellung von Zielgruppen stellt deshalb eine **valide Pseudonymisierung** dar, weil die gebildeten Hashwerte z.B. bei Anwendung des Hashing-Algorithmus SHA 256 als robuste Hashfunktion **irreversibel**, d.h. **nicht rückführbar** sind, **und** eine **Kollisionsfreiheit** gewährleisten, d. h. dass man aus zwei Eingangswerten nicht denselben Hashwert als Ausgangswert erzeugen kann [ENISA, Data Pseudonymisation: Advanced Techniques & Use Cases, 2021, S. 12].
- Die **Synthetisierung 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. 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.

(5) Im Fall der **Entfernung der IP-Adresse** und **Synthetisierung von Tracking-Parametern** vor Übertragung der Daten an Drittanbieter wie Google ist von einer wirksamen Pseudonymisierung nach Lesart des EDPB als „zusätzliche Maßnahme" für die **„Schrems II"-Compliance** auszugehen [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.]:

- 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 synthetisch erzeugten Client IDs und Order IDs der Drittanbieter sein kann [Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, S. 11 f.], ist laut dem beschriebenen technischen Funktionsprinzip angesichts der Systemarchitektur von JENTIS eine robuste Trennung der Dateninstanzen gegeben, die eine Zuordnung für Drittanbieter ausschließen.

- Nur dann, wenn eine Re-Identifizierung ausgeschlossen ist, weil die verarbeitende Stelle nicht über die erforderliche Zuordnungsregel verfügen würden, wäre eine Anonymisierung der übertragenen Parameter an Drittanbieter im Einklang mit Erwägungsgrund 26 DSGVO in Betracht zu ziehen und eine entsprechende Verarbeitung vom Anwendungsbereich der DSGVO auszuklammern. Verfügen jedoch die am Tracking beteiligten Parteien wie JENTIS über die User-ID als „Schlüssel" für die Zuordnung zu synthetisch erzeugten Client- und Order IDs von Drittanbietern, ist ebenfalls mit Blick auf die Einschätzung der „Fokusgruppe Datenschutz" des Bundesministeriums des Innern aufgrund der Pseudonymisierung von einem Personenbezug auszugehen [Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, S. 22].
- Nach einer aktuellen und fachlich einschlägigen **Rechtsprechung des Handelsgerichts des Kantons Zürich** zum Schutz des Persönlichkeitsrechts nach Art. 28 des ZGB (Schweiz) ist eine Pseudonymisierung für den Empfänger, der die pseudonymisierten Datensätze keiner bestimmten Person zuordnen kann, persönlichkeitsrechtlich als Anonymisierung zu werten [vgl. HGer ZH, Urt. v. 04.05.2021 – HG190107-O]. Wenngleich diese Rechtsprechung nicht im Hoheitsgebiet der EU ergangen ist, hat sie zumindest Indizienwirkung.
- Soweit ersichtlich, erhalten Drittanbieter wie Google bei den skizzierten Datenübermittlungen im Nachgang des Endgerätezugriffs lediglich eine von JENTIS **synthetisch erzeugte 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.
- Ebenso ist **kein Zugriff auf** die **JENTIS Systeme** 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 [vgl. auch Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3. Aufl. 2020, Art. 4 Rn. 12].

3. Bewertung des Drittlandtransfers

(1) Für in Rede stehenden abstrakten **Zugriffsmöglichkeiten** auf Server von Drittanbietern nach Reduzierung und Synthetisierung von Tracking-Parametern durch US-Sicherheitsbehörden **lassen sich im Einklang mit der Rechtsprechung** des französischen Verwaltungsgerichts Conseil d'État [Beschl. v. 13.10.2020 – 444937] zur Zulässigkeit der Nutzung von Cloud-Diensten von Microsoft Azure auf Servern in den Niederlanden folgende Maßnahmen bei der Nutzung der JENTIS Saas-Lösung in vertretbarer Weise **als „zusätzliche Sicherungsmaßnahmen"** im Sinne der EuGH-Rechtsprechung [EuGH, 16.7.2020 – C-311/18 – Schrems II] **werten**:

- Standort der JENTIS Server von A1 Telekom Austria in Österreich. Keine Verarbeitung der Rohdaten aus Serveranfragen des Browsers von Nutzern außerhalb der EU/des EWR;
- Zugriffsbeschränkungen auf JENTIS-Systeme mittels Identity und Access Management;
- Vorhalten einer abgeschotteten Datenhaltung ohne Zugriff durch Drittanbieter wie Google aus den USA aufgrund fehlender Zugriffsmöglichkeiten der Drittanbieter auf JENTIS-Server, Endgeräte der Nutzer oder der pseudonymen JENTIS User-ID;
- Verhinderung eines expliziten Datenaustausches zwischen den Rohdaten aus dem Endgerät der Website-Besucher und Drittanbietern;
- Abschottung von Serverinstanzen unterschiedlicher Kunden und Zugriffsbeschränkungen;
- Reduktion: Entfernung der IP-Adresse vor Übermittlung der Tracking-Parameter an Drittanbieter
- Restriktion: Risikovermeidung durch Funktionseinschränkung von Tracking-Diensten, z. B. ungenaue Standortbestimmung aufgrund der Entfernung der IP-Adresse und Nutzung von IP-Geolokalisierungs-Datenbanken sowie Ausschluss von endgeräteübergreifendem Tracking aufgrund der Nichtnutzung der originalen Client ID z. B. im Google Analytics-Account;
- Valide Pseudonymisierung aufgrund der Synthetisierung von Client ID, User Agent, Order ID sowie weiterer Datenparameter und fehlender Zugriffsmöglichkeiten von Drittanbietern wie Google auf Zuordnungsregeln;
- Valide Pseudonymisierung und Verschlüsselung sowie fehlende Zugriffsmöglichkeiten von Drittanbietern wie Google auf Zuordnungsregeln in JENTIS Systemen.

(2) Vor diesem Hintergrund **können** die **beschriebenen Zusatzmaßnahmen** gemäß dem technischen Funktionsprinzips (Pkt. III. 1.) in Kombination mit einem Abschluss von Standardvertragsklauseln derzeit vorbehaltlich anderslautender Rechtsprechung, Beschlüsse von Aufsichtsbehörden oder Lösungen auf politischer Ebene eine **Rechtfertigung** für den **Drittlandtransfer** gemäß Art. 46 Abs. 2 lit. c) DSGVO **darstellen**.

(3) Insbesondere wird bei Nutzung von JENTIS der Anforderung des EDPB entsprochen [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.], als „zusätzliche Maßnahmen" i. S. d. EuGH-Rechtsprechung „Schrems II" Maßnahmen der Pseudonymisierung vor Übermittlung von Daten in eine Cloud anzuwenden. Denn JENTIS ermöglicht, dass Identifikatoren, die für entsprechende Use Cases verwendet werden, nicht im Klartext, sondern ausschließlich als pseudonyme Kennung in die Serverinstanzen von Drittanbietern übertragen werden.

(4) Die von JENTIS ermöglichten Zusatzmaßnahmen stellen „technischen oder organisatorischen Garantien" gemäß **Ziff. 14 der Standardvertragsklauseln** dar und ermöglichen die Erfüllung der Pflicht zur Durchführung und Dokumentation eines „**Transfer Impact Assessments**". Die beschriebenen Maßnahmen stellen eine Mitigation der Risiken eines Zugriffs von Sicherheitsbehörden im Sinne von „**zusätzlichen Maßnahmen**" bei entsprechender Konfiguration der JENTIS Systeme durch den Administrator dar.

4. Zusammenfassung

Es bleibt festzuhalten: Mithilfe der **JENTIS-Lösung** lassen sich den lokal und **regional unterschiedlichen Ansichten** von Gerichten und Aufsichtsbehörden zu internationalen Datenübermittlungen – etwa die Ablehnung eines risikobasierten Ansatzes durch die österreichische Aufsichtsbehörde – sowie den individuellen Compliance-Vorgaben **im Einzelfall** vollumfänglich **Rechnung tragen**.

JENTIS ermöglicht mit der hybriden 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 internationale Datenübermittlungen in Drittländer ohne angemessenes Schutzniveau 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 Anforderungen an Drittlandtransfers reagieren.

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** beim Drittlandtransfer (vgl. Pkt. II.) **ausgeräumt** werden.

Die **JENTIS SaaS-Lösung ermöglicht** im Fall der beschriebenen Konfiguration den Nachweis von „**zusätzlichen Maßnahmen“,** die ergänzend zum Abschluss von Standardvertragsklauseln eine Rechtfertigung für den Drittstaatentransfer darstellen können und auf diesem Wege die **„Schrems II“-Compliance** in der Supply Chain sicherstellen.

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.**