JENTIS

Server-side Tracking with a Data Capture Platform (DCP)

How to achieve maximum data quality
for your marketing and remain compliant
in the first-party era.

simply better data

Introduction

The value of data has increased rapidly over the past two decades. For many digitally driven companies, they are an essential raw material for sales and growth.

Before the digital revolution, companies were evaluated on the basis of their assets, among other things. An oil company's value was determined by the size of its oil fields and the value of the machinery it owned to extract the oil. Material goods were often the key to value creation.

In the digitized world, a large number of the largest companies derive their value from virtual goods - from the behavioral data of their users.

Data is the new oil. Not only the large tech corporations have based their successful business models on targeted advertising, persona classification or product recommendations.

Large, medium-sized and small companies in other sectors have long recognized the potential of data-driven strategies for e-commerce and digital marketing.

But while the importance of accurate behavioral data is increasing, its availability is in free fall: anti-tracking measures and data protection regulations are causing a massive drop in data quality.

Many companies lose their most important raw material. In order to ensure sales and growth, they have to unite apparent opposites: increase data quality and ensure data protection.

This requires a paradigm shift and an innovation in data acquisition.

The End of third-party Cookies

Since Web 2.0, companies have been able to count on accurate behavioral data from their website users and monetize them effectively, such as through remarketing efforts. The third-party cookie, which identifies browsers across websites, was central to this. But with the arrival of adblockers and tracking preventers, the tide has turned. They not only block third-party cookies, but prevent data collection itself.

The world's most popular browser, Google Chrome, will no longer support third-party cookies starting in mid-2024. For data-driven companies, that means a shift in thinking.

The future belongs to Cookieless tracking. Only those who make the switch to server-side first-party data in good time can benefit from new opportunities and competitive advantages.

Great Challenge, great Opportunity

Data quality is declining, but the technical requirements for data collection are increasing: In order to prevent data loss through adblockers and tracking preventions, it is necessary to collect first-party data on the server side.

The clock is ticking for the transition. Because Google has set the end of third-party cookies from mid-2024.

At the same time, data protection regulations such as GDPR and ePrivacy require companies to protect their users' data and have data collection under control.

Sounds like a lot? It is. But no matter how great the challenge, companies are finding new growth opportunities.

Because those who switch to first-party data collection benefit from more precise data for their digital marketing and from the competitive advantage over competitors who continue to rely on conventional tracking.

In addition, there is the possibility of simply and flexibly complying with data protection regulations and making oneself independent of large corporations.

Fortunately, today it's easier than ever to solve the challenges in one fell swoop and seize the opportunities. The Data Capture Platform (DCP) with server-side tracking makes it possible.

The cookieless era on the web has begun.

What is a Data Capture Platform (DCP)?

The Data Capture Platform is the answer to the problems in data capture.

A DCP collects high-quality first-party data on websites using server-side tracking.

It ensures data protection compliance and forwards "clean", highly accurate data to all your existing marketing tools and data platforms. These include, for example, reporting tools such as Google Analytics or customer data platforms.

With DCPs, you can easily and conveniently control the tracking on your website yourself – without having to rely on third-party providers. And not only on the web: DCPs also collect data from other sources such as apps, e-commerce shops or SmartTVs and offer the possibility of enriching data in real time.

Everything on one Platform

Traditional client-side tracking - and server-side tracking by themselves - cannot meet these needs.

DCPs on the other hand combine server-side tracking and data protection functions on one platform. They are easy to integrate into existing tech stacks and make it a lot easier for marketers and analysts to track the data they need to implement successful campaigns.

In short: DCPs ensure the best possible data quality, full data control, data protection compliance and the highest level of connectivity.

The Properties of the DCP:

1. The collection of first-party data in high quality and accuracy
2. The collection of data from a wide range of data sources, e.g. websites, e-commerce shops, apps, SmartTVs
3. Full control over data collection, privacy by design architecture and thus a high level of data protection
4. The easy forwarding of data to Marketing- and Analytics-Tools, e.g. Google Analytics or Customer Data Platform.

Advantages and Benefits of a Data Capture Platform

Highest data quality for better marketing

For companies that rely on digital marketing or produce digital products, the correct, high-quality collection of data is the basic prerequisite for sales and success. Wrong data lead to wrong conclusions and wrong decisions.

DCPs rely on first-party data collection. Since this is server-side tracking, this can happen unaffected by adblockers and tracking preventions.

The recorded data is therefore more accurate and has fewer gaps. For example, customer journeys can be better understood from the first contact to the conversion.

This subsequently enables more effective allocation of marketing budgets, better attribution and higher return-on-ad-spend (ROAS).

Full data control for easy compliance

A DCP gives companies complete control over which user data is collected and which third-party tools in their own tech stack receive which data.

Data control and privacy-by-design architecture make it much easier to comply with data protection regulations and to react flexibly to regulatory changes. Companies can thus avoid data protection penalties due to GDPR & Co and the associated damage to their image.

Future security and independence

The interests of the tech giants do not always coincide with the interests of their own company. Therefore, data sovereignty and data control are required in order to become independent of dominant market participants and service providers such as Google or Meta in the long term - but still be able to continue using their tools.

With data capture platforms, companies can react flexibly to legal, technological and market developments, depending on the situation.

Maximum connectivity for easy implementation

As an independent platform specializing in tracking at the beginning of the value chain, high connectivity is an important property of data capture platforms. DCPs seamlessly forward data to the tech stack in their own company using connectors.

As a result, DCPs play with existing tech stacks and are easy to integrate without you having to make major changes.

What Data Sources does a DCP use?

With a data capture platform, you can use a wide range of data sources.

These include, for example:

- Website data
- E-commerce data
- App data
- SmartTV data

How does a DCP work?

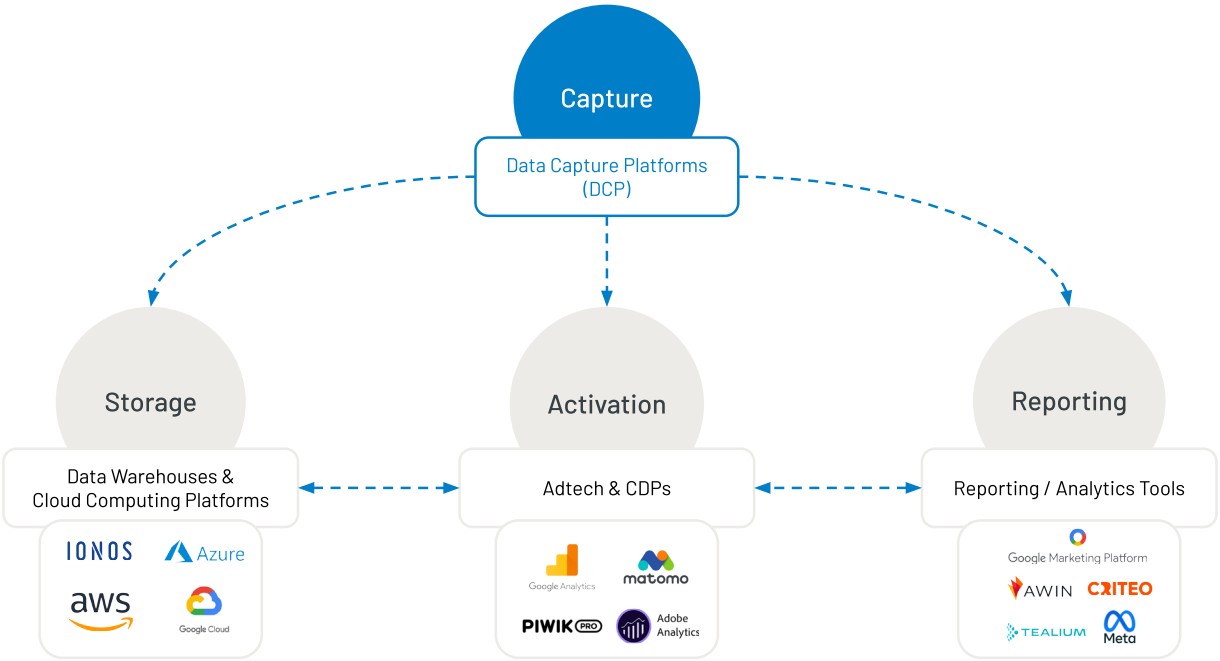
DCPs in the Value Chain

DCPs are at the very beginning of the data value chain: at the point of collection. Correct tracking directly at the source is crucial for the quality and legal compliance of first-party data. Deficiencies in this process can hardly be made up for in the further course of value creation and have a disproportionately negative effect, for example when the data is later activated as part of a marketing campaign.

A DCP routes the captured first-party data easily and flexibly to tools and platforms in your tech stack.

For example in cloud databases, reporting tools or adtech applications.

Matching the tracking to the consent of the website user is also essential. DCPs therefore have the option of connecting to consent management platforms. In this way, the user's consent information can be automatically passed on to the tracking setup.



Basic Functions of a DCP

Almost all companies use a tag manager to implement third-party tracking on their websites.

A further development of the Tag Manager is the so-called **server-side tracking**, also called **server-side tagging**.

Server-side tracking shifts the scope of tag management from the user's browser to a server. The user's browser therefore no longer runs a large number of tracking codes and cookies from third-party providers (third parties), but only your own first-party tracking code and a first-party cookie.

(More on this in the chapter "Server-side tracking explained")

DCPs provide server-side tag management to control tracking and **the integration** to forward the collected data out-of-the-box to tools and platforms in their own tech stack. It is important that before forwarding there is the option to modify the data and to preserve the data protection rights of the user or to comply with legal requirements. This includes, among other things:

Data minimization: The ability to remove e.g. user IDs, browser information or geolocation before forwarding.
Data modification: The possibility of protecting the data protection rights of its users through pseudonymization or complete anonymization before forwarding to third parties.

Server-side Tracking explained

Traditional Tracking (Client-side Tracking)

So far, tracking on websites has generally been carried out by third-party providers, for example providers of analytics tools or data platforms. They record the necessary behavioral data directly on their customers' websites.

The advantage for the third-party providers is that they can dispose of the collected data and receive valuable raw data – something that their customers are usually denied.

In turn, customers have the advantage of not having to worry about tracking. In return, you receive limited data reports and services.

On a technical level, this tracking works by embedding the respective Javascript tracking code from the third-party provider on a website. This code is executed in the user's browser, where third-party cookies are also placed in order to be able to track the user's behavior.

This type of tracking is called Client-side tracking or browser-side tracking because the tracking happens in the user's browser (client).

Disadvantages of Client-side Tracking

The main disadvantage of client-side tracking is that it can be detected and blocked relatively easily by adblockers and browsers. Today, this causes massive data loss and falsifies data on a large scale.

This form of tracking also poses a high data protection risk: website owners themselves have little control over what is tracked on their websites at all.

Another thing to keep in mind is that most websites implement multiple, sometimes dozens of, third-party data service providers. This means that just as many tracking code units have to be installed on the websites and just as many cookies have to be placed in the browsers of the users.

This leads to an immense inflation of the size of websites, which greatly affects the loading speed. It has been proven that bad loading times not only severely disrupt the user experience and thus the traffic, but are also penalized by Google with a downgrading in search results.

Server-side Tracking: The most powerful Way to capture first-party Data.

From third-party to first-party Data

Due to the problems surrounding client-side tracking, the change from third-party to first-party data collection, also known as "cookieless tracking", is currently taking place worldwide.

The difference here is that you do without third-party tracking code and cookies and collect your data yourself.

To do this, it is necessary to use your own first-party tracking code and a first-party cookie on the website.

First-party cookies are already being used to ensure essential functions of websites and are therefore completely under the control and responsibility of the owners.

Cookieless does not mean that there will be no cookies at all in the future. First-party cookies remain supported by browsers. They are also used for tracking.

Server-side Tracking

Instead of a large number of tracking codes, server-side tracking places a single JavaScript tracking code on the website. With this code and the associated first-party cookie, you can now collect first-party data yourself and send it to your own server, where you can modify it and finally forward it.

Server-side tracking with a DCP, explained step by step using Google Analytics as an example:

1. You install a first-party tracking code on your website.

2. With a server-side tag manager on your data capture platform, you define which actions of a user should be tracked on the website. For example: traffic source, page views, button clicks, scroll depth, length of stay.

3. A user surfs your website. A first-party cookie is set in the browser to make it recognizable on your own website. Third-party providers and other websites cannot track the user with this cookie.

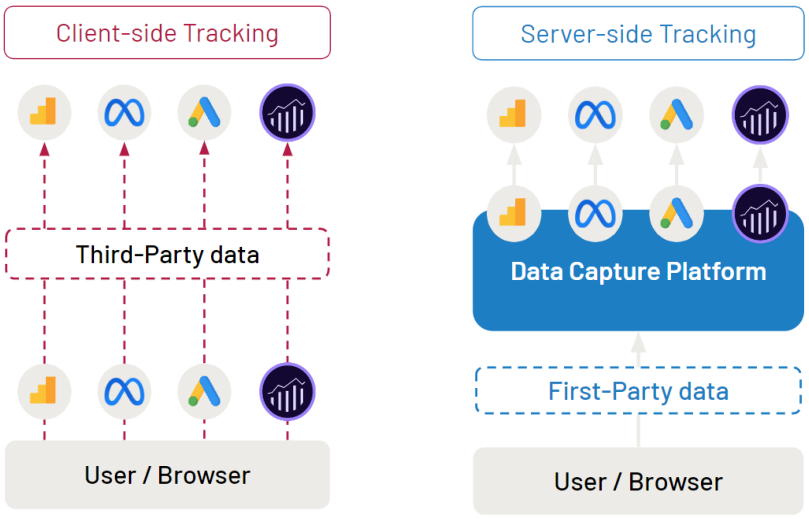
4. You now record the behavior of the user. Unlike before, the data does not go directly to third-party providers such as Google, but first to your own tracking server with which your DCP works with.

5. You can define in your DCP which data should be in which form to which of your marketing tools and data platforms should be forwarded. For example, if you want to use Google Analytics you can connect the tool to your DCP via an integration with your DCP.

6. You want to be sure that using Google Analytics is GDPR compliant. With your DCP, you can modify the data at the touch of a button, for example, by pseudonymization. In this way, you can use Google Analytics without making your users recognizable to Google.

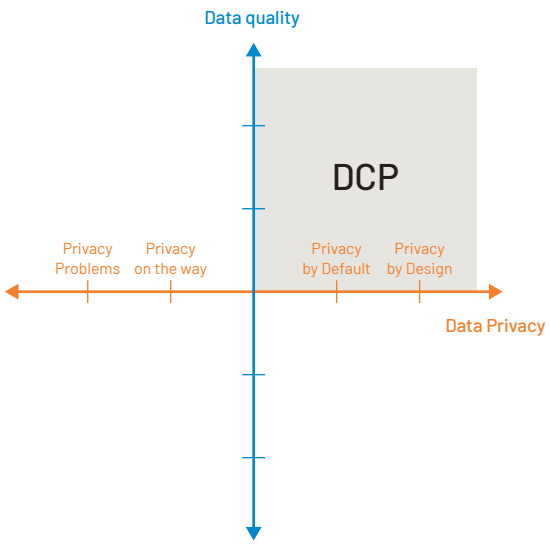
7. Your DCP forwards the data to Google Analytics, which you can now use as usual in compliance with the GDPR.

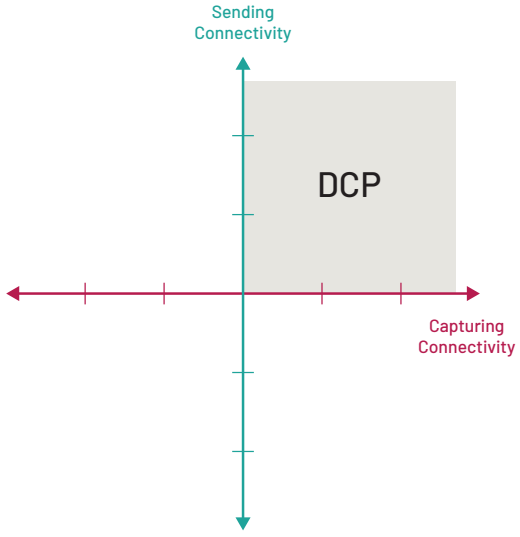
Client-side and server-side Tracking in direct Comparison



DCPs versus CMP, CDP, Tag Manager

A DCP is characterized by first-party data acquisition of the highest quality, privacy by design architecture with comprehensive data protection functionalities and a very high level of connectivity, both in terms of data collection and data forwarding. These requirements are not met by other tool categories in the data value chain.





How is a DCP different from...

... a Consent Management Platform (CMP)?

CMPs collect user consent, but do not collect behavioral data themselves. A DCP, on the other hand, is used for data acquisition. DCPs need connections to CMPs in order to be able to automatically process user consent and adjust tracking accordingly.

... a Customer Data Platform (CDP)?

CDPs serve to activate and segment data. DCPs do not offer these functions, but take on the upstream collection and forwarding of first-party data in a legally compliant manner, e.g. to a CDP.

... a Data Clean Room?

The matching of data with data sets between market participants takes place in a Data Clean Room. DCPs can, but do not have to, offer this functionality.

... Tag Management Systems

Tag management is an important part of a DCP but not the same, since DCPs also allow data to be checked and modified. Pure tag management systems do not offer this option and therefore cannot guarantee data protection.

... Analytics- and Reporting Tools

DCPs are not used for reporting or visualizing data, but forward accurate and data protection-compliant data to the respective analytics and reporting tools.

Managed Tracking vs. in-house Solutions

Organizations use server-side tracking in two different ways:
As an in-house development (in-house) and as a managed service (Saas), e.g. B. in the form of a DCP.

For **custom developments**, there are open frameworks, such as Server-side Google Tag Manager (SS-GTM). In this case, Google provides a tag manager. However, operation, implementation, further development and maintenance must be carried out by the user.

In practice this means:

- You have to host the solution and maintain it 24/7
- You have to develop and maintain the tool integrations (mostly) yourself.
- You have to develop and maintain the CMP linking
- Support is mainly provided by the community (agencies can also take over these tasks as well)
- With US providers there is a risk of data problems (Schrems II)

On the other hand, there is the managed service or software-as-a-service (SaaS) approach for data capture platforms. In this case, vendors provide complete products that take over a number of tasks as part of the service.

In practice this means:

- You don't have to worry about hosting and monitoring
- You don't have to worry about the tool integrations
- You don't have to take care of CMP linking
- Support is provided by a helpdesk or a personal contact, according to the SLA

The choice of variant depends on in-house development resources and data protection requirements.

How is the Market for DCPs developing?

By the end of third-party cookies in 2024 at the latest, market participants must have switched to some form of server-side tracking, otherwise they must expect serious losses in data quality and corresponding effects on the effectiveness of marketing campaigns and data strategies.

At the same time, data protection authorities in the European Union began to execute the regulations of the GDPR and to impose penalties in the first few years after the grace period. The GDPR itself has become a global model for data protection. Numerous US states have passed strict data protection laws of their own. With PIPL, China has taken its own path, which is also very restrictive for the private sector.

For companies and other organizations, this means that they have to be prepared for and react to different legal frameworks.

These framework conditions are currently leading to strong growth in the implementation of simple server-side tracking solutions and, in particular, in data capture platforms that cover all challenges.

However, care should be taken to ensure that providers of DCPs meet the criteria, particularly with regard to data quality, data protection and connectivity.

We have summarized the most important points when selecting a server-side tracking provider in a checklist for you.

Server-side Tracking

How to find the right provider

Because we know companies often struggle with finding the right information on implementing server-side tracking and evaluating vendors, we have created this checklist to give you guidance. The market for server-side tracking is growing rapidly but these points are essential and will remain relevant as the technology progresses.

Server-side tracking technology checklist:

1. At this point in your research, you will have learned about the benefits server-side tracking can provide for your business. Next, get an overview of the server-side tracking providers on the market.

2. When evaluating vendors, make sure to check how they handle the following criteria:

Data quality

- Is first-party data capture possible?
- Is data capture unaffected by ad-blockers?
- Is data capture unaffected by tracking preventions in browsers?

Compliance

- Are the servers located in the EU and operated by a European company? (Schrems II)
- Is compliant data anonymisation and pseudonymisation available?
- Can you get written confirmation of GDPR and ePrivacy compliance from the vendor?

Connectivity

- Which tool integrations are available?
- Which ecommerce plug-ins are available?
- Can your CMP be integrated with the server-side tracking product?
- How much customisation is possible?

Setup

- How is the solution implemented?
- How much time and resources are needed?
- How much support is available?
- How good is the documentation?
- Do you need specific SLAs?

3. Request offers from vendors.

4. Make sure to compare the total costs of ownership (licence, implementation cost, etc.).

5. Select the vendor that meets your criteria.

If you take these criteria into consideration when selecting your server-side tracking provider, you can maximise the data quality, data sovereignty and data compliance you get to ensure the resilient success of your online business.

JENTIS Data Capture Platform – The leader in server-side tracking

The JENTIS Data Capture Platform (DCP) features the most advanced server-side tracking technology on the market, powerful built-in compliance features and 100+ tool integrations.

Main Components

Server-side Tracking

Server-side tracking is the engine of the JENTIS Data Capture Platform and offers attractive features for companies that want precise data analysis, data protection and flexibility in processing user data.

Hosting

JENTIS takes care of your reliable, EU-based hosting so you can focus on optimising your marketing campaigns with superior data quality.

Tag Manager

JENTIS Tag Manager gives you full control over your server-side tracking setup. The user-friendly interface and several assistants make it easy to optimise your tracking according to your individual requirements.

Privacy Controls

Ensure compliance with international data protection regulations with JENTIS' advanced data protection features.

Connectors

Our proven connectors allow you to quickly and easily integrate your existing marketing and analytics tools into your tracking setup.

Advanced Features

Essential Mode

Collect data in a legally compliant way, even without consent, with JENTIS Essential Mode so you can better understand what visitors are really doing on your website.

Data Enrichment

Add valuable information to your website data with real-time data enrichment. More detailed analysis means better decisions.

Synthetic User

With Synthetic User from JENTIS, you can overcome the limitations of traditional tracking methods and gain valuable insights from 100% of your website data – while ensuring data privacy.

Raw Data

Gain independence from Big Tech for the first time by taking control of your raw data and using it in advanced business intelligence and data science applications.

ID Pooling

ID Pooling offers for the first time the possibility to activate data from visitors who are currently lost due to lack of consent. Achieve your growth goals through better performance marketing.

We‘re happy to help!

JENTIS is the technology leader in the field of data capture platforms and server-side tracking in Europe. Our highly developed technology guarantees the best data quality with excellent data protection with managed hosting within the EU.

Contact us if you would like more information and individual advice – free of charge and without obligation.

We‘re excited to help you transition to the cookieless future.

Your contact person:
Andreas Weichselbaum
Head of Sales

andreas@jentis.com
Tel.: +43 1 9974354 - 43
Meet Andreas

JENTIS GmbH
Schönbrunner Straße 231,
1120 Vienna, Austria

Tel.: +43 1 9974354
E-mail: office@jentis.com
www.jentis.com