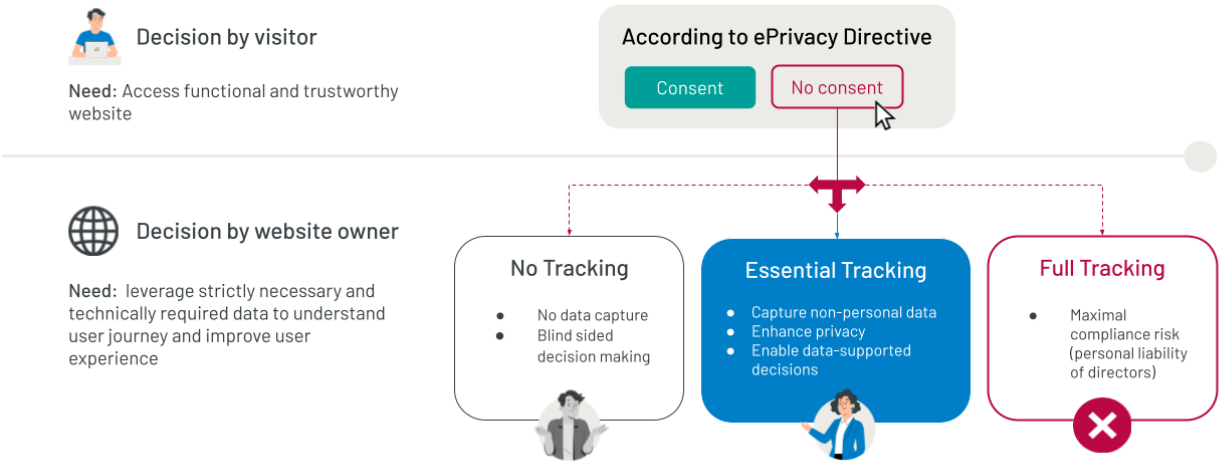
JENTIS Essential Mode

Example configuration
Audience Measurement

JENTIS Essential Mode enables legally compliant capture of strictly necessary and technically required data as a fall back in case a user has not provided consent. The Essential Mode and this example configuration is based on the memorandum "Data protection evaluation of the "Essential Mode" of the JENTIS Saas solution" by Spirit Legal Fuhrmann Hense Partnership of Lawyers.[1]



[1] See Executive Summary in the Annex. For the full version of the memorandum, contact andreas@jentis.com.

JENTIS GmbH
Schoenbrunner Straße 231
1120 Vienna, Austria

T: +43 1 9974354
E: office@jentis.com
www.jentis.com

CRN.: 529675i
IBAN: AT38 2011 1842 8146 2300
BIC: GIBAATWWXXX

Background

Data protection law in the EU (ePrivacy Directive, Art. 5) requires website operators to ask for and obtain consent from users before reading and writing to users' devices. However, it is possible to store or access technical or strictly necessary information on the user device to provide a functional and user-friendly website not requesting for consent.[2]

In effect, user consent is not required for cookies that:

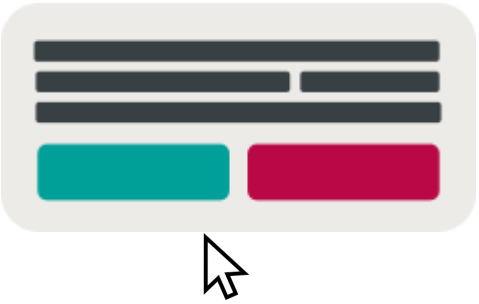
- enable evaluation of the published content and user-friendliness of the website; and / or
- evaluate or improve the effectiveness of design decisions made on the website.

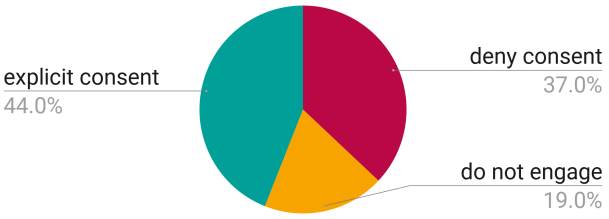
Currently data protection law in the EU does not allow to rely on this exception when the controller of data is using a third party tool for tracking with joint control over data.

Challenge

The main challenge in relying on the above exception is to leverage the website data with winning valuable information and customer trust.

Based on the survey conducted by YouGov[3] in Germany, when faced with the consent choice 37% deny consent, 19% do not engage with the consent banner and only 44% of users give the explicit consent.





[2] Exception to Art.5.3 ePrivacy Directive
[3] Level of consent to the usage of cookies in selected countries worldwide as of June 2021 released in August 2021 link

Without consent of a user the website operator is faced with a choice:

- **stop tracking completely**

  or

- **find a technical solution to enable compliant capture of first party data.**

With a turnkey technical solution for compliant capture of first party data, website operators in Germany can make use of up to 56% additional data.

On the other hand, building a standalone technical solution to capture first party data from scratch requires significant resources, such as financial investment, highly skilled IT personnel, legal experts to assess and confirm compliance, as well as overall high effort to maintain it up to date.

Solution

JENTIS Data Capture Platform (DCP) is a turnkey solution to combine first party data capture based on user consent and as a fall back even without user consent. To be able to rely on the consent exception, JENTIS created Essential Mode to compliantly leverage strictly necessary and technically required data.
From a legal compliance perspective, JENTIS Essential Mode offers a sustainable tool for capturing strictly necessary and technically required data without user consent.

From a technical perspective, JENTIS Essential Mode gives an opportunity to start data capture, when consent is not given.

From a marketing perspective, JENTIS Essential Mode helps to leverage website data to make informed decisions about the user experience, on page user journey and design of the website.

Unique JENTIS features allowing to capture data in Essential Mode:

- First Party data capture shields user devices against direct third party access;
- Twin Server Technology allows to control transfers of user data to third parties;
- Full control over data streams allows website operators to solely define the purpose of processing;
- Pseudonymisation and anonymisation functions are available for each data parameter;
- Compliant Cloud selection ensures that captured data is de-personalised in the EU before any international data transfer outside of the EU.

5 Steps to configure JENTIS Essential Mode

1. General JENTIS setup:
    a. implement A-Record in your DNS setup
    b. place the JTM-Code on the website pages where data should be captured
2. Configure First Party JENTIS Cookies:
    a. as a result of the setting JENTIS, three basic JENTIS First Party cookies will be running on the respective page in the user browser (see below).
3. Configure JENTIS Tag Manager:
    a. Identify third-party tags to be used
    b. Define data parameters (variables) to be captured
    c. Modification of data parameters: defining data parameters to be anonymised, pseudonymised, deleted or replaced.
4. Connect to the CMP of choice in JENTIS DCP
5. Test & publish

Basic JENTIS First Party cookies:

jts-rw	JENTIS first party identifier (User-ID)	installed by default, by default the storage period is 24 months, to use of JENTIS User ID in Essential Mode storage period must be configured to a maximum of 13 months
jctr_sid	JENTIS session identifier (Session ID)	installed by default, storage period 30 minutes
jts_log	activates JENTIS Debug-Log function for developers (only set in Preview Mode for JTM users and developers).	installed by default, storage period 12 months

Prerequisites & requirements

Consent Management Platform

JENTIS offers connectors to more than 15 verified CMPs. With the JENTIS Consent Manager, you can manage the connection between your web analytics vendors and a specific CMP and provide the required information for each data processing activity — such as purpose, legal basis, data categories, vendor address etc.

To enable JENTIS Essential Mode, a connection to a designated verified CMP is required to detect any consent or no consent signal.

Data Processing Agreement

Signing the Data Processing Agreement (DPA) with JENTIS is part of the onboarding process. Our DPA consists of the Standard contractual clauses and includes supplementary provisions.

Legitimate Interest Assessment

To document compliant implementation of JENTIS Essential Mode, EU data protection law requires to conduct Legitimate Interest Assessment. To receive an example of Legitimate Interest Assessment please contact us.

Privacy Policy Update

JENTIS starts capturing and processing essential data in JENTIS Essential Mode with the user's first visit to the website by placing strictly necessary cookies. Website provider should transparently inform its users about the scope of the essential data processing.

Example configuration

We use JENTIS on the Heroes of Data Privacy (HoDP) website. In this example, JENTIS is configured to capture data in both cases: with and without consent. JENTIS Essential Mode is triggered as a Fall Back scenario when a visitor does not provide consent and the purpose of the data capture is limited to audience measurement.

URL: www.heroesofdataprivacy.com

The HoDP website sends data via JENTIS to Google Analytics, resulting in the following statistical reports per each website page:

- aggregated number of website visits;
- statistics on page loading times;
- statistics on time spent on each page and bounce rate;
- statistics, including conversions, based on user actions (click, selection);
- statistics on the geographical area of origin of requests.

JENTIS Essential Mode can also be configured to retrieve additional statistical reports in Google Analytics, such as scrolling depth statistics, aggregated time statistics on an hourly and daily basis. These statistical reports are not included in the HoDP website following the purpose limitation and data minimisation principle.

Here is an example of data parameters configured in JENTIS Essential Mode

Data parameter	Requirement for strictly necessary data[4]	JENTIS Essential mode Configuration on HoDP Website
Client ID / User ID	substituted by fictitious Client ID / User ID	JENTIS creates a separate JENTIS ID (jts-rw) by random generation. In addition, a generated unique User ID (linked to JENTIS ID) is replacing the Google Client ID on the JENTIS Server. This function enables analytics tools to attribute multiple events (pageviews, clicks) to a pseudonymous "user" or "session".
IP Address	pseudonymised	JENTIS does not store User IP Address when Essential Mode is activated. JENTIS shares only JENTIS Server IP Address in communication with third parties.
Click IDs and other identifiers contained in URLs	removed or substituted by newly generated values	All query parameters are completely removed UTM parameters are removed /not processed
UUID	removed or substituted by newly generated values	JENTIS DCP does not generate / process UUID
User Agent	removed or substituted by newly generated User Agent	Randomly generated by JENTIS

[4] Memorandum "Data protection evaluation of the "Essential Mode" of the JENTIS Saas solution" by Spirit Legal Fuhrmann Hense Partnership of Lawyers

Referrers	Pseudonymised / modified	Referrers are shortened by default
Client / user specific IDs	removed or substituted by newly generated values	Identifiers like gjid and gid for GA are simulated on the JENTIS Server Side. Randomly generated value to represent a user specific Client / User ID in GA is created for each event newly and separately.
Fingerprinting	Not allowed	No combination of browser and device settings is used for identification of the users To prevent fingerprinting all metadata from a user device (language settings, screen resolution, etc) is substituted by randomly generated values On the product road map: smart time framing as prevention of fingerprinting
Merging of IDs	not allowed	JENTIS User ID is not merged with other user (client) data like CRM ID or systems registration data
Purpose limitation	Must be limited to what is strictly necessary	Data parameters were removed, substituted by newly generated random data, pseudonymised or modified otherwise to ensure processing of only strictly necessary statistical data With JENTIS, a website operator has full control to define the purpose of processing
Storage limitation	Must be limited to max. 13 months	Limited to 13 months

		JENTIS allows full flexibility to define the period of storage for most data parameters
Timestamps	Cannot be used in original value, must be removed, modified, blurred	JENTIS allows website operators to process timestamps and modify them to the extent they are no longer attributable to a single user: by batching, blurring and / or clustering

Data Protection Memorandum

JENTIS GmbH

Working translation from German to English

SPIRIT LEGAL®

Annex (InfoPack)

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.