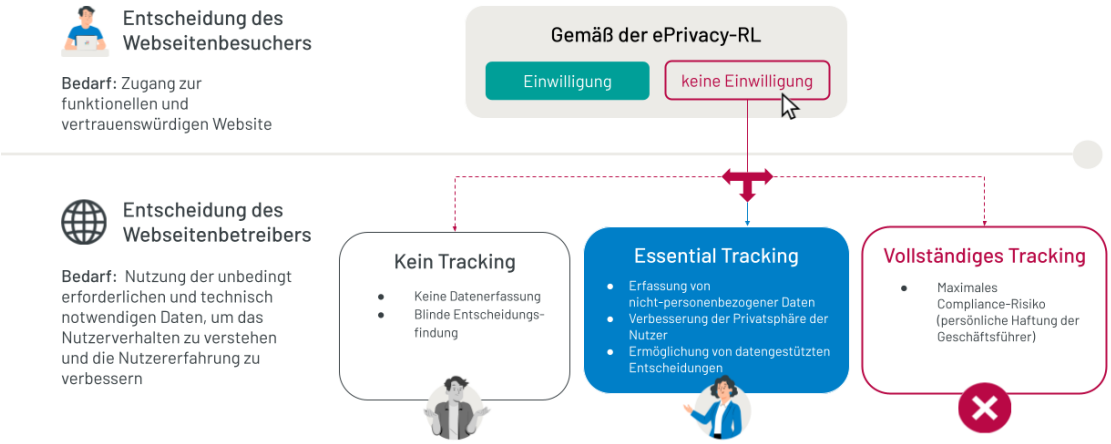
JENTIS Essential Mode

Beispielkonfiguration
Reichweitenmessung

Der JENTIS Essential Mode ermöglicht die rechtskonforme Erfassung von unbedingt erforderlichen und technisch notwendigen Daten als Fallback-Lösung für den Fall, dass ein Nutzer keine Einwilligung erteilt hat. Der Essential Mode und diese Beispielkonfiguration basieren auf dem Memorandum "Datenschutzrechtliche Bewertung des Essential Mode der JENTIS Saas-Lösung" von Spirit Legal Fuhrmann Hense Partnerschaft von Rechtsanwälten.[1]



[1] Siehe Executive Summary im Anhang. Die vollständige Fassung des Memorandums kann unter andreas@jentis.com angefordert werden.

JENTIS GmbH
Schönbrunner 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

Hintergrund

Nach dem EU-Datenschutzrecht (Datenschutzrichtlinie für elektronische Kommunikation, Artikel 5) müssen Webseitenbetreiber die Einwilligung der Nutzer einholen, bevor sie deren Geräte auslesen und beschreiben. Es ist jedoch möglich, ohne die Einwilligung des Nutzers einzuholen, technische und unbedingt erforderliche Informationen auf dem Gerät des Nutzers zu speichern oder darauf zuzugreifen, um eine funktionale und benutzerfreundliche Website bereitzustellen.[2]

In der Tat ist die Einwilligung des Nutzers nicht erforderlich für Cookies, die:

- der Bewertung des veröffentlichten Inhalts und der Benutzerfreundlichkeit der Website dienen; und / oder
- die Wirksamkeit der auf der Website getroffenen Designentscheidungen bewerten oder verbessern.

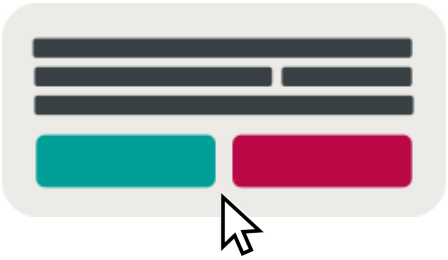
Derzeit ist es nach dem EU-Datenschutzrecht nicht möglich, sich auf diese Ausnahmeregelung zu berufen, wenn der für die Datenverarbeitung Verantwortliche ein Tracking-Tool eines Drittanbieters verwendet, mit dem er gemeinsam verantwortlich ist.

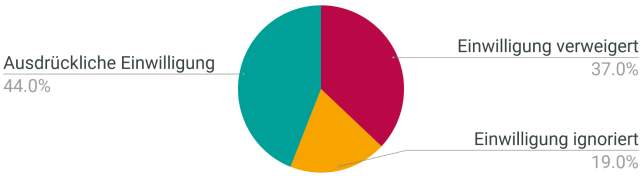
Herausforderung

Die größte Herausforderung bei der Inanspruchnahme der oben genannten Ausnahmeregelung besteht darin, die Webseitendaten optimal zur Gewinnung wertvoller Informationen und des Vertrauens der Kunden zu nutzen.

Laut einer von YouGov[3] in Deutschland durchgeführten Umfrage verweigern 37% der Nutzer ihre Einwilligung, wenn sie vor die Wahl gestellt werden, 19% stimmen dem Einwilligungsbanner nicht zu und nur 44% der Nutzer geben ihre ausdrückliche Einwilligung.

[2] Ausnahme von Artikel 5 Abs.3 der Datenschutzrichtlinie für elektronische Kommunikation
[3] Grad der Einwilligung zur Verwendung von Cookies in ausgewählten Ländern weltweit (Stand: Juni 2021), veröffentlicht im August 2021 Link





Ohne die Einwilligung des Nutzers steht der Webseitenbetreiber vor der Wahl:

- Das Tracking entweder komplett einzustellen

  oder

- Eine technische Lösung zu finden, die eine einwilligungsfreie Erfassung von First-Party-Daten ermöglicht.

Mit einer maßgeschneiderten technischen Lösung für die rechtskonforme Erfassung von First-Party-Daten können Webseitenbetreiber in Deutschland bis zu 56% zusätzliche Daten nutzen.

Der Aufbau einer eigenständigen technischen Lösung zur Erfassung von First-Party-Daten erfordert jedoch erhebliche Ressourcen, wie z.B. finanzielle Investitionen, hochqualifiziertes IT-Personal, Rechtsexperten zur Bewertung und Bestätigung der Konformität sowie einen insgesamt hohen Aufwand, um sie auf dem neuesten Stand zu halten.

Lösung

Die JENTIS Data Capture Platform (DCP) ist eine maßgeschneiderte Lösung, welche die Datenerfassung auf der Grundlage der Einwilligung des Nutzers und als Ausweichlösung auch ohne Einwilligung des Nutzers ermöglicht. Um sich auf die Ausnahmeregelung der Einwilligung berufen zu können, hat JENTIS den Essential Mode entwickelt, um die unbedingt erforderlichen und technisch notwendigen Daten rechtskonform zu nutzen.
Aus rechtlicher Sicht bietet der JENTIS Essential Mode ein nachhaltiges Instrument zur Erfassung unbedingt erforderlicher und technisch notwendiger Daten ohne Einwilligung des Nutzers.

Aus technischer Sicht bietet der JENTIS Essential Mode die Möglichkeit, die Datenerfassung auch dann zu starten, wenn keine Einwilligung vorliegt.

Aus Marketing-Perspektive hilft der JENTIS Essential Mode dabei, Website-Daten zu nutzen, um fundierte Entscheidungen über das Nutzererlebnis, die On Page User Journey und das Design der Website zu treffen.

Einzigartige JENTIS-Funktionen ermöglichen die Datenerfassung im Essential Mode:

- Die First-Party-Datenerfassung schützt die Endgeräte des Nutzers vor dem direkten Zugriff Dritter;
- Die Twin Server Technologie ermöglicht die Kontrolle der Übermittlung von Benutzerdaten an Dritte;
- Die vollständige Kontrolle über die Datenströme ermöglicht es dem Webseitenbetreiber, den Zweck der Verarbeitung selbst zu bestimmen;
- Pseudonymisierungs- und Anonymisierungsfunktionen sind für jeden Datenparameter verfügbar;
- Die Auswahl einer rechtskonformen Cloud stellt sicher, dass die erfassten Daten in der EU entidentifiziert werden, bevor sie an Drittländer außerhalb der EU übermittelt werden.

5 Schritte zur Konfiguration des JENTIS Essential Mode

1. Allgemeine JENTIS-Einrichtung:
    a. A-Record in Ihren DNS-Einstellungen anlegen
    b. Platzieren Sie den JTM-Code auf die Seiten, auf denen die Daten erfasst werden sollen
2. First Party JENTIS Cookies konfigurieren:
    a. Als Ergebnis der JENTIS-Einrichtung werden drei grundlegende JENTIS First-Party-Cookies auf der jeweiligen Seite im Browser des Benutzers laufen (siehe unten).
3. JENTIS Tag Manager konfigurieren:
    a. Identifizieren Sie die zu verwendenden Drittanbieter-Tags
    b. Definieren der zu erfassenden Datenparameter (Variablen)
    c. Änderung der Datenparameter: Definition der Datenparameter, die anonymisiert, pseudonymisiert, gelöscht oder ersetzt werden sollen.
4. Verbinden mit dem CMP nach Wahl in JENTIS DCP
5. Testen & veröffentlichen

Grundlegende JENTIS First Party Cookies:

jts-rw	JENTIS First Party Kennung (User-ID)	Standardmäßig installiert, die Standardspeicherdauer beträgt 24 Monate, zur Nutzung der JENTIS User ID im Essential Mode muss die Speicherdauer auf maximal 13 Monate konfiguriert werden
jctr_sid	JENTIS Sitzungskennung (Session ID)	Standardmäßig installiert, Speicherdauer 30 Minuten
jts_log	Aktiviert die JENTIS Debug-Log-Funktion für Entwickler (nur im Vorschaumodus für JTM-Benutzer und -Entwickler eingestellt).	Standardmäßig installiert, Speicherdauer 12 Monate

Voraussetzungen & Anforderungen

Consent Management Plattform

JENTIS bietet Konnektoren zu mehr als 15 verifizierten CMPs. Mit dem JENTIS Consent Manager können Sie die Verbindung zwischen Ihren Webanalyse-Anbietern und einer bestimmten CMP verwalten und die erforderlichen Informationen für jede Datenverarbeitungstätigkeit bereitstellen - wie Zweck, Rechtsgrundlage, Datenkategorien, Anbieteradresse usw.

Um den JENTIS Essential Mode zu aktivieren, ist eine Verbindung zu einer bestimmten CMP erforderlich, um ein Signal für eine Einwilligung oder eine fehlende Einwilligung zu erkennen.

Vereinbarung zur Datenverarbeitung

Die Unterzeichnung des Data Processing Agreement (DPA) mit JENTIS ist Teil des Onboarding-Prozesses. Unser DPA besteht aus den Standardvertragsklauseln und enthält ergänzende Bestimmungen.

Bewertung des berechtigten Interesses

Um die konforme Implementierung des JENTIS Essential Mode zu dokumentieren, ist nach EU-Datenschutzrecht eine Bewertung des berechtigten Interesses durchzuführen. Um ein Beispiel für eine Bewertung des berechtigten Interesses zu erhalten, bitten wir Sie, uns zu kontaktieren.

Update der Datenschutzerklärung

JENTIS beginnt mit der Erfassung und Verarbeitung essentieller Daten im JENTIS Essential Mode mit dem ersten Besuch des Nutzers auf der Webseite durch das Setzen der unbedingt erforderlichen Cookies. Der Webseitenbetreiber sollte seine Benutzer transparent über den Umfang der Verarbeitung der essentiellen Daten informieren.

Beispielkonfiguration

Wir verwenden JENTIS auf der Webseite von Heroes of Data Privacy (HoDP). In diesem Beispiel ist JENTIS so konfiguriert, dass Daten in beiden Fällen erfasst werden: mit und ohne Einwilligung. Der JENTIS Essential Mode wird als Fallback-Szenario ausgelöst, wenn ein Besucher keine Einwilligung erteilt und der Zweck der Datenerfassung auf die Messung der Besucherzahl beschränkt ist.

URL: www.heroesofdataprivacy.com

Die HoDP-Webseite sendet Daten über JENTIS an Google Analytics, was zu den folgenden statistischen Berichten pro einzelne Seite führt:

- Aggregierte Anzahl der Webseitenaufrufe;
- Statistiken über die Ladezeiten der Seiten;
- Statistiken über die Verweildauer auf jeder Seite und die Absprungrate;
- Statistiken einschließlich Konversionen, basierend auf Benutzeraktionen (Klick, Auswahl);
- Statistiken über das geografische Herkunftsgebiet der Anfragen.

Der JENTIS Essential Mode kann auch so konfiguriert werden, dass zusätzliche statistische Berichte in Google Analytics abgerufen werden können, wie z.B. Statistiken zur Scrolltiefe, aggregierte Zeitstatistiken auf stündlicher und täglicher Basis. Diese statistischen Berichte werden gemäß dem Grundsatz der Zweckbindung und Datenminimierung nicht in die HoDP-Webseite aufgenommen.

Hier ist ein Beispiel für Datenparameter, die im JENTIS Essential Mode konfiguriert wurden:

Datenparameter	Erfordernis der unbedingt erforderlichen Daten[4]	JENTIS Essential Mode Konfiguration auf der HoDP Website
Client-ID / User-ID	Ersetzt durch fiktive Client-ID / User-ID	JENTIS erzeugt eine eigene JENTIS ID (jts-rw) durch Zufallsgenerierung. Zusätzlich ersetzt eine generierte eindeutige User-ID (verknüpft mit der JENTIS-ID) die Google-Client-ID auf dem JENTIS-Server. Diese Funktion ermöglicht es Analysetools, mehrere Ereignisse (Pageviews, Klicks) einem pseudonymen "User" oder einer "Session" zuzuordnen.
IP-Adresse	Pseudonymisiert	JENTIS speichert die IP-Adresse des Benutzers nicht, wenn der Essential Mode aktiviert ist. JENTIS gibt bei der Kommunikation mit Dritten nur die IP-Adresse des JENTIS-Servers weiter.
Click IDs und andere in URLs enthaltene Identifikatoren	Entfernt oder durch neu generierte Werte ersetzt	Alle Abfrageparameter werden vollständig entfernt. UTM-Parameter werden entfernt / nicht verarbeitet
UUID	Entfernt oder durch neu generierte Werte ersetzt	JENTIS DCP erzeugt / verarbeitet keine UUID

[4] Memorandum "Datenschutzrechtliche Bewertung des "Essential Mode" der JENTIS Saas Lösung" von Spirit Legal Fuhrmann Hense Partnerschaft von Rechtsanwälten

Benutzeragent	Entfernt oder durch einen neu generierten User Agent ersetzt	Zufällig generiert von JENTIS
Referrer	Pseudonymisiert / modifiziert	Referrer werden standardmäßig gekürzt
Client-/ User- spezifische IDs	Entfernt oder durch neu generierte Werte ersetzt	Identifikatoren wie gjid und gid für GA werden auf der JENTIS Server Seite simuliert. Ein zufällig generierter Wert, der eine benutzerspezifische Client-/User-ID in GA darstellt, wird für jedes Ereignis neu und separat erstellt.
Fingerprinting	Nicht erlaubt	Es wird keine Kombination von Browser- und Geräteeinstellungen zur Identifizierung der Nutzer verwendet. Um Fingerprints zu verhindern, werden alle Metadaten eines Benutzergeräts (Spracheinstellungen, Bildschirmauflösung, usw.) durch zufällig generierte Werte ersetzt. Auf der Produkt-Roadmap: Smart Time Framing als Prävention von Fingerprinting
Zusammen-führung von IDs	Nicht erlaubt	Die JENTIS User ID wird nicht mit anderen Benutzerdaten (Kunden) wie CRM-ID oder Systemregistrierungsdaten zusammengeführt.
Zweckbindung	Muss sich auf das unbedingt Erforderliche beschränken	Die Datenparameter wurden entfernt, durch neu generierte Zufallsdaten ersetzt, pseudonymisiert oder anderweitig verändert, um sicherzustellen, dass nur

		die unbedingt erforderlichen statistischen Daten verarbeitet werden.
Begrenzung der Speicherung	Muss auf max. 13 Monate limitiert sein	Limitiert auf 13 Monate JENTIS erlaubt die flexible Festlegung der Speicherdauer für die meisten Datenparameter
Zeitstempel	Kann nicht im Originalwert verwendet werden, muss entfernt, verändert oder verwischt werden.	JENTIS ermöglicht es Webseitenbetreibern, Zeitstempel zu verarbeiten und so zu verändern, dass sie nicht mehr einem einzelnen Benutzer zugeordnet werden können: durch Stapelung, Unschärfe und / oder Bündelung.

Data Protection Memorandum

JENTIS GmbH

SPIRIT LEGAL®

Anhang (InfoPack)

Verfasser/in	**Datum des Dokuments**
RA Peter Hense & RA Tilman Herbrich (CIPP/E)	*10 Februar 2023, v2.4*

Projekt

Datenschutzrechtliche Bewertung des „Essential Mode" der JENTIS Saas-Lösung

Executive Summary

Das vom EU-Datenschutzrecht und der Rechtsprechung vorgeschriebene Einwilligungserfordernis gilt für jeden Zugriff auf und jede Speicherung von Informationen aus den Endgeräten der Nutzer **(I.3.)**. In Anbetracht der BGH-Entscheidung „Cookie-Einwilligung II" **(I.1.)**, der gesetzlichen Regelung in § 25 TTDSG sowie aktuell angestoßener Untersuchungen von Aufsichtsbehörden und ersten Gerichtsurteilen ist das Einwilligungserfordernis beim Website-Tracking eine strikte Vorgabe.

Eine Ausnahme von diesem strikten Einwilligungserfordernis – „unbedingte Erforderlichkeit" ist in Art. 5 Abs. 3 S. 2 ePrivacy-RL geregelt **(II.1.).** Auch die Rechtsprechung und die derzeitige Auslegung des Wortlauts der Art. 5 Abs. 3 S. 1 ePrivacy-RL lässt darauf schließen, dass unter bestimmten Umständen die Berufung auf nachgelagerte Verarbeitungen beim Server-Side-Tracking ohne direkten Zugriff auf das Endgerät **(II.2.)** nicht unter dieses strenge Einwilligungserfordernis fällt. Wichtig ist, dass die Ausnahmen von der strikten Einwilligungspflicht nicht auf Third-Party-Dienste anwendbar sind.

In der Praxis ist die Umsetzung der Ausnahmen vom Einwilligungserfordernis aufgrund komplexer und schwer zu lösender Herausforderungen bei der Integration von Tracking-Anwendungen ohne eine langfristige und nachhaltige technische Lösung, die auch rechtskonform ist und wirksamen Datennutzung unterstützt, praktisch mit hohen Risiken verbunden **(II.3.)**.

JENTIS Data Capture Platform (DCP) bietet als Privacy Enhancing Technology eine langfristige Hilfestellung zur Sicherstellung der „Datenschutz"-Compliance in der Supply Chain und ermöglicht den Kunden flexible Konfigurationen der SaaS-Lösung, um der Volatilität der jeweiligen individuellen Risikolage von Unternehmen Rechnung zu tragen. Die JENTIS-Twin-Server Technologie **(III.1.)** ermöglicht die wirksame Verwendung von Website-Daten in beiden Situationen – bei expliziter Einwilligung des Nutzers (Tracking-Modus) und bei nicht vorhandener Einwilligung des Nutzers (als Fall-Back Lösung - JENTIS Essential Mode). Die Unternehmen können den „JENTIS Essential Mode" als Fallback-Lösung für das First-Party-Tracking so konfigurieren, dass die Anwendung der Ausnahmevorschriften vom Einwilligungserfordernis für den Endgerätezugriff konform und effektiv umgesetzt werden **(III.2.)**. Dadurch wird eine „Nutzungsanalyse" in einem reduzierten Umfang ohne Nutzerstimmung möglich, wenn der Nutzer das Cookie-Banner gar nicht anklickt oder keine Einwilligung erteilt. . Dies wird anhand einer Beispielkonfiguration für den JENTIS Essential Mode demonstriert **(III.2.c.aa.)**.

Die serverseitigen Übermittlungen der vom JENTIS-Server modifizierten (und bereinigten) Browser-Nutzer-Daten an Drittanbieter-Server können in Übereinstimmung mit Positionierungen von Aufsichtsbehörden als einwilligungsfreie nachgelagerte Verarbeitungsphase im konkreten Einzelfall auf

überwiegende berechtigte Interessen gemäß Art. 6 Abs. 1 S. 1 lit. f) DSGVO gestützt werden **(III.3.)**. In Einklang mit der Ansicht der ENISA kann die Modifikation der Datenparameter als Privacy Enhancing Technology betrachtet und als wirksames Mittel der Pseudonymisierung eingesetzt werden.

Mithilfe von JENTIS können Unternehmen die datenschutzrechtlichen Vorgaben an das Tracking vollständig umsetzen und die Rechtsunsicherheiten beseitigen. Website-Betreiber können bei Nutzung von JENTIS wirtschaftliche Vorteile ihrer jeweils eigenen First-Party-Daten nutzen, ohne ihre Daten oder die jeweilige unternehmerische Compliance durch unkontrollierte und intransparente Verarbeitung auf Seiten von Drittanbietern in rechtlicher Hinsicht zu gefährden **(IV.)**. Über die JENTIS-Technologie erhalten Unternehmen die vollständige Kontrolle beim Server-Side-Tracking zurück.