Data Protection Memorandum

Working translation from German

JENTIS GmbH

Author

Tilman Herbrich

Date of document

01 August 2024

Contact person:

Dr. Mira Suleimenova

Project:

Data protection assessment of the core components of the JENTIS Software as a Service (SaaS) solution

Executive Summary

JENTIS GmbH (“ **JENTIS** ”) requests an assessment for the data protection evaluation of the core components of the JENTIS Data Capture Platform (“ **DCP** ”).

As a Privacy Enhancing Technology , JENTIS DCP offers a sustainable solution to ensure data quality, complete control over one's own first-party data and "data protection" compliance in the supply chain and enables customers to flexibly configure the server-side tracking solution in order to take into account the volatility of the respective individual risk situation of companies **(A.)** .

This memorandum outlines the legally compliant requirements, authority practice and case law for the collection of tracking data from consented and non- consented users as well as for the transfer of data points to third-party systems for the use of analysis and marketing functionalities according to the law, official practice and case law, and outlines the measures to be taken to ensure an adequate level of data protection **(BI)** . In particular, JENTIS offers the JENTIS Essential Mode as a fall-back solution, a way of reducing user data to a minimum if consent is not given, so that, depending on the risk affinity of companies, exceptions to the consent requirement for full reach measurement can be justified **(BI3.)** .

Individual configuration options make it possible to ensure data protection compliance by implementing the requirements of the European Data Protection Board (“ **EDPB** ”) for Privacy by Design and Privacy by Default **(B.II.1.)** .

When using the JENTIS DCP, TCF v2.2, continuous compliance can be ensured throughout the use of certified analysis and marketing tools **(B.II.2.).**

In the case of the use of third-party services from a third country without an adequacy decision by the EU Commission or potential data transfers from the USA to corresponding third countries, such as when using Google DV 360, the JENTIS DCP can be used to ensure a synthesis of the user's data parameters as an effective means of pseudonymisation in accordance with the recommendations of the EDPB. The implementation of valid pseudonymisation is to be qualified as a technical mitigation of any access risks by security authorities as part of the implementation of a "Transfer Impact Assessment" in accordance with Section 14 of the standard contractual clauses **(B.II.3.)** .

Best practices for companies serve as recommendations for the legally compliant use of the JENTIS DCP, which are designed in the form of a checklist **(B.III.)** .

Data Protection Memorandum

Working translation from German

JENTIS GmbH

SPIRIT LEGAL®

Table of contents

Data Protection Memorandum

Working translation from German

JENTIS GmbH

A. Facts

(1) With the Data Capture Platform (“ **DCP** ”), JENTIS offers a multi-component, server-side tracking technology hosted in Germany or optionally in Europe that can be used to significantly increase data quality and capture high-quality first-party data. The increase in data quality is achieved by the fact that data from website users can be processed in a **first-party context,** regardless of ad blockers and tracking protection mechanisms [1]in third-party systems such as Google Analytics or Adobe Analytics, using a unique **server-side tracking technology** .

(2) The JENTIS DCP offers **three** main **advantages** :

- **Quality:** The JENTIS DCP enables marketing teams to allocate budgets more efficiently, increase campaign profitability and improve return on investment for marketing campaigns by enabling data protection through privacy by design and configuration options. The JENTIS DCP orchestrates data by simplifying the process of data collection, management and meaningful data sharing with third parties, thus promoting efficient workflows.
- **Controls:** With the JENTIS DCP, website operators regain control over the collection of their own user data points. Data can be processed in full by users who have given their consent, but also to a lesser extent by users who have refused consent, in accordance with data protection regulations. The JENTIS DCP can be configured to suit the specific needs of the customer and adapted to individual requirements.
- **Privacy Enhancing :**
    - The JENTIS DCP enables **legally compliant handling** of the integration of third-party analysis and marketing services. JENTIS offers the technical possibility of streaming certain data selected by the website operator in the first-party context to JENTIS servers and transmitting it from there to various other data recipients, so that the Website operator has the opportunity to directly influence the data supply chain and protect their users' data. .
    - The JENTIS DCP uses **server-side tagging to enable** a reducing and substituting filtering of data streams before they are forwarded to third-party providers such as Google or Facebook. When the JENTIS DCP is used, third-party tags implemented in the website's source code such as JavaScripts , iFrames and image pixels are modified in such a way that neither direct access to the end device nor direct transmission of user data such as the IP address and user IDs as part of a direct server request from the user's browser to third-party servers takes place. In this way, a direct connection between the user's browser and the third-party provider is avoided from the outset.
    - The JENTIS DCP enables the **synthesis** of user data. Synthetic data at a basic level is artificially generated data that is created from the original data and preserves the statistical properties of this original data, but without any reference to an identified or identifiable person.[2]

(5) With the help of the JENTIS DCP, the third-party cookie phase -out announced by Google can be effectively mitigated without loss of reach. For the future necessary collection, processing and activation of first-party

[1] E.g. ITP of the Safari browser and ETP of Firefox.
[2] EDPS, techsonar 2021-2022, p. 10 ; López/ Elbil , European Law Blog, On synthetic data: a brief introduction, 2022 .

data in advertising ecosystems as the most important step towards successful online marketing, JENTIS offers Utiq as a deterministic and persistent ID solution, a legally compliant and valid partnership for the monetization of data and its attribution to measure the success of advertising campaigns.[3]

(6) The core elements of the JENTIS SaaS solution include the following system components of the product description and system architecture (see the enclosures below):

- JENTIS Container Manager and Tag Manager
- JENTIS Consent Manager
    - Includes Essential Mode
- JENTIS Tool Connector
- JENTIS Tracker
- JENTIS Server Suite and Twin Server

(7) JENTIS processes user data on behalf of and in accordance with the configuration of the processing systems made by the website operator and does not process any user data for its own purposes. JENTIS provides a data processing agreement in accordance with Art. 28 GDPR.

(8) Additional and enhanced features of the JENTIS SaaS solution and aspects of IT security are not covered by this evaluation.

B. Legal analysis

(1) Given inadequate industry solutions for server-side tracking and the lack of practicality to meet the requirements for explicit consent for third country transfer communicated by supervisory authorities **(I.)** , there is a growing need for long-term and sustainable strategies for the lawful and successful use of data by third parties with global infrastructures.

(2) Middleware concepts such as the JENTIS SaaS solution represent a solution for the integration and risks in the area of website tracking. **JENTIS** enables **flexible configuration** of the SaaS solution in order to take into account the volatility of the respective **individual risk situation** of companies. In this way, the JENTIS twin server technology enables Companies to ensure compliance with legal **requirements** in the **supply chain when using third-party tracking technologies (II.).**

I. Data protection classification of tracking via the JENTIS DCP

1. Data collection options via JENTIS DCP

JENTIS specializes in 1st party data capturing using server-side tracking, which integrates data protection and tracking on a single platform. The solution replaces conventional tag management systems by mirroring user sessions on the server side (twin browser technology). This enables companies to collect data in a legally compliant manner, process it and integrate it with various marketing and analysis tools, allowing marketers and analysts to collect high-quality data from different channels (such as different websites or e-commerce shops) and use it in their existing systems. The ability to negate ad blockers and tracking

[3] See Whitepaper „Beyond the 3rd Party Cookie. The Revolution of the Marketing Infrastructure", p. 4 ff.

preventions also increases the amount of data. The company always retains complete control over the data, which opens up a new level of data sovereignty.

a) JENTIS Container and Tag Manager2

(1) The JENTIS Container ensures that an independent system is made available for each customer and that there is no connection with other customers. The JENTIS Tag Manager is a system that ensures orchestration of tags from third-party systems and structured loading depending on user preferences when selected in the Consent Management Platform (" **CMP** "). Depending on the customer configuration of the tag management system, the JENTIS Tag Manager can either be loaded synchronously with the CMP or asynchronously only after consent has been granted.

(2) Due to the implementation of a script in a website, the JENTIS Container and the JENTIS Tag Manager are run in parallel by default when the website is accessed, i.e. synchronously with the JENTIS CMP (see point I. 2.b.). Loading the tag management system enables the subsequent activation and management of additional program codes if the user gives their consent. Without the user's consent, no separate storage of user IDs or targeted access to the end device takes place.

In addition, the JENTIS Container and JENTIS Tag Manager allow users' data parameters to be exchanged in a specific order, in particular by organizing and systematizing the data packets.

To load the JENTIS Container and JENTIS Tag Manager, a user's browser sends an https request to the web server's domain, transmitting the user's IP address as well as system and browser information to the website operator.

(3) Unless otherwise provided by case law, loading the JENTIS Container and JENTIS Tag Manager in the server response can be based on the exception in Section 25 Paragraph 2 No. 1 TTDSG (see point BI 3. a.). The JENTIS Container and JENTIS Tag Manager are used to route information and exchange data elements in a predetermined order - namely the activation of additional tags depending on the user preferences made in the connected CMP.

(4) Compared to other tag management systems, using the JENTIS Tag Manager does not involve any infrastructure risk with increased hurdles for justification as with using the Server Side Google Tag Manager. This is because using the Server Side Google Tag Manager embeds the company's entire tech stack in the Google Cloud Platform . This also means a loss of control over access to user data for non-critical tracking services with pure EU infrastructure.[4]

Even if the Server Side Google Tag Manager is not hosted on the Google Cloud Platform , the regulations for third country transfers must be observed, not only in the USA (see point II. 4.).

b) JENTIS Tracker, JENTIS Server Suite and JENTIS Twin Server

(1) With the JENTIS Tracker, website operators can collect first-party data based on the tracking configuration in the JENTIS Tracker via cookies in the first-party context and push it to the JENTIS Server Suite on the server side. The storage period of the JENTIS cookies can be set individually.

[4] Vgl. Mertens/Bielova/Roca/Santos et. al., Google Tag Manager: Hidden Data Leaks and its Potential Violations under EU Data Protection Law.

(2) The JENTIS Server Suite is the backbone of the JENTIS SaaS. JENTIS processes the data exclusively on documented instructions in accordance with the configuration of the JENTIS Server Suite by the website operator. With the standard and advanced functions of the JENTIS Server Suite, website operators can modify (anonymize and pseudonymize), enrich and/or synthesize users before forwarding them to third-party systems. The JENTIS Server Suite is based on Twin Server technology. The JENTIS Twin Server is an integral part of the JENTIS Server Suite. By duplicating the server request from a user's browser, data points can be completely removed, filtered, changed by modification or replaced with artificial values by means of synthesis. The original server request can either be completely deleted or retained.

After the user data from the server request has been processed, enriched, substituted, modified or synthesized, it can be streamed from the JENTIS Server Suite to third-party systems such as Google Analytics.

(3) Website operators can independently adapt the scope of processing to their own needs and legal requirements by individually configuring the JENTIS Server Suite. User data can be processed in accordance with the requirements for requesting legally compliant consent from consented users **(I.2.)** and/or to a reduced and modified extent in accordance with the Essential Mode feature without requesting consent - based on the exception in Section 25 Paragraph 2 TTDSG - from non- consented users **(I.3.)** .

The transfer of the substituted data streams to third-party systems can be based on the legal basis pursuant to Art. 6 (1) lit. f) GDPR as the processing downstream of the terminal device access if a documented balancing of interests is carried out **(I.4.)** .

2. Data collection from consented users

a) Consent requirement for device access for tracking for analysis and marketing purposes

(1) The consent requirement according to Article 5, paragraph 3, sentence 2 of the ePrivacy Directive (Section 25, paragraph 1 of the TTDSG in Germany) applies to any access to and storage of information from users' end devices – regardless of whether the access occurs within the framework of the same communication. [5]According to **the BGH** the application of Section 25 Paragraph 1 TTDSG **blocks** the **application** of other provisions of the **GDPR for this process due to the conflict of laws rule according to Article 95 GDPR,** e.g. Article 6 Paragraph 1 lit. f) GDPR. [6]According to the unanimous opinion of the ECJ and the BGH, it is **irrelevant for the existence of the consent requirement** whether the **terminal device information** is **personal data . or anonymous** data.[7]

(2) Case **law** so far, unanimously prohibits, among other things, the **use** of **tracking providers** on a website **without requesting** voluntary and informed **consent** .[8]

(3) Case law and regulatory positions have adequately defined **requirements** for the **design** of **consent banners** .[9]

[5] EDSA, Guidelines 02/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive, Rn. 26 ff.
[6] Vgl. BGH I ZR 7/16 – Cookie-Einwilligung II. Rn. 59.
[7] Vgl. EuGH, Urt. v. 01.10.2019 – C-673/17, Rn. 70.
[8]See Cologne Higher Regional Court, judgment of November 3rd, 2023 – 6 U 58/23 ; LG Frankfurt, judgment of October 19, 2021 – 3-06 O 24/21; LG Munich, judgment of November 29, 2022 – 33 O 14776/19.
[9]See ECJ, judgment of 1 October 2019 – C-673/17, para . 7 2 ; DSK, Guidance for providers of telemedia, 2022, p. 35 ff.

(4) According to ECJ case law, the website and app operator bears the **burden of proof for the validity of the consent** . This is because the ECJ has recently expressly imposed on the controller the burden of explanation and proof for the legality of the data processing in accordance with Art. 6 Para. 1 GDPR, based on Art. 5 Para. 2 GDPR.[10]

b) JENTIS Consent Manager

(1) The **JENTIS Consent Manager connects** in the browser to **other** installed **CMPs** such as OneTrust or User Centrics in order to receive the consent information from those systems and then control further processing accordingly. The use of the **JENTIS Consent Manager** enables the query of consent that complies with data protection requirements, e.g. . B. for the use of third-party tools such as Google Analytics.

However, services for providing user preferences such as the **JENTIS Consent Manager** may be permitted without requesting user consent.[11]

(2) According to f the DSK, cookies and similar technologies may also be used, for example, for any additional functions of the basic website service if these are requested by the user, which is the case,when using CMPs. [12]JENTIS DCP processes the consent of other CMP providers in order to enable a differentiated connection to other third-party tools based on the user's consent decision. The integration and provision of the functions of the CMPs by JENTIS DCP is justifiable **and permissible** to be viewed **without consent** in a reasonable manner .

(3) When connecting the JENTIS **Consent Manager** to another installed CMP, **no user IDs** stored long-term in the CMP cookies **are processed by JENTIS** . [13]Since JENTIS cannot access other CMP cookies that the customer has integrated into its website, JENTIS creates its own consent ID on the server side to fulfill the obligation to log user consent in accordance with Art. 7 Para. 1 GDPR and to give the website operator the opportunity to fulfill any requests for information from those affected . Contrary to what the DSK argues in its Telemedia Guidance, [14]JENTIS, as an external service provider, has no way of storing user preferences for the settings in the CMP in a cookie, but ensures that existing consent information is correctly displayed in its systems for downstream processing . The processing of the consent ID can therefore be described as “absolutely necessary” in accordance with Art. 5 Para. 3 S. 2, Var. 2 ePrivacy Directive or Section 25 Paragraph 2 No. 2 TTDSG (cf. Point I. 3.a.bb.).

3. Data collection from non- consented users

With the JENTIS Essential Mode **(b.), JENTIS offers** a way to reduce user data to a minimum if consent is not given, so that exceptions to the consent requirement can be made depending on the risk affinity of companies **(a.)** .

---

[10] ECJ, judgment of 4 May 2023 – C-60/22, paras . 53 et seq.; on consent, see most recently ECJ, judgment of 4 July 2023 – C-252/21, paras . 95, 152.
[11] 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 , p. 37 .
[12] DSK, Guidance for providers of telemedia, 2021, p. 21 .
[13] See DSK, Guidance for Telemedia Providers , 2021, p. 26 .
[14] DSK, Guidance for providers of telemedia, 2021, p. 26 .

a) Exceptions to the consent requirement for device access

There are two exceptions to the obligation to request consent for access to and storage of information from users' end devices during online tracking in Art. 5 Para. 3 Sentence 2 of the ePrivacy Directive, which have also been adopted unchanged in Section 25 Para. 2 of the TTDSG.

(aa) Necessity for implementation and facilitation of electronic communication

(1) For the technically necessary transmission of the user's IP address and other terminal device information such as browser and device information for HTTP-based applications, the exception in Section 25 Paragraph 2 No. 1 TTDSG is generally applicable.

(2) According to this, consent is not required if **technical storage** or access to terminal device information takes place for the purpose of **carrying out** electronic **communication . However, this is subject to the prerequisite that the sole purpose of the processing is** to carry out or facilitate electronic communication .[15] According to the European Data Protection Board and individual supervisory authorities , the exception in Article 5, paragraph 3, sentence 2 of the ePrivacy Directive/Section 25, paragraph 2, no. 1 of the TTDSG includes [16]:

- the ability to route information across the network, in particular by identifying 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.

bb) Absolute necessity to provide a desired service

(1) The **second exception** in Article 5 paragraph 3 sentence 2 of the ePrivacy Directive, according to which **access** to terminal device information **is absolutely necessary in order to provide** an information society service requested by the user , is in any case not relevant for the purposes of advertising and market research according to the judgment of the Federal Court of Justice (I ZR 7/16 – Cookie Consent II).

(2) According to **the opinion** of the **DSK**, the **interpretation** of the term **"strictly necessary"** when considering Recital 66 of the ePrivacy Directive, is a **restrictive** (narrow) **understanding** . The absolute necessity cannot therefore **be** based [17]on **economic considerations** for the implementation of a business model .

(3) The DSK places **stricter requirements on the robustness of the exception for the use** of **cookie IDs** (user IDs). Such storage is only absolutely necessary in **a few cases** , as many functions that require storage

[15] Art. 29 Data Protection Working Party, WP 194, Opinion 04/2012 on the exemption of cookies from the consent requirement, p. 3 f.
[16] Art. 29 Data Protection Working Party, WP 194, Opinion 04/2012, p. 3 f.
[17] DSK, Guidance for providers of telemedia, 2022, para . 76; Austrian VGH, judgment of 31 October 2023 – para . 2020/04/0024.

or access to terminal device information cannot 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 language or background color settings.

(4) In the view of the Data Protection Conference, the relevant **criteria** for determining **absolute necessity are** [18]:

- **Time** of storage – When may the reading and storage process take place?
- **Content** of the information – What information is stored and read?
- **Duration** of storage of information – How long is information stored on the end devices and for how long can it be read?
    - The storage period may only be as long as is necessary to implement the granular function of the telemedia service.
    - In principle, session cookies are more necessary than long-lasting cookies.
- **Readability** of information – Who can read and use information from the end device?
    - If information is stored on the user's device when using a telemedium, it must be technically ensured that this information can only be read subsequently by the operators of the respective website. One of the decisive factors here is the domain of a cookie, which determines who can read the information.
    - This is not the case with third-party services, so it must be ensured that third-party service providers only use the information read out for the website accessed by users.

(5) In the context of a **necessity test ,** related to **third-party tracking** , e.g. for user analyses, one will arrive at the conclusion with sufficient certainty that without modification of the tracking parameters there can be **no absolute necessity** according to Section 25 Paragraph 2 TTDSG, since third-party tracking always expands the circle of data recipients beyond the actual service provider.

As long as tracking carried out by the website and app operator themselves is possible with the same suitability without the use of third-party providers, taking into account the above-mentioned ECJ case law and the DSK's opinion on online tracking, the use of third-party providers will not be necessary.[19]

b) JENTIS Essential Mode as a fall-back solution

(1) Subject to any future position to the contrary by supervisory authorities or case law, JENTIS enables website operators to configure website tracking in such a way that the exception to the consent requirement in Art. 5 Para. 3 Sentence 2 ePrivacy Directive or Section 25 Para. 2 No. 2 TTDSG is applied in a legally compliant manner.

[18] DSK, Guidance for providers of telemedia, 2022, para . 93 f.
[19] DSK, Guidance for providers of telemedia, 2021, p. 27.

By using first-party data and **minimizing** data **parameters to** what is technically necessary or **absolutely necessary,** the customer can use the **Essential Mode feature to track user data as a fallback solution** if the user does not give their consent.

The validity of the exception pursuant to Section 25 Paragraph 2 No. 2 TTDSG for the necessary access to the end device in the form of a first-party cookie requires that the "Essential Mode" [20]within the **JENTIS DCP** is activated and becomes independent in a certain way through the customer. Below is an example of the configuration of the Essential Mode feature (see point (4) aa). By activating the Essential Mode feature, only the dashboard in the user interface of the account is adjusted. The website operator has full control over the system settings and configurations and must configure the JENTIS Server Suite independently.

In principle, the application of the exception provisions is not precluded by the fact that the JENTIS first-party cookie is used **multifunctionally, because it is used for several different purposes** .[21]

(2) The delivery of the **first-party cookie by JENTIS** to the JENTIS server based on the server request from the user's browser requires access to the end device capacities of the user's browser.

The storage of a **first-party cookie** in the **server response** of the JENTIS server together with a randomly generated **client ID serves** to recognize the end device as a **JENTIS tracker** (see point I.1.b.) in order to enable a reducing and substituting **filtering** of **data streams** before they are forwarded to third parties such as Google or Adobe. This prevents the loss of control when using tracking applications from the outset and ensures **lawful Data processing**.

(3) The reduction and **modification** of the **data parameters** for server-side tracking, which are requested during user communication with the website, made possible by the JENTIS Twin Server technology , **can,** in accordance with the opinion of the European Data Protection Supervisor (" **EDPS"**), be justifiably **based on** the **exception to the consent requirement** pursuant to Art. 5 (3) Sentence 2 Var. 2 ePrivacy Directive and Section 25 (2) No. 2 TTDSG .

The **EDPS** has published a ' **toolkit** ' to **determine** the **assessment** of the **'necessity'** of measures in accordance with Article 52(1) of the Charter .[22]

According to media reports, the data protection organisation "La Quadrature du Net" also believes that these **criteria can serve as a guide** for the **interpretation** of the **concept** of " **necessity** " according to Article 5, paragraph 3, sentence 2 of the ePrivacy Directive . Likewise, in the " Guidelines 2/2019 " [23]on the interpretation of the concept of necessity, the **EDPB has referred to** the EDPS **toolkit** for the non-public sector **. Therefore** , [24]it is also correctly stated in the **specialist literature** that the checklist can be used to determine the "absolute necessity" in Art. 5 Para. 3 Sentence 2 ePrivacy Directive and Section 25 Para. 2 No. 2 TTDSG.[25]

---

[20] Essential fashion.
[21] DSK, Guidance for providers of telemedia, 2021, p. 24 .
[22] EDPS, Assessing the necessity of measures restricting the fundamental right to protection of personal data: A toolkit, 2017, p. 5 .
[23] EDPB, Guidelines 2/2019 on the processing of personal data pursuant to Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, V2.0.
[24] EDPB, Guidelines 2/2019 on the processing of personal data pursuant to Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, V2.0, p. 9, footnote 19 .
[25]Hense, in: Taeger /Pohle, Computer Law Handbook, 2022, 37. EL, Project-specific data protection, para . 112.

Subject to future case law and supervisory authority positions, the methodology can **form a** basis for the activation of selected functionalities on websites and **Counteract legal uncertainty described under point B** .

(4) According to the EDPS, necessity implies the need for a combined, evidence-based assessment of the effectiveness of the measure in achieving the objective pursued and whether it is less intrusive compared to other options for achieving the same objective. The **checklist for assessing necessity** consists of **four** consecutive **steps** . Each step corresponds to a set of questions that facilitate the assessment of necessity.[26]

aa) Example configuration for Essential Mode

Below we propose an **example configuration** for the **Essential Mode** of **JENTIS** , which, in our opinion, based on the application of the EDPS Necessity Toolkit for the interpretation of necessity, allows the use of tracking proxy technology to be justified in a reasonable manner as " **absolutely necessary** " without the need for user consent and with the acceptance of residual risks.

- **Step 1 EDPS Necessity Toolkit:** The detailed factual description of the technical functional principle for cleaning up tracking data from third-party services such as Google Analytics and reducing user data as well as purpose definition required for the EDPS toolkit to determine the necessity of terminal device access has been provided.
- **step 2 EDPS Necessity Toolkit** : The questions required for step 2 of the EDPS Toolkit to determine the scope of the intervention intensity of the JENTIS DCP have also been answered in view of the detailed description of the individual data processing steps.
- **step 3 EDPS Necessity Toolkit:** As step 3 of the EDPS toolkit, the objective of a basic statistical analysis of usage behavior on the website, along with a reduced measurement of conversions , was identified as a use case in order to optimize, improve and further develop digital offerings in line with the state of the art in accordance with the entrepreneurial freedom guaranteed by Art. 16 Para. 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 can legitimately be restricted. According to Art. 23 Para. 1 lit. i) GDPR, 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 under Art. 16 Para. 1 of the Charter of Fundamental Rights.
- **Step 4 EDPS Necessity Toolkit:** JENTIS SaaS ensures that specific aspects for the necessity assessment according to step 4 of the EDPS Toolkit can be covered by the Essential Mode. In the **Example configuration** of the **Essential Mode** by**JENTIS** the following has been taken into account:
    - **Modifying the client ID of third-party services such as Google Analytics:**
        - The client ID/user ID of third-party services such as Google Analytics, which enables a unique assignment of the end device, must be completely synthesized, i.e. replaced by a fictitious, randomly generated client ID/user ID.

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

- The JENTIS user ID is stored as a first-party cookie via the customer's domain in the user's browser. The processing of the user ID assigned by JENTIS itself represents the only reference for recognizing 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 device information , represents a pseudonym** within the meaning of Section 15 Paragraph 3 of the Telemedia Act, whereby the BGH still referred to the legal definition in Section 3 Paragraph 6a of the BDSG (old version).[27]
- The storage period of JENTIS cookies in Essential Mode should be set to a maximum of 13 months.
- The restriction required by Art. 4 No. 5 GDPR that the additional information is stored separately and secured by technical and organizational measures that ensure that the data is not assigned to an identifiable person is implemented. Regardless of whether the additional information can be a direct assignment or an assignment rule, [28]the technical and organizational security is ensured by means of a **robust separation** of the system cluster **server instances** as part of **server-side tracking** by JENTIS.
- Processing by the JENTIS servers takes place on separate data instances, on which user inventory data (e.g. e-commerce shop) may be stored.

○ **Shortening the IP address:**

- 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 anonymization** of IP addresses by shortening the last octet after the full IP address has been transmitted, case law considers this as **pseudonymization within** the meaning of Section 3 Paragraph 6a of the BDSG (old version), as shown by a legally binding decision by the Frankfurt Regional Court on the web analysis service " Piwik ".[29]
- The court rejected the classification of shortening the IP address as a means of anonymisation, in particular because a website operator who has registration data from user accounts could assign it to identification features at any time in real time.

○ **Removing click IDs in URLs:**

- If the user accesses a customer website via the search engine google.com, the Google Click ID should be removed as a URL parameter (“ gclid ”) .[30]

○ **Modification of customer-specific IDs:**

- Likewise, data parameters that enable users to be uniquely identified, such as order IDs or lead IDs, are not processed by JENTIS but are generated as a random product.
- A random UUID (Universally Unique Identifier, a 128-bit number) is generated.

[27] BGH, judgment of 28 May 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.
[28] Schwartmann /Weiß, Draft for a Code of Conduct for the use of GDPR-compliant pseudonymization, 2019, v1.0, p. 11 .
[29]lg Frankfurt, judgment of 18 February 2014 – 3-10 O 86/12, para . 36; concurring Weidert /Klar, BB 2017, 1858, 1859.
[30] Testing Google Ads automatic tagging.

- **Modifying the user agent:**
  - The user agent is deleted and replaced by a newly generated user agent.
- **No fingerprinting:**
  - No combination of browser and device settings may be used to identify and recognize users.
- **Purpose reduction:**
  - The purposes of the "Analysis" use case were limited to enabling the evaluation of published content and the user-friendliness of the website and to evaluating or improving the effectiveness of the website's design decisions.
  - From the customer's perspective, the use of analysis should be limited to the creation of anonymous statistics.
- **No merging of IDs:**
  - The JENTIS user ID will not be merged with other user data such as a CRM ID or systems with registration data.
- **Blur levels for timestamps :**
  - If a user can be re-identified or a single user can be singled out based on the timestamp of a browser session, the time data can be replaced by synthesized values (fictitious timestamps) using the JENTIS Twin Server technology.
  - Alternatively, with the help of JENTIS Twin Server technology, a minimum level of blurring of the timestamps may be sufficient if there is a simultaneous minimum volume in the respective measured time period in a homogeneous group. The degree of blurring of the timestamps (clusters on an hourly or minute basis) in each individual case depends on the achievement of a homogeneous minimum volume of users, i.e. a group of users who share the same attributes.

bb) Requirements of the supervisory authorities

(1) In addition to the EDPS Toolkit, the **application** of the **DSK 's interpretation criteria** for 'strict necessity' (see point I.3.a.bb.) and the **CNIL's criteria** for the use of tracking proxies does **not lead to a different result** .

(2) The **DSK** 's **strict requirements** regarding the robustness of the exemption for the **use of user IDs** stored in cookies (cookie IDs) are met by applying the functional principle of JENTIS' Essential Mode:

- First of all, the DSK does not rule out the validity of the exception in Article 5 paragraph 3 sentence 2 of the ePrivacy Directive and Section 25 paragraph 2 no. 2 of the TTDSG for the measurement of reach and/or analysis of website visitor numbers per se.[31]
- The time at which the session cookie is stored and the client ID is read out takes place during the delivery of the website after interaction with the cookie banner.

[31] DSK, Guidance for providers of telemedia, 2021, p. 2 2 .

- According to the above example configuration of Essential Mode for Google Analytics, all identifiers with the exception of the JENTIS user ID are reduced and synthesized **.** 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 combined - or for up to 13 months. According to the DSK's guidance, the criterion of storage period is only one of several criteria and is not decisive on its own for the legal assessment of "absolute necessity".[32]
- Access to end devices occurs exclusively through JENTIS servers as the processor. There is no client-side access to end devices through servers from Google or other third parties.
- In particular, if JENTIS is configured accordingly, the requirement of Art. 5 Para. 3 Clause 2 ePrivacy Directive and Section 25 Para. 2 No. 2 TTDSG "telemedia service expressly requested by the user" is also met. In line with the DSK's view, the interests of the website users are primarily taken into account. The interests of third-party providers are not taken into account due to the modification of data parameters. The interests of the data subjects are strengthened by the following aspects:
    - Preventing direct access by third parties to users ' end devices ;
    - Access restrictions and control over the sharing of data with third parties
    - Privacy enhancement by minimizing user data parameters to prevent recognition and
    - Ensuring legal compliance.

(3) Finally, the **requirements** of the French supervisory authority (" **CNIL** ") for proxy solutions [33]when using tracking services can also be met with the help of the technical capabilities of JENTIS , 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. The BayLDA has endorsed this legal opinion.[34]

- no transmission of the user's full IP address to servers of tracking services.
- The client IDs and user IDs assigned by third parties are completely replaced by the JENTIS server.
- According to the example configuration of the Essential Mode for Google Analytics, the browser and device information does not allow identification by third parties due to the artificial values created, especially for the user agent. In this way, fingerprinting can be prevented. The algorithm that replaces the browser information ensures a sufficient level of collisions (i.e. a sufficient probability that two different identifiers will produce an identical result after modification).
- 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 recognize the browser user or deterministically communicated IDs (CRM, unique ID) do not allow cross-site or cross-device recording of user behavior.
- All user data that could enable re-identification by tracking providers will be deleted.

[32] DSK, Guidance for providers of telemedia, 2021, p. 2 6 f.
[33] CNIL, Mesure d'audience and transferts de données.
[34] BayLDA , 12th Annual Report 2022, p. 50 ff .

cc) Application of authority requirements to Essential Mode

(1) In summary, JENTIS Essential Mode enables website operators to rely on the exception to the consent requirement pursuant to Art. 5 Para. 3 Sentence 2 Var. 2 ePrivacy Directive and Section 25 Para. 2 No. 2 TTDSG due to the following aspects:

- Preventing direct access by third parties to users' end devices
- Complete control over individual data points
- Reducing or modifying data points
- Access restrictions and control over the sharing of data with third parties
- Setting conditions for data transfer
- Enabler of improving user privacy
- Ensuring legal compliance.

(2) The corresponding application of the JENTIS Twin Server technology makes it even more difficult to assign a browser of a terminal device to a usage profile as the only reference for later recognition of the browser and therefore represents an **effective measure as a privacy-** enhancing technology which, in the context of first-party terminal device access, represents the least interference with the fundamental rights of website visitors under Article 7 and Article 8(1) of the EU Charter of Fundamental Rights.

(3) The crucial question of what "absolutely necessary" should mean in the exceptions to the strict consent requirement under Article 5(3) of the ePrivacy Directive will be decided by the courts and not the legislature. In the new EDSA "Guidelines 2/2023 on Technical Scope of Art. 5(3) of ePrivacy Directive ", one still looks in vain for corresponding interpretation criteria, whereas the Austrian Higher Administrative Court, [35], has clearly rejected the "economic" interpretation of "absolute necessity" postulated by media companies.

Nor can it depend on a "technical necessity" of any kind, as Recital 24 of the ePrivacy Directive clearly supports the principle of technology neutrality. "Strictly necessary" is to be interpreted in line with the purpose of the regulation, which is the protection of privacy. Only an interpretation that focuses on the processing result can justify the use of privacy enhancing technologies. Access to end devices that is intended to serve the protection of privacy can therefore be considered permissible.

(4) If reliance on the exception under Art. 5 Para. 3 Sentence 2 of the Privacy Directive or Section 25 Para. 2 of the TTDSG is possible, the user's consent is not required. Nevertheless, it is essential to verify whether the **legal basis in Art. 6 Para. 1 Sentence 1 lit. f) GDPR** is applicable for the respective service. For the necessary **documentation** of the balancing of interests in accordance with Art. 6 Para. 1 Sentence 1 lit. f) GDPR [36], **a LIA (Legitimate Interests Assessment)** should be conducted in accordance with the configuration of the JENTIS DCP carried out by the customer in order to be able to provide evidence of the balancing of interests carried out in individual cases and to ensure **compliance** in the supply chain. JENTIS provides the customer with a Legitimate Interests Assessment for a sample configuration of the Essential Mode.

[35] Austrian Higher Administrative Court, judgment of 31 October 2023, Ref . Ro 2020/04/0024.
[36] EDPB, WP 260, Annex .

4. Transfer of substituted data to third-party systems via JENTIS Tool Connector

(1) **Downstream processing** , i.e. the processing that follows justified access to the end devices, such as the analysis of web and app usage in own and third-party systems, is not subject to the **scope** of the TTDSG, but to the **GDPR** . [37]For downstream processing, the legal basis of Art. 6 (1) GDPR must therefore be applied.[38]

(2) Further processing operations that follow the end device access by JENTIS servers include the server-side transmission of the cleansed tracking data to third-party servers such as Google.

The JENTIS DCP can be configured so that neither the client ID assigned by third parties such as Google nor the user's IP address are transmitted. When the JENTIS server communicates with third parties such as Google, only the cleansed tracking data - the newly generated client ID, the IP address of the website server, the synthesized user agent and the synthesized order ID - would be transmitted.

The transmission to third parties such as Google after modification of the tracking parameters can be justified on the legal basis of Art. 6 (1) sentence 1 lit. f) GDPR, if a Legitimate Interests Assessment is carried out for the customer-specific use cases.

(3) In addition to the usual data substitutions that lead to pseudonymization and anonymization, JENTIS SaaS also enables the technical possibility of synthesizing data. The creation of **synthetic data** from real raw data **corresponds** to the creation of data values based on a **random principle,** as far as the **classification of the modification as a** measure of **pseudonymisation** is concerned.

- Pseudonymization is a suitable privacy pattern in the context of "privacy by design" [39]and can be applied to "JENTIS" at the processing level and before passing 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 end device information, already constitutes a pseudonym within the meaning of Section 15 Paragraph 3 of the Telemedia Act, whereby the BGH based this on the legal definition in Section 3 Paragraph 6a of the BDSG (old version). [40]The same must consequently also apply to other identifiers such as device IDs, IDFA, GAID and universal IDs.
- The **ENISA** (European Union Agency for Cybersecurity) describes " **synthetic data** " in the context of data protection law as a new area of data processing in which data is processed in such a way that it realistically resembles real data (both personal and non-personal) but does not refer to a specific identified or identifiable person or to the "real extent of a data parameter to be evaluated".[41]
- According to **the EDPS, "** synthetic **data " can** be considered [42]as a privacy enhancing technology **and in this sense can be used as a pseudonymization measure.** According to **ENISA , synthesis**

[37]See ECJ judgment of 15 June 2021 – C-645/19 – One-Stop-Shop, para. 74 ; BT-Drs. 19/27441, p. 38 ; EDSA, Opinion 5/2019 on the interaction between the ePrivacy Directive and the GDPR, p. 23 .
[38] DSK, Guidance for providers of telemedia, 2022, p. 31 .
[39]See BGH, judgment of May 15, 2018 – VI ZR 233/17 Rn . 26.
[40] BGH, judgment of 28 May 2020 – I ZR 7/16 – Cookie Consent II , para . 72 ; agreeing with regard to GDPR Menke, K&R 2020, 650, 652; Baumgartner/Hansch, ZD 2020, 435, 436.
[41] Vgl . ENISA, Data Protection Engineering, 2022, S. 17 .
[42] EDPS, techsonar 2021-2022. S. 10 .

primarily serves to ensure the **confidentiality** of **processing** , [43]which has the character of "additional measures" in technical and organizational terms within the meaning of Art. 32 GDPR.

- In the case of use cases when using the JENTIS DCP, e.g. in website analysis, it is possible for website operators to recognize the user via the **JENTIS user ID**. As long as at least the "third-party client ID" and, ideally, other **tracking parameters** such as the user agent and any customer-specific IDs are **synthesized after the JENTIS DCP has been configured accordingly** , the transmitted data records do not contain any personal reference from the recipient's perspective because the assignment rule for the JENTIS user ID to an end device is solely managed by JENTIS and website operators. Only JENTIS as the processor and the website operator and not third-party providers such as Google, have the assignment rule - e.g. via the JENTIS user ID - for the pseudonymous tracking parameters. It can then be assumed that **pseudonymization is effective** 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 parties is to be classified as pseudonymization within the meaning of Art. 4 No. 5 GDPR [44]**under the same conditions** as the **creation** of **hash values from real raw data. As long as the artificial values** used in place of client IDs and user IDs are **irreversible** , the **collision-free nature** of the processed data parameters is **ensured and** the user's **IP address has been replaced** , taking into account the unanimous assessment of hash values, it can be assumed **that pseudonymisation complies with the GDPR in the absence of any conflicting positions or case law** .

(4) The restriction required under Art. 4 No. 5 GDPR that the **additional information is stored separately** and secured by technical and organizational measures that ensure that the data is not assigned to an identifiable person, **is implemented** during communication between 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, [45]according to the product description, given the system architecture of JENTIS, a robust separation of the data instances is provided, which excludes assignment for third-party providers.

(5) As far as can be seen, third-party providers such as Google only receive a **newly generated client ID from JENTIS following access to the end device in the data transmissions outlined above** , which does not match the client ID or user ID assigned by Google for Google Analytics and therefore does **not allow Google to link** the information provided **about the usage behavior** of website visitors.

(6) Similarly, **third parties** such as Google cannot access the JENTIS DCP based on the available technical documentation provided. There is **no** direct **communication** between the user's **browser and third parties** . As far as can be seen, there is no ruling other than the case law of the ECJ regarding the personal reference of IP addresses whether a personal reference can still be assumed if only a third party has the assignment rule for the transmitted pseudonymous data sets, but there is no legal possibility of accessing identification features.[46]

---

[43] Vgl . ENISA, Data Protection Engineering, 2022, S. 17 .
[44] Vgl. zum Hashing als valide Maßnahme zur Pseudonymisierung Schwartmann/Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymisation, 2019, v1.0, S. 26; ENISA, Pseudonymisation techniques and best practices, 2019, S. 33; ENISA, Data Pseudonymisation: Advanced Techniques & Use Cases, 2021, S. 12; Artikel 29-Data Protection Working Party, WP 216, Opinion 05/2014 in Anonymisation Techniques, S. 20.
[45] Schwartmann /Weiß, Draft for a Code of Conduct on the use of GDPR compliant pseudonymization , 2019, v1.0, p. 11 f .
[46]See also Klar/Kühling, in: Kühling/Buchner, DS-GVO/BDSG, 3rd edition 2020, Art. 4 para. 12.

(7) In line with the view of the ECJ, [47]the transmission of the cleaned tracking data is to be classified as a downstream processing phase that falls within the scope of the GDPR. Due to the protective measures taken - such as the removal of the IP address and the assignment of newly generated values for the client ID and order ID, for which Google has no assignment rule - the legal basis for the transmission can be **justifiably applied in accordance** with **Art. 6 (1) sentence 1 lit. f) GDPR, subject to any future case law to the contrary** .

However, it is imperative to verify whether the **legal basis in Art. 6 Para. 1 Clause 1 Letter f) GDPR** is applicable. For the necessary **documentation** of the balancing of interests in accordance with Art. 6 Para. 1 Clause 1 Letter f) GDPR, [48]**a LIA** (**Legitimate Interests Assessment)** must be conducted in order to provide evidence of the balancing of interests. JENTIS provides the customer with a Legitimate Interests Assessment for a sample configuration of the Essential Mode.

II. How JENTIS DCP helps eliminate legal risks

1. GDPR compliance through privacy by design and privacy by default

(1) **Privacy by Design** as a **concept was** introduced [49]in the course of the presentation of a scientific contribution on "Privacy Enhancing Technologies" (PET) by John Borking in 1995 , and developed into a systemic approach by Ann Cavoukian until 2010.[50] and is **internationally recognized** .

(2) During the product development of the JENTIS DCP, the building blocks for implementing the concept of Privacy by Design were incorporated in accordance with the EDPB Guidelines 4/2019 on Article 25 Data Protection by Design and by Default[51] This **(a.)** ensures the implementation of Privacy by Design principles and t**(b.)** enables the GDPR-compliant use of online marketing tools.

(3) JENTIS DCP as a SaaS product takes into account "Privacy by Design" strategies as guidelines to ensure that the implementation of the concept of "Privacy by Design" and "Privacy by Default" by the website operators (its customers) is available and possible. To this end, data-oriented strategies such as "minimize", "hide", "separate" and "abstract" as well as process-oriented strategies such as "inform", "control", "enforce" and "demonstrate" have been implemented.[52]

Based on these privacy design strategies, the objectives required by the EDPB can be fully achieved when using the JENTIS DCP with the appropriate configuration:

aa) Transparency

(1) In order to fulfill the objective of transparency, the data subject should be able to understand how personal data is processed so that they can understand and exercise their rights under Articles 15 to 22 of the GDPR. [53]The **principle of transparency is primarily implemented through easily accessible data protection**

[47] ECJ , judgment of June 15, 2021 - C-645/19 - One-Stop-Shop, paragraph 74 .
[48] EDPB, Guidelines on transparency under Regulation 2016/679, WP 260, rev.01, Annex .
[49] Borking, Privacy-Enhancing Technologies: The Path to Anonymity.
[50] Cavoukian, Privacy by design: the definitive workshop.
[51] EDPB-Guidelines 4/2019 on Article 25 Data Protection by Design and by Default.
[52] Vgl. Agencia Espanola Proteccion Datos (AEPD), A Guide to Privacy by Design 2019, S. 23 f.
[53] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 15.

information written in clear and plain language in accordance with Articles 12-14 of the GDPR (see Recital 39 of the GDPR).

(2) The design and default settings elements [54]required by the EDPB for the transparency principle can be fully implemented in the JENTIS DCP. Therefore, the obligation of **transparency** under the GDPR applies to three **core areas** that are of significant importance for the practical work and design of the JENTIS DCP:

- The **information** provided to the data subject .
- The **manner** in which controllers communicate with data subjects regarding their rights.
- Enabling the **exercise of data subject rights** .

(3) With the help of the JENTIS DCP, website operators have full control and knowledge of the data parameters captured from the user's end device and forwarded to third-party systems. Therefore, in accordance with Art. 12 ff. of the GDPR, the information obligations can be fully met.

bb) Lawfulness

(1) The processing of personal data must be based on a valid legal basis (Article 5 (1) (a) and Article 6 (1) GDPR). The measures and safeguards implemented should ensure that the entire processing cycle is consistent with the legal basis. The **design and default settings elements** for the principle of lawfulness [55]required by the EDPB can be fully implemented within the framework of the JENTIS DCP.

(2) Depending on the respective processing phase, the use of certain identifiers and the respective use cases, different legal bases for processing when using "JENTIS DCP" come into consideration, depending on whether it is a direct terminal device access (cf. I.2. and I.3. above) or a downstream processing phase (cf. I.4. above).

(3) Furthermore, if machine learning algorithms are used for use cases , there is no automated decision in the individual cases within the meaning of Art. 22 (1) GDPR, since there is no significant impairment of the fundamental rights of data subjects due to the avoidance of direct access by third-party systems.

cc) Purpose Limitation

(1) As a further **guiding principle** of privacy by design and default, the JENTIS DCP enables compliance with the purpose limitation principle as set out in Art. 5 (1) **lit. a) GDPR** if customer data from, for example, CRM systems is used according to a specific customer configuration, deviating from the default settings for connecting Audiences Tools via the JENTIS Tool Connector.

(2) JENTIS does not pursue any purposes of its own, but processes all data on instructions after the JENTIS DCP has been configured by the website operators, which are documented in the data processing contract and in the configuration settings.

(3) With the help of the JENTIS DCP, website operators can ensure the necessary purpose compatibility in accordance with Art. 6 (4) GDPR.

---

[54] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 15.
[55] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, S. 16.

dd) Fairness

(1)According to EDPB, the obligation of **fairness** under the GDPR (Article 5(1) (a) GDPR) is met, inter alia, by implementing the following **core elements** , which are of significant importance for the practical work and design of the JENTIS DCP and are not covered by other objectives [56]:

- Ensuring autonomy and interaction by involving data subjects in the use of data and clear communication on the exercise of data subjects' rights;
- Ensuring " truthfulness " by avoiding inappropriate and misleading processing;
- No discrimination against users through the use of discriminatory segments and
- Use of fair algorithms to reduce algorithmic bias and provide transparency to those affected.

The **JENTIS DCP** was designed to ensure fair processing.

The use of JENTIS DCP enables **complete Implementation** of data subject rights such as requests for information, requests for deletion and objections to processing by ensuring that website operators have full control over data processing.

After data subjects exercise one of the options and communicate the request to JENTIS, JENTIS DCP can fully automate the implementation of these rights on behalf of and at the request of the customer.

(2) In order to avoid **discriminatory conclusions** based on **algorithmic bias** , i.e. when computer systems reflect the implicit values and prejudices of people – for example when assigning users to inappropriate segments – [57]JENTIS has conducted an evaluation of the machine learning models for the later formation of synthetic users based on an " algorithm audit".

Beyond possible algorithmic biases that may be due to programming errors, **no discriminatory factors can be** identified based on the product description.

ee) Data Minimisation

(1) The **core elements** of the principle of data minimization as an objective for privacy by design and privacy by default can be fully **implemented within** the framework of the JENTIS DCP . According to EDPB[58] these include :

- Data avoidance and limitation,
- Access restrictions to data records,
- Data relevance and necessity of the data in relation to the purpose of processing,
- Aggregation and
- Pseudonymization according to the state of the art.

[56] See . Guidelines 4/2019 on Article 25 Data Protection by Design and by Default , p. 18.
[57]See Spindler/Horváth, in: Spindler/Schuster, Law of Electronic Media, 4th ed ., Art. 22 GDPR Rn. 8; Herberger, NJW 2018, 2825, 2827.
[58] Guidelines 4/2019 on Article 25 Data Protection by Design and by Default , p. 21.

(2) Apart from the possibility of **valid pseudonymisation** of clear data at raw data level (cf. points I.3. and 4.) and **comprehensive access restrictions , which can be ensured by configuring the JENTIS DCP, user data is aggregated** , for example, in extended applications such as synthetic users and ID pooling .

(3) The storage period of the raw data can be set individually. In the standard configuration, the storage period for raw data is 10 days.

The duration of the JENTIS cookies in the first-party context can also be customized for the JENTIS Tracker. Using the JENTIS Server Suite, data parameters can be reduced to a minimum or modified to ensure compliance with the data minimization principle depending on the intended use.

ff) Accuracy and Storage Limitation

(1) The additional objectives of data accuracy and storage limitation according to Art. 5 (1) lit. d) and e) GDPR can be fully [59]**implemented** by website operators due to the **flexible configuration options** of the JENTIS DCP .

(2) Customers decide which data is collected via the JENTIS DCP and fed into third-party systems via the JENTIS Tool Connector, and can freely determine the storage period.

gg) Integrity and Confidentiality

(1) Ensuring the requirements for integrity and confidentiality (Art. 5 para. 1 lit. f) GDPR) as an objective of Privacy by Design and Privacy by Default is one of the **core principles** in JENTIS SaaS.

(2) By implementing appropriate state-of-the-art technical and organizational measures , such as pseudonymization and encryption, JENTIS ensures the security of processing (Art. 32 GDPR). In addition, the provision of the JENTIS DCP using the IONOS server structure enables the implementation of data separation, shielding from external influences and processing in a logically isolated virtual network within the cloud infrastructure.

(3) The current **technical and organizational measures** of JENTIS and IONOS can be viewed in the **appendix** to **the data processing agreement .**

JENTIS applies an information security management system in accordance with **ISO 27001:2023** . In accordance with the procedures of TV AUSTRIA, it is certified that JENTIS applies a management system in accordance with the above-mentioned standard for the following scope: The provision of services in the field of data collection on websites and from other digital data sources using JENTIS technologies.

hh) Accountability

The extensive accountability obligations for those responsible in Art. 5 Para. 2 GDPR according to the ECJ case law means [60]that website operators should fully document and present the decision path for configuring the JENTIS DCP in order to be able to prove compliance with Art. 25 GDPR in the event of disputes. The JENTIS UI (User Interface) enables website operators to fulfill this accountability obligation.

[59] EDPB, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default v2.0, p. 23 ff.
[60] ECJ , judgment of October 27, 2022 – C-129/21, paragraph 80 f.

2. TCF Compliance

When using the JENTIS DCP, compliance with the Transparency and Consent Framework **(TCF v2.2) is ensured** . With the help of the JENTIS DCP, all vendor-specific requirements from the IAB TCF Policy[61] be fulfilled.

3. "Schrems II" compliance for third country transfers

(1) In the event that an **analysis service from the USA** such as Google Analytics is integrated, the third country transfer to Google LLC can be based [62]on the EU Commission's adequacy decision of July 10, 2023 due to the active certification [63]of Google LLC under the Data Privacy Framework List [64].

(2) If a **data transfer** to **India, China or Russia takes place** due to the use of Google DV 360, for example, [65]and cannot be based on an adequacy decision by the EU Commission [66], since such a decision does not exist for data transfers to India, China or Russia, additional safeguards for the third country transfer are required. In a commissioned study, the EDSA classifies India [67]as a third country without an adequate level of protection, particularly with regard to the intelligence powers of security authorities.

The same applies if only analysis services based in the USA are used, but which do not have active certification under the Data Privacy Framework List [68]; in this respect, too, a third country transfer requires further justification because the EU Commission's adequacy decision of 10 July 2023[69] then does not apply.

(3) Even by **locating** servers in **Europe, the third country issue cannot be avoided** from the outset , as the Cologne Higher Regional Court recently confirmed for the use of Google Ads with servers located in the EU.[70]

(4) In the opinion of the **DSK** , the request for **explicit consent** pursuant to Art. 49 (1) lit. a) GDPR for the **third country transfer** in the consent dialog or in the data protection information must be distinguished from the consent to the use of tracking tools to track user behavior and cannot be replaced by the latter. [71]The scope and regularity of such transfers regularly contradict the nature of Art. 49 GDPR as an exception and the requirements of Art. 44 sentence 2 GDPR.[72]

In addition, the Cologne Higher Regional Court considered a general notice in the cookie banner of a website that the level of data protection in the USA was not equivalent to that in the EU to be insufficient.[73]

---

[61] IAB Europe Transparency & Consent Framework Policies .
[62] US Department of Commerce, Data Privacy Framework List.
[63] EU Commission adequacy decision of 10 July 2023
[64] US Department of Commerce, Data Privacy Framework List .
[65] See https://www.iccl.ie/digital-data/europes-hidden-security-crisis/ .
[66] Adequacy decisions of the EU Commission .
[67] Czarnocki et al., Government access to data in third countries .
[68] US Department of Commerce, Data Privacy Framework List .
[69] EU Commission adequacy decision of 10 July 2023 .
[70] OLG Cologne, judgment of 3 November 2023 – 6 U 58/23 ; also expert opinion commissioned by the DSK on the current status of US surveillance law on the application of US surveillance law 50 US Code § 1881a (Section 702 FISA) and Heckmann, Data protection-compliant use of cloud solutions from unsafe third countries, Scientific Report, 2021, p. 16 .
[71] DSK, Guidance for providers of telemedia, 2021, p. 32.
[72] See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 of 25 May 2018, p. 9.
[73] OLG Cologne, judgment of November 3, 2023 – 6 U 58/23 .

(5) Due to the requirements of the ECJ case law [74]on third country transfers, the only option that remains is to agree on standard contractual clauses [75](SCC). However, securing third country transfers using **standard contractual clauses** (" **SCC"** , Art. 46 para. 2 lit. c) GDPR) requires additional measures **(" Supplementary Measures) .**

Which " **Supplementary Measures** " to be taken must be evaluated on the basis of the " Recommendations 01/2020 on measures […] " in version 2.0 published by the [76]**EDPB** on June 18, 2021 following the EU Commission's new SCC . Without documentation of additional risk mitigation measures , the application of the SCC will not be accepted by supervisory authorities. **Additional measures** may include, for example, the **anonymization** or advanced **pseudonymization** of data as well as extensive **encryption technologies** , if it is ensured that the recipients in the third country do not have access to the allocation rule for the pseudonymized data within the meaning of Art. 4 No. 5 GDPR or the data to be processed.[77]

The **Higher Regional Court of Cologne** and the **Federal Administrative Court** (Austria) have unanimously ruled that the **shortening of IP addresses** , state-of-the-art **encryption in transit and** encryption **at rest** are not **sufficient** . [78]The European **supervisory authorities** impose **strict requirements for additional measures** when using unmodified tracking services from US providers .

According to section 14 of the standard contractual clauses provided by the EU Commission, [79]there is an obligation to carry out and document a " **Transfer Impact Assessment** ", in which an analysis and mitigation of the risks of access by security authorities must be carried out on the basis of "Additional Measures " as additional contractual, technical and organizational measures.

Using the JENTIS Server Suite, data parameters can be reduced to a minimum, modified or synthesized. According to **the EDPS,** " **synthetic data** " can be considered as a privacy enhancing technology (**Privacy Enhancing Technology**) as an "additional measure " to secure third country transfers. In [80]**ENISA** 's view, synthesis primarily serves to ensure the **confidentiality** of **processing** , [81]which has the character of "additional measures" in technical and organizational terms within the meaning of Art. 32 GDPR.

If SCCs are concluded, it would have to be ensured in terms of content that these additional contractual, technical and organizational measures, which were evaluated in the context of a Transfer Impact Assessment, are adequately documented in Annex II of the SCC.

III. Best practices for website operators

In summary, for GDPR compliant use of the JENTIS DCP the following recommendations should be implemented:

---

[74] ECJ, 16 July 2020 – C-311/18 – Schrems II .
[75] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries according to Regulation (EU) 2016/679.
[76] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
[77]Paal/ Kumkar , MMR 2020, 733.
[78] OLG Cologne, judgment of November 3, 2023 – 6 U 58/23 ; BVwG , decision of May 12, 2023 W245 2252208-1/36E .
[79] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries according to Regulation (EU) 2016/679.
[80] EDPS, techsonar 2021-2022, p. 10 .
[81] See . ENISA, Data Protection Engineering, 2022, p. 17 .

- ☐ **No loading** of **third-party tags** as triggers for end device access **before Granting** a declaration of **consent**
- ☐ Adaptation of the **request** for a **declaration of consent** with regard to the analysis tools for both the end device-related processing and the downstream analysis of the tracking data
  - The consent dialogue with the app users should **include the following Information** in accordance with case law and supervisory authorities includes:
    - Recital 42 S. 4 GDPR: Identity of the controller and purposes of processing
    - ECJ, judgment of 1 October 2019 – C-673/17, para . 72 ff.: [82]Function, duration, recipient
    - EDSA, Guidelines 05/2020 on consent under Regulation 2016/679 [83]: identity, purposes, data categories, revocation, recipients, third country transfer
  - It is recommended **not to** use **standard texts , but concrete** To integrate **descriptions of the processing operations of the consent declarations into the CMP. According to the Guidelines 05/2020 on consent** pursuant to Regulation 2016/679 of the EDPB, [84]this also includes information on processing with **joint responsible persons** .
  - For this purpose, the information can be displayed at different levels in the CMP, whereby the essential information must be kept available on the first level.[85]
  - According to the unanimous opinion in case law and supervisory authority opinions, in order to fulfil the criterion of voluntary consent (Article 4 No. 11 GDPR), an **equivalent Rejection buttons** on the first level of the CMP.[86]
  - **no data** is required to prove consent (Art. 7 Para. 1 GDPR). **A long-term stored ID** is assigned to the app user's device.[87]
  - Finally, it must be ensured that consent that has already been given **can be revoked at any time** (Article 7, paragraph 3 GDPR). This can be achieved by linking the CMP settings in the data protection notices or app settings.
- ☐ For the transfer of substituted data streams to third-party systems and when configuring the JENTIS DCP with the JENTIS Essential Mode feature activated**,** a **Legitimate Interests assessment should be conducted** to document the balancing of interests in accordance with Art. 6 (1) (f) GDPR.
- ☐ **Conclusion** of a **data processing agreement with JENTIS**
- ☐ **Adjustment** of the **Privacy policy on the operators website**
- ☐ To justify the third country transfer: Request documentation from the third party to **verify** the **conclusion** of the **standard contractual clauses** with third-party providers and **conduct** a documented **transfer impact assessment** in accordance with Section 14 of the standard contractual clauses.

[82] ECJ, judgment of October 1, 2019 – C-673/17, para . 72 ff.
[83] Guidelines 05/2020 on consent under Regulation 2016/679.
[84] Guidelines 05/2020 on consent under Regulation 2016/679 .
[85] DSK, Guidance for providers of telemedia, 2022, para . 36 .
[86] DSK, Guidance for providers of telemedia, 2022, para . 132 ff ; OLG Cologne, judgment of January 19, 2024 – 6 U 80/23 ; LG Munich, judgment of November 29, 2022 – 33 O 14776/19, LG Berlin, 52 O 79/22 (2).
[87] DSK, Guidance for providers of telemedia, 2022, para . 79 .