TradeTracker.com®
performance marketing

GDPR – FAQ

1 Table of Contents

2 FAQ

2.1 Legal position, contracts and addendum

Q: Why does TradeTracker positions itself as a Data Controller?

A: Since initially TradeTracker decides what information to track and how to do so based on which technology. Following this, TradeTracker informs the advertiser on what to implement to be able and make use of the services of the network and under which economic model these services are carried out.

Q: TradeTracker determined legitimate interest to be the basis for its tracking activities, to process certain personal data. What grounds for the balancing test have been used to substantiate this?

A: First and foremost, it is based on the outcome of the balancing test and the principle that the data used in the course of executing the tracking activities are based on data which carries a very low risk of negative impact on the data subject's interest and will not result in a high risk to individuals being tracked.

Q: As an affiliate, am I a data controller or data processor?

A: For example, affiliates are a data controller when they provide for a newsletter subscription or otherwise having a (contracted) relationship with visitors – being their customers.

Whether one is controller or processor by the relevant party. It is important to understand the position of the party, as defined in the GDPR. A data controller is the entity which determines the purpose and manner for which data is processed, either by itself or alongside others. This means that the data controller determines 'why' data is processed. The data processor, on the other hand, does not make decisions as to why the data should be processed. However, it can make some limited decisions about 'how' the data should be processed. This means, for example, a data processor may make decisions about the type of software used in the processing, but it may not make decisions about the essential elements of the processing. A key essential element of processing is which personal data to process. Therefore, if a data processor, while assisting the data controller in achieving its purposes, decides what data should be processed to achieve those aims, it will most likely become a data controller jointly with the first controller.

Q: Under what legal basis does the merchant or affiliate process personal information?

A: This is up to each party to determine. TradeTracker processes personal data as a Data Controller with regards to the tracking of transactions under article 6.1 (f) – legitimate interest. Under Article 6.1 of the GDPR, processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Q: A merchant still wants TradeTracker to sign a Data Processing Agreement (DPA). Will we sign them?

A: No, we will not sign a data processing agreement, but instead an arrangement. Both the merchant and TradeTracker are Data Controller, making us Joint Controllers. Also, certain information will remain in the TradeTracker system even after the contractual obligations are completed, for the sake of reporting to other (previously) involved parties. This is part of the reason why TradeTracker is (also) a Controller.

Q: As a merchant, I cannot sign TradeTracker's Data Processing Arrangement addendum because I am a Data Controller myself.

A: TradeTracker also positions itself as a data controller, not a processor for the purpose of the affiliate program. Under article 26 of the GDPR where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers. They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14 of the GDPR, by means of an arrangement between them.

Q: As a publisher I would like TradeTracker to sign a Data Processing Agreement (DPA).

A: No, this is not standard procedure since TradeTracker (also) positions itself as a data controller for the purpose of the affiliate program. The affiliate and TradeTracker are a Data Controller, making us Joint Controllers for which parties need to agree on how to handle respective responsibilities.

Q: An agency is considered the processor of a merchant, the agency wants TradeTracker to sign a Data Processing Agreement (DPA). Should parties sign a DPA?

A: TradeTracker is a Data Controller in respect of the affiliate program. In this case the merchant and TradeTracker are joint controllers, where the agency has certain obligations it needs to meet under the Data Processing Agreement it has in place with the merchant. Therefore Article 26 arrangements need to be in place between the Agency and TradeTracker and the addendum is often sufficient. If the agency insists to have (only) standard data-removal articles added to the addendum, to meet their obligations, this amendment is possible since it is a general requirement under GDPR for data to be removed upon request.

Q: Should information be provided by merchants and affiliates in their privacy polies with regards to their use of TradeTracker?

A: There is no need to explicitly mention the individual parties you share data with or use as (sub-) processor. However, the category of recipients needs to be specified as third parties, in which case the TradeTracker service relates to e.g. online marketing services. Customers are allowed to create their own statement or alternatively may use the following text example:

[Merchant/Affiliate] makes use of the services of TradeTracker.com. Their role is to help advertisers and publishers understand which advertisements displayed by publishers have generated which sales, leads or other actions for advertisers. This allows the advertiser to pay a publisher only when the advertisement displayed (or any alternative required action) by the publisher refers an individual to the advertiser and that individual makes a purchase. TradeTracker uses data, including cookies, to achieve this understanding. This data relates to individuals but does not identify them by name. It is pseudonymous data and relates to a single referral by an individual from one website to another, and then a confirmation that a purchase was made.

TradeTracker also maintains a database of references to individual's devices, so that we can understand whether an advertisement viewed on one device, for example a phone, caused a purchase to be made by that individual on one of their other devices, for example a laptop. This database does not allow people to be identified by name, which is not possible for TradeTracker itself to achieve.

TradeTracker does not build profiles which show individuals internet purchase history over a period of time. TradeTracker also does not target individuals with advertisements for products and services based on their perceived interests. Their role is simply to measure the effectiveness of specific online advertisements.

2.2 Tracking and cookies

Q: Can anyone opt-out for TradeTracker cookies? If yes, how?

A: Yes, there is a possibility to opt-out for TradeTracker cookies. Publishers can apply the TradeTracker 'deny-handler' to opt-out from TradeTracker cookies.

If in addition to denying TradeTracker cookies, under GDPR the user must also be able to opt-out from their personal data being processed. This opt-out is possible via the cookie page on the TradeTracker domain, referred to by the merchant or affiliate as indicated in their own privacy policy. This opt-out sets a functional cookie on the user's system and avoids any tracking over cookies from the TradeTracker domain. As result the user has opted-out from TradeTracker processing personal data. The result is active until the user removes the cookie from his system or provides an opt-in. There is no alternative method for TradeTracker, or any provider using similar processes due to the nature of the business and limited scope of personal data it is involved with, to otherwise avoid users being tracked by cookies.

Q: What is the difference between cookie consent and data consent?

A: Cookie consent is required for placing any non-functional cookie. Irrespective whether personal data is included in such cookie. Data consent is one of the lawful grounds to processing personal data, referring to article 6.1(a). Hence giving consent to cookies being placed and data processed can be two very different things.

Q: If TradeTracker applies legitimate interest as a lawful basis to process personal data, why does TradeTracker still make use of cookies for its tracking activities?

A: TradeTracker does not depend on consent from the individual / data subject, due to the legitimate interest as a legal basis for processing personal data. The processing of personal data and consent for cookies however are two separate things to consider.

For the use of cookies, consent is (usually) required under the ePrivacy Directive. Cookies placed by TradeTracker do not contain personal data, but may be considered personal themselves. Hence, they are not subject to *data consent* which is another legal basis for processing personal data. As per our terms and conditions for publishers, they are required to obtain consent for cookies. TradeTracker assumes the publisher has obtained the visitor's consent for cookies unless TradeTracker is informed otherwise. If cookies are accepted, the tracking may occur via cookies.

In certain countries, like the Netherlands, affiliate cookies are exempted from requiring consent as required under the current ePrivacy Directive. Hence, the explicit consent is not required for this type of cookies unless they contain personal data.

TradeTracker makes use of cookies and other non-cookie-based tracking methods. Unless there is an explicit opt-out for the TradeTracker tracking services (under the opt-out for personal data processing), various tracking methods like fingerprint may be used since they do not require explicit consent from the user. To lawfully process the (pseudonymized) personal data in this functional "analytical tracking process", TradeTracker applies legitimate interest as a lawful basis to do so.

Q1/2: What happens to the tracking of transactions when the individual refuses cookies to be set on the affiliate domain? Can TradeTracker still track transactions based on alternative tracking methods?

A1/2: If a user explicitly opts-out of cookies and this information is adequately passed on to TradeTracker, the user expects cookies to not be set. In general, only when the user explicitly requests to opt-out from TradeTracker processing their personal data the transaction is not tracked. Alternative tracking methods are used otherwise, and transactions will generally be tracked.

Q2/2: What happens to the tracking of transactions when the individual accepts cookies to be set on the affiliate domain, but subsequently refuses on the merchant domain? Can TradeTracker still track transactions based on alternative tracking methods?

A2/2: If a user explicitly opts-out of cookies and this information is adequately passed on to TradeTracker, the user expects cookies to not be set. In general, only when the user explicitly requests to opt-out from TradeTracker processing their personal data the transaction is not tracked. Alternative tracking methods are used otherwise, and transactions will generally be tracked. Users will always be able to opt-out from TradeTracker by following the appropriate process as indicated in the privacy policy.

Q: In case of server-to-server tracking, does there need to be an arrangement between the merchant and TradeTracker?

A: Yes, if data provided to TradeTracker is considered personal data. For example, the Order ID is considered personal data and consequently parties need to make arrangements with regards to that data. Such arrangements are provided for under the standard merchant agreement and alternatively standard GDPR-addendum.

Q: The cookie consent tool facilitated by TradeTracker does not provide an option to reject cookies. Why not?

A: Under the current ePrivacy Directive there is no obligation to provide a possibility to reject cookies. Instead, the website provides a well-informed consent requirement to the user. The alternative is to leave the website.

2.3 Safeguards and policies

Q: How long does TradeTracker store the personal data, like IP addresses or other customer and transaction data?

A: TradeTracker only stores the data for as longs as is required to achieve the purpose for the particular processing of the data but removes any personal data [maximum 24 months] after the contract is terminated or after transactions are invoiced and paid out to the affiliate depending on the type of data.

Q: Where is data transferred to, outside the EEA?

A: Data related to the services of TradeTracker and performance of the contractual obligations between the network, merchants and affiliates are physically stored in the EU / EEA.

Q: Do TradeTracker employees see the same information as merchants and affiliates? Is it sufficient to mask the last octet of the IP address in the interface to comply with GDPR?

A: The TradeTracker platform is built to provide limited access to users, depending on their need to work with any such information. Masking the last octet of IP-addresses in the merchant and Yes, this is sufficient in the interfaces since it is only visible to the users operating under the contractual terms. Outside the UI the data is pseudonymized and therefore complies with GDPR. The information available to TradeTracker staff is used for fraud prevention.

Q: If a consumer requests for all data related to the person to be removed, how does TradeTracker adhere to this request?

A: Based on the limited personal data gathered by TradeTracker, the only information to possibly be removed is transactions data connected to an IP address. However, this can only be achieved by either receiving order IDs from the merchant, or the user sharing the IP address. The latter not being reliable due to its changing character.

Alternatively, the user refers to personal details (like contact details) provided as an affiliate. These can be anonymized upon request or alternatively will be removed according to internal policies.

Q: In the case of an affiliate transaction, who is responsible for the processing of personal data as the consumer passes from the affiliate site to the merchant domain and also interacts with the network servers?

A: As the consumer starts its journey on the affiliate site, the affiliate is responsible to safeguard the visitor's personal data. For example, by operating under SSL protocols. This means, that as the visitor continues its journey to the merchant it passes via TradeTracker servers through secured connection TradeTracker is responsible for the adequate processing and safeguarding of the data. Subsequently, as the visitor browser the site of the merchant, it is the merchant's responsibility to safeguard the data.

Q: Which technical and organizational measures does TradeTracker have in place to safeguard data?

A: <u>Availability</u>

Data centres and applied infrastructure are built in clusters in various regions. All data centres are online and serving customers; no data centre is "cold." In case of failure, automated processes move customer data traffic away from the affected area. Core applications are deployed in an N+1 configuration, so that in the event of a data centre failure, there is sufficient capacity to enable traffic to be load balanced to the remaining sites. Furthermore, Processor makes use of DDOS mitigation technologies.

<u>Integrity</u>

Data processing locking mechanisms make sure the Data is only processed if prior processes have completed successfully. Meaning integrity of the data is guaranteed.

Confidentiality

Personal Data is encrypted, and only selected employees have access to the processing actions of the Data and when an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee or otherwise involved with the company.

Security audits

Adequate review of policies and applications are executed every six months. TradeTracker is assisted by third party legal advisors to review continued compliance.

Portability

Upon request of Controller, Processor or Data Subject, TradeTracker undertakes to provide records of any Data Subject and has devised a streamlined process to adhere to such requests in a timely manner.

Accountability

TradeTracker makes use of various monitoring and logging tools on both application and infrastructure level. All data processed through such activities is fully compliant with privacy policies.

Individual records containing any Personal Data are stored with a time to live (TTL) and will be removed or destroyed / anonymized at such point.

Physical security

Amazon Web Services (AWS) delivers a scalable cloud computing platform with high availability and dependability, providing the tools that enable AWS to run a wide range of applications.

Among others, the following measures are adhered to by AWS: AWS data centres are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data centre floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.