Data Protection Memorandum

JENTIS GmbH

SPIRIT LEGAL®

Author	**Date of the document**
RA Peter Hense & RA Tilman Herbrich (CIPP/E)	*11 June 2022 V2.1*

Project

Evaluation of the JENTIS SaaS solution for implementing the requirements from the CJEU "Schrems II" ruling

Executive Summary

The industry solutions proposed so far such as server-side tracking, which enable qualitative website tracking despite the increasing adoption of ad blockers and tracking prevention systems, do not change the strict requirements for the transfer of personal data to third countries such as the USA without an adequate level of data protection as defined by the CJEU case law in the "Schrems II" ruling **(I.1.)**. The issue with transfer to third countries has become considerably more serious since the beginning of 2022 with unanimous pan-European decisions by supervisory authorities on Google Analytics and early indications in the court case law **(I.2.)**. When using the server-side Google Tag Manager, there is also the problem that the entire tech stack of the company is embedded in the Google Cloud Platform, which means a loss of control over access to user data even for non-critical tracking services with pure EU infrastructure. Even if the server-side Google Tag Manager is not hosted in the Google Cloud, this problem is not solved.

Due to complex and difficult-to-solve tracking application integration challenges and insufficient industry solutions, there is a growing need for long-term sustainable strategies for legally compliant and effective data usage **(I.3.)**. JENTIS, as a Privacy Enhancing Technology, offers long-term support to ensure "Schrems II" compliance in the supply chain and allows customers to flexibly configure the SaaS solution to take into account the volatility of each company's individual risk situation.

A number of significant legal uncertainties have arisen in practice regarding the third-country issue in website tracking: Starting with the impractical requirements for requesting consent for transfers to a third country without an adequate level of data protection via a consent management platform **(I.1.)**, to the interpretation of what is meant by "additional measures" to safeguard third-country transfers under the EU Commission's new standard contractual clauses **(II.2./II.3.)**, to dealing with the announcement of the planned "Trans Atlantic Data Privacy Framework" as a successor agreement to the EU-US Privacy Shield, which was declared invalid by the CJEU **(II.4.)**.

Based on the outlined operating principle of the JENTIS systems **(III.1.)**, "Schrems II" compliance in the supply chain can be ensured when using third-party providers such as Google for website tracking **(III.3.)** by synthesising the data parameters of the user's browser session as an effective measure of pseudonymisation in accordance with the recommendations of the EDPB **(III.2.)**. In line with the EDPS' view, "synthetic data" can be considered a Privacy Enhancing Technology and used as an "additional measure" for data transfers outside the European Union. Singling-out or re-identification of individual users is no longer possible for tracking providers in the third country when identifiers are synthesised on JENTIS systems within the European Union. JENTIS can therefore fully implement the "Schrems II" requirements for international data transfers and eliminate legal uncertainties.

When using JENTIS, website operators can enjoy the economic benefits of their own first-party data without putting their data or their respective corporate compliance at risk from a legal perspective through uncontrolled and non-transparent processing on the part of third parties **(IV.)**. With the help of JENTIS technology, companies regain complete control with server-side tracking.

Legal Appraisal

I. Status analysis - legal classification of processing in website tracking

The implementation of JavaScripts or HTML elements such as iFrames or image pixels of tracking services, e.g. the Google Analytics 4.0 "gtag. js" in the source code of a website, requires access to end device information and, due to the HTTPS request of the user's browser (client) initiated by the JavaScript, a transmission of the website visitor's personal data to servers of third parties such as Google in the USA [see ECJ, judgement of 29.07.2019 - C-40/17, para. 26 - Fashion ID].

The legal framework for international data transfers is decisively shaped by developments in the industry, court decisions, and audits by supervisory authorities in their respective area of responsibility. The transfer of personal data such as IP addresses [see ECJ, judgement of October 19, 2016 - C-582/14, para. 47 - Breyer] and client and user IDs [see BGH, judgement of May 28, 2020 - I ZR 7/16 - Cookie consent II, para. 72] to the USA as a third country without an adequate level of protection within the meaning of Chapter 5 GDPR is not avoided by the transition from client-side tracking to pure server-side tracking (1.). The requirements for the lawfulness of international data transfers have become considerably stricter since the beginning of 2022 due to unanimous pan-European decisions by supervisory authorities on Google Analytics as well as first court rulings (2.).

1. Developments in the industry

(1) It may be noticed that since 2017, beyond Ad-blockers, also common browser providers such as Safari and Firefox offer the tracking prevention systems "ITP" (Intelligent Tracking Prevention v2.3) of the browser "Safari" or "ETP" (Enhanced Tracking Prevention) by default, which prevent third-party and, partly, first-party tracking for analytics and advertising purposes from the outset. These technical developments in the browser landscape have negative consequences for the tracking of user behaviour:

- known tracking scripts are blocked and not executed,
- third- and essential first-party cookies are blocked by default,
- the runtime of even first-party cookies and the use of the end device capacity "LocalStrorage" is restricted (7 days to 24 hrs),
- marketing attributions can no longer be made continuously,
- the customer journey can only be tracked for short periods of 1-7 days,
- lack of robust data makes targeted optimization of marketing campaigns difficult.

(2) Previous approaches to solutions such as server-side tracking, for example via the Server Side Google Tag Manager (SSGTM) or the Facebook Conversions API to circumvent ad blockers and tracking are not exempt from compliance with data protection requirements. On the contrary, the supervisory authority in Baden-Württemberg ("LfDi BaWü") clarifies in the "FAQ on Cookies and Tracking" (p. 16): Even with server-side tracking, the requirements from both the TTDSG and the GDPR must be complied with.

(3) The legal starting point for the application of the TTDSG is the access to information from a server request made by the browser due to the implementation of JavaScripts in the source code or the

website [LG München, reference decision dated 08.12.2021 - 33 O 14776/19]. According to the "LfDi BaWü", server-side tracking, in addition to terminal access, is a processing operation pursuant to Art. 4 No. 2 GDPR when personal data is transmitted.

(4) While data from end devices is not sent to the third party via the user's browser, they are sent by means of a redirection via a server-side API (Facebook) or a server of the website operator on the Google Cloud Platform or via Docker containers on the company's own systems (SSGTM) [see for example Papadogiannakis et al., User Tracking in the Post-cookie Era, 2021, p. 1 f.]. When using the SSGTM, the situation is exacerbated by the fact that the company's entire tech stack is embedded in the Google Cloud Platform, resulting in a loss of control over access even for non-critical tracking services with pure EU infrastructure.

(5) Privacy enhancing technologies such as the JENTIS Tag Manager and the JENTIS Server Suite (see III.), allow the data parameters to be modified on the basis of the tags loaded from third parties collected during the data processing that takes place when a website is called and can ensure legally compliant use in the supply chain by means of privacy by design.

2. Current legal situation regarding data transfers to third countries without an adequate level of protection

a) Requirements for the transfer of user data to third countries

(1) For data transfers to third parties such as Google located in a third country outside the EU/EEA for which the EU Commission has not issued an adequacy decision pursuant to Article 45 (1) of the GDPR, an alternative justification for the third country transfer is necessary.

(2) As a justification for the transfer of data to Google LLC in the USA without an adequate level of protection in the case of the use of e.g. Google Analytics [cf. Data Protection Conference ("DSK"), decision of 12.05.2020 - Notes on the use of Google Analytics], practically the only remaining option following the ECJ case law [ECJ, 16.7.2020 - C-311/18 - Schrems II] is the agreement of standard contractual clauses ("SCC").

(3) In the ECJ ruling of 16.7.2020, not only was the EU-US Privacy Shield declared invalid, but - depending on the legal situation in the destination country - further measures or guarantees were requested for a legally permissible third country transfer based on the standard contractual clauses [ECJ, 16.7.2020 - C-311/18 - Schrems II]. This means that not only has the EU-US Privacy Shield ceased to be a legal basis for data transfers to the USA. Also, any data transfer and data access by U.S. companies based on SCC pursuant to Art. 46(2)(c) GDPR require additional technical and organisational measures to protect against access by U.S. authorities and to ensure effective legal protection for data subjects against unauthorised access.

b) Current audits of supervisory agencies and NGOs in law enforcement

(1) In a partial decision dated 22 December 2021 and a partial decision dated 22 April 2022, the Austrian authority decided that the technical and organisational measures communicated by Google in the SCC, such as the shortening of the IP address after transmission to the USA, are not sufficient to meet the requirements of the ECJ case law for third country transfers when using

Google Analytics. Above all, the descriptions provided by Google in the SCC "Google Ads Data Processing Terms" (including Google Analytics) in Annex II and points 8 and 9 - for example, on the shortening of the IP address after transfer - were insufficient and did not correspond to the additional measures defined by the EDPB for third-country transfers.

(2) The supervisory authority in Baden-Württemberg ("LfDi BaWü"), the CNIL (France), the Autoriteit Persoonsgegevens (Netherlands) as well as Datatilsynet from Norway and Denmark have endorsed this view meanwhile. Previously, the EDPS had already found that the use of Google Analytics on websites of the European Parliament was inadmissible due to insufficient "supplementary measures". The CNIL clarified in its "FAQs on Google Analytics" in June 2022 that it is not possible to configure Google Analytics so that no personal data or only anonymous data is transferred to countries outside the EU.

(3) The background to the supervisory procedures and sanctions is the 101 complaints filed by the NGO "NOYB" across Europe concerning the unlawful use of Google Analytics and Facebook Connect by large companies.

(4) According to Clause 7 of the Google Analytics Terms of Service, website operators are fully liable for compliance with all data protection laws, including Chapter 5 of the GDPR. In the event of a claim against Google for unlawful third country transfers, Google grants itself a comprehensive indemnity against liability in Section 8 of the Terms of Use. In the white papers published by Google on international data transfers in November 2021, Google also points out that the explanations do not constitute legal advice and that Google Analytics customers must assess the legal risks independently.

c) Current case law on inadmissible transfers to third countries

(1) The risk situation for data transfers to the USA when using Google Analytics is aggravated by first court decisions. In a recent decision on the integration of Google Fonts in a website via APIs, the LG München (judgement of 20.01.2022 - 3 O 17493/20) already awarded the data subject a cease-and-desist claim as well as a claim for damages in the amount of EUR 100.00 due to the transmission of a user's IP address to servers of Google LLC in the USA when visiting a website. The Munich Regional Court substantiated the violation of the general right to protection of personality by establishing that user data is processed by Google LLC in an uncontrolled manner and that the USA do not have an adequate level of protection according to the case law of the ECJ.

(2) Previously, the VG Wiesbaden (decision of 01.12.2021 - 6 L 738/21.WI) had already ruled that the use of the Consent Management Platform ("CMP") "Cookiebot" on a website constituted a unlawful transfer of IP addresses to the USA and that the transfer to a third country was not justified. The decision in the interim injunction proceedings was essentially overturned by the VGH Kassel (decision of 17.01.2022 - 10 B 2486/21) in the appeal proceedings due to procedural requirements for interim relief. A final clarification could only take place in proceedings on the merits.

(3) The Council of State in Belgium ruled on 06.05.2022 (case no: 253.677) that a decision to select a US contractor in the context of a public tender procedure by the Council of State should be suspended on the grounds that the authority had not sufficiently assessed whether the contractor complied with the requirements of the GDPR, in particular the provisions on transfer and further processing by another company, Smart Analytics, based in Russia.

(4) To the authors' knowledge, further court cases related to third-country transfers are pending, and therefore further enforcement can be expected in the future.

3. Conclusion: Need for long-term strategies for risk management

(1) There are already noticeable risks in the short and medium term when using tracking services due to the integration of third parties that use global infrastructures such as cloud services.
(2) Website operators need alternative solutions that allow for a modification of data processing during tracking. In the "FAQ on Cookies and Tracking" (p. 16), the LfDI BaWü suggests that such middleware solutions, which interpose themselves between the communication of the end device, the web server and third-party servers, can enable legally compliant use in server-side tracking.
(3) JENTIS, as a privacy enhancing technology, provides long-term assistance to ensure privacy by design and allows customers to flexibly configure the SaaS solution to accommodate the volatility of each company's individual risk situation.

II. Legal uncertainties due to technological diversity in website tracking

Significant legal uncertainties have arisen in practice regarding the data protection requirements for website tracking. The legal uncertainties primarily concern (1.) what the requirements are for requesting consent for transfers to a third country without an adequate level of protection via a consent management platform and (2.) what is meant by "additional measures" to secure third-country transfers due to the use of cloud-based applications for the realisation of server-side tracking mechanisms in accordance with the new SCC..

Recent decisions of the supervisory authorities on Google Analytics prove the high requirements for the legally compliant design of standard contractual clauses, especially with regard to the assessment of the "additional measures" designated in the annexes of the SCC (3.).

Finally, the agreement announced on 25 March 2022 between US President Biden and EU Commission President Ursula von der Leyen on a new "Trans Atlantic Data Privacy Framework" ("TADPF") as a successor agreement to the EU-US Privacy Shield, which was declared invalid by the ECJ, is currently subject to considerable legal uncertainties (4.).

1. Legal uncertainty consent to transfer to a third country: is a practicable implementation possible?

Even the use of consent management platforms based on cloud solutions, e.g. from AWS, Microsoft Azure or Google as infrastructure, can prevent compliance with the requirements of the ECJ ruling "Schrems II" from the outset, as the case in the VG Wiesbaden (decision of 01.12.2021 - 6 L 738/21.WI, not final) indicated. Even if one claims a CMP without any third-country risk, the request for consent for the third-country transfer due to tracking services such as Google Analytics is associated with practical hurdles that are hardly surmountable.

As an exception for a third-country transfer, the implementation of an explicit consent pursuant to Art. 49 (1) p. 1 lit. a) GDPR is associated with considerable complexity and risks. On the one hand, supervisory authorities reject the legal admissibility of consent for the transfer to tracking services in third countries. On the other hand, fulfilling the information requirements regarding recipients and all third countries in the context of requesting consent in a CMP is associated with practical hurdles that are hardly surmountable [cf. JENTIS Blog, Dealing with legal uncertainties in website tracking]:

(1) When assessing which processing operations are covered by Article 49 (1) sentence 1 (a) GDPR, a cautious standard must be applied. The European Data Protection Board ("EDPB") requires prior information on the specific existing risks stemming from the lack of an adequate level of protection in the third country. Abstract references to a lack of adequacy in the third country are not sufficient [see EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 of 25.5.2018, p. 9 f.]. Thus, it is necessary to highlight the possible risks for the data subjects resulting from the fact that the third country does not provide an adequate level of protection and that no appropriate safeguards are in place.

In addition, the "comprehensive indication" of recipients in the third country and the respective third country must be precisely described. Therefore, if this information is not provided, the derogation does not apply [see EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 of 25.5.2018, p. 9].

(2) From the point of view of the Data Protection Conference, the use of tracking tools to track user behaviour cannot, in principle, be based on consent under Article 49(1)(a) of the GDPR [DSK, Orientierungshilfe für Anbieter:innen von Telemedien, 2021, p. 32]. The scope and regularity of such transfers would regularly contradict the character of Art. 49 GDPR as an exception and the requirements of Art. 44 p. 2 GDPR [cf. 2 GDPR [see also EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 of 25.5.2018, p. 9; see also CNIL, "FAQs on Google Analytics", June 2022].

(3) In practical implementation, when using Google Analytics, for example, one will regularly fail to be able to transparently map the extensive information obligations of the EDPB in a consent layer in order to achieve an acceptable consent rate. This is because the listing of the respective third country to which the data is transferred, as well as all of the more than 50 subcontractors for Google Analytics as a recipient, is hardly practical to handle in a legally secure manner due to the scope. For example, Google reserves the right in Section 10.1 Data Processing Terms for Google Ads to process personal data in any country in which Google or subcontractors maintain facilities.

In the case of Google Analytics, website visitors would have to be informed in a CMP for each third country about missing data subject rights, complaint possibilities with supervisory authorities and missing data processing principles. The notices would have to be provided for each third country without an adequate level of protection, such as Taiwan, the Philippines, Brazil, Mexico, Malaysia and India [cf. e.g. on India study commissioned by the EDPB, Government access to data in third countries, 2021]. Only for third countries such as Japan and Argentina there are adequacy decisions by the EU Commission according to Art. 45 GDPR.

(4) Conclusion: Even with consent-based marketing using CMP solutions, the third-country problem cannot be meaningfully overcome when using Google services. A configuration of a CMP that meets the requirements of the supervisory authorities is currently associated with hardly surmountable practical hurdles due to a lack of case law.

2. Legal uncertainty third country transfer: what are "additional safeguards"?

(1) Following the ECJ case law [ECJ, 16.7.2020 - C-311/18 - Schrems II], the only practical justification for data transfer to insecure third countries, e.g. the USA, is the agreement of standard contractual

clauses. Any data transfer and data access by US companies based on SCC as pursuant to Art. 46(2)(c) GDPR requires additional technical and organisational measures to protect against access by US authorities and to ensure effective legal protection for data subjects against unauthorised access.

(2) Thus, the data exporter - i.e. any entity such as website operators that transfers personal data to the third country's sphere of influence, including data transfers from group companies based in Europe with a US parent company - must in future first check whether the obligations in the third country can be met and an adequate level of protection is guaranteed. If this is not the case - as is the case in the USA in particular due to the scope of Section 702 FISA and E.O. 12333 and the access authorizations of the security authorities - concrete compensatory measures must be taken to ensure that the level of protection is really complied with [Heckmann, Datenschutzkonforme Nutzung von Cloud-Lösungen aus unsicheren Drittländern, Wissenschaftliches Gutachten, 2021, p. 15; Heinzke, GRUR-Prax 2020, 436].

(3) Even if servers are located in Europe, the third-country issue cannot be avoided from the outset. According to the expert opinion commissioned by the DSK on the current status of US surveillance law and surveillance powers, US providers of electronic communications services are subject to the US surveillance law 50 U.S. Code § 1881a (Section 702 FISA), even if they store the data outside the USA, namely within the EU. Similarly, when using cloud resources from US companies, as in the case of the server side Google Tag Manager under the CLOUD Act, if the data is stored on servers within the EU, the US provider could be required to hand over the data [Heckmann, Datenschutzkonforme Nutzung von Cloud-Lösungen aus unsicheren Drittländern, Wissenschaftliches Gutachten, 2021, p. 16; Paal/Kumkar, MMR 2020, 733].

(4) According to point 14 of the SCC, there is an obligation to carry out and document a "Transfer Impact Assessment", in which an analysis and mitigation for risks of access by security authorities must be carried out on the basis of "additional measures" as additional contractual, technical and organisational measures.

Which "additional measures" are to be taken is to be evaluated on the basis of the "Recommendations 01/2020 on measures [...]" in version 2.0 published by the EDPB on 18.06.2021 as a follow-up to the new SCC of the EU Commission. Without documentation of additional risk mitigation measures, the application of the SCC will not be accepted by supervisory authorities. Additional measures may include, for example, anonymization or advanced pseudonymization of data as well as extensive encryption technologies, if it is ensured that recipients in the third country do not have access to the attribution rule for the pseudonymized data within the meaning of Art. 4 No. 5 GDPR or the data to be processed [Paal/Kumkar, MMR 2020, 733].

(5) Conclusion: With regard to the use of tracking services, it must be evaluated on a case-by-case basis how a valid pseudonymization can be carried out in advance of the transfer of user data to a third party, e.g. Google, in order to ensure "Schrems II" compliance.

3. legal uncertainty Google & Co.: Are "additional measures" in SCC sufficient?

The European supervisory authorities impose strict requirements on "additional measures" in SCC for the non-modified use of tracking services from US providers (cf. already point I.2.b.):

(1) In essence, the supervisory authorities throughout Europe consider the "additional measures" cited by Google in the SCC "Google Ads Data Processing Terms" (including Google Analytics) in Annex II and points 8 and 9 - for example, to shorten the IP address after transmission by Google - to be insufficient, so that the requirements of the "Schrems II" case law are not met.

(2) In its partial decision of 22 December 2021, the Austrian authority had pointed out that unique online identifiers such as IP addresses and unique identifiers such as cookie IDs (in the case of Google Client ID and User ID) are used as a starting point for surveillance by intelligence services. It cannot be ruled out that intelligence services have previously collected information that can be used to trace data from server requests back to individual users.

The fact that the NSA, as the US security agency, accesses cookies, in particular from Google Analytics, to monitor internet traffic was already sufficiently explained in 2013 in media reports following the Snowden revelations.

(3) This view has since been endorsed by the supervisory authority in Baden-Württemberg, the CNIL (France), the Autoriteit Persoonsgegevens (Netherlands) as well as Datatilsynet from Norway and Denmark.

Previously, the EDPS had already found that the use of Google Analytics on websites of the European Parliament violated the requirements for third-country transfers under Art. 44 et seq. GDPR.

The CNIL had explicitly clarified that UUIDs (Universally Unique Identifiers) such as cookie IDs do not constitute pseudonymous data, but have the purpose of identifying a user. Similarly, the DSK had already rejected the assumption of pseudonymisation (Art. 4 No. 5 GDPR) when using advertising IDs, cookie IDs or unique user IDs [DSK, Orientierungshilfe Telemedien, 2019, p. 15].

(4) The CNIL explicitly highlighted in its "FAQs on Google Analytics" of June 2022 that for the use of Google Analytics, the mere conclusion of the standard contractual clauses provided is not sufficient to meet the requirements of Article 46(2)(c) of the GDPR. Likewise, it was not possible to configure Google Analytics in such a way that no data would be transmitted to countries outside the EU.

Therefore, website operators would have to take additional measures themselves in the sense of the "Schrems II" case law in order to legitimise the use of Google Analytics. According to the CNIL, additional measures such as valid pseudonymisation prior to the transmission of user data to Google can be achieved by tracking proxy solutions such as the JENTIS Twin Server technology (cf. point III.).

(5) Following the EDPB recommendations, for effective pseudonymisation as an "additional measure" within the meaning of the ECJ decision "Schrems II" when using cloud services - such as the server side Google Tag Manager, appropriate procedures for pseudonymisation must be applied in advance of the transfer to the third party [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, para. 94 f.]. Transport encryption or "data-at-rest" encryption, as indicated by Google in the procedure, do not constitute "additional measures" that ensure a substantially equivalent level of protection. Therefore, the automatic truncation of IP addresses on servers in the EU before the data

is collected on servers of Google is also unlikely to be sufficient to meet the EDPB's requirements for "additional measures". Even if one completely rejects a risk-based approach in Chapter 5 of the GDPR, as the Austrian authority did in its partial decision of 22.04.2022, a legally compliant use of tracking services is possible if these measures specified by the EDPB are fulfilled.

(6) Conclusion: In the case of tracking services such as Google Analytics, whether as a client-side or server-side tracking solution, it is necessary to subject the data parameters for tracking - IP address, user agent, client ID, user ID and, if applicable, order IDs - to valid pseudonymisation in advance of transmission so that the requirements from the ECJ ruling "Schrems II" can be fully implemented.

The JENTIS solution enables the implementation of effective pseudonymisation by modifying/synthesising the processed data parameters in order to be able to document the requirements for "additional measures" in a reliable manner.

4. Legal uncertainty TADPF: Will there be a new adequacy decision for the US?

Finally, the agreement announced on 25 March 2022 between US President Biden and President of the European President Ursula von der Leyen on a new "Trans Atlantic Data Privacy Framework" ("TADPF") as a successor agreement to the EU-US Privacy Shield, which was declared invalid by the ECJ, is currently subject to considerable legal uncertainties.

(1) So far, no negotiated text of the agreement exists as a basis for a possible Executive Order in the USA and a possible adequacy decision of the EU Commission according to Art. 45 GDPR. In a response from the EU Commission to a question from the EU Parliament on 11.05.2022, it was stated that the details still had to be worked out and these still had to be implemented in legal texts.

(2) Only on this basis could the EU Commission propose a draft for a new adequacy decision for the USA and initiate the corresponding adoption procedure. The adoption procedure includes obtaining an opinion from the EDPB and a positive vote by the member states in the so-called comitology procedure. The European Parliament has a right of control over the adequacy decisions of the European Commission as an implementing act within the meaning of Art. 291 of the Treaty on the Functioning of the European Union. Only when these procedures have been concluded within the framework of implementing acts can the Commission adopt a new adequacy decision pursuant to Art. 45 GDPR.

(3) It should be noted that any adequacy decision by the EU Commission does not give carte blanche for data transfers to the USA. As with the predecessor agreement, the EU-US Privacy Shield, US companies will be required to self-certify with the US government, i.e. it will be necessary to check whether an active certification actually exists for the respective data recipient.

(4) Notwithstanding this, the following three risks, which have not yet been addressed by the negotiating partners, must be dealt with:

Firstly, there is the question of how to deal with sub-processors, in the case of Google Analytics more than 50 sub-processors, as recipients of data in third countries without an adequate level of protection, such as Taiwan, the Philippines, Brazil, Mexico, Malaysia and India. For these third countries, there is no adequacy decision by the EU Commission.

Secondly, it is still uncertain whether the Supreme Court's decision of 04.03.2022 in the "FBI ./. Fazaga" case will have an impact on the current negotiations between the EU and the USA. This is because the "Independent Data Protection Review Court" envisaged in the TADPF could be called into question by the Supreme Court decision due to the upholding of the "state secret privilege", according to which important information on the persons affected by the surveillance measures does not have to be disclosed [cf. Lejeune, Trans-Atlantic Data Privacy Framework despite U.S. Supreme Court decision in FBI v. Fazaga?, 31.03.2022].

Thirdly, the Hessian Data Protection Commissioner rightly points to the fact that according to Art. 44 p. 2 GDPR, all provisions of Chapter 5 of the GDPR must be applied in such a way that the level of protection of the GDPR is not undermined [Roßnagel, ZD 2022, 305 f.]. It follows that the TADPF and any adequacy decision for the US based on it must ensure a level of protection equivalent to the GDPR in factual terms. For this, the establishment of an "Independent Data Protection Review Court" and the assurance of access restrictions on the part of the US security authorities and intelligence services alone will not necessarily be sufficient. Against this background, the Hessian Data Protection Commissioner recommends the development and design of technology systems as well as data protection advice oriented towards the requirements of the "Schrems II" case law [Roßnagel, ZD 2022, 306].

5. Conclusion: Need for long-term risk management strategies

In the face of inadequate industry solutions for server-side tracking (cf. pt. I.1.) and a lack of practicability to meet the requirements for explicit consent for third-country transfers communicated by regulators, there is a growing need for long-term and sustainable strategies for legally compliant and successful data use by third parties with global infrastructures.

Middleware concepts such as the JENTIS SaaS solution provide a solution to the interconnections and risks in the area of website tracking. JENTIS allows flexible configuration of the SaaS solution to accommodate the volatility of each company's individual risk situation. In this way, the JENTIS SaaS solution enables companies to ensure "Schrems II" compliance in the supply chain when using third-party tracking technologies.

III. How JENTIS helps to eliminate legal risks

(1) The JENTIS SaaS solution enables hybrid tracking in a combination of client-side and server-side tracking. JENTIS offers the possibility to transfer data from one's own website to JENTIS servers and from there to various other data recipients and in this function acts like a technical pre-filter.

In this process, user data is initially collected directly as first-party data on the website. With the help of server-side tagging, the JENTIS SaaS solution enables a reducing and substituting filtering of data streams before they are forwarded to third parties such as Google or Facebook. This prevents the loss of control when using tracking applications from the outset.

Independently of this, the JENTIS SaaS solution includes a stand-alone CMP solution that enables tracking data to be passed on to AdTech providers on the basis of user consent in accordance with data protection requirements.

(2) The JENTIS SaaS solution consists of the following central system components:

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

All JENTIS systems are hosted in Austria on A1 Telekom Austria servers. A third-country risk as with common cloud services is avoided from the outset.

(3) In order to use the JENTIS SaaS solution, both a DNS entry on the user's own website and the implementation of a JavaScript basic tracking code in the source code of the website are necessary. Subsequently, the JENTIS SaaS solution can be used to collect first-party data from website users without being accessed by third parties.

When using the JENTIS solution, third-party tags implemented in the source code of the website, such as JavaScripts, iFrames and image pixels, are modified in such a way that neither direct terminal access by nor direct transmission of user data, such as the IP address and user IDs, to third-party servers takes place as part of a direct server request from the user's browser. Due to the JENTIS middleware, a direct connection between the user's browser and the third party is avoided from the outset.

The administrator receives unique logins from JENTIS in order to use the JENTIS interface. Through this interface, the administrator can work with both the JENTIS Tag Manager, which is hosted exclusively on servers, and the JENTIS Consent Manager.

(4) Specifically, depending on the administrator's configuration, the following categories of data are processed:

Data parameter	Description
IP address	This must be transmitted for technical reasons and is then processed anonymously at the JENTIS server.
JENTIS User-ID	This is a randomly generated combination of numbers and is primarily used to recognise the visitor.
Customer-specific IDs	These are order IDs, for example. This data is not processed further by JENTIS, but is generated anew as a random product.
Client IDs for external tools	Some external tools require a client ID themselves in order to recognise visitors. Such client IDs are regenerated on the JENTIS server and a fictitious client ID is sent to the external tool.
Browser environment data	This data is read from the visitor's browser and sent to the JENTIS server. This is static data that is determined by the visitor's device.
User action data	This data is read from the visitor's browser and sent to the JENTIS server. This is data that describes the visitor's actions on the website.

(5) For the legal assessment of the described risks and legal uncertainties (point II.), two essential processing steps with regard to user data arise on the basis of the functional principle set out in the technical documentation of JENTIS:

Firstly, terminal access, triggered by the user's browser request to JENTIS servers to recognise a user's browser via first-party cookies by assigning a randomly generated JENTIS user ID for the specified use cases. The duration of the JENTIS can be set to be session-related or persistent up to 24 months according to the risk affinity of the customer.

- At this point, the third-country issue has no effect. All JENTIS systems are hosted on servers of A1 Telekom Austria.
- For the question of under which conditions JENTIS can be used in "Privacy Mode" as "technically necessary" without the consent of the users is the subject of a separate assessment.

Secondly, the server-side transmission of cleansed tracking data (session ID, user ID, user agent, demographic location data) after filtering to servers of providers such as Google in third countries.

- Given the transfer of "cleansed tracking data", the requirements of Art. 44 et seq. GDPR can be fulfilled in accordance with the positions of the supervisory authorities as outlined below.

Based on the outlined functional principle of the configured JENTIS systems (1.), "Schrems II" compliance in the supply chain (3.) can be ensured by means of synthesising the data parameters of the user's browser session as an effective means of pseudonymisation (2.).

1. Operating principle of the configured JENTIS systems

(1) JENTIS acts as middleware as a kind of gatekeeper between the browser and the third-party server. This makes it possible to pseudonymised all collected data before transferring it to a third party in a GDPR-compliant manner (see point III. 2.).

(2) The administrator determines in the JENTIS Tag Manager which data should be read out in the visitor's browser and sent to JENTIS. At the level of the data parameters, the administrator can determine whether the individual data parameters are relevant dates for the third-country transfer.

In this way, the system can be parameterised according to the requirements of the applicable law in the region of use (GDPR [EU], PECR [UK], CCPA [CA], LGPD [BR], PIPL [CN], etc.).

(3) The administrator determines which external third-party provider should receive data from JENTIS by adding "trackers". In doing so, the administrator configures each of these trackers in such a way that it is clearly determined which data parameter is to be transferred to the external third party. For each data parameter to be transferred that has been classified as relevant, the administrator also determines whether a removal of the data parameters or a synthesis of the data parameters [cf. point III. 2.] should be carried out before transfer to the external provider.

The detailed removal or synthesis of the data parameters is possible because the user's browser session is mirrored 1:1 on a JENTIS Twin Server. In this way, individually risky data parameters can be minimised or exchanged according to the needs of the website operator, as deemed appropriate by the competent supervisory authority.

The raw data of the user's browser session can be completely deleted.

(4) In the JENTIS Server Suite, a modification of the tracking data takes place in the data backend to the effect that, for example, the IP address of the website visitor is completely removed before it is passed on to the third parties. As an option, it is conceivable that before the user's IP address is removed, an assignment to the country and city of the end device from which the request was sent is inserted using a geo-database stored on the web server. The IP address is necessary to determine the location. In the course of further processing, only demographic location data (country/city) is transmitted to third parties, but not the identifying components of the visitor's IP address.

Third-party data, such as client IDs or user IDs in the case of Google Analytics, which enable a unique assignment of the end device, are not processed within the JENTIS Server Suite and are sent to the respective third party as a synthetically generated fictitious client ID.

Similarly, data parameters that enable unique identification of users, e.g. order IDs, are not processed by JENTIS, but are regenerated as a random product.

(5) The cleansed tracking data, i.e. the synthesised and exchanged IDs of the third parties as well as the demographic location data (country/city) together with information on user behaviour (e.g. events), are transmitted from the JENTIS server to the third-party server, e.g. Google server. Neither the client ID assigned by Google nor the user's IP address is transmitted.

(6) With the help of the (private) user ID generated by JENTIS, the JENTIS server and not the user's client now makes a request to the third-party provider, e.g. Google, for delivery of the Analytics script.

(7) The processing of user data for website tracking using the JENTIS solution enables customers, depending on the use case, to configure JENTIS systems in such a way that it is possible to tread on legally solid ground without being exposed to the legal uncertainties described in point II. The effective pseudonymisation required by the EDPB before transfer to third parties [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, para. 94 f.] can be implemented in JENTIS systems by synthesising relevant data parameters.

2. Assessment of the transmissions of synthetically generated client IDs to third parties

(1) The server-side transmission of the cleansed tracking data (synthetically generated client ID and order ID as well as event data) to third parties such as Google is to be assessed as a processing operation relevant for the third-country transfer that follows the terminal access by JENTIS.

(2) Neither the client ID assigned by Google nor the IP address of the user is transmitted. When the web server communicates with JENTIS servers and then with Google servers, cleansed tracking data - the synthetically generated client ID, the IP address of the web server, the synthesised user agent and the synthesised order ID - are transmitted, depending on the configuration of the JENTS systems (see point I. 1.).

(3) The creation of synthetic data from raw data can be classified as an "additional measure" to secure the third-country transfer in the sense of the "Schrems II" case law.

- The ENISA (European Union Agency for Cybersecurity) describes "synthetic data" in the context of data protection law as a new area of data processing in which data is prepared in such a way that it realistically resembles real data (both personal and non-personal), but does not relate to a specific identified or identifiable individual or to the "real extent of a data parameter to be assessed" [see ENISA, Data Protection Engineering, 2022, p. 17].
- According to the EDPS, "synthetic data" can be considered as privacy enhancing technology and in this sense can be used as an "additional measure" for data transfers outside the European Union or within organisations that do not require identification of a specific individual.
- According to ENISA, synthesisation primarily serves the confidentiality of processing [cf. ENISA, Data Protection Engineering, 2022, p. 17], which has the character of "additional measures" in technical and organisational terms within the meaning of Art. 32 GDPR.
- A blanket legal classification of synthetic data is prohibited. As far as the risk of re-identification cannot be excluded because synthetic data are mixed with real data, synthetic data are not to be classified as anonymous data [EDPS, Synthetic data: what use cases as a privacy enhancing technology, 2021, p. 3]. ENISA also rules out the assumption of anonymisation in the case of mixing real data and synthetic data [cf. ENISA, Data Protection Engineering, 2022, p. 18].

- In regards to the use cases when using JENTIS, e.g. for website analysis, the recognition of the user via the JENTIS user ID is possible for website operators. As long as at least the "client ID of the third-party provider" and ideally other tracking parameters such as user agent and any order IDs are synthesised after appropriate configuration of the JENTIS systems, the transmitted data record has no personal reference from the recipient's point of view because the assignment rule via the JENTIS user ID to an end device lies exclusively with JENTIS and website operators. Only JENTIS as the processor and the website operator, but not third parties such as Google, have the assignment rule - e.g. via the JENTIS user ID - for the pseudonymous tracking parameters. It must then be assumed that there is effective pseudonymisation in accordance with Art. 4 No. 5 GDPR.
- The CNIL recently explicitly highlighted proxy solutions, such as those provided by JENTIS with the Twin-Server technology, as a lawful instrument for solving the "Schrems II" problem in its "FAQs on Google Analytics of 07.06.2022". Proxy solutions would have to fulfil the following prerequisite:
    - No transmission of the user's IP address. If the proxy server has matched the location against a geo-IP database, the information must be such that no re-identification is possible.
    - The algorithm performing the replacement should ensure a sufficient level of collision (i.e. a sufficient probability that two different identifiers will produce an identical result after hashing and that the result of hashing for the same identifier will not always be the same).
    - Referrers must be deleted.
    - Parameters contained in the collected URLs must be deleted (e.g. the Click IDs and URL parameters that enable the internal routing of the website);
    - Information that may contribute to fingerprinting, such as "user agents", must be reprocessed to remove the rarest configurations that may lead to re-identification.
    - No collection of identifiers between multiple digital offers (cross-site) or from own customer systems (e.g. CRM ID);
    - Deletion of all other raw data that may lead to re-identification.
- With the help of JENTIS, all requirements for proxy servers of the CNIL can be fulfilled. This is because the synthesis of user data corresponds to the formation of hash values as proposed by the CNIL, as described below.

(4) The formation of synthetic data from real raw data corresponds to the formation of hash values as far as the classification of the synthesisation as a measure of pseudonymisation is concerned.

- Pseudonymisation is a suitable privacy pattern within the framework of "privacy by design" [see BGH, judgement of 15.5.2018 - VI ZR 233/17, para. 26] and can already be applied at the raw data level in the case of "JENTIS". According to the BGH, a randomly generated number (cookie ID) stored in cookies, which is assigned to the user's registration data as terminal device information, already constitutes a pseudonym within the meaning of section 15 (1) of the German Federal Data Protection Act (BDSG). Section 15 (3) of the German Telemedia Act (TMG), whereby the BGH still referred to the legal definition in Section 3 (6a) of the old version of the German Federal Data Protection Act

(BDSG) [BGH, Urt. v. 28.05.2020 - I ZR 7/16 - Cookie Einwilligung II; agreeing with regard to GDPR Menke, K&R 2020, 650, 652; Baumgartner/Hansch, ZD 2020, 435, 436]. The same must apply in consequence to other identifiers such as Device IDs, IDFA, GAID and Universal IDs.

- Furthermore, the application of hashing techniques to users' clear data is supported by European authorities [ENISA, Data Pseudonymisation: Advanced Techniques & Use Cases, 2021, p. 12; Article 29-Data Protection Working Party, WP 216, Opinion 05/2014 in Anonymisation Techniques, p. 20; EDPS/AEPD, Introduction to the Hash Function as a personal data Pseudonymisation technique, 2019, p. 21] and the commentary regarded as pseudonymisation within the meaning of Art. 4 No. 5 GDPR [Stentzel/Jergl, in: Gierschmann/Schlender/Stentzel/Veil, GDPR, Art. 4 No. 5 Rn. 6; Arning/Rothkegel, in: Taeger/Gabel, GDPR/BDSG, 3rd ed, Art. 4 marginal no. 144]. By means of a sufficient hash function, input data is transformed into a key text (hash value) on the basis of an algorithm, which is in any case not reversible with a proportionate effort and is always the same for the same input data [see ENISA, Data Pseudonymisation: Advanced Techniques & Use Cases, 2021, p. 12; Article 29-Data Protection Working Party, WP 216, Opinion 05/2014 in Anonymisation Techniques, p. 20].
- The use of hash functions in the context of the creation of target groups also constitutes pseudonymisation within the meaning of Article 4 No. 5 of the GDPR according to the assessment of the "Focus Group on Data Protection" of the Federal Ministry of the Interior [Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, p. 26].
- The creation of hash values from raw data such as email addresses, telephone numbers [see ENISA, Pseudonymisation techniques and best practices, 2019, p. 33] and citizen numbers [see Article 29-Data Protection Working Party, WP 216, Opinion 05/2014 in Anonymisation Techniques, p. 20] for the creation of target groups therefore constitutes valid pseudonymisation because the hash values created, e.g. when using the hashing technique, can be used for the creation of target groups. e.g. when using the hashing algorithm SHA 256 as a robust hash function, are irreversible, i.e. not traceable, and guarantee freedom from collision, i.e. it is not possible to generate the same hash value as an output value from two input values [ENISA, Data Pseudonymisation: Advanced Techniques & Use Cases, 2021, p. 12].
- The synthesis of real raw data such as the client ID or user ID assigned by third parties is considered pseudonymisation within the meaning of Art. 4 No. 5 GDPR under the same conditions as the creation of hash values from real raw data. As long as the artificial values used in place of client IDs and user IDs are irreversible, the collision-free nature of the processed data parameters is ensured and the user's IP address has been replaced, it can be assumed that pseudonymisation complies with the GDPR, taking into account the unanimous opinion on hash values in the absence of conflicting opinions or case law.

(5) In the case of the removal of the IP address and synthesis of tracking parameters before transfer of the data to third parties such as Google, effective pseudonymisation is to be assumed as an "additional measure" for "Schrems II" compliance according to the EDPB's reading [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, para. 94 f.]:

- The restriction required by Art. 4 No. 5 GDPR that the additional information is stored separately and secured by technical-organisational measures that ensure that no allocation of the data to an identifiable person takes place is guaranteed during the communication of the different server instances of JENTIS. Regardless of whether the additional information such as the JENTIS user ID can be a direct assignment or an assignment rule for the synthetically generated client IDs and order IDs of the third parties[Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, p. 11 f.], according to the technical operating principle described, given the system architecture of JENTIS, there is a robust separation of the data instances that excludes an assignment for third parties.
- If re-identification is excluded because the processing entity would not have the necessary mapping rule, anonymisation of the transferred parameters to third parties would have to be considered in line with recital 26 of the GDPR and a corresponding processing excluded from the scope of the GDPR. However, if the parties involved in the tracking, such as JENTIS, have the user ID as a "key" for the assignment to synthetically generated client and order IDs from third parties, a reference to a person must also be assumed due to the pseudonymisation in view of the assessment of the "Focus Group on Data Protection" of the Federal Ministry of the Interior [Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, p. 22].
- According to a current and technically relevant case law of the Commercial Court of the Canton of Zurich on the protection of the right of personality under Art. 28 of the Swiss Civil Code (ZGB), pseudonymisation is to be regarded as anonymisation under the law of personality for the recipient who cannot assign the pseudonymised data records to a specific person [cf. HGer ZH, Urt. v. 04.05.2021 - HG190107-O]. Although this case law was not handed down in the territory of the EU, it at least has an indicative effect.
- As far as can be seen, third parties such as Google only receive a client ID synthetically generated by JENTIS in the course of the outlined data transfers after the end device access, which does not correspond to the client ID or user ID assigned by Google for Google Analytics and therefore does not enable Google to assign the information provided about the usage behaviour of website visitors.
- Likewise, no access to the JENTIS systems by third parties such as Google is possible on the basis of the technical documentation provided. There is no direct communication of the user's browser with third parties. As far as can be seen, there is no case law other than that of the ECJ on the personal reference of IP addresses on the question of whether a personal reference is still to be assumed if only a third party has the assignment rule for the transmitted pseudonymous data records, but there is no legal possibility for access to identifiers. [cf. also Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3rd ed. 2020, Art. 4 marginal no. 12]

3. Assessment of the third-country transfer

(1) Given the abstract access possibilities to third-party servers by US security authorities after reduction and synthesis of tracking parameters and in line with the case law of the French administrative court Conseil d'État [Beschl. v. 13.10.2020 - 444937] on the admissibility of the use of Microsoft Azure cloud services on servers in the Netherlands, the following measures within the JENTIS SaaS solution can reasonably be considered as "additional security measures" within the meaning of the ECJ case law [ECJ, 16.7.2020 - C-311/18 - Schrems II]:

- Location of A1 Telekom Austria's JENTIS servers in Austria. No processing of raw data from browser server requests from users outside the EU/EEA;
- Access restrictions to JENTIS systems by means of identity and access management;
- Maintaining compartmentalised data storage without access by third parties such as Google from the USA due to the lack of third parties' access options to JENTIS servers, users' end devices or the pseudonymous JENTIS user ID;
- Preventing explicit data exchange between raw data from the website visitor's end device and third parties;
- Segregation of server instances of different clients and access restrictions;
- Reduction: removal of the IP address before transmission of tracking parameters to third parties
- Restriction: risk avoidance through functional restriction of tracking services, e.g. inaccurate location determination due to removal of the IP address and use of IP geolocation databases as well as exclusion of cross-device tracking due to non-use of the original client ID e.g. in the Google Analytics account;
- Valid pseudonymisation due to the synthesis of client ID, user agent, order ID and other data parameters and the lack of access to mapping rules by third parties such as Google;
- Valid pseudonymisation and encryption and lack of access to mapping rules by third parties such as Google in JENTIS systems.

(2) Against this background, the described additional measures in accordance with the technical operating principle (point III. 1.) in combination with a conclusion of standard contractual clauses may currently constitute a justification for the third-country transfer pursuant to Art. 46 (2) lit. c) GDPR, subject to contrary case law, decisions by supervisory authorities or solutions at the political level.

(3) In particular, the use of JENTIS complies with the EDPB's requirement [Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Version 2.0, para. 94 f.] to apply pseudonymisation measures as "additional measures" within the meaning of the ECJ's "Schrems II" case law before transferring data to a cloud. This is because JENTIS enables identifiers that are used for corresponding use cases to be transferred to the server instances of third parties not in plain text, but exclusively as a pseudonymous identifier.

(4) The additional measures enabled by JENTIS constitute "technical or organisational safeguards" according to Clause 14 of the Standard Contractual Clauses and enable the fulfilment of the obligation to conduct and document a "Transfer Impact Assessment". The measures described represent a mitigation of the risks of access by security authorities in the sense of "additional measures" if the JENTIS systems are configured accordingly by the administrator.

4. Summary

It remains to be said: With the help of the JENTIS solution, the locally and regionally differing views of courts and supervisory authorities on international data transfers - such as the rejection of a risk-based approach by the Austrian supervisory authority - as well as the individual compliance requirements can be fully taken into account in each individual case.

JENTIS enables a long-term and sustainable strategy with its hybrid server-side tracking technology, on the one hand to master industrial challenges in the course of the 3rd-party cookie phase-out and on the other hand to put international data transfers to third countries without an adequate level of protection on a secure footing.

Due to the individual configuration options of the JENTIS Server Suite, companies are also prepared for different decisions by supervisory authorities in the future and can react to new requirements for transfers to third countries at short notice.

IV. Summary of the results

In conclusion, when using the JENTIS SaaS solution for the implementation of third-party tracking tools such as Google Analytics, the described legal uncertainties regarding third-country transfers (cf. point II.) can be eliminated with the appropriate configuration.

In the case of the described configuration, the JENTIS SaaS solution enables the proof of "additional measures" which, in addition to the conclusion of standard contractual clauses, can constitute a justification for the third-country transfer and in this way ensure "Schrems II" compliance in the supply chain.

Website operators can take advantage of the economic benefits of their own first-party data when using JENTIS, without endangering this data or the respective corporate compliance in legal terms through uncontrolled and non-transparent processing on the part of third parties..