Data Protection Memorandum

JENTIS GmbH

Author	Date
RA Peter Hense & RA Tilman Herbrich (CIPP/E)	*10 February 2023, v2.4.*

Project

Data protection evaluation of the "Essential Mode" of the JENTIS Saas solution

Executive Summary

The consent requirement prescribed by EU data protection law and case law applies to any access to and storage of information from users' terminal equipment **(I.3.)**. In view of the BGH decision "Cookie consent II" **(I.1.)**, the legal regulation in § 25 TTDSG, as well as currently initiated investigations by supervisory authorities and initial court rulings, the consent requirement for website tracking is a stringent requirement.

An exception to this stringent consent requirement - "strict necessity" - is regulated in Art. 5 (3) sentence 2 of the ePrivacy Directive **(II.1.)**. Case law and the current interpretation of the wording of Art. 5 (3) p. 1 ePrivacy Directive also suggests that, under certain circumstances, relying on downstream processing in server-side tracking without direct access to the terminal equipment **(II.2.)** does not fall under this stringent consent requirement. Importantly, the exceptions to the stringent consent requirement do not apply to third-party services.

In practice, the implementation of the exceptions to the consent requirement is practically associated with high risks due to complex and difficult-to-solve challenges in integrating tracking applications (a majority of them) without a long-term and sustainable technical solution that is also legally compliant and supports effective data use. **(II.3.)**.

JENTIS Data Capture Platform (DCP), as a Privacy Enhancing Technology, provides long-term support to ensure "data privacy" compliance in the supply chain and allows customers flexible configurations of the SaaS solution to accommodate the volatility of each company's individual risk situation. The JENTIS twin-server technology **(III.1.)** enables effective use of website data in both situations -- when user consent is explicit (tracking mode) and when user consent is not available (as a fall-back solution -- JENTIS Essential Mode). Companies can configure the "JENTIS Essential Mode" as a fallback solution for first-party tracking so that the application of the exceptions to the consent requirement for terminal access are implemented in a compliant and effective manner **(III.2.)**. This enables "usage analysis" to a reduced extent without user consent if the user does not click the cookie banner at all or does not give consent.

The server-side transfers of the browser user data modified (and cleaned) by the JENTIS server to third-party servers can be based on overriding legitimate interests in accordance with Art. 6 (1) sentence 1 lit. f) of the GDPR as a consent-free downstream processing phase in specific individual cases **(III.3.)**. In line with ENISA's view, the modification of data parameters can be considered a Privacy Enhancing Technology and can be used

as an effective means of pseudonymisation.

With the help of JENTIS, companies can fully implement the data protection requirements for tracking and address the legal uncertainties. Website operators can take economic advantage of their own first-party data when using JENTIS, without putting their data or respective corporate compliance at risk from a legal perspective due to uncontrolled and non-transparent processing on the part of third-party providers **(IV.)**. Via JENTIS technology, companies regain complete control in server-side tracking.

Table of Contents

Legal assessment

I. Analysis of the current situation - legal classification of the processing in website tracking

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 both **access to information stored in the terminal equipment** and, due to the https request of the user's browser (client) initiated by the JavaScript, a **transmission of personal data** of the website visitor. Hereinafter, website visitors will also be referred to as users.

1. Consent to access terminal equipment for tracking for analysis and marketing purposes

(1) In its judgment of 28 May 2020[1], following the preliminary ruling by the ECJ in the "Planet 49" case, the BGH finally ruled that for the **use of cookies** (and similar technologies), which are set on a user's terminal equipment after registration for a competition and enable an **evaluation of the user's behaviour** on websites of advertising partners and thus **interest-based advertising**, **consent is in principle required** from the user according to interpretation of § 15 para. 3 of the German Telemedia Act (now § 25 of the German Telemedia Data Protection Act) in conformity with Art. 5(3) sentence 1 of Directive 2002/58/EC as amended by Directive 2009/136/EC (ePrivacy Directive).

According to the wording of the **Directive**, the consent requirement applies to any access to and storage of information from users' terminal equipment and, in the BGH's view, due to the conflict of laws rule pursuant to Art. 95 GDPR, **blocks** the **application** of other provisions of the **GDPR for this process** than in relation to the consent (Art. 4 No. 11, Art. 6 para. 1 sentence 1 lit. a), Art. 7 GDPR). According to the concurring opinion of the ECJ and the BGH, it is **irrelevant** for the existence of the consent requirement whether the **terminal equipment information** is **personal** or **anonymous** data.[2]

(2) **Initial court decisions** have, among other things, prohibited the use of Google Analytics on a website without requesting voluntary and informed consent.[3]

(3) According to the European supervisory authorities, it does not matter for the applicability of this case law whether the **access** to and the **storage** of the information on the terminal equipment is carried out by

[1] I ZR 7/16 – cookie-consent II.
[2] Cf. ECJ, Judg. of. 01.10.2019 – C-673/17, para. 70.
[3] Cf. LG Rostock, Judg. of. 15.09.2020 – 3 O 762/19; LG Köln, Dec. of. 29.10.2020 – 31 O 194/20 and Dec. of. 13.04.2021 – 31 O 36/21; LG Frankfurt, Judg. of. 19.10.2021 – 3-06 O 24/21; LG München, Reference resolution of 08.12.2021 – 33 O 14776/19.

means of cookies or **other technologies** such as **tracking pixels.**[4] The term "access to terminal equipment" also includes access to local storage, local shared objects and server-side technologies such as the use of browser fingerprinting technologies like "canvas fingerprinting".[5]

2. Current audits by supervisory authorities and NGOs for the enforcement of the law

(1) According to the German Data Protection Conference (Datenschutzkonferenz, DSK), the **request for consent** from the website visitor is mandatory for the **terminal equipment related storage** of and **access** to user IDs and IP addresses by means of cookies and similar tracking methods and the **transmission of personal data**, e.g. when using Google Analytics, also to Google LLC in the USA.[6] Specifically in Germany, audits of website tracking on the part of supervisory authorities and NGOs have increased noticeably in recent times.

(2) On 27.09.2021, the European Data Protection Board (EDPB) decided to set up a "Cookie Banner Task Force" pursuant to Art. 70 (1) (u) GDPR in order to promote uniform law enforcement across Europe. The reason for this is not least the call campaign of the NGO "Noyb" in July 2021 for the submission of user complaints against unlawful cookie banner designs in relation to website tracking. In August 2021, Noyb alone reported that 422 formal complaints were submitted to the supervisory authorities.

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

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

3. Failure of previous industry solutions for website tracking

(1) Previous industry solutions such as offering "first-party cookies" from third-party providers ("3rd party as 1st party") do not change the data protection requirements for the permissibility of tracking if, for example, due to the processing of Domain Name System (DNS) records, tracking resources from third-party

[4] Cf. DSK, orientation guide for telemedia providers, 2021, p. 24; European Data Protection Commitee (EDSA) in its Guidelines 8/2020 on the targeting of social media users, version 2.0, para. 71 f.).
[5] LG Rostock, Judg. of. 15.09.2020 – 3 O 762/19; ICO, Guidance on the use of cookies and similar technologies, 2020; DSK, orientation guide for telemedia providers, 2021, p. 7.
[6] DSK, Decision of 12. Mai 2020 – notes on the use of Google-Analytics.

providers are delivered by the same domain from which the website is operated.[7] In other words, first-party cookies can be used in the same way as third-party cookies and enable, for example, "cross-site tracking".[8]

(2) Likewise, advertising technology solutions such as server-side tracking via the server-side Google Tag Manager (SSGTM) or the Facebook Conversions API do not exempt from compliance with data protection requirements, even if the information from terminal equipment 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).[9]

(3) Most recently, announcements by Google in spring 2021 to eliminate third-party cookies and instead offer a "Federated Learning of Cohorts (FLoC)" or "FLEDGE" with scatter losses caused a turnaround in the industry. Nevertheless, the Information Commissioner Officer (ICO) criticises these approaches and demands proof from controllers that these approaches do not lead to increased fingerprinting and transparency about how Google processes corresponding GPS signals.[10]

(4) Finally, the use of the industry standard Transparency and Consent Framework v2.0 (TCF v 2.0) of the industry association Interactive Advertising Bureau Europe (IAB Europe) to request voluntary and informed consent for tracking services is currently exposed to **risks**.

At the beginning of February 2022, the **Belgian supervisory authority** (Autorité de protection des donnée - Gegevensbeschermingsautoriteit) decided in a penalty notice against IAB Europe amounting to EUR 250,000.00 that **processing** by means of the **TC consent string violates** various obligations under the **GDPR**, in particular, due to the complexity of the processing, it does not comply with the transparency requirements and the corresponding processing is therefore unlawful.[11] The IAB Europe filed an action against the decision of the Belgian authority before the Market Court Brussel (Hof van beroep). On 07.09.2022, the court proceedings were suspended due to two questions referred by the Market Court to the European Court of Justice on the personal reference of the TC string and the responsibility of IAB Europe for the processing.[12] The preliminary ruling procedure at the ECJ and the subsequent continuation of the proceedings before the Market Court Brussels remain to be seen.

(5) Without modification of the data parameters and the data processing that takes place when the website is called up due to the loaded tags from third-party providers, as is possible, for example, through the

---

[7] Veale/Borgesius, AdTech and Real-Time Bidding under European Data Protection Law, 2021, p. 6.
[8] IPOL Study: JURI commitee, EU-Parlament, Regulating targeted and behavioural advertising in digital services, 2021, p. 44, para. 49.
[9] Cf. Papadogiannakis et al., User Tracking in the Post-cookie Era, 2021, p. 1 f.
[10] CNIL, Alternatives to third-party cookies, 23.11.2021; ICO, Data protection and privacy expectations for online advertising proposals, 2021, p. 24 f.
[11] Cf. Veale/Nouwens/Santos, Note on the administrative fine against IAB Europe, 2022; cf. on the criticism of TCF v2.0 in gernal Cèlestin Matte and others, 'Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework' (2020) p. 794; Midas Nouwens and others, 'Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence' (2020), p. 3 et seq.; Nataliia Bielova and others, 'Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?' (2020) p. 4 f.; Michael Veale and Frederik Borgesius, 'Adtech and Real-Time Bidding under European Data Protection Law' (2021), p. 28.
[12] Market Court Brussel (Court of Appeal), Dec. of. 07.09.2022.

use of RudderStack with the appropriate configuration (see Point II below.), the consent requirement from § 25 (1) TTDSG applies without restriction for access to information on terminal equipment.

II. Legal uncertainties due to technological diversity in website tracking

Legal uncertainties have sometimes arisen in practice with regard to the data protection requirements for website tracking. The legal uncertainties arose due to the legislative vacuum after the BGH decision "Cookie Consent II", which was filled by lawyers and marketers with views favourable to them, some of which were diametrically opposed to already existing judicial and regulatory decisions.
Scope for interpretation is primarily seen in the question of when cookies and similar tracking technologies fall under the legal criterion of "strictly necessary" (Art. 5 para. 3 p. 2 ePrivacy Directive) **(1.)** as well as which other legal connecting factors exist so that an exception to the requirement of informed consent can be assumed **(2.)** Due to insufficient industry solutions, the need for long-term strategies for legally compliant and successful data use is growing **(3).**
Tracking proxy solutions such as the JENTIS Twin Server technology play a significant role in this.

1. Legal Uncertainty: Exceptions to the consent requirement for access to terminal equipment

The Directive provides for two exceptions to the obligation to request user consent for access to and storage of information from users' terminal equipment in website tracking, which have also been adopted unchanged in § 25 (2) TTDSG.[13]

a) Necessity for carrying out and facilitation of electronic communication

For the technically required transmission of the user's IP address and other terminal equipment information, such as browser information in HTTP-based applications, the exception in Art. 5 para. 3 sentence 2 ePrivacy Directive is generally relevant.
According to this, **consent is not required** if **technical storage** of or access to terminal equipment information is **carried out** for the purpose of **electronic communication**. However, it is a prerequisite that carrying out or facilitation of electronic communication is the **sole purpose** of the processing.[14] According to the European Data Protection Board as well as individual supervisory authorities, the following are covered by the exception in Art. 5 para. 3 sentence 2 ePrivacy Directive:[15]

[13] DSK, Orientation guide for telemedia providers, 2021, p. 19. The preliminary questions are: 1. Is Europe jointly responsible (Joint Controller) with CMPs, publishers and vendors? 2. Does the TC string constitute personal data?
[14] Art. 29-Data Protection Working Party, WP 194, opinion 04/2012 on the exception of cookies from the consent requirement, p. 3.
[15] Art. 29-Data protection working party, WP 194, opinion 04/2012 on the exception 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 the information over 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 packets, and
- the ability to detect transmission errors or data loss.

The **exception** for carrying out or facilitation of communications therefore **includes cookies** that fulfil one (or more) of these characteristics, but only for the sole purpose of transmission or facilitation; i.e. the transmission of the communication must be impossible without the use of the cookie for the exception to apply.[16]

b) Strictly necessary to provide a requested service

(1) The **second exception** in Art. 5 para. 3 sentence 2 of the ePrivacy Directive - **access** to terminal equipment information is **"strictly necessary"** to provide an information society service requested by the user - is, according to the decision of the BGH, in any case not relevant for purposes of advertising and market research.[17] According to the Art. 29 Working Party[18], **three material conditions** must be met:

1) The service is explicitly requested by the user: The user has taken an affirmative action to request a service with a clearly defined scope.
2) Information society service is usually understood as 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 (additional) functionalities provided by the basic service "website". In individual cases, this may also include interaction with a chatbot, map service and streaming content.[19] In the DSK's view, cookies and similar technologies may be used, for example, for any additional functions of the basic service website if they are requested by the user, which is not yet the case when the website is merely called up.[20]
3) Access to terminal equipment information must be "strictly necessary" to provide the service - website, app or individual functionalities.

(2) The **resilience** of this **exception provision** depends primarily **on** the degree of restriction of the **interpretation** of the concept of **necessity.** However, a limiting factor is that the **case law** of the **ECJ** examines

[16] ICO, Guidance on the use of cookies and similar technologies, p. 13.
[17] BGH, Judg. of. 28.05.2020 – I ZR 7/16 – cookie-consent II.
[18] Art. 29-Data Protection Working Party, WP 194, opinion 04/2012 on the exception of cookies from the consent requirement, p. 4.
[19] Agreeing with DSK, Orientation guide for telemedia providers, 2021, p. 20.
[20] DSK, Orientation guide for telemedia providers, 2021, p. 23.

whether **restrictions** to the rights to protection of personal data and respect for private life are strictly necessary for the processing of personal data. The ECJ[21] stated that

> *"[...] derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary [...]".*

Furthermore, in the **"M5A-ScarA" case**[22], the **ECJ** stated on the basis of the balancing of interests clause (Art. 6 (1) p. 1 lit. f) GDPR) that **processing is only "necessary"** if it **cannot reasonably be achieved** as effectively **by other means** which are **less intrusive** on the **fundamental rights and freedoms** of the data subjects, in particular the rights to respect for private life and protection of personal data as guaranteed in Art. 7 and 8 of the EU Charter of Fundamental Rights.[23] Furthermore, the requirement of the necessity of the data processing had to be examined together with the so-called **principle of "data minimisation"**, which was enshrined in Art. 6 para. 1 sentence 1 lit. c) of Directive 95/46 (now Art. 5 para. 1 lit. c) GDPR) and required that the personal data

> *"[...] must be 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed' [...]".*

(3) In the **view** of the **DSK**, a **restrictive understanding** applies to the interpretation of the term **"strictly necessary"** in view of Recital 66 of the ePrivacy Directive. Therefore, **economic considerations** for the realisation of a business model **cannot** be taken as a basis for the strict necessity.[24]
The DSK places **stricter requirements** on the resilience of the exception for the **use** of **cookie IDs** (user IDs). **Only in a few cases** there is a **strict necessity** for such a storage, **since** many **functions** that require storage of or access to terminal equipment information can be **carried out without individualisation**. As a **negative example,** the DSK cites the use of a **long-term stored ID** for the following use cases :

- Logging of consent in a consent management platform (CMP)
- Load balancing and
- Saving settings for language or background colour.

In the opinion of the DSK, the **application of the exceptions** to the consent requirement for the use of one and the same **cookie** for several **different purposes** is not excluded. However, the prerequisite is that one of the exceptions in § 25 (2) no. 2 TTDSG is relevant for each individual purpose.[25]

---

[21] ECJ, Judg. of. 04.05.2017 – C-13/16, para. 30 – Rigas.
[22] ECJ, Judg. of. 11.12.2019 – C-708/18, para. 48 – M5A-ScarA.
[23] Cf. also ECJ, Judg. of. 17.06.2021 – C-597/19, para. 110 m. w. N. – Telenet BVBA.
[24] DSK, Orientation guide for telemedia providers, 2021, p. 22.
[25] DSK, Orientation guide for telemedia providers, 2021, p. 24.

In the view of the **Data Protection Conference**, decisive criteria for determining the **service** explicitly **desired by users** are:[26]

- Granular definition of which function of the telemedia service requires which specific storage duration and method of reading of information on the terminal equipment;
- Determining whose primary interests this function serves: the provider's own interests, the interests of the users of the website, the interests of the integrated third-party service provider or the interests of third parties.

The decisive **criteria** for determining **strict necessity** are:

- Time of storage - When may the readout and storage process take place?
- Content of the information - What information is stored and read out?
- Duration of information storage - How long is information stored on the terminal equipment and for how long can it be read out?
    - The period of storage may only be chosen as long as is necessary for the implementation of the granular function of the telemedia service.
    - In principle, session cookies are more necessary than long-lasting cookies.
- Readability of information - For whom is information from the terminal equipment readable and usable?
    - If information is stored on the user's terminal equipment when using a telemedium, it must be technically ensured that this information can subsequently only be read by the operator of the respective website.
    - If this was not already the case with third-party cookies, it must be ensured that third-party service providers use the readout information exclusively for the website accessed by the user.

c) Interim conclusion on user tracking without reducing the data parameters

In the context of a **necessity test** related to **third-party tracking** for user analyses, one will come to the conclusion with sufficient certainty that without modification of the tracking parameters, there cannot be a **strict necessity** according to Art. 5 (3) sentence 2 ePrivacy Directive, since third-party tracking always expands the circle of data recipients beyond the actual service provider or contractual partner, sometimes even in an uncontrolled manner.

As long as a first-party analysis carried out by the website operator itself is possible without the use of third-party providers, one will not arrive at the necessity for the use of third-party providers, taking into account the aforementioned ECJ case law and the opinion of the DSK on website tracking.[27]

2. Delimitation of terminal equipment access, storage and downstream processing

[26] DSK, Orientation guide for telemedia providers, 2021, p. 26 f.
[27] DSK, Orientation guide for telemedia providers, 2021, p. 27.

(1) If there is **no direct and immediate access to or storage** of information on the **terminal equipment resources** of a user, for example in the case of a programmatic processing chain or server-side ex post observations of log files created for technical reasons, it can be argued in accordance with the **view of the ECJ** and the **supervisory authorities** that the **processing** of forwarded **usage data** (especially the IP address of the user) for website analysis or in the context of the placement of an advertising material tailored to the individual interests of a user is no longer **covered by Art. 5 (3) sentence 1 of the ePrivacy Directive**. (no access to the terminal equipment and no storage of information from the terminal equipment). Rather, this processing constitutes a downstream processing phase outside of the scope of protection of the ePrivacy Directive.
Downstream processing phases are to be measured solely against the **standard of the GDPR** and allow for more flexible handling. This refers to processing processes that take place after the processing phases "access" and "storage" covered by the wording of Art. 5 (3) sentence 1 of the ePrivacy Directive, such as the transmission or use of tracking data.

(2) In the decision on the **One-Stop-Shop procedure**[28], the **ECJ** agreed with the EDPB's view that the scope of application of the "special rule" in Art. 5(3) ePrivacy Directive only covers the storage and reading of personal data by means of cookies. However, the rule in Art. 5(3) 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 interaction between the ePrivacy Directive and the GDPR", the **EPDB clarified** for the case of targeting that the **GDPR** alone is to be used **for** the assessment of the **lawfulness** of, for example, the *"[...] storage and analysis of data regarding web browsing activities for purposes of online behavioural advertising or security purposes [...]".*
In this sense, the **Conseil d'État** has already taken the position on a CNIL fine notice against Google due to a lack of consent for user tracking that the one-stop-shop mechanism contained in the GDPR for the control and sanctioning of operations to access or write cookies in users' terminal equipment is not applicable, as these fall within the scope of the ePrivacy Directive.

(3) Finally, the Federal Government's draft law for the TTDSG explicitly refers to the **application of the GDPR for downstream processing phases.**[29]

(4) Even if it is assumed that **server-side tracking is always** a downstream processing phase without access to the terminal equipment and thus exclusively opens the scope of application of Art. 6 (1) GDPR, recourse to Art. 6 (1) sentence 1 lit. b) or lit. f) GDPR is inadmissible according to the unanimous opinion of European supervisory authorities, at least in the case of the use of third-party tracking such as Google SSGTM.

[28] ECJ, Judg. of 15.06.2021 – C-645/19 – One-Stop-Shop, para. 74.
[29] BT-Drs. 19/27441, p. 38.

The legal basis according to **Art. 6 para. 1 p. 1 lit. b) GDPR comes to nothing** because the processing would have to be necessary for the fulfilment of a contract. A visit to a website with e-commerce offers or editorial content does not even establish a contractual relationship of any kind, let alone is it strictly necessary to create user profiles or analyse user behaviour in order to deliver content, ship goods or provide services without a separate and transparent agreement (e.g. user account).
In the EDPB Guidelines 2/2019, it was clarified that the legal basis of Art. 6 (1) p. 1 lit. b) GDPR could not be used for contract performance for purposes of "service improvement", "online behavioural targeting" and "personalisation of content". Accordingly, analysis procedures or processing for the purpose of personalised advertising do not fall under this legal basis.[30]
Against the backdrop of the strict ECJ case law on the **three-stage balancing of interests** within the framework of **Art. 6 (1) sentence 1 lit. f)[31] of the GDPR**, one will also have to reject overriding legitimate interests in the case of third-party tracking.

> *"[...] that provision lays down three cumulative conditions so that the processing of personal data is lawful, namely, first, the pursuit of a legitimate interest by the data controller or by a third party; second, the need to process personal data for the purposes of the legitimate interests pursued; and third, that the interests or freedoms and fundamental rights of the person concerned by the data protection do not take precedence (see, to that effect, as regards Article 7(f) of Directive 95/46…).[...]".*

Taking into account the ECJ case law on the second step of necessity[32] and the opinion of the Data Protection Conference on website tracking, one will not arrive at the necessity for the use of third party providers without further modification of the tracking.[33]

(5) For this reason, a further reduction of the processed data parameters and thus of the degree of intervention under fundamental rights is required in order to be able to apply Art. 6 (1) sentence 1 lit. f) of the GDPR in a robust manner.

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

In view 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 transfer communicated by supervisory authorities, there is a growing need for long-term and sustainable strategies for legally compliant and successful data use by third-party providers with global infrastructures.

[30] Agreeing with DSK, Orientation guide for telemedia providers, 2021, p. 30; preliminary ruling pending before the ECJ, C-252/21.
[31] Cf. ECJ, Judg. of. 17.Juni.2021 – C-597/19, para. 106 m. w. N. – M.I.C.M.
[32] Cf. ECJ, Judg. of. 17.Juni.2021 – C-597/19, para. 110 m. w. N. – M.I.C.M.
[33] Cf. DSK, Orientation guide for telemedia providers, 2021, p. 31 with reference to DSK, Orientation guide for telemedia providers, 2019, p. 13 as well as p. III Annex I.

Middleware concepts such as the JENTIS SaaS solution provide a solution to the interdependencies 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 Twin Server technology enables companies to ensure meeting legal **requirements** in the **supply chain** when using third-party tracking technologies.

III. How JENTIS helps to eliminate legal risks

(1) The **JENTIS SaaS solution** enables data protection-compliant **server-side tracking**. In doing so, JENTIS offers the possibility to transfer 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 or proxy**.
The 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-party providers such as Google or Facebook. This gives the website operator, as the data controller, full control over the data when using third-party tracking applications.

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

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

All **JENTIS DCP components** are operated **exclusively** in the **European Union** (Austria and Germany).

(3) To use the JENTIS SaaS solution, both a DNS setup for one's own website and the implementation of a JavaScript basic tracking code from JENTIS 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 it being accessed by third-party providers.

When using the JENTIS solution, first-party data received from the user's terminal equipment is streamed to the **JENTIS Twin Server,** where, if configured accordingly, all **third-party components are removed** and **replaced** in such a way that **neither** direct **terminal equipment access nor direct transmission** of user data, such as the IP address and user IDs, is carried out to third-party servers as part of an immediate server request from the user's browser.

Because of the Twin Server, which is located between the user's terminal equipment and the third-party provider, a direct connection between the user's browser and the third-party provider is interrupted from the outset. Twin server technology allows first-party data to be converted into modified artificial data (twin data)

before it can be passed on to third-party servers. JENTIS Twin data can be retained as original data or configured as pseudonymised or anonymised data.

The customer receives unique login data from JENTIS in order to use the JENTIS interface. In this interface, the customer can make settings for both the JENTIS Tag Manager, which is hosted exclusively on servers, and the JENTIS DCP.

(4) Through the JENTIS solution, the client has the control to decide which data variables to process, remove, modify and forward. The customer has a choice of more than 400 variables. The following table provides examples of how the JENTIS customer can pseudonymise data parameters:

Data parameters	Description
IP address	For technical reasons, this must be transmitted and, depending on the configuration, is then either shortened by the last octet at the JENTIS server or completely removed after comparison with a geo-database and replaced by an artificial value.
User ID from JENTIS	It is a randomly generated combination of numbers and is primarily used to recognise the website visitor.
Custom IDs	These are, for example, order IDs. This data is not processed further by JENTIS, but is newly generated as a random product.
Client IDs for external tools	Some external tools require a client ID themselves to recognise website visitors. Such client IDs are regenerated at the JENTIS server and a fictitious client ID is sent to the external tool.
Browser environment data	This data is read in the browser of the website visitor and sent to the JENTIS server. This is static data that is determined by the website visitor's device.
User action data	This data is read in the website visitor's browser and sent to the JENTIS server. This is data that describes the website visitor's actions on the website.
Time stamp	The time stamp - consisting of date and time (UTC) from the server request of the website visitor's browser - is sent to the JENTIS server.

Only the following **five steps** are required to **configure** the **JENTIS Twin Servers**:

- **First**, **identification** of the third-party tags and **data parameters** queried in each case is required.
- **Second**, the risky data parameters to be modified (by **pseudonymisation or anonymisation**) are determined.
- **Third,** the **modification** of the defined **data parameters** takes place in the **JENTIS Suite.**
- **Fourth**, **testing** of the modification of data parameters should be done **for quality assurance**.
- **Fifth**, after successful testing, the JENTIS solution can go **live**.

(5) For the **legal evaluation** of the described **risks and legal uncertainties** (point II.), **two important processing steps** arise in relation to user data:

On the one hand, the terminal equipment access, triggered by the request of the user's browser to JENTIS servers to recognise a user's browser via first-party cookies by assigning a randomly generated JENTIS User ID for the use cases defined by the customer. The duration of the JENTIS User ID can be defined individually based on a session or persistently for the duration of up to 24 months according to the risk affinity of the customer.

On the other hand, the server-side transmission of the tracking data (session ID, user ID, user agent, demographic location data) takes place after the cleaned tracking data is filtered to servers of providers such as Google in third countries.

Based on the outlined functional principle of the configured JENTIS DCP **(1.)** with the corresponding configuration Essential Mode, the request for consent can be waived. The first-party access to terminal equipment can be classified as "strictly necessary" **(2.)** and the data transfer to third-party providers in the context of individual use cases can be carried out with modification of the data parameters of the user's browser session by means of pseudonymisation **(3.)** based on the legal basis of Art. 6 (1) sentence 1 lit. f) GDPR.

1. Operating principle of the configured JENTIS DCP

The following functional principles of the JENTIS DCP can only be enabled with the appropriate configuration by customers:
(1) JENTIS acts as middleware as a kind of gatekeeper between the browser of the website visitor and the servers of third-party providers. This allows all collected data to be pseudonymised by modification before transfer to third-party providers in compliance with the GDPR (cf. in-depth section III. 3 and the JENTIS Privacy Knowledge Base). The customer determines in the JENTIS Tag Manager which data should be read out in the browser of the website visitor and sent to JENTIS. At the level of the data parameters, the customer can determine whether the individual data parameter is a relevant date 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.).

(2) The customer determines which external third-party provider should receive data from JENTIS by adding "trackers". The customer 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 provider. For each data parameter to be transferred that has been classified as relevant, the customer also determines whether a removal of the data parameters, a pseudonymisation through modification of the data parameters [cf. point III. 2.] should be carried out before transfer to the external provider.

(3) The detailed removal and pseudonymisation by modifying 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 relevant 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 last digit of the website visitor's IP address is shortened before processing and forwarding to the third-party providers. It is conceivable as an option to insert an assignment to the country and city of the terminal equipment from which the request was sent before removing the user's IP address 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 then transmitted to third parties, but not the identifying components of the website visitor's IP address.
Data from third-party providers, such as client IDs or user IDs from third-party providers in the case of Google Analytics, which enable a unique assignment of the user device, are pseudonymised within the JENTIS Server Suite if configured accordingly and the newly generated IDs are sent to the respective third-party provider as a newly generated fictitious client ID. It should be noted that the reference of newly generated IDs and the JENTIS user ID is stored. In this way, users and sessions can be recognised by customers.
Likewise, if configured accordingly, data parameters that allow users to be uniquely identified, e.g. order IDs, are not processed by JENTIS but are regenerated as a random product.

(5) The cleaned tracking data, i.e. the modified and exchanged IDs of the third-party providers together with information on user behaviour (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 customer's own IDs or the user's IP address are transmitted.

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

2. Evaluation of terminal equipment access by JENTIS server as “strictly necessary”

When using the JENTIS Tag Manager (a), the JENTIS DCP (b) and the JENTIS Twin Server Technology, the delivery of the first-party Java script and the first-party cookie of JENTIS based on the server request of the user's browser to the JENTIS server requires access to the terminal equipment capacities of the user's browser (c)..

With the corresponding configuration of the JENTIS DCP, this process can be classified as "strictly necessary" according to Art. 5 para. 3 p. 2 ePrivacy Directive (cf. III. 2. c.).

a) JENTIS Tag Manager

(1) The **https request is sent to JENTIS,** when the website with implemented JENTIS Basic Tracking Code and DNS record is called up by the user. 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 according to Art. 5 para. 3 sentence 2, var. 1 ePrivacy Directive can be applied. This results from an application of the criteria developed by the EDPB (cf. point II. 1. a.). For the transmission of the user's IP address and further terminal equipment information such as browser information, which is only technically induced, the exception in Art. 5 para. 3 sentence 2 of the Directive is in principle relevant, insofar as no further unfiltered user data is transmitted to third party providers.
(2) The use of the **JENTIS Tag Manager** facilitates electronic communication by transferring information to third-party providers via programming interfaces, among other things. In the Tag Manager, the respective code snippets of the third-party providers are implemented without a website operator having to make any elaborate changes to the source code of the website itself. Instead, the integration takes place through a container. In this way, the Tag Manager offers users without in-depth IT knowledge the possibility of embedding 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 systematising the data packets.

b) JENTIS and Consent Managers

(1) The **JENTIS DCP connects** in the browser to **other** installed **CMPs**, such as, for example, User Centrics, in order to receive the consent information from them and afterwards to manage further processing by itself. The use of the **JENTIS DCP** makes it possible to request consent in accordance with data protection

requirements, e.g. for the use of third-party tools such as Google Analytics. In the meantime, services to provide user preferences such as the **JENTIS DCP** may be permitted without requesting user consent.[34]

(2) Cookies and similar technologies in view of the DSK may be used, for example, for any additional functions of the basic website service if they are requested by the user, which is the case, for example, with the use of CMPs. JENTIS DCP processes the consent of other CMP providers.[35] The integration and availability of the CMP functions through JENTIS DCP may be reasonably regarded as **permissibly free of consent.**

(3) JENTIS does not process any long-term stored **user IDs of the CMP**[36] in cookies of the CMP when connecting the JENTIS DCP to another installed CMP. Since JENTIS cannot access other CMP cookies that the customer has integrated into its website, JENTIS stores a Consent ID on the server side to fulfil the logging obligation of user consent according to Art. 7 (1) GDPR and to fulfil any requests for information from data subjects. As an external service provider, JENTIS does not have the possibility to store the user preferences for the CMP settings in a cookie, which is different from what the German Data Protection Conference (DSK) argues in its Telemedia Guidance.[37] Therefore, the processing of the Consent ID can be classified as "strictly necessary" according to Art. 5 para. 3 p. 2, var. 2 ePrivacy Directive or § 25 para. 2 no. 2 TTDSG.

c) JENTIS Essential Mode / Fall-Back-Solution

The JENTIS Twin Server technology enables the effective use of website data in both situations - with explicit user consent (tracking mode) and when user consent is not available (as a fall-back solution - JENTIS Essential Mode). Companies can configure the "JENTIS Essential Mode" as a fallback solution for first-party tracking in such a way that the application of the exceptions to the consent requirement for terminal equipment access are implemented in a compliant and effective manner. This enables "usage analysis" to a reduced extent without user consent if the user does not click on the cookie banner at all or does not give consent. This is demonstrated using an example configuration for the JENTIS Essential Mode **(aa)** based on the requirements of supervisory authorities **(bb).**

(1) Subject to any future statements by supervisory authorities or case law to the contrary, the application of the exception to the consent requirement in Art. 5 para. 3 sentence 2 ePrivacy Directive or § 25 para. 2 no. 2 TTDSG is ensured with the corresponding configuration of JENTIS.
By using first-party data and **minimising** the **data parameters to** what is technically required or **strictly necessary**, the customer can track user data in Essential Mode or **as a fall-back solution** if the user does not give consent. The resilience of the exception according to § 25 para. 2 no. 2 TTDSG for the necessary access to

[34] Art. 29-Data Protection Working Party, WP 194, Opinion 04/2012 on the exception of cookies from the consent requirement, S. 7 f., ICO, Guidance on the use of cookies and similar technologies, S 37.
[35] DSK, orientation guide for telemedia providers, 2021, S. 21.
[36] Cf. to this DSK, orientation guide for telemedia providers, 2021, p. 26.
[37] DSK, orientation guide for telemedia providers, 2021, p. 26.

the terminal equipment in the form of a first-party cookie requires that the "Essential Mode" has been activated by **JENTIS** and is **configured** in a certain way (cf. pt. III. 2. c. aa.).
In the starting point, the fact that the first-party cookie is used **multifunctionally** by JENTIS because it serves several **different purposes** does not prevent the application of the exception provisions.[38]

(2) The **delivery** of the **JENTIS first-party cookie** based on the server request of the user's browser to the JENTIS server requires access to the terminal equipment capacities of the user's browser.
The **storage** of a **first-party cookie** and a randomly generated **client ID** in the **server response** of the JENTIS server **serves** to recognise the terminal equipment in order to enable a **reductive** and **substitutive filtering** of **data streams** with the help of server-side tagging before they are forwarded to third-party providers such as Google or Facebook. This prevents the loss of control in the use of tracking applications from the outset and enables **lawful data processing.**

(3) The **reduction** and **modification** of the **data parameters** for server-side tracking, which are queried in the course of user communication with the website (cf. point III. 1.), carried out by the JENTIS Twin Server technology, can also be justifiably **based** on the **exception from the consent requirement** pursuant to Art.5 (3) sentence 2 Var. 2 ePrivacy Directive and §25 (2) No. 2 TTDSG, in line with the opinion of the European Data Protection Supervisor (**EDPS**).
The **EDPS** has published a **"toolkit"** for **determining** the **"necessity"** of measures in accordance with Art. 52 (1) CFR.[39]

> *"[...] 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 processing personal data. [...]"*

According to media information, these **criteria** can also **serve** as guidance for the **interpretation** of the **term "necessity"** according to Art. 5 para. 3 sentence 2 ePrivacy Directive, according to the view of the data protection organisation "La Quadrature du Net". 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.[40] Therefore, it is also correctly argued in the **literature** that the checklist can be used for the determination of "strict necessity" in Art. 5(3) sentence 2 ePrivacy Directive and § 25(2) no. 2 TTDSG.[41]

[38] DSK, orientation guide for telemedia providers, 2021, p. 24.
[39] EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: a toolkit, 2017, p. 2.
[40] EDPB, Guidelines 2/2019 for the processing of personal data pursuant to Article 6(1)(b) of the GDPR in the context of the provision of online services to data subjects, V2.0, p.9, fn. 19.
[41] Hense, in: Taeger/Pohle, Computerrechts-Handbuch, 2022, 37. Ed., Projektspezifischer Datenschutz, para. 112.

Subject to future case law and regulatory positioning, the **methodology** can form a basis for the activation of selected functionalities on websites and **counteract** the **legal uncertainty** described in point II 1. b. above.

According to the EDPS, **necessity** implies the need for a combined, evidence-based assessment of the effectiveness of the measure in relation to the objective pursued and whether it is less intrusive than other options for achieving the same objective. The **checklist for the assessment of necessity** consists of **four** consecutive **steps.** Each step corresponds to a set of questions that facilitate the assessment of necessity.[42]

(4) The following is an **example configuration** for **JENTIS Essential Mode** that we believe, based on the application of the EDPS Necessity Toolkit to interpret necessity, reasonably justifies the use of tracking proxy technology as **"strictly necessary"** without the availability of user consent.

aa) Example configuration: statistical analysis of user behaviour on websites with Google Analytics through JENTIS DCP

- **Step 1 EDPS Necessity Toolkit:** The detailed factual description of the technical functional principle for cleaning the tracking data of third-party services such as Google Analytics and reducing the user data as well as the definition of purpose, which is required for the EDPS Toolkit to determine the necessity of the terminal equipment access, has been provided (cf. point III. 1).
- **Step 2 EDPS Necessity Toolkit:** The answers to the questions required for step 2 of the EDPS Toolkit to determine the scope of the intensity of intervention of the JENTIS DCP have also been provided in view of the detailed description of the individual data processing steps (cf. point III. 1.).
- **Step 3 EDPS Necessity Toolkit:** As step 3 of the EDPS Toolkit, the objective of a fundamental statistical analysis of website usage behaviour was identified as a use case in order to optimise, improve and further develop digital offerings in accordance with the state of the art in the exercise of the entrepreneurial freedom guaranteed by Art. 16 (1) of the EU Charter of Fundamental Rights. According to the EDPS, Art. 23 GDPR 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 Art. 23 (1) (i) GDPR, this also includes the protection of the rights and freedoms of other persons, i.e. also of legal persons and their entrepreneurial freedoms to be taken into account according to Art. 16 (1) CFR.
- **Step 4 EDPS Necessity Toolkit:** In accordance with Step 4 of the EDPS Toolkit, specific aspects for the **following example configuration** of the **Essential Mode** of **JENTIS** were taken into account when checking the necessity:
    - **Modification of the client ID of Google Analytics:**

[42] EDPS, Assessing the necessity of measures restricting the fundamental right to protection of personal data: a toolkit, 2017, p. 10.

- The client ID/user ID of Google Analytics, which enables a unique assignment of the terminal equipment, must be completely modified, i.e. replaced by a fictitious client ID/user ID.
- The JENTIS User ID is stored as a first-party cookie in the user's browser via the client's domain. The processing of the user ID assigned by JENTIS itself is the only reference for the recognition of the user's browser.
- According to the BGH, a randomly generated number (**cookie ID**) stored in cookies, which is assigned to the user's registration data as **terminal equipment information**, constitutes a **pseudonym** within the meaning of §15 (3) of the German Data Protection Act (TMG), whereby the BGH still referred to the legal definition in § 3 (6a) BDSG (old version).[43]
- The storage period of the JENTIS cookies should be set to a maximum of 13 months.
- The restriction required under Art. 4 No. 5 GDPR for effective pseudonymisation, it must be guaranteed that the additional information is stored separately and secured by technical and organisational measures ensuring that no allocation of the data to an identifiable person takes place. Regardless of whether the additional information may be a direct assignment or an assignment rule[44], the technical and organisational safeguarding is ensured by means of a **robust separation** of the system cluster **server instances** within the framework of **server-side tracking** by JENTIS.
- Processing by the JENTIS servers takes place on separate data instances, on which inventory data of users (e.g. e-commerce shop) may be stored.

- **IP address shortening:**
  - The user's IP address is shortened by the last octet on JENTIS servers; there is no communication between the user's browser and Google servers. In the case of **partial de-identification** of IP addresses by shortening the last octet after transmission of the complete IP address, **pseudonymisation** within the meaning of § 3 (6a) BDSG (old version) is to be assumed according to case law, as shown by a final decision of the Regional Court of Frankfurt on the web analytics service "Piwik".[45]
  - In doing so, the Court rejected the classification of the shortening of the IP address as a means of anonymisation, in particular because a website operator who has registration data from user accounts could make an assignment to identification features in real time at any time.
- **Removal of click IDs in URLs:**

[43] BGH, Judg. of. 28.05.2020 – I ZR 7/16 – cookie-consent II, para. 72; agreeing with regard to the GDPR Menke, K&R 2020, 650, 652; Baumgartner/Hansch, ZD 2020, 435, 436.
[44] Schwartmann/Weiß, draft code of conduct on the use of GDPR-compliant pseudonymisation, 2019, v1.0, p. 11.
[45] LG Frankfurt, Judg. of. 18.2.2014 – 3-10 O 86/12, para. 36; agreeing Weidert/Klar, BB 2017, 1858, 1859.

- Should the user access a customer website via the google.com search engine, the Google Click ID should be removed as a URL parameter ("gclid").

- **Modification of custom IDs:**
  - Similarly, data parameters that allow users to be uniquely identified, e.g. order IDs or lead IDs, are not processed by JENTIS, but are regenerated as a random product.
  - Here a random UUID (Universally Unique Identifier, a 128-bit number) is newly generated.
- **Modification of the User Agent:**
  - The user agent is deleted and replaced by a newly created user agent.
- **No fingerprinting:**
  - There shall be no combination of browser and device settings to identify and recognise users.
- **Purpose limitation:**
  - The purposes within the "Analysis" use case were limited to enabling the evaluation of published content and the user-friendliness of the website and to evaluate or improve the effectiveness of design decisions made on the website.
  - From the customer's point of view, the use of analytics should be limited to the generation of anonymous statistics.
- **No merging of IDs**
  - The JENTIS User ID is not merged with other user data such as a CRM ID or systems containing registration data.
- **Degree of blur for timestamps**
  - If a re-identification of a user or a singling-out of an individual user is possible based on the timestamp of a browser session, the JENTIS Twin Server technology can be used to replace the time information with fictitious values (fictitious timestamps).
  - Alternatively, with the help of the JENTIS Twin Server technology, a mere minimum blurring of the timestamps can be sufficient if there is a simultaneous minimum volume of users in a homogeneous group in the respective measured time period. The degree of blur for the timestamps (clusters on an hourly or minute basis) depends on the achievement of a homogeneous minimum number of users, i.e. a group of users who share the same attributes.

bb) Requirements of the supervisory authorities

(1) Irrespective of this, **no other result** is reached even when **applying** the **interpretation criteria** of the **DSK** for "strict necessity" (cf. point II. 1. b.) and the **CNIL** for the use of tracking proxies.
(2) The **strict requirements** of the DSK on the resilience of the exception for the use of **user IDs** stored in cookies (cookie IDs) are fulfilled on the basis of the functional principle of the Essential Mode of JENTIS:

- First of all, the DSK does not exclude the resilience of the exception in Art 5 (3) sentence 2 ePrivacy Directive and § 25 (2) no. 2 TTDSG for the audience measurement and/or analysis of website visitor numbers per se.[46]
- The time of storage of the session cookie and the reading of the client ID takes place in the course of the delivery of the website after interaction with the cookie banner.
- According to the above example configuration of Essential Mode for Google Analytics, all identifiers except the JENTIS user ID are reduced and modified. The first-party cookie is stored in the user's browser via the customer's domain.
- The storage period of first-party cookies can be set individually depending on the risk affinity either for a few minutes - individual visits (sessions) can then no longer be merged - or up to 24 months. According to the guidance of the German DSK, the criterion of the storage period is only one of several criteria and is not alone decisive for the legal assessment of "strict necessity".[47]
- Access to the terminal equipment is exclusively carried out by the servers of JENTIS as the processor. There is no client-side terminal equipment access by servers of Google or other third-party providers.
- In particular, if JENTIS is configured accordingly, the requirement of Art. 5 (3) sentence 2 of the ePrivacy Directive or § 25 (2) no. 2 of the TTDSG "telemedia service explicitly requested by the user" is also met. This is because, in line with the opinion of the DSK, the interests of the users of the website are taken into account first and foremost. The interests of the third-party providers due to the modification of data parameters are not taken into consideration. The interests of those affected are strengthened by the following aspects:
    - Preventing direct access by third parties to users' terminal equipment;
    - Access restrictions and control over the sharing of data with third-party providers; and
    - Ensuring legal compliance.

(3) Finally, JENTIS also meets the requirements of the French supervisory authority (CNIL) for proxy solutions when using tracking services, which, as far as can be seen, is the first European authority to recommend the use of proxy solutions for the use of Google Analytics.

- no transmission of the user's full IP address to servers of tracking services.
- The client IDs and user IDs assigned by third-party providers are completely replaced by the JENTIS server.
- According to the example configuration for Google Analytics, the browser and device information does not allow any identification by the third-party providers due to the created artificial values, especially for the user agent. In this way, fingerprinting can be prevented. The algorithm that performs the substitution of the browser information ensures a sufficient level of collision (i.e. a sufficient probability that two different identifiers provide an identical result after modification).

[46] DSK, Orientation guide for telemedia providers, 2021, p. 22.
[47] DSK, Orientation guide for telemedia providers, 2021, p. 26 f.

- Referrers can be deleted (note: if the referrer is removed, the quality of the analysis suffers).
- Any tracking parameters contained in the collected URLs can be individually deleted or replaced (e.g. the "UTM parameters", but also the URL parameters that enable the internal routing of the website).
- The client ID assigned by the tracking proxy to recognise the browser user or deterministically communicated IDs (CRM, unique ID) do not allow cross-site or cross-device recording of user behaviour.
- All user data that could enable re-identification by tracking providers will be deleted.

cc) Interim result

In summary, it can be stated that due to the following aspects, the exemption from the consent requirement pursuant to Art. 5 para. 3 sentence 2 var. 2 ePrivacy Directive and § 25 para. 2 no. 2 TTDSG applies when using the Essential Mode of JENTIS:

- Prevention of direct access by third parties to the user's terminal equipment
- Complete control over individual data points
- Reduction or modification of data points
- Access restrictions and control over data sharing with third parties
- Setting conditions for data sharing
- Ensuring legal compliance.

The corresponding application of the JENTIS Twin Server technology impedes further the assignment of a terminal equipment's browser to a usage profile as the only reference for the subsequent recognition of the browser and therefore represents an **effective measure** which, in the context of first-party terminal equipment access, represents the least intrusion into the fundamental rights from Art. 7 and Art. 8 para. 1 EU Charter of Fundamental Rights of website visitors.

Insofar as an appeal to the exception provision in Art. 5 para. 3 sentence 2 of the Privacy Directive or Art. 25 para. 2 of the TTDSG is possible, the consent of the users is not required. Nevertheless, it is mandatory to check whether the **legal basis of Art. 6 para. 1 sentence 1 lit. f) GDPR** is relevant for the respective service. For the required **documentation** of the assessment of interests according to Art. 6 (1) sentence 1 lit. f) GDPR [EDPB, WP 260, Annex], **a so-called LIA** (**Legitimate Interests Assessment**) should be carried out in accordance with the configuration of the JENTIS DCP by the customer in order to be able to provide evidence of the assessment of interests in the individual case and to ensure **compliance** in the supply chain. JENTIS can provide the customer with a Legitimate Interests Assessment for the example configuration of the Essential Mode.

3. Assessment of transmissions of newly generated client IDs to third parties

(1) Further processing operations that follow the terminal equipment access by JENTIS servers are the server-side transfers of the cleaned tracking data to third-party providers such as Google.
Neither the client ID assigned by Google nor the IP address of the user is transmitted. When the JENTIS server communicates with third-party providers such as Google, only the cleaned tracking data - the newly generated client ID, the IP address of the website server, the modified user agent and the modified order ID - are transmitted (see point III. 1.).
The transmission to third-party providers such as Google after modification of the tracking parameters can be based on the legal basis in Art. 6 para. 1 sentence 1 lit. f) GDPR if a **legitimate interests assessment** is carried out for the customer-specific use cases.

(2) The creation of **modified and fictitious data** at **random** from real raw data **corresponds** to the creation of **hash values** , as far as the modification of data can be classified as a measure of **pseudonymisation**.

- Pseudonymisation is a suitable privacy pattern within the framework of "Privacy by Design"[48] and can be applied to "JENTIS" at the level of processing and before passing it on to third-party providers.. According to the BGH, a randomly generated number (cookie ID) stored in cookies, which is assigned to the user's registration data as terminal equipment information, already constitutes a pseudonym within the meaning of §15 (3) of the German Telemedia Act (TMG), whereby the BGH still refers to the legal definition in the old version of § 3 (6a) German Data Protection Act.[49] Consequently, the same must also apply to other identifiers such as device IDs, IDFA, GAID and universal IDs.
- **ENISA** (European Union Agency for Cybersecurity) describes artificially generated data ("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 person or to the "real extent of a data parameter to be assessed".[50] In this context, synthetic data may also constitute personal data, but modified in such a way as to limit the possibility of re-identifying individuals.[51]
- According to **ENISA**, such "**modified data**" can be considered as **privacy enhancing technology** and in this sense can be used as a measure of pseudonymisation.[52] According to **ENISA**, such

[48] Cf. BGH, Judg. of. 15.5.2018 – VI ZR 233/17 para. 26.
[49] BGH, Judg. of. 28.05.2020 – I ZR 7/16 – cookie-consent II, para. 72; agreeing with regard to the GDPR Menke, K&R 2020, 650, 652; Baumgartner/Hansch, ZD 2020, 435, 436.
[50] ENISA, Data Protection Engineering, 2022, p. 17.
[51] ENISA, Data Protection Engineering, 2022, p. 17.
[52] ENISA, Data Protection Engineering, 2022, p. 10.

modifications primarily serve the **confidentiality** of the **processing**,[53] which has the character of "additional measures" in technical and organisational terms within the meaning of Art. 32 GDPR.

- When using JENTIS for a Use Case, e.g. website analysis, the recognition of the user is possible via the **JENTIS user ID** 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 customer-specific IDs are **replaced**, i.e. **modified**, **by artificial values** after appropriate configuration of the JENTIS DCP, the transmitted data records have no personal reference from the recipient's point of view, because the assignment rule via the JENTIS user ID to a terminal equipment lies exclusively with JENTIS and website operators. Only JENTIS as the processor and the website operator, but not third-party providers 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 **modification of real raw data** such as the client ID or user ID assigned by third-party providers is to be classified as pseudonymisation within the meaning of Art. 4 No. 5 of the GDPR **under the same conditions** as the **creation** of **hash values** from real raw data.[54] 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.

(3) The **restriction required** by Art. 4 No. 5 GDPR, that the **additional information is stored separately** and secured by technical and 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 newly generated Client IDs and Order IDs of the third-party providers,[55] according to the described technical operating principle, given the system architecture of JENTIS, a robust separation of the data instances is given, which excludes an assignment for third-party providers.

(4) As far as can be seen, third-party providers such as Google only receive a **client ID newly generated** by JENTIS in the course of the outlined data transfers after the terminal equipment 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 allocate the information provided **about the usage behaviour** of website visitors.

---

[53] Cf. ENISA, Data Protection Engineering, 2022, p. 17.
[54] Cf. on hashing as a valid measure for pseudonymisation Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, S. 26; ENISA, Pseudonymisation techniques and best practices, 2019, S. 33; ENISA, Data Pseudonymisation: Advanced Techniques & Use Cases, 2021, S. 12; Artikel 29-Data Protection Working Party, WP 216, Opinion 05/2014 in Anonymisation Techniques, S. 20.
[55] Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, S. 11 f.

(5) Likewise, **no access to** the **JENTIS DCP** by **third-party providers** such as Google is possible on the basis of the technical documentation provided. The user's **browser does not communicate** directly **with third-party providers**. 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 can still be assumed if only a third party has the allocation rule for the transmitted pseudonymous data records, but there is no legal possibility for access to identification features.[56]

(6) In line with the ECJ's view,[57] the transfer of the cleansed tracking data is to be classified as a downstream processing stage falling within the scope of the GDPR (cf. point II. 2.). Due to the protective measures taken - removal of the IP address, allocation of newly generated values for the client ID and order ID, for which Google does not have an allocation rule - the **legal basis** pursuant to **Art. 6 (1) sentence 1 lit. f) of the GDPR** 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 of Art. 6 para. 1 sentence 1 lit. f) GDPR** is relevant. A **so-called LIA (Legitimate Interests Assessment)** should be carried out for the required **documentation** of the balancing of interests according to Art. 6 (1) sentence 1 lit. f) GDPR[58] in order to be able to provide proof that the balancing of interests has been conducted. JENTIS can provide customers with a Legitimate Interests Assessment for an example configuration of the Essential Mode.

IV. Summary of the evaluation results

As a result, when using the **JENTIS SaaS solution** for the implementation of third-party tracking tools such as Google Analytics, the described **legal uncertainties** (cf. point II.) can be **eliminated** with the appropriate configuration.
It remains to be said: The locally and **regionally differing views** of courts and supervisory authorities on the use of tracking proxy solutions to enable the lawful use of tracking services, as well as the individual compliance requirements **in individual cases**, can be fully **taken into account** with the help of the JENTIS Twin Server technology.

With its server-side tracking technology, **JENTIS enables** a **long-term** and **sustainable** strategy, **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 data processing within the scope of tracking applications 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 legal requirements at short notice.

[56] Cf. also Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3. ed. 2020, Art. 4 para. 12.
[57] ECJ, Judg. of 15.06.2021 - C-645/19 - One-Stop-Shop, para. 74.
[58] EDPB, Guidelines on transparency under Regulation 2016/679, WP 260, rev.01, Annex.

By using JENTIS, website operators can benefit from the **economic advantages** of their own first-party data **without endangering** this data or the respective corporate **compliance** in legal terms through **uncontrolled** and **intransparent processing** on the part of third-party providers.

V. Recommendations for the operation of the JENTIS DCP

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

- Evaluation of the functionality through a software demo or this memorandum;
- Configuration of the JENTIS DCP by customers;
- Required **documentation** of the balancing of interests according to Art. 6 para. 1 p. 1 lit. f) GDPR[59] by means of **a LIA** (Legitimate Interests Assessment), in order to fulfil the accountability and documentation obligations for the balancing of interests that has taken place; JENTIS can provide customers with a Legitimate Interests Assessment for an example configuration of the Essential Mode.
- Transparent information in the privacy policy of the website;
- Opt-out options for users through automated systems such as opt-out links, which are specifically pointed out in the privacy policy or the JENTIS CMP;
- Conclusion and documentation of data processing agreement with JENTIS;
- Conclusion and documentation of the accompanying data protection agreements (data processing, joint controller or controller-2-controller agreement with third-party providers).

[59] EDPB, Guidelines on transparency under Regulation 2016/679, WP 260, rev.01, Annex.