Data Protection Memorandum

JENTIS GmbH

SPIRIT LEGAL®

Translation from German to English

Author

RA Peter Hense & RA Tilman Herbrich (CIPP/E)

Date of the document

17 October 2021 V1.1

Project

Data Protection Assessment of JENTIS SaaS Solution

Executive Summary

Prior existing industry solutions such as server-side tracking to enable qualitative website tracking despite the increasing prevalence of ad-blockers and tracking prevention systems do not change anything in terms of compliance with the data protection legal requirements **(I.1.)**.

Following the "Cookie consent II" decision by the German Federal Court of Justice, German courts of first instance and the Data Protection Conference (DSK) consider the unrestricted use of tracking services such as Google Analytics to be permissible only if consent is given **(I.2.a-b.)**. The TTDSG that will come into force on December 1, 2021, will not result in any changes of the existing legal situation **(I.2.d.)**.

The use of third-party tracking services without further modification is accompanied by two major legal uncertainties due to comprehensive investigations of website tracking by supervisory authorities and NGOs **(I.2.c.)**: on the one hand, the request for valid consent **(II.1.)** and, on the other hand, the justification of the third-country transfers to the USA due to the transmission of personal data in server requests of the user's browser to third-party providers such as Google **(II.2.)**.

Exceptions to the strict consent requirement - "strict necessity" pursuant to the Article 5(3)(2)(e) of the ePrivacy Directive **(II.1.a.)** or the reliance on downstream processing in server-side tracking - are not applicable to third-party services, even when recognized methods of interpretation, taking into account case law, are fully exhausted **(II.1.b.)**.

Based on the description of the technical functionality provided by JENTIS **(III.1.)**, if the JENTIS system is configured accordingly, it is possible to apply the exceptions to the consent requirement (under the Privacy Directive Article 5(3)(2)) for access to information stored in the terminal equipment **(III.2.)**. The client ID (without IP address) synthetically generated by JENTIS, given that requirements are met in the specific individual case, can be transferred server-side to third-party providers without consent at the downstream processing phase and be based on legitimate interests pursuant to the GDPR Article 6 (1) (1)(f) **(III.3.)**.

In addition, the JENTIS solution offers the possibility of implementing sufficient security measures, which can be currently considered as "supplementary measures" within the meaning of the judgment of the ECJ of July 16, 2020 in the "Schrems II" case **(III.4.)**. Subject to any future case law to the contrary, configuration of the JENTIS systems enabling valid pseudonymization of user data can be qualified as technical mitigation of the risks of access by security authorities as part of the performance and documentation of a "Transfer Impact Assessment" under the Section 14 of the EU Commission's Standard Contractual Clauses.

Table of Contents

Legal appraisal

I. Analysis of the *Status Quo* — Legal Classification of Processing in the Field of Website Tracking

1. Developments in the Industry

It may be noticed that since 2017, beyond the Ad-blockers, common browser providers such as Safari and Firefox rely on 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 analysis and advertising purposes from the outset.
Most recently, announcements by Google in spring 2021 to eliminate third-party cookies and offer only Federated Learning of Cohorts (FLoC) caused a turmoil in the industry. These technical developments in the browser landscape have negative consequences:

- 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.

Previous industry solutions such as offering "first party cookies" from third-party providers ("3rd party as 1st party") do not change the data protection law requirements for the permissibility of tracking if, for example, due to the processing of Domain Name System (DNS) records, tracking resources from third-party providers are delivered from the same domain from which the website is operated [Veale/Borgesius, AdTech and Real-Time Bidding under European Data Protection Law, 2021, p. 6]. In other words, first-party cookies can be used in the same way as third-party cookies, and can enable, for example, "cross-site tracking" [IPOL Study: JURI commitee, EU Parliament, Regulating targeted and behavioral advertising in digital services, 2021, p. 44, fn. 49].

Similarly, advertising technology solutions such as server-side tracking via the server-side Google Tag Manager (SSGTM) or the Facebook Conversions API are still subject to the data protection compliance requirements, even if the information from end devices is not sent to the third-party providers via the user's browser but 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 its own systems (SSGTM) [see, for example, Papadogiannakis et al, User Tracking in the Post-cookie Era, 2021, p. 1 f.].

Without modification of the data processing that takes place when the website is called up due to the loaded tags from third-party providers, such as by the JENTIS Tag Manager and the JENTIS Server Suite (cf. pt. III.), the data protection requirements apply without restriction.

2. Current Legal Situation

The implementation of JavaScripts or HTML elements such as iFrames or Image-Pixels from third-party providers in the source code of a website requires not only the access to the information on the end device as well as the transfer of personal data of the website visitor on the basis of the initiated https-request by JavaScript sent to the user's browser (client).

a) Consent to access the end device for tracking purposes of analysis and marketing

(1) Following the preliminary ruling by the ECJ in the "Planet49" case, on 28.05.2020 the German Federal Court of Justice (BGH), finally decided [I ZR 7/16 - Cookie Consent II] that, the consent from the user is required for the **use of cookies** (and similar technologies), that are set on a user's terminal device after the registration for a competition and that enable **an analysis of user behavior** on websites of advertising partners and thus enable **interest-based advertising**. In general, such **consent is necessary** according to the interpretation of the Section 15 (3) of the German Telemedia Act (TMG) in conformity with Article 5 (3) (1) of the Directive 2002/58/EC as amended by Directive 2009/136/EC (ePrivacy Directive). According to the wording of the provisions of the Directive, the consent requirement applies to the access to and storage of information from users' terminal equipment and, in the view of the BGH, the conflict of laws rule pursuant to Art. 95 GDPR blocks the application of other GDPR rules for this process than those relating to consent (see GDPR Article 4(11), Article 6(1)(1)(a), Article 7).

(2) Initial court decisions have, among other things, prohibited the use of Google Analytics on a website without requesting freely given and informed consent [cf. LG Rostock, Urt. v. 15.09.2020 - 3 O 762/19; LG Köln, decision of 29.10.2020 - 31 O 194/20 and decision of 13.04.2021 - 31 O 36/21].

(3) It is irrelevant for the applicability of this case law whether the **end device access** takes place by means of cookies or **other technologies**. This includes access to Local Storage, Local Shared Objects as well as the use of browser fingerprinting technologies such as "canvas fingerprinting" [LG Rostock, Urt. v.. 15.09.2020 - 3 O 762/19; ICO, Guidance on the use of cookies and similar technologies, 2020].

b) Transmission of personal data through server requests of the browser.

Due to the Java scripts and HTML elements such as iFrames or Image-Pixels for tracking tools implemented in the source code of the website, a **server request** is triggered from the browser of the user (https-request) to the server of the third-party provider (e.g. google-analytics.com), whereby both the full IP address of the user and the client ID as well as, if applicable, the user ID are transmitted as **personal data** [cf. on the personal reference of dynamic IP addresses ECJ, judgment of 19.10.2016 - C-582/14, para. 47 - Breyer] to Google LLC in the USA. The **data transfer** constitutes a specific processing operation according to the legal definition provided in GDPR Article 4(2).

It has been clarified by the highest court that a data transfer (IP address and browser information) to a third party provider takes place if tracking technologies are implemented in the source code of a website operator that result in the placement of a cookie in the end device of the users and thereby cause the transmission of IP addresses and browser information [ECJ, judgment of 29.07.2019 - C-40/17, para. 26 - Fashion ID].

*"[...] For this to occur, the browser transmits to the server of the third-party provider **the IP address** of that visitor's computer, as well as the browser's technical data, so that the server can establish the format in which the content is to be delivered to that address. In addition, the browser **transmits** information relating to the desired content. [...]"*

c) Current audits by supervisory authorities and NGOs on legal enforcement

(1) According to the German Data Protection Conference (Datenschutzkonferenz, DSK), for the **access via the end device** to user IDs and IP addresses by means of cookies and similar tracking methods and **the transfer of personal data**, e.g., when using Google Analytics, also to Google LLC in the USA the **request for consent** from the website visitor is absolutely necessary [DSK, decision of 12.05.2020 - Notes on the use of Google Analytics]. Specifically in Germany, audits of website tracking on the part of supervisory authorities and NGOs have increased enormously in recent times:

(2) On 27.09.2021, the European Data Protection Board (EDPB) decided to establish a "Cookie Banner Task Force" under GDPR Article 70(1)(u) to promote consistent law enforcement across Europe. The reason for this is not the least the call to action campaign by the NGO "Noyb" that was launched in July 2021 for the submission of user complaints against inadmissible cookie banner designs in relation to website tracking. In August 2021, 422 formal complaints were officially submitted to the supervisory authorities.

(3) Similarly, in August 2021, the Berlin Commissioner for Data Protection and Freedom of Information confronted 50 website operators with unlawful tracking and initiated investigations.

(4) Finally, the Federation of German Consumer Organizations (Verbraucherzentrale Bundesverband e.V. (vzbv) issued warnings to 100 companies for unlawful tracking in September 2021 and announced that it would take legal action in civil proceedings if the website operators failed to take action.

d) No change in the legal situation as of December 1, 2021 under Section 25 TTDSG

The legal situation in Germany will remain unchanged when the **TTDSG** comes into force on December 1, 2021. Both Section 15 (3) (1) of the German Telemedia Act (TMG), as interpreted by the German Federal Court of Justice in its "Cookie Consent II" pursuant to the Article 5 (3) of the ePrivacy Directive, and Section 25(1) of the German Telecommunications and Telemedia Data Protection Act (TTDSG) require the consent of the person concerned for the storage of and access to information on terminal device. The interpretation of Section 15 (3) of the German Telemedia Act (TMG) and Section 25 of the German Teleservices Data Protection Act (TTDSG) made by the German Federal Court of Justice in its Cookie Consent II ruling is two forms of Member State implementation of the same - in this respect unambiguous - requirements of Article 5 (3) of the ePrivacy Directive.

Due to the almost identical wording of the TTDSG Section 25 and Article 5 (3) of the ePrivacy Directive, there is therefore no de facto change in the legal situation [Kühling/Sauerborn, CR 2021, 271, 279; Schuma cher/Sydow/von Schönfeld, MMR 2021, 603, 604; Schwartmann/Benedikt/Reif, MMR 2021, 99, 100]. On the contrary, the legal situation shaped by the case law of the Federal Court of Justice is now confirmed by Section 25 TTDSG.

Nevertheless, in view of the explicit legal regulation in Section 25 TTDSG on the strict consent requirement for website tracking, the implementation pressure in practice is growing. In view of currently initiated investigations by supervisory authorities and the establishment of the EDPB "Cookie Banner Task Force", further legal enforcement and possible sanctions are to be expected.

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

Finally, in the case of data transfers to providers located in a third country outside the EU, for which the EU Commission has not issued an adequacy decision pursuant to GDPR Article 45(1), **a justification for the third country transfer** is necessary.

(1) 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 country of destination - further measures or guarantees may be required for a legally admissible third country transfer based on the Standard Contractual Clauses [ECJ, 16.7.2020 - C-311/18 - Schrems II].

This means that not only does the EU-US Privacy Shield cease to be a legal basis for data transfers to the USA. Any data transfer and data access by U.S. companies based on **Standard Contractual Clauses (SCC)** pursuant to GDPR Article 46(2)(c) also requires **additional technical and organizational measures** to protect against access by U.S. authorities.

(2) According to official information from the EDPB, German supervisory authorities are currently conducting intensive investigations of data transfers. Data transfers to companies such as Google, Facebook, Microsoft and Amazon are affected. In case of missing implementation of the legal requirements under the GDPR Articles 44 and the following, measures such as prohibition orders, usage bans and fines are threatened or implemented.

II. Legal uncertainties due to technological advancements

At times, considerable legal uncertainties have arisen in practice with regard to the data protection requirements for website tracking. The legal uncertainties relate primarily to **(1)** the question of when cookies and similar tracking technologies fall under the legal criterion of "strictly necessary" (Article 5(3)(2) of the ePrivacy Directive) and can thus be exempted from the requirement of informed consent and **(2)** what is meant by "additional measures" to safeguard third-country transfers in accordance with the new Standard Contractual Clauses.

1. Legal uncertainty: criteria for exceptions to the consent requirement

a) Exception to the consent requirement for terminal access (Article (5)(3)(2) ePrivacy Directive)

There are two exceptions to the obligation to request user consent for access to and storage of information from users' terminal equipment in website tracking:

aa) Necessity for the performance and facilitation of electronic communications

For the technically necessary transmission of the user's IP address and other end device information, such as browser information for HTTP-based applications, the relevant exception is provided in Article 5(3)(2) of the ePrivacy Directive.

According to this provision, **consent is not required** if **technical storage** of or access to information on terminal equipment is carried out for the purpose of **performing or facilitating electronic communications**. However, it is a prerequisite that the performance or facilitation of electronic communication is the sole purpose of the processing [Art. 29 Data Protection Working Party, now EDPB, WP 194, p. 3]. In the opinion of the European Data Protection Board and individual supervisory authorities , the following are covered by the exception in Article 5(3)(2) of the ePrivacy

Directive [Art. 29 Data Protection Working Party, WP 194, Opinion 04/2012 on the exemption of cookies from the consent requirement, p. 3 f., ICO, Guidance on the use of cookies and similar technologies, p 13]:

- the ability to route information across the network, in particular by identifying the communication endpoints;
- the ability to exchange data elements in their intended order, in particular by numbering the data sets; and
- the ability to detect transmission errors or data loss.

The **exception** for the performance or facilitation of communications therefore **also includes cookies** that meet one (or more) of these characteristics, but only for the sole purpose of transmission; this means that the transmission of the communication must be impossible without the use of the cookie for the exception to apply [ICO, Guidance on the use of cookies and similar technologies, p 13].

(bb) Strict necessity for the provision of a requested service.

(1) The **second exception** in Article 5(3)(2) of the ePrivacy Directive - **access** to terminal device information is "**strictly necessary**" to **provide** a service requested by the user from the information society - is not relevant for the purposes of advertising and market research, at least not according to the German Federal Court of Justice [I ZR 7/16 - Cookie Consent II]. In the opinion of the Art. 29 Data Protection Working Party [WP 194, Opinion 04/2012 on the exemption of cookies from the consent requirement, p. 4], **three essential requirements** must be met:

1) The service is explicitly requested by the user: The user has performed an affirmative action to request a service with a clearly defined scope.

2) The information society service usually means the sum of several functionalities, i.e. the entire website as such. However, the Art. 29 Working Party also indicates that the exception rule also applies to individual functionalities provided by the "website" service. This may include interaction with a map service as well as streaming content.

3) Access to terminal information must be "strictly necessary" to provide the service - website, app, or individual functionalities.

(2) The **resilience** of this **exception rule** depends primarily on the degree of restrictiveness of the **interpretation of the concept of necessity**. However, a limiting factor is that ECJ case law considers whether restrictions to the rights to protection of personal data and respect for private life are strictly necessary for the processing of personal data:

"exceptions and limitations to the protection of personal data must be limited to what is strictly necessary" [ECJ, judgment of 04.05.2017 - C-13/16, para. 30 - Rigas].

Furthermore, in the **"M5A-Scara"** case on video surveillance, the **ECJ** stated on the basis of the balancing of interests clause (Article 7(f) of Directive 95/46/EC) **that processing is only then "necessary" if it** cannot **reasonably** be achieved as **effectively** by other means which are **less intrusive** on the fundamental rights and freedoms of persons concerned, in particular the rights to respect for private life and protection of personal data guaranteed by Articles 7 and 8 of the Charter. In addition, the requirement of necessity of data processing must be examined in conjunction with the so-called principle of "**data minimization**", which is enshrined in Art. 6(1)(1)(c) of Directive 95/46 (now GDPR Article 5(1)(c)) and requires that the personal data shall be:

"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."

(3) In the context of a **necessity test** related to **third-party tracking** for outreach measurements, it is sufficiently certain that without modification of the tracking parameters, no strict necessity pursuant to Article 5(3)(2) of the ePrivacy Directive can be established, since third-party tracking always expands the group of data recipients beyond the actual service provider or contractual partner. As long as first-party tracking carried out by the website operator itself is possible without the use of third-party providers, it will not be possible to arrive at the necessity for the use of third-party providers, taking into account the aforementioned ECJ case law and the opinion of the Data Protection Conference (DSK) on website tracking [DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter von Telemedien, p. 13 as well as p. III Annex I].

b) No consent for downstream processing stages

(1) If there is **no direct and immediate access** to a user's **end device resources**, for example in the case of a programmatic processing chain or server-side ex post examination of log files created for technical reasons, it can be argued, in line with the view of the EDPB and the expert literature, that the **processing** of forwarded usage data (especially the IP address of the user) for the purpose of measuring outreach or in the context of placing an advertisement tailored to the individual interests of a user is **no longer covered by Article 5(3)(1) of the ePrivacy Directive** (no access to the end device and no storage of information from the end device). Rather, it represents a **downstream processing phase**.

These downstream phases are to be measured solely against the **standard of the GDPR** and allow for more flexible handling. This refers to processing operations that take place after the processing phases "access" and "storage" defined by the wording in Article 5 (3)(1) of the ePrivacy Directive such as the transmission or use of tracking data.

(2) In the decision on the **One-Stop-Shop mechanism** [ECJ, judgment of 15.06.2021 - C 645/19, para. 74], the ECJ endorsed the EDPB's view that the scope of the "special rule" in Article 5 (3) of the ePrivacy Directive only covers the storage and reading of personal data by means of cookies. However, the provision in Article 5(3) of the ePrivacy Directive does not apply to all prior operations and subsequent processing of personal data by means of corresponding technologies.

In its "Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR", the EDPB **clarified** for the case of targeting that the **GDPR** alone should be referenced to assess the **lawfulness** of, for example, the "[...] the storage and analysis of data regarding web browsing activity for purposes of online behavioural advertising or security purposes [...]."

In this sense, the Conseil d'État [decision of 04.03.2021 - N 449212] has already taken the position on a CNIL fine against Google for a lack of consent on user tracking that the One-Stop-Shop mechanism included in the GDPR for the control and sanctioning of the operations to access or write cookies in the terminal equipment of users is not applicable, as they fall within the scope of the ePrivacy Directive.

(3) Finally, the German government's draft legislation explicitly refers to the **application of the GDPR to downstream processing phases** [BT-Drs. 19/27441, p. 38].

(4) Even if one would come to a conclusion that **server-side tracking** is to be classified as a downstream processing phase without access to the end user device and thus opens up the scope of application to the GDPR Article 6 (1) , it will not be possible to **eliminate consent without considerable risks**. None of the European supervisory authorities consider the GDPR Article 6 (1)(1) (b) or (f) as the valid legal basis for third-party tracking like Google SSGTM.

The legal basis under the **GDPR Article 6 (1) (1)(b) does not apply** because the processing would have to be necessary to fulfill a contract. A visit to a website with ecommerce offers or editorial content does not even necessarily establish a contractual relationship, let alone does not justify the creation of user profiles or analysis of user behavior for the delivery of content, the shipment of goods or the provision of services without granular and transparent agreement (e.g. user account) strictly necessary.

The EDPB's Guidelines 2/2019 clarified that the legal basis of Article 6 (1)(1)(b) of the GDPR cannot be used for contract performance for the purposes of "service improvement", "online behavioral targeting" and "personalization of content". Analysis procedures or processing for the purpose of personalized advertising do not fall under this legal basis.

Against the background of the strict ECJ case law on **the three-stage balancing of interests** for the almost identical predecessor provision of the GDPR Article 6 (1)(1)(f) - Art. 7 (f) of the Directive 95/46/EC - [see ECJ, judgment of 29.07.2019 - C-40/17, para. 95 with further references - Fashion ID], one will also have to reject overriding legitimate interests in the case of third-party tracking.

“Article 7(f) of that directive thus lays down three cumulative conditions for the processing of personal data to be lawful, namely, first, the pursuit of a legitimate interest by the data controller or by the third party or parties to whom the data are disclosed; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, the condition that the fundamental rights and freedoms of the data subject”

Taking into account the ECJ case law on the second step of necessity (see point II. 1. a. bb.) and the opinion of the Data Protection Conference on website tracking, it will not be possible to arrive at necessity for the use of third-party providers without further modification of the tracking [DSK, Orientierungshilfe für Anbieter von Telemedien, p. 13 as well as p. III Annex I].

(5) Conclusion: For this reason, a further reduction of the tracking parameters is required, e.g., via the JENTIS solution (see point III.), in order to be able to apply Article 6 (1)(1)(f) of the GDPR in a robust manner.

2. Legal uncertainty regarding third country transfers: What are "additional measures"?

(1) In the wake of the ECJ case law [ECJ, 16.7.2020 - C-311/18 - Schrems II], the only **practical justification** for data transfers to unsecure third countries, e.g. the USA, is the **Standard Contractual Clauses ("SCC")**. The safeguarding of third country transfers via **SCCs**, which has been in place since 2004, requires additional measures **("Supplementary Measures")**.

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

(3) Some of the expert literature doubts whether measures that can close the protection gaps raised even exist in practice, so that until the successor agreement to the EU-US Privacy Shield is reached, it may be necessary to switch to European servers [Schröder, in: Kühling/Buchner, DS-GVO BDSG, 3rd ed. 2020, Art. 46 DS-GVO marginal no. 18]. In the case of relocating the servers to Europe as the sole measure there is however the problem that it is also difficult to enforce an obligation not to hand over the data to U.S. authorities, since U.S. companies can also be obliged to hand over data on European servers under the CLOUD Act [Heckmann, Datenschutzkonforme Nutzung von Cloud-Lösungen aus unsicheren Drittländern, Wissenschaftliches Gutachten, 2021, p. 16; Paal/Kumkar, MMR 2020, 733].

(4) The EU Commission's new Standard Contractual Clauses for third-country transfers dated 4.06.2021, must be concluded on a mandatory basis for new contracts as of 27.09.2021. For old contracts, the previous SCCs have a transition period until 27.12.2022.

According to Clause 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 based on "Supplementary Measures" must be carried out.

(5) Which "supplementary measures" are to be taken is to be evaluated on the basis of the "Recommendations 01/2020 on measures [...]" version 2.0 published by the **EDPB** on 18.06.2021 as a follow-up to the new SCC. Without documentation of additional measures for risk mitigation, the application of the SCC will not be accepted by supervisory authorities.

Additional measures may include, for example, anonymization or 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 encryption keys or the data to be processed [Paal/Kumkar, MMR 2020, 733]. Data trustees, such as those already introduced by Microsoft in the past, can also be considered [Johnson/Brechtel, ITRB 2020, 285 et seq.]

III. How JENTIS helps eliminate legal risks

(1) The **JENTIS SaaS solution** enables **hybrid tracking** in a combination of client-side and server-side tracking. JENTIS offers the option of transferring data from its own website to JENTIS servers and from there to various other data recipients, and in this function itself acts like a technical pre-filter.

In this process, user data is initially collected directly as first-party data on the website. The JENTIS SaaS solution uses **server-side tagging** to reduce and substitute filtering of data streams before they are forwarded to third-party providers such as Google or Facebook. Independently of this, the JENTIS SaaS solution includes a **standalone 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, MediaCom System Architecture, Appendix 1]:
- JENTIS Tag Management
- JENTIS Consent Manager
- JENTIS Server Suite.

(3) To use the JENTIS SaaS solution, both a DNS setup on the user's own website and the implementation of a JavaScript base tracking code from JENTIS in the source code of the website [JENTIS Funktionsbeschreibung, v0.92, p. 7] are required. Subsequently, the JENTIS SaaS solution can be used to collect first-party data from website users without third-party access.

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 end device access nor direct transmission of user data, such as the IP address and user IDs, takes place as part of an unmediated server request from the user's browser to third-party servers. A direct connection between the user's browser and the third-party provider is avoided from the outset in this way.

(4) The administrator receives unique access data from JENTIS in order to use the JENTIS interface. In this interface, the administrator can make settings for both the JENTIS Tag Manager and the JENTIS Consent Manager.

(5) In detail, the following data categories are processed, depending on the administrator's configuration.

Data Parameters	**Description**
IP-Adress	For technical reasons, it must be transmitted and is then processed anonymously at the JENTIS server.
User-ID from JENTIS	It is a randomly generated combination of numbers and is mainly used to recognize the visitor.
Customer specific IDs	These are, for example, order IDs. This data is not processed further by JENTIS, but is generated again as a random product.

Client-IDs for external Tools	Some external tools require a client ID themselves in order to recognize 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 in 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 by the visitor's browser and sent to the JENTIS server. This is the data that describes the visitor's activities on the website.

1. Functional description of the configured JENTIS systems

Depending on the use case, the processing of user data through website tracking with the integration of the JENTIS solution makes it possible to configure the JENTIS systems as shown below in such a way that such processing takes place on legally solid ground without being exposed to the legal uncertainties described in Point II above. Regardless of the configuration and reduction of tracking parameters, the JENTIS Consent Manager allows you to request consent for the customer's martech stack.

- **Step 1: Loading the website and request to JENTIS server**

The local browser of the website visitor communicates with the JENTIS server as long as the website of the respective company is loaded in the following situations:

- Loading the library
- Sending Consent ID and Consent information
- Sending tracking data in case of positive minimal consent.

During this process, the browser asks the company's DNS for the IP address of the tracking subdomain. This IP address is from then on be used for communication with JENTIS as a first-party server.

As soon as the visitor enters the domain of the company's website in the address line of the browser or follows a link, the company's website is loaded. The JavaScript JENTIS-Base-Tracking code is built into the website that is loaded. This code is executed when the page is loaded and causes the compressed JENTIS package to be loaded from the JENTIS CDN.

- **Step 2: Visitor recognition and generation of the JENTIS user ID**

The JENTIS Server enables recognition of the user's browser via a first-party cookie and assigns the user a randomly generated JENTIS User ID. With the help of the JENTIS cookie, data is read from the end device and this data is used for the purposes specified by the administrator for the third parties. Any tracker that processes at least one item of personally identifiable data without the "anonymization" function being activated for this data item in the JENTIS Tag Manager, will be added to the JENTIS Consent Manager's list of consents.

- **Step 3: Filtering tracking data in the JENTIS Tag Manager**

In the JENTIS Tag Manager, the administrator determines which data in the visitor's browser should be read and sent to JENTIS. For each data parameter, the administrator determines whether the data has a personal reference or it is data without a personal reference. In this way, the system can be calibrated according to the requirements of the applicable law in the region of use (GDPR [EU], PECR [UK], CCPA [CA], LGPD [BR], PIPL [CN], etc.).

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 to clearly determine which data parameter should be passed to the external third party provider. For each data parameter to be transferred, which has been classified as personal data, the administrator also determines whether anonymization is to be performed by removing the data parameters before they are passed on to the external provider.

- **Step 4: Generating the tracking library**

Depending on the settings the administrator has made for the trackers, a JavaScript file containing the tracking functions (variables, events, triggers, vendors, tags) is generated. This tracking function is coordinated with the functionality of the JENTIS Consent Manager. As soon as consent is given by the visitor for at least one tracking tool, the processing can commence and data is sent to the JENTIS Server.

- **Step 5: "Triggering" the tracking in the browser**

The third-party tags are now modified so that the user's browser no longer communicates directly with the third-party servers, but only with the JENTIS systems. Once the data is received at the JENTIS server, it is technically stored in the RAM of the JENTIS server. Before the first persistion or processing is performed, the data can be modified by the administrator, depending on the default settings.

- **Step 6: Removing the IP address and creating a synthetic client ID**

(1) In the JENTIS Server Suite, the tracking data is modified in the data backend so that, for example, the IP address of the website visitor is completely removed before it is passed on to the third-party providers. It is conceivable as one of the options that before the user's IP address is removed, a geo-database stored on the web server is used to assign the country and city of the terminal device from which the request was sent. The IP address is necessary to determine the location. In the course of further processing, only demographic location data (country/city) is then transmitted to third parties, but not the identifying components of the visitor's IP address.

(2) 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.

(3) Data from third-party providers, such as client IDs in the case of Google Analytics, which enable unique assignment of the end device, are not processed within the JENTIS Server Suite and are sent to the respective third-party provider as a synthetically generated fictitious client ID.

- **Step 7: Removal of the raw data**

If there is a legal basis for forwarding personal data to a tool in a secure third country, the original data is also processed in a non-persistent manner. After this processing (max. 30 seconds), the data is completely discarded on the JENTIS server. Exception: There is a legal basis under the GDPR to store this data as raw data.

- **Step 8: Transmission of the "cleaned" tracking data to third-party providers**

Using the (own) 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, to deliver the Analytics script.

The cleaned tracking data, i.e. the synthesized and exchanged IDs of the third-party providers as well as the demographic location data (country/city) together with information on user behavior (e.g. events), are transferred 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 are transmitted.

For the **legal assessment of the risks and legal uncertainties described** (Sec. II.), there are **two main processing steps** with regard to user data based on the technical functional principles outlined in the JENTIS functional description (v0.92):

- **First**, the access to the end device, triggered by the user's browser request to the JENTIS Server (step 1 to step 5).

- **Second**, the server-side transmission of the cleaned tracking data (session ID, user ID, demographic location data) to Google servers (step 8).

2. Evaluation of the terminal access by JENTIS as "strictly necessary".

The delivery of the JENTIS first-party cookie to the JENTIS Server as a result of the server request from the user's browser requires access to the user's browser. This process is not subject to the restrictions of informed consent.

a) Application of the exceptions in Article 5 (3) (2) ePrivacy Directive

(1) First of all, when the website is called up using the **JENTIS Tag Manager**, an **https-request** is sent to **JENTIS**. Based on this request, the **user's IP address** as well as system and browser information are **transmitted** to JENTIS.

The mere integration of a tag manager as a "container solution" does not require the user's consent, because the exception to the consent requirement pursuant to Article 5 (3) (2)(1) of the ePrivacy Directive can be applied. This results from an application of the criteria developed by the EDPB (see Part II.1.a.). For the transmission of the user's IP address and other terminal device information, such as, for example, browser information, which is merely technically initiated, the exception in Article 5 (3) (2) of the Directive is generally relevant, provided that no other user data is transmitted to third-party providers without being filtered.

The use of the **JENTIS Tag Manager** facilitates electronic communication by transferring information to third-party providers via programming interfaces, among other things. The tag manager implements the respective code snippets of the third-party providers without the website operator having to make time-consuming changes to the source code of the website. Instead, the integration is done by a container that places a so-called "placeholder" code in the source code. As a result, the Tag Manager allows users without in-depth IT knowledge to embed complex third-party tools on the website. In addition, the JENTIS Tag Manager allows users to exchange data parameters in a specific order, especially by ordering and systematizing data sets.

(2) Third-party tags, such as code snippets or even pixels, are also **activated** on the website by the JENTIS Tag Manager. An evaluation of the end device information and personal data of the users collected by the tags does not take place by the tag manager itself, but these are forwarded to the respective service.

The forwarding initiated by the tag manager also constitutes processing within the meaning of the GDPR Article 4(2). For the **transmission of user data for analysis or marketing purposes**, a **strict consent requirement** applies in principle based on the BGH decision "Cookie consent II" (I ZR 7/16).

(3) The implementation of the **JENTIS Consent Manager** enables requesting consent that complies with data protection requirements for the use of third-party tools such as Google Analytics.

Yet, services to provide user preferences such as **JENTIS Consent Manager** may be allowed without requesting user consent [Art 29 Data Protection Working Party, WP 194, Opinion 04/2012 on the exemption of cookies from the consent requirement, p 7 f.; ICO, Guidance on the use of cookies and similar technologies, 2020 p 37]. In line with the opinion of the Art. 29 Data Protection Working Party (WP 194), according to which the exception provision in Article 5 (3) (2) of ePrivacy Directive also applies to individual functionalities provided by the "website" service, the integration and provision of the functions of the **JENTIS Consent Manager** in a justifiable manner is to be regarded as permissible **without consent**.

(4) Modification of data with the help of the JENTIS Server Suite is a **consent-free alternative** to the **transfer of user data for analysis or marketing purposes**, provided that the administrator of the JENTIS SaaS solution has carried out the proposed configurations as described in the Section III. 1 (see Section III. 3 regarding the assessment of data transfer). **Separate consent** for the use of the Tag Manager **is then not required.**

(5) The **European Data Protection Supervisor** (EDPS) has published a **"Toolkit" for determining for the assessment of the "necessity"** of measures in accordance with Article 52(1) EU Charter [EDPS, Assessing the Necessity of Measures Restricting the Fundamental Right to Protection of Personal Data: A Toolkit, 2017, p. 5].

"[…] The Toolkit consists of this introduction, which sets out the content and purpose of the Toolkit, a practical step-by-step Checklist for assessing the necessity of new legislative measures and a legal analysis of the necessity test applied to the processing of personal data. […]"

According to information in the media and in view of the data protection organization "La Quadrature du Net", these **criteria** can also serve as **guidance** for the interpretation of the term "**necessity**" under the Article 5 (3)(2) ePrivacy Directive. Similarly, the EDPB has **referred** to the **EDPS toolkit** for the non-public sector in the "Guidelines 2/2019" for the interpretation of the notion of necessity [p. 9, fn. 18 and fn. 19].

Subject to a different case law in the future and positions taken by supervisory authorities, the **methodology** can form a basis for activation of selected functionalities on websites and **resolve** the conflict of objectives for the application of the strict consent requirement in individual cases as described under point II 1. a. above.

According to the EDPS, **necessity** implies the need for a combined, fact-based assessment of the effectiveness of the measure in light of the objective pursued and of whether it is less intrusive compared to other options for achieving the same goal.

The **Necessity Assessment Checklist** consists of four sequential steps. Each step corresponds to a series of questions that facilitate the assessment of necessity [EDPS, A Toolkit, 2017, p. 10].

(6) As part of the **legal assessment** for the use of the JENTIS solution for further risk mitigation, the EDPS toolkit for determining "necessity" (see point II. 2. c-d) was **used for justifying the application of Article 5 (3) (2) of the ePrivacy Directive**:

- For **Step 1** of the EDPS toolkit to determine the necessity of end device access, the detailed factual presentation of the technical operating principle for cleaning up tracking data from third-party services such as Google Analytics and reducing user data as well as defining the purpose has been carried out (see point III. 1).
- The answering of questions required for **Step 2** of the EDPS Toolkit to determine the extent of the intervention by the JENTIS systems has also been carried out in view of the detailed description of the individual data processing steps (cf. point III. 1.).
- As **Step 3** of the EDPS Toolkit, the objective of a fundamental statistical analysis of the usage behavior of websites was identified as the Use Case in order to optimize, improve and further develop digital offerings in accordance with the technical state of the art and the entrepreneurial freedoms guaranteed by Art. 16 (1) of the EU Charter. According to the EDPS, the GDPR Article 23 contains a list of objectives on the basis of which the rights of natural persons and the obligations of the controller may legitimately be restricted. According to the GDPR Article 23 (1) (i), this also includes the protection of the rights and freedoms of other persons, i.e. also legal persons and their entrepreneurial freedoms to be taken into account according to Art. 16 (1) of the EU Charter.
- According to **Step 4** of the EDPS Toolkit, specific aspects for the JENTIS first-party cookie user analyses were taken into account when assessing the necessity of processing the user ID assigned by JENTIS itself as the sole reference for recognizing the browser of a user's terminal device.
    - In the opinion of the BGH, a randomly generated number (**cookie ID**) stored in cookies, which is assigned to the user's registration data as **terminal device information**, constitutes a **pseudonym** within the meaning of 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 the GDPR [Menke, K&R 2020, 650, 652; Baumgartner/Hansch, ZD 2020, 435, 436].

- The restriction required by the GDPR Article 4(5) that the additional information is kept separately and is securely with the help of technical and organizational measures to ensure that no data can be linked to an identifiable person takes place is guaranteed. Regardless of whether the additional information used qualifies as a direct link or an attribution rule [Schwartmann/Weiß, Entwurf für einen Code of Conduct zum Einsatz DSGVO konformer Pseudonymisierung, 2019, v1.0, p. 11], technical and organizational security is ensured by means of a **robust separation** of the **server entities** in the context of **server-side tracking** by JENTIS.
- The user IP address is completely removed at the own web servers (**Step 6**); there is no communication of the user's browser with Google servers. Even in the case of partial disidentification of IP addresses by shortening the last part after transmission of the complete IP address, case law considers pseudonymization as defined by Section 3 (6a) of the old version of the German Federal Data Protection Act (BDSG), as shown by a final decision of the Frankfurt Regional Court on the web analytics service "Piwik" [LG Frankfurt, Urt. v. 18.2.2014 - 3-10 O 86/12 (para. 36); approvingly Weidert/Klar, BB 2017, 1858, 1859]. The court rejected the classification of the shortening of the IP address as a means of anonymization, in particular because a website operator who has registration data from user accounts could make an assignment to identifiers in real time at any time.
- Similarly, JENTIS does not process data parameters that allow users to be uniquely identified, such as order IDs, but generates them as a random product.
- Data from third-party providers, such as client IDs in the case of Google Analytics, which enable a unique attribution to the end device, are not processed within the JENTIS Server Suite and are sent to the respective third-party provider as a synthetically generated fictitious client ID.
- The purposes within the use case "Analysis" have been limited to enable the evaluation of published content and the usability of the website and to evaluate or improve the effectiveness of design decisions of the website.
- The JENTIS User ID is not merged with other user data such as a CRM ID or systems containing registration data.
- Processing by the JENTIS Servers takes place on separate data entities, on which inventory data of users (e.g. e-commerce store) may be stored.
- From the customer's point of view, the use of analytics should be limited to the creation of anonymous statistics.

- ○ The storage period of JENTIS cookies can be configured individually and is 13 months.

b) Interim result

Subject to a future position of the European Data Protection or the Data Protection Conference or case law to the contrary, the application of the exception to the consent requirement in Article 5(3)(2) of the ePrivacy Directive is guaranteed for the technical functionality principles of JENTIS. The use of the JENTIS SaaS solution to further obstruct (make it difficult) the link of a browser of an end device to a usage profile as the sole reference for subsequent recognition of the browser is therefore **an effective measure** in the context of first-party terminal device access, which represents the least degree of interference with the fundamental rights under Article 7 and Article 8 (1) of the EU Charter of the website visitors.

If it is possible to invoke the exception under Article 5 (3) (2) of the Privacy Directive, the consent of the user is not required. Nevertheless, it is imperative to check whether the legal basis under the GDPR Article 6 (1) (1) (f) is relevant for the respective service. To document the test on balance of interests according to GDPR Article 6 (1) (1) (f) [EDPB, WP 260, Appendix], a **so-called LIA** (Legitimate Interests Assessment) should be carried out by the administrator in accordance with the configuration of the JENTIS Systems, in order to be able to provide evidence of the assessment of interests in individual cases.

3. Evaluation of the transmission of synthetically generated client IDs to third-party providers

(1) As next processing operation to be assessed, subsequent to the terminal access by JENTIS, is the server-side transmission of the cleaned tracking data (synthetically generated client ID and order ID as well as event data) to the third-party provider such as Google Server (**Step 8**).

(2) As a result, neither the client ID assigned by third-party providers such as Google nor the IP address of the user is transmitted. The same applies to any recorded Order IDs. The formation of **synthetic data** from raw data **corresponds** to the formation of **hash values**, as far as the classification of the synthesization of the third-party IDs as a measure of pseudonymization is concerned.

The use of **hashing methods** is supported by supervisory authorities [For example, Article 29 Data Protection Working Party, WP 216, Opinion 5/2014 on anonymization techniques, p. 24 f.; Bayerisches Landesamt für Datenschutzaufsicht, Facebook Custom Audience bei bayerischen Unternehmen, press release dated 4. 10.2017] and the commentaries regarded as **pseudonymization within the meaning of the GDPR** Article 4(5) [Stentzel/Jergl, in: Gierschmann/ Schlender/ Stentzel/ Veil, GDPR, Art. 4 No. 5 Rn. 6; Arning/Rothkegel, in: Taeger/Gabel, DSGVO/BDSG, Art. 4 Rn. 144]. The creation of hash functions also constitutes pseudonymization within the meaning of the GDPR Article 4(5) according to the assessment of the "Focus Group on Data Protection" of the Federal Ministry of the Interior [Schwartmann/Weiß, Entwurf für einen Code of Conduct, Pseudonymisierung, 2019, v1.0, p. 22].

The **restriction required** by the GDPR Article (4)(5), that the **additional information is stored separately** and secured by technical and organizational measures to ensure that no linking of the data to an identifiable person takes place, **is guaranteed** during the communication of the different server entities of **JENTIS**. Regardless of whether the additional information such as the JENTIS User ID can be a direct link or an attribution rule for the synthetically generated client IDs and Order IDs of the third-party providers [Schwartmann/Weiß, Entwurf für einen Code of Conduct zum Einsatz DSGVO konformer Pseudonymisierung, 2019, Version 1.0, p. 11], according to the described technical operating principle, given the system architecture of JENTIS (**Appendix 1**), there is a robust separation of the data entities that excludes an attribution for third-party providers.

Only if re-identification is ruled out because the processing entity would not have the required attribution rule, would anonymization of the transferred parameters to third-party providers have to be considered in line with the GDPR Recital 26 and the 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-party providers, it must also be assumed, in view of the assessment of the "Focus Group on Data Protection" of the German Federal Ministry of the Interior, that there is a reference to a person due to the mere pseudonymization [Schwartmann/Weiß, Entwurf für einen Code of Conduct, Pseudonymisierung, 2019, v1.0, p. 22].

As far as can be seen, third-party providers such as Google only receive **a client ID synthetically generated** by JENTIS during the outlined data transfers after the end device access (**Step 8**), which does not match with the client ID or the user ID assigned by Google for Google Analytics and therefore **does not allow Google to attribute the information** provided about the **usage behavior** of website visitors.

Likewise, **no access** to the **JENTIS Systems** by **third-party providers** such as Google is possible on the basis of the technical documentation provided. Similarly, there is **no** direct **communication** of the user's **browser** with **third-party providers**. As far as can be seen, there is no case law other than the outlined case law of the ECJ and BGH on the question of whether a reference to a person is still to be assumed if only a third party has the attribution rule for the transmitted pseudonymous data records, but there is no legal possibility for access to identifying features to personal reference of IP addresses [see point I. 2.c.; see also Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3rd ed. 2020, Art. 4 marginal no. 12].

(3) Even if one assumes a possibility of attribution by Google itself for the transmitted Session ID and User ID (**Step 3** and **Step 7**) and assumes a processing of pseudonymous data, **consent is not required** for the **data transfer** in a justifiable manner.

This is because, in line with the ECJ's view (see pt. II. 1. b.), the transfer of the cleansed tracking data must be classified as a downstream processing stage that falls within the scope of the GDPR. Due to the protective measures taken - removal of the IP address, assignment of synthetically generated values for the Client ID and Order ID, for which Google does not have an attribution rule - the **legal basis pursuant to the GDPR Article 6 (1) (1) (f)** can be applied in a justifiable manner for the transfer, subject to a different case law in the future.

However, it is mandatory to check whether the legal basis from the GDPR Article 6 (1) (1) (f) is relevant for the respective service. A so-called LIA (Legitimate Interests Assessment) should be carried out for the necessary documentation of the test on balancing of interests pursuant to the GDPR Article 6 (1) (1) (f) [EDPB, WP 260, Annex] in order to be able to provide evidence of the balancing of interests that has taken place.

4. Assessment of the third country transfer

For the data transfers in question (Step 8) to servers of third-party providers such as Google in the U.S., it is possible to make an assessment in accordance with the case law of the French administrative court Conseil d'État [Beschl. v. 13.10. 2020 - 444937] on the permissibility of using cloud services from Microsoft Azure on Servers in the Netherlands, the following measures when using the JENTIS Saas solution can reasonably be considered "additional security measures" within the meaning of ECJ case law [ECJ, 16.7.2020 - C 311/18 - Schrems II]:

- Location of the JENTIS Servers in Europe;
- Maintaining a compartmentalized data storage without access by third-party providers such as Google from the U.S. due to the lack of access possibilities of third-party providers to JENTIS Servers, end devices of the users or the pseudonymous JENTIS user ID;
- Restriction: risk avoidance through functional restriction of tracking services, e.g. lack of location determination due to removal of the IP address and exclusion of cross-device tracking due to non-use of the original client ID e.g. in the Google Analytics account;
- Valid pseudonymization due to the assignment of client ID and Order ID to mere synthetic values and the lack of access to assignment rules by third-party providers such as Google;
- Valid pseudonymization and encryption as well as lack of access to mapping rules by Google in JENTIS systems.

Against this backdrop, the **additional measures** described in accordance with the technical functionality principle (Section III. 1.) in combination with the conclusion of Standard Contractual Clauses **can currently constitute** a **justification** for the **third country transfer** pursuant to the GDPR Article 46 (2)(c), subject to contrary case law, decisions by supervisory authorities or solutions at the political level.

The supplementary measures outlined by JENTIS represent "technical or organizational guarantees" as defined in **Clause 14 of the Standard Contractual Clauses** and enable the fulfillment of the obligation to conduct and document a "**Transfer Impact Assessment**". The measures described can represent a mitigation of the risks of access by security authorities in the sense of "**Supplementary Measures**" if the JENTIS systems are configured accordingly by the administrator.

In "Strict" mode, JENTIS also offers a guarantee of compliance with the legal framework, provided that the administrator configures the system correctly. If there is a justification for forwarding personal data to a tool in a secure third country, the original data is also processed in a non-persistent manner. After this processing (max. 30 seconds), the data is completely discarded on the JENTIS server.

IV. Summary of the results

In conclusion, if the **JENTIS SaaS solution** is used to implement third-party tracking tools such as Google Analytics, the **legal uncertainties** described above (cf. point II) **can be eliminated** if the solution is configured appropriately.

Due to the application of the exception provision under Article 5 (3)(2) of the ePrivacy Directive, the **request for user consent** for access to end devices **can be waived** in a justifiable manner. The transfer to third-party providers after modification of the tracking parameters can be based on the legal basis in the GDPR Article 6 (1)(1)(f) if a Legitimate Interests Assessment is carried out for the specific use case.

Finally, in the case of the configuration described above, **JENTIS SaaS solution enables** proof of **additional security measures**, which, in addition to the conclusion of Standard Contractual Clauses, can constitute a justification for the third-party transfer.

V. Recommendation for legally compliant use of the JENTIS Saas solution

The following measures are recommended for legally compliant use of the JENTIS Saas solution:

- Evaluation of the functionality though a Software-Demo or through this Memorandum;
- Configuration of the JENTIS systems by the customer's administrator in accordance with the technical functional principle (point III. 1.);

- Necessary documentation of the balancing of interests according to the GDPR Article 6 (1) (1) (f) [EDPB, WP 260, Appendix] by means of a LIA (Legitimate Interests Assessment), in order to fulfill the accountability obligations for the balancing of interests that has taken place;
- Transparent information in the privacy policy on the website;
- Opt-out options for users through automated systems such as opt-out links, which are particularly pointed out in the privacy policy or the JENTIS CMP.
- Conclusion and documentation of the data processing agreement with JENTIS.
- Conclusion and documentation of the accompanying data protection agreements (commissioned processing, joint controller or controller-2-controller agreement with third party provider).