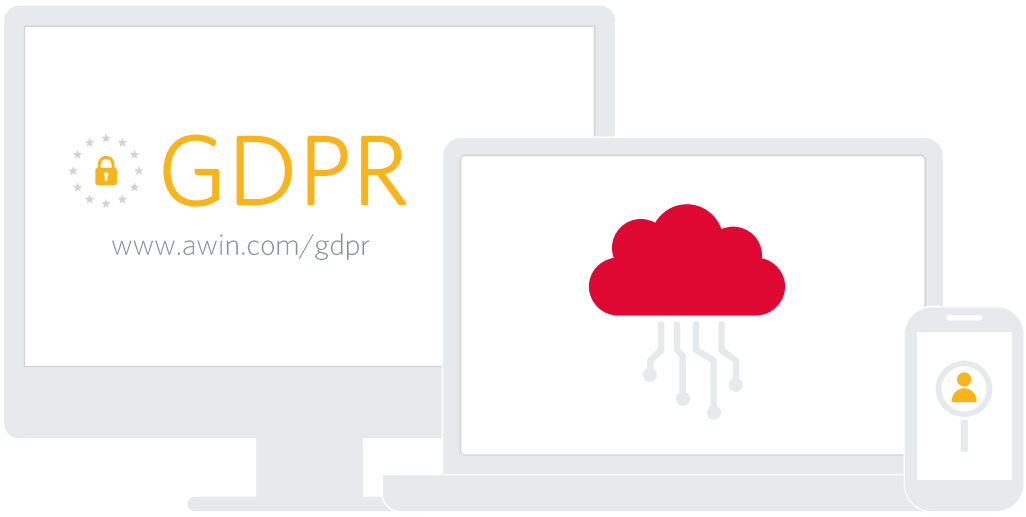
GDPR, ePrivacy & Awin

GDPR was a once in a generation opportunity to rethink data protection laws across Europe. For businesses working within the digital industries, it's critical they both grasp the intricacies of GDPR and ePrivacy. In this whitepaper we attempt to explain the implications for affiliate marketing and offer practical guidance for publishers and advertisers.



Contents

Awin & the GDPR

The General Data Protection Regulation (GDPR) came into force on 25 May 2018. It represented a significant change to the way personal data is regulated in the EU, replacing an existing legal framework which did not foresee the rapid increase of the use of personal data by businesses that has become commonplace in the last 20 or so years.

In the lead up to the coming into force of GDPR, every affiliate marketing network and SaaS platform carried out their own due diligence and sought legal guidance on their legal position for processing data and how they believe they fit within the advertiser/publisher ecosystem.

GDPR represented a significant change to the way personal data is regulated in the EU

Because there is no consistency in how affiliate networks use data, there is still no consensus, which inevitably can create confusion within the industry. This document seeks to outline the logic behind Awin's position and our expectations of the businesses we partner with.

01

GDPR in a nutshell

The GDPR, including the UK GDPR, is designed to empower EU/UK consumers and enshrine their rights regarding how their data is used. For digital industries this takes on heightened importance because the definition of what is considered personal data has been expanded to include anything that can single out an individual but isn't necessarily overtly personally identifiable. So, while an email address is obviously personal data, the scope also includes pseudonymous identifiers such as an IP address or order ID.

In order to process this data, businesses need to choose a legal basis, of which there are six. For some activities it is obvious but for many digital marketing companies they typically pick either *'consent'* or *'legitimate interest'*. More on these later.

Privacy by design demands businesses fundamentally rethink how they develop new tools and technology, guaranteeing privacy and data controls are part of the DNA of upgrades and releases.

Privacy by design demands businesses fundamentally rethink how they develop new tools and technology.

Data minimisation requires companies to only track the data they need to perform the outlined processing function.

Additionally, employee training and the appointment of individuals dedicated to enforcement are two important considerations.

Aside from the legal basis there are also some core principles enshrined in the GDPR.

Failure to adhere to the rules could result in the ultimate sanction; significant fines.

GDPR is therefore far-reaching and all-encompassing. But beyond this piece of legislation, the existing rules around digital marketing, enshrined in the member states' acts implementing the ePrivacy Directive, should also be considered in depth.

02
The full picture with ePrivacy

The ePrivacy Directive (or ePrivacy for short), gives people specific privacy rights in relation to electronic communications, the most significant area for affiliate marketing being the use of cookies and similar technologies. In the UK, these rules are set out in PECR, the Privacy and Electronic Communications Regulations. Here, we'll refer to the ePrivacy Directive for consistency.

The ePrivacy Directive complements general data protection laws and sets out more-specific privacy rights on electronic communications. There is complexity in understanding what ePrivacy means for Awin and any business operating in the EU which stems from the nature of the law.

Whereas the GDPR as its name entails is a regulation and as such is directly applicable as-is, ePrivacy in its current form is merely a directive, leaving the implementation up to the member states. The final text of the ePrivacy law has thus been determined by the individual member states and as a result, the requirements around cookies (and similar technologies) are subject to different requirements throughout Europe.

Therefore although GDPR is universally adopted, ePrivacy is subject to local interpretation.

This legal uncertainty will be resolved once the long-anticipated ePrivacy Regulation comes into effect, until then however, businesses operating in multiple jurisdictions have to consider seeking local guidance to ensure compliance.

To add a further layer of confusion, GDPR and ePrivacy cannot be interpreted in isolation. In some jurisdictions ePrivacy may require GDPR level consent for cookies (regardless of whether or not personal data is collected through that cookie). We have attempted to draw a clear distinction between the two when addressing data consent and cookie consent below.

GDPR and ePrivacy cannot be interpreted in isolation

Therefore, although this guidance is intended to tackle the GDPR's impact on affiliate marketing, we will also make references to ePrivacy to tackle data regulation in its entirety.

03
How does the GDPR impact the affiliate marketing industry?

GDPR's increased scope and application to types of personal data meant that, depending on the context, certain types of data that may have been previously unregulated by privacy laws, became

subject to regulation. This includes device IDs, cashback member ID, customer reference numbers and other technical identifiers. Furthermore, GDPR places stricter requirements for obtaining user consent for personal data processing.

It's important to note that in its purest form and in relation to Awin's specific services, the nature of the personal data processed for affiliate marketing is non-sensitive and largely technical.

Compare the channel to others that make use of personal data to build consumer profiles to target through ads; typically affiliate marketing doesn't engage with remarketing or programmatic techniques.

However, some brands will be working with affiliates who run this type of activity on a CPA basis through the affiliate channel and in some instances behavioural advertising and other performance-based marketing, which relies heavily on user profiling for the sending of targeted advertising, are subject to greater regulatory obligations.

Some other affiliate networks use affiliate generated data to build profiles for personalisation and remarketing services. Therefore, they may feel they need a legal basis other than legitimate interest to do so, which in turn carries different regulatory obligations which affiliates must adhere to.

Therefore, publishers will inevitably find themselves in a position where one network's obligations are different to another. When GDPR first came into force in March 2018, affiliate networks, led by Awin, attempted to create an industry consensus by meeting to agree on a consistent approach. While this wasn't possible, all attendees agreed to put their name to an industry statement.

Awin's recommendation for publishers is to contact all networks they're working with and be clear on what those networks' privacy requirements are and why.

Publishers will inevitably find themselves in a position where one network's obligations are different to another

04

Awin's preparation for the GDPR

One of the main impacts of the GDPR was that all businesses were compelled to examine their uses of personal data in the context of the scope, principles and rights provided by the GDPR. Awin carried this assessment out in the course of a detailed Privacy Impact Assessment (PIA). Awin's PIA has multiple objectives, amongst others to:

01

Create a detailed overview of all data collected in the course of Awin's tracking activities

02

Assess whether Awin acts as a controller or processor in respect of that data

03

Assess the purpose and legal basis of each processing activity

04

Carry out a 'balancing test' where legitimate interest has been identified as the legal basis of processing.*

05

Identify safeguards necessary to protect the data

06

Minimise the use of personal data wherever possible

*This test is used to assess whether Awin's assumptions in choosing legitimate interest are valid.

In interpreting Awin's position under the GDPR, it is important to understand how Awin processes personal data and what impact that has on the privacy of the individuals.

05

Personal data uses

In the regular course of its business, Awin processes data on the following categories of individuals:

01	02	03	04
Awin personnel	Publisher, advertiser and supplier personnel	Publishers where the publisher is an individual	Consumers whose purchases are tracked by Awin

For the purposes of this paper, we will only be detailing the tracking activity through which personal data is processed in respect of consumers. This is because all other processing activities are merely carried out for administering business and, pursuant to regulatory guidelines, such data is considered unlikely to result in a high risk to individuals.

We will only be detailing tracking activity

06

Consumer data

Awin primarily uses consumer data for tracking. Tracking enables Awin to understand a consumer's online journey across particular websites made after viewing or clicking an advertisement. The purpose of tracking is to attribute sales and marketing effort by a publisher to a particular transaction, to enable advertisers to reward publishers on a per transaction basis. Tracking also allows Awin to provide publishers and advertisers with related reports.

Cross Device Tracking enables Awin to understand a consumer journey when it starts on one device, with a transaction completing on another.

To carry out tracking, Awin uses tracking domain cookies, journey tags and device fingerprinting. Here's a brief explanation of how these technologies work:

Tracking domain cookies	Journey tags	Device fingerprinting
Cookies served by the Awin domain when a consumer clicks on an advertisement displayed on a publisher service.	JavaScript code integrated into the advertiser's website, to enable Awin to receive transactional information.	Method by which Awin is able to uniquely identify a device by considering certain attributes (incl. screen size/resolution and user configurations).

Cross Device Tracking makes use of the tracking domain cookies and the journey tag, in the same way, and for the same purposes, as tracking. Additionally, Cross Device Tracking develops pseudonymous consumer profiles, which are then used to match multiple devices to a single consumer.

All data Awin uses for tracking is pseudonymous, non-sensitive, largely technical and not related to behaviour, or predictions or evaluations of consumer interest or personalities.

07

Data controller or processor?

Every business that handles data must decide what role they play in processing that data.

This is an important consideration because there are different implications based on the role played. Deciding on whether you are a 'controller' or 'processor' of data is logically linked to what you do with the data tracked and the decisions you make about it.

You will be a controller if you determine:

Why	How
data should be processed; *and/or*	it should be processed to achieve the intended purpose.

Processors, on the other hand, never decide why to process data, they leave this to the controller who has instructed them. Processors can make limited decisions about how to go about processing data for the purposes determined by the controller, but these can only be 'non-essential' decisions.

This means that essential decisions should always be left to the controller, including decisions about what data to process to achieve the controller's purpose or the economic model of the purpose pursued.

The main thing to bear in mind is that the roles are allocated based on fact.

It is not possible to enter a contract which says, for example, "X will be controller, Y will be processor", if, factually, Y has been making decisions about what data to process for X's purposes; in this case Y will end up in the role of joint controller alongside X. If Y decides to process data for their own purposes, they will be a sole controller for that new purpose.

In affiliate marketing, the advertiser is always a controller because only the advertiser can decide 'why' to process data; only the advertiser can decide, for example "Let's do some marketing online and pay commissions on a CPA basis".

08
But what about networks and publishers? Are they processors or joint controllers with the advertiser?

Awin's position is that Awin is a joint controller with the advertiser, along with publishers. There is, in fact, a joint controller relationship between all three parties. This is because Awin has decided the economic model, and both Awin and publishers decide what data to process to deliver the advertiser's affiliate marketing campaign.

This is because of the way transactions are tracked, queried and reported.

We think this conclusion is the only one that accurately reflects how things work in practice.

If, let's say, Awin or publishers were to try to work within the constraints of a data processor role, they would need to get any new data processing approved by each respective advertiser in advance every time. They cannot make these decisions themselves; this seems both impractical and unworkable.

Awin has decided the economic model, and both Awin and publishers decide what data to process

09
How does this differ from other networks' positions?

Some networks have chosen a data processor position which means they don't then have to determine a legal basis for processing data and are therefore unable to determine a legal basis for their publishers.

They may choose to ensure advertisers engage publishers directly to ensure they are not liable for any potential data breach by a publisher, removing themselves directly from the publisher/advertiser relationship.

One of the additional challenges of being a data processor is the potential impact on your ability to make decisions about future development of your services and technology.

For example, Awin would need to inform advertisers if we entered into a data processor agreement with them, that they would be unable to make use of bug fixes, updates, upgrades, or additional features of Awin's products or services until the advertiser instructed Awin in writing to do so.

It is important to remember Awin's interpretation of the processor/controller position differs to other networks. Having sought legal advice, we are confident our position reflects the correct status.

Essentially, we believe the following statements outline our controller position:

01

Advertisers don't decide what to track. They choose a network, but the network decides how their technology works and what data gets used. Without this status a network would never be able to iterate any new technology without obtaining a new processor agreement from every partner.

02

Networks determine the economic model.

03

Networks instruct advertisers, such as telling them to keep the tracking up and running.

Direct marketing can be done with a single piece of data (such as an email address). This makes it workable for a controller to say to the processor/direct marketing business, "send emails to this list of email addresses". Affiliate marketing is more complex, which makes ensuring that the advertiser gives all the instructions to all their affiliates, unworkable.

10
What privacy arrangements does Awin have?

As joint controllers, the respective parties are required to enter into an arrangement in which the roles and responsibilities of all players are defined. As opposed to data processing agreements where one party acts as a controller and the other party as a processor, the parties have more freedom in determining the form and content of the arrangement and are not required to include the GDPR level obligations of a processor.

For advertisers, Awin provides a joint controller data processing addendum to the advertiser agreement that specifically addresses the data processing required for Awin's services.

For publishers, data processing terms are contained in annexes to our standard publisher agreement so that we are clear on which party is responsible for what. These terms cover, for example, how Awin and publishers will handle enquiries from consumers about data, or how they will deal with a data breach should this happen.

By making these responsibilities clear, it helps to prevent advertisers, publishers and Awin being liable for each other's breaches of GDPR.

By making these responsibilities clear, it helps to prevent advertisers, publishers and Awin being liable for each other's breaches of GDPR.

It also means that, as a controller, publishers will need to comply with more of the obligations of GDPR. However, all parties involved already need to do this when processing data for their own purposes. The consequence is that they will now also need to apply these obligations to the data processed when delivering customers for an advertiser.

The main benefit is that on the Awin network, if it is done in accordance with GDPR and relevant agreements or terms, the parties are able to decide for themselves how to process data. We strongly believe this is the case anyway and authorities would consider us joint controllers. By creating a contractual obligation that matches factual reality, everyone should be clear on what obligations they should assume under the GDPR.

Finally, in deciding our position we considered what data authorities are likely to categorise Awin and its advertisers and publishers as.

11
Legitimate interest and balancing test

As a controller, Awin is required to justify the processing of personal data before it will be considered lawful. There are six legal bases under which this can be done:

When assessing Awin's legitimate interest, the interests of the full affiliate ecosystem were taken into account. A balancing test was then carried out in which it was confirmed that tracking carries a very low risk of undue negative impact on the data subjects' interests or fundamental rights and freedoms.

This means Awin will not depend on individual consent as the legal basis for the processing of personal data under GDPR, as part of its tracking services.

It was confirmed that tracking carries a very low risk of undue negative impact on the data subjects'

12
Why not consent?

It's initially important to state that there continues to be a great deal of confusion around consent. This is partly because there is no industry consensus on the topic but primarily because, alongside GDPR consent, there is also consent related to the existing ePrivacy Directive.

These laws are separate but also co-exist. In the data privacy context, think of the GDPR as being broad and all-encompassing on all aspects of personal data regulation. ePrivacy by contrast is specifically concerned with direct marketing and the functions of online tracking, such as the use of cookies or similar technologies.

Inevitably there is some overlap which arises because cookies often contain personal data, but it is a mistake to assume that cookies and personal data are one and the same.

Under GDPR, there are plenty of ways to legally process personal data without relying on data consent and in fact, it is fair to say that data consent is the least convenient and most burdensome legal basis for data processing.

There is no industry consensus on the topic but primarily because, alongside GDPR consent, there is also consent related to the existing ePrivacy Directive

Under the ePrivacy Directive, cookie consent is always required to set cookies, unless the cookies are strictly necessary to deliver a service requested by the individual. So, cashback and reward publishers, for example, may not need cookie consent for affiliate cookies because affiliate cookies are necessary for a cashback or rewards-based type of service to work.

Obtaining data consent isn't without its challenges. In doing so the onsite user experience may be negatively impacted and the individual may refuse to consent anyway.

When personal data is processed based on data consent, the individual is given greater data rights, which will need to be respected in future. Furthermore, the data consent must be managed and recorded at a particular level of detail. Additionally, providing a service or content cannot be denied to consumers and users because they have refused to give data consent, unless the service depends on that data consent.

Perhaps most importantly, to obtain valid data consent, the individual must be provided with enough information to make an informed decision.

Because Awin is an affiliate network, we use limited personal data for tracking referrals to advertiser websites, the consequent transactions and our reporting, but we never reuse this data to build behavioural user profiles or for other marketing purposes. We also don't collect any other data for:

01	02	03
Building behavioural user profiles	Behaviourally targeting	Marketing for any other purposes

To be undertaken lawfully, those types of processing tend to require a data consent because they are perceived to have a greater impact on individuals' privacy. By avoiding this type of processing, Awin can rely on legitimate interest to justify its processing and avoid requirements for data consent from publishers or advertisers to legally track transactions.

This applies to the processing of personal data as individuals travel from the publisher website to advertiser websites, via our domains, tracking the confirmation of the transaction and the subsequent reporting available in the user interface.

Respecting consent

It's important to consider that if a controller picks consent as a legal basis they may not be able to use another legal basis should consent prove problematic to obtain.

According to the Article 29 Working Party Guidelines on consent under Regulation 2016/679, if consent is chosen as a legal basis for any part of the processing the controller must respect that and stop that part of the processing if an individual withdraws consent. It adds:

If consent is chosen as a legal basis for any part of the processing the controller must respect that

"Sending out the message that data will be processed on the basis of consent, while actually some other lawful basis is relied on, would be fundamentally unfair to individuals. In other words, the controller cannot swap from consent to other lawful bases. For example, it is not allowed to retrospectively utilise the legitimate interest basis in order to justify processing, where problems have been encountered with the validity of consent."

Because of the need for prior disclosure of a legal basis, a controller must decide in advance which one of the six bases will be adopted.

14

The ePrivacy Directive

Since the ePrivacy Directive was implemented into national laws across the EU, everyone is required to obtain cookie consent when setting cookies.

Awin has required publishers to obtain cookie consent under our terms with publishers since 2012. This is to make sure that publishers comply with these rules, but also to obtain cookie consent for Awin's cookies, on behalf of Awin. This is typical of networks like ours, which don't have a natural or convenient opportunity to engage with individuals to obtain cookie consent.

15

So why are we talking about Cookie Consent all over again?

Cookie consent has been back under discussion in recent years because, in most EU member states, laws implementing the ePrivacy Directive relied on the definition of consent in local data laws for the cookie consent definition.

So, when GDPR replaced local data laws, the definition used for cookie consent was also replaced.

It is significant because the standard of consent necessary for GDPR is higher than under some pre-existing local data laws and this has been further clarified under case law and in guidance issued since the GDPR came into force.

14

How does GDPR impact Cookie Consent?

The upshot is that obtaining cookie consent is now more involved. The specific difference being that, because cookie consent must be unambiguous, the common approach of using implied consent is not sufficient. Cookie consent should also be given before cookies are set.

To obtain a valid cookie consent under the new consent definition, the individual must do something active to indicate their agreement. You are surely familiar with universal consent tools or consent management platforms (CMPs); technology that serves up a message when a user arrives on a website and seeks permission to track that consumer's onsite activity.

Most website operators, including publishers and advertisers use such consent tools to obtain consent for the cookies served on their website, including Awin's cookies when working on the Awin platform.

17

So how are Cookie Consent and Data Consent different?

Because cookies are inherently less complicated than all the things that could be done with personal data, complying with the increased consent standards is much easier when obtaining cookie consent than when obtaining data consent.

This is because there is less to explain to the individual, fewer record keeping obligations and fewer additional rights to offer the individual.

The compliance risk is also lower, because the huge fines brought in by GDPR do not apply to cookie consent, unlike data consents used for cookies.

Even though laws implementing the ePrivacy Directive rely on the GDPR for the definition of consent, they still have their own fines and penalties for non-compliance.

18

How does this impact the way publishers and advertisers work with Awin?

Obtaining cookie consent continues to be required by Awin for its publishers and advertisers, both to obtain cookie consent for themselves and for Awin's cookies.

We also review publishers' and advertisers' compliance with these requirements and ask them to correctly obtain cookie consent if it appears to us that they are not.

However, Awin does not mandate how cookie consent must be obtained.

Complying with existing obligations has been made harder for publishers

Awin offers a consent tool which may be used for cookie consent, but we are also happy for publishers and advertisers to use other consent tools, or to obtain valid consent in other ways.

We recognise GDPR is not straightforward, especially for smaller publishers or advertisers, and we try to minimise the burdens of compliance for our partners in whichever ways are possible.

One way is to justify our data processing based on legitimate interest, so we do not need to ask publishers or advertisers to obtain any data consent for us. This is not an option for cookie consent; if a website operator does not need to set the cookie to deliver a service requested by an individual, cookie consent cannot be avoided.

19

Awin's position in a nutshell

Awin is a joint controller with advertisers and most publishers.

This negates the need to sign data processing agreements.

It gives the network the flexibility to develop new technology and decide the basis for future technology upgrades and releases.

Awin is using legitimate interest as a legal basis for processing data.

Awin does not require its partners to seek consent for GDPR.

Awin requires all advertisers and publishers to seek valid cookie consent in compliance with applicable data laws.

Publishers and advertisers are free to obtain consent in whichever way they see fit, however, Awin offers an easy to install consent tool.

20

What does this all mean if I am an advertiser or publisher working with Awin?

As a business operating under the GDPR, you have certain obligations as a controller. Additionally, when working with Awin you have some tasks in ensuring that affiliate tracking is operated lawfully on your website. We have created a checklist on the most important things to consider:

- Check whether you are required to register with your local data protection authority;
- Update your terms and conditions and privacy policy if needed;
- Enter into agreements or arrangements with all third parties with whom you process data;
- Make sure you have contact details where individuals can contact you with privacy-related queries;
- Make sure you have a legal basis for all processing activities;
- Gather consent for cookies where ePrivacy requires you to do so and make sure your consent mechanism covers all your activities.

21

Where do I find out more?

Awin has a GDPR hub, found here.

Awin's FAQs on data protection and security

Over the past years we have seen a steady increase in the number of queries we receive around our data processing activities. The questions range from compliance with the GDPR to more technical queries around data security. Below we have listed the most frequent questions from both advertisers and publishers.

Is Awin GDPR compliant?

As a company headquartered and operating in Europe and dealing with personal data on a daily basis, GDPR compliance is core to Awin's business. Awin has undergone a Privacy Impact Assessment to ensure compliance with the GDPR and has implemented a number of safeguards to ensure ongoing compliance. Awin is continuously monitoring legal guidance and decisions and is committed to ensuring that all of its operations remain compliant in light of any developments.

Do you have an appointed data protection officer? How can we reach them?

Yes, Awin has appointed a data protection officer. You can reach the DPO at global-privacy@awin.com.

What personal data do you capture, store or process in the course of tracking?

The data Awin uses for tracking is pseudonymous, non-sensitive, largely technical and not related to behaviour, or predictions or evaluations of consumer interest or personalities.

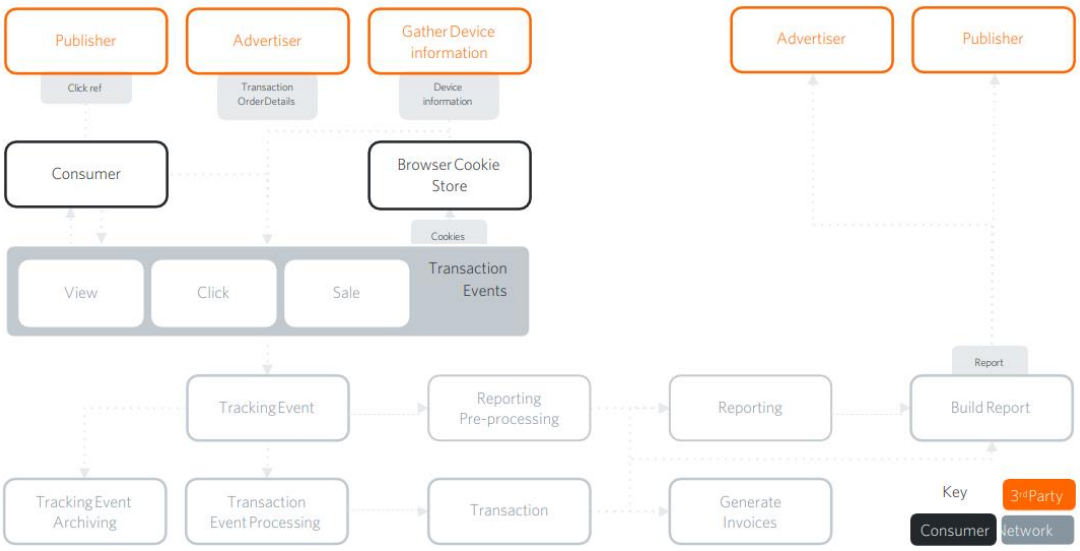
A tracking cookie would, for example, collect the following pieces of data:

Cookie Date	Expiry Date of Cookie	IP Address (truncated)	IP Hash
GeoIP	Advertiser ID	Publisher ID	Banner ID
Group ID	Product ID	Click/Network Reference	Referrer
	Overwritten Publisher ID	Platform	

Does Awin collect any sensitive personal data?

No, Awin does not collect any sensitive data during the tracking or administering of its business with advertisers, publishers and suppliers. Awin may collect sensitive data on its employees where required by law.

What is the flow of data that Awin tracks?



Please note, this is not an exhaustive dataflow diagram, but identifies the major processing functions.

Where do you physically store this data?

Within the EU/UK.

To host the application and data, do you use the services of a host or a cloud provider?

Yes, Equinix (London/Slough) which are our co-located data centres. Cloud providers: AWS (Ireland and Frankfurt, Germany) and Azure (Amsterdam).

How long do you store the data? Do you have processes in place for automatically deleting the data?

Awin retains data in line with its retention policy. Unless otherwise specified in the policy (and permitted by law), personal data is deleted after 36 months. We have implemented automated deletion routines to ensure data is deleted upon expiry of the applicable retention period.

Are you ISO 27001 certified?

In February 2022 we successfully passed the Stage 2 audit of ISO 27001 assessment certification against the in-scope systems and services, by independent auditors from BSI, and in March the ISO 27001 certification was attained. Yearly surveillance audits and re-certification audits will be in place.

Describe the process for regular monitoring, reviewing and auditing of the service provided by your third-party suppliers.

Suppliers are subject to vendor risk management which includes vendor due diligence upon onboarding and regular reviews thereafter.

Do you separate customer data?

We logically separate data. ACLs are used within the Awin User Interface to ensure that data is logically segregated and that it cannot be accessed or corrupted by other clients.

Do you conduct penetration tests?

Yes, penetration tests are performed by a reputable third party on an annual basis. We also have a Bug Bounty Program in place.

Do you have controls in place to restrict and monitor the installation of unauthorized software onto your systems?

All software needs to be onboarded via the Vendor Information Security review process. Users are provided with a library in Microsoft store of allowed apps. Any other software is installed by Internal IT after approval.

Do you use any third-party organisations as sub-processors of the personal data?

Yes, Awin uses a number of processors; a full list of processors can be shared upon request. These service providers have undergone privacy and information security reviews and a data processing agreement is in place where necessary.

Do you transfer any of the data outside of the EU?

Awin transfers outside of the EU only where there are appropriate safeguards in place to do so.

Please describe the technical and organisational measures you have in place to safeguard the data.

Awin's technical and organisational measures (TOMs) include:

- Pseudonymising and anonymising data wherever possible (IP address truncation has been rolled out, e-mail addresses are hashed when used, customer ID information is pseudonymised)
- Physical security measures (card protection, restricted guest access)
- The use of credential-based access rights, whereby rights are granted on a need-to-know basis. Right to access data is granted when there is a business case for that person to have access.
- A mandatory training programme for employees on both data protection and data security.

Updated policies around data security including Awin's Business Continuity Plan, Incident Reporting Policy, Information Handling Policy, etc.

Do you regularly test/assess/update the TOMs?

Yes, the TOMs are reviewed on a yearly basis and in the unlikely event of any security or data breach.

Do you encrypt, anonymise or psuedonymise personal data to ensure it cannot be read by unintended parties?

The data collected in the course of tracking is pseudonymous (IP addresses are truncated, e-mail addresses used for cross-device tracking are hashed by default). All data in transit is encrypted when traversing over public networks (utilizing TLS or IPSec encryption based on current industry standards). Removable devices, laptops and mobile devices have full disk-encryption enabled.

Please describe the physical security of your buildings.

Access to all sites (offices and data centre) are controlled by key card access. Guests are not permitted to access these sites unaccompanied by a member of staff. Access to Data Center locations is limited to pre-approved personnel within the IT teams. All access to these locations is logged and feature industry-leading physical security controls.

Do you have firewall protection integrated within your systems?

All of Awin's internal services are connected to the internet by firewalls, which protect services against external attacks, internally firewalling further segregate and protect our services. Our Operations Team run vulnerability scans on our external systems each week.

What measures do you have in place for limiting access to data?

As part of our preparation for the GDPR we have reviewed our access control policy and have reinforced commitments such as:

- Access control arrangements are followed to restrict access to Awin facilities, business applications, information systems, networks and computing devices.
- All individuals with access to IT systems, information systems, applications, networks and computing devices are authorised before they are granted access privileges.
- The principle of least privilege should be followed.
- Separation of duties should be considered.
- Access to Awin facilities must be strictly controlled, with access granted on an individual basis to authenticated and authorised personnel using appropriate physical security controls.
- Access rights cannot be granted collectively or shared within a group.
- In general, access to information systems containing personal or confidential information must require 2-factor authentication.

Do you have security breach notifications in place?

Breaches are handled and reported in line with our incident response plan. In case of a personal data breach (or an unlawful disclosure of confidential information), notifications are made to the impacted parties and/or relevant authority in line with legal obligations.

How do you ensure the data protection authority would be notified within 72-hours in case of a data breach?

Any breach needs to be reported to the DPO of Awin immediately. This is a critical element in ensuring the 72-hour deadline is met and is therefore emphasised in all training, informational

materials and policies for employees. Once the information has reached the DPO, the DPO will take care of the notification to the data protection authority, as required.

How do you ensure the rights of individuals?

Awin has processes around ensuring fulfilment of the rights of individuals as enshrined in GDPR. All requests should be addressed to global-privacy@awin.com where the request will be actioned in accordance with the relevant process.

Have all your staff involved in the processing of customer data received training on Data Protection and Information Security?

Yes, we provide both Privacy and Information Security compulsory training upon onboarding employees. Additionally, we implement yearly refresher trainings. Do note that our training is concluded with a test at the end, to ensure sufficient knowledge.

Please provide a link to your privacy policy.

https://www.awin.com/gb/privacy

Can you provide sample wording to refer to Awin within our privacy policies?

You may use any wording of our policy for the purposes of your disclosures.

Can we sign a data processing agreement as an advertiser?

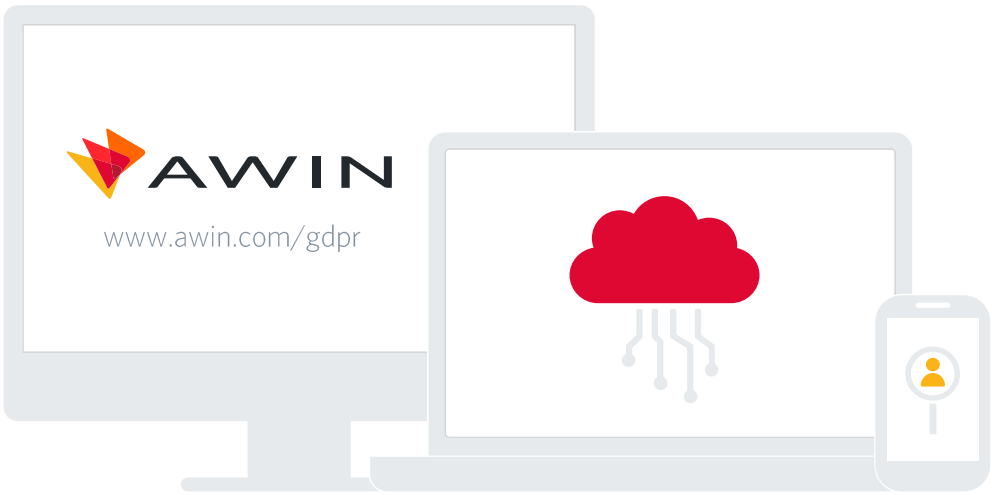
Yes, this already automatically forms part of your affiliate marketing advertiser agreement with Awin.

Can we sign a data processing agreement as a publisher?

This is not necessary as all relevant provisions are already included in the publisher terms, as annexes to those terms. Please review these terms.

Who can I turn to with further queries?

Our account managers will be able to respond to general queries around data protection. In case you would like to speak with our DPO directly, you can email global-privacy@awin.com



AWIN