GDPR, ePrivacy & Awin

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

Contents

Introduction

Awin & the GDPR

The General Data Protection Regulation (GDPR) will come into force on 25th May 2018. It represents 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 years.

Every affiliate marketing network and SaaS platform has been carrying out their own due diligence and seeking legal guidance on what their legal position is for processing data and how they believe they fit within the advertiser/publisher ecosystem.

Because there is no consistency in how affiliate networks use data, there is no consensus which has inevitably created 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 is designed to empower EU consumers and enshrine their rights about 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 will need to choose a legal basis, of which there are six. For some companies it will be obvious but for many digital marketing companies they will need to typically pick either *'consent'* or *'legitimate interest'*. More on these later.

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

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.

Data minimisation requires companies 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.

Failure to adhere to the new 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 (more colloquially known as the Cookie Directive), 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.

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 to businesses operating in Europe, 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.

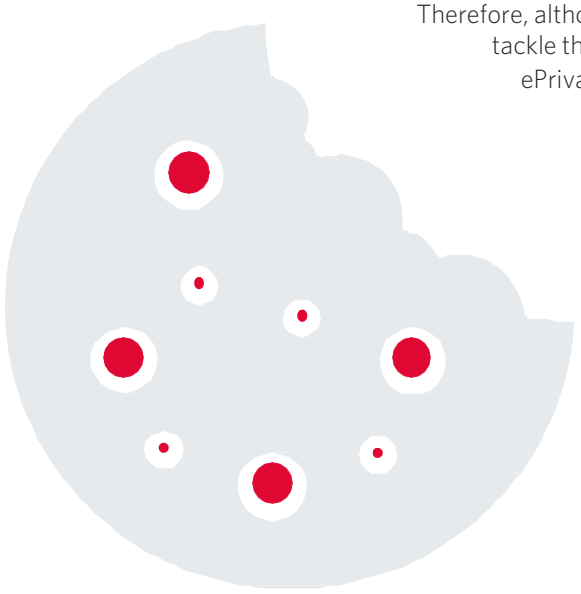
Therefore GDPR must be universally adopted whereas ePrivacy is subject to local interpretation.

This legal uncertainty will be resolved once the 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 consents and cookie consents 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?

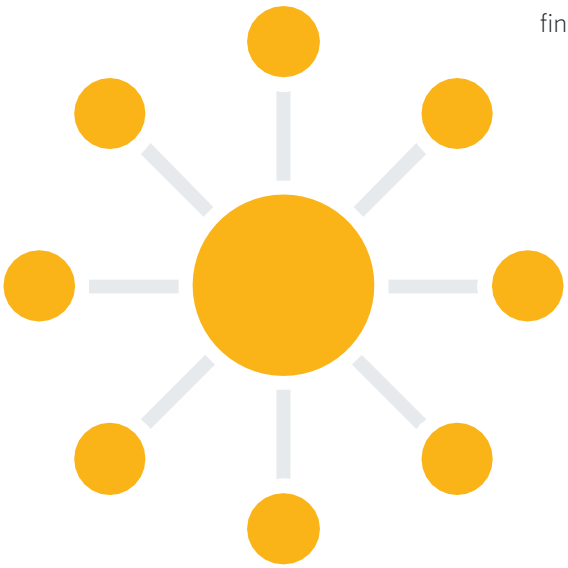
GDPR's increased scope and application to types of personal data which, depending on the context, may be currently unregulated, is of relevance to our industry as this data will now be subject to regulation. This includes device IDs, cashback member IDs, customer reference numbers and other technical identifiers. Furthermore, GDPR enacts stricter requirements for obtaining user consent for personal data processing.

We do not anticipate a considerable impact to affiliate marketing. In its purest form, and in relation to Awin's specific services, the nature of the personal data processed 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 we expect that in some instances behavioural advertising and other performance-based marketing, which relies heavily on user profiling for the sending of targeted advertising, may be 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 different legal basis to do so, which in turn carries different regulatory obligations which affiliates must adhere to.



Consequently, publishers will inevitably find themselves in a position where one network's obligations are different to another's. Affiliate networks, led by Awin, attempted to create an industry consensus in March 2018 by meeting to agree on a consistent approach. While this wasn't possible, all attendees did agree to put their name to an official industry statement.

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

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

04

Awin's preparation for the GDPR

One of the main impacts of the GDPR is that all businesses are compelled to examine their uses of personal data in the context of the new scope, principles and rights provided by the GDPR. Awin carried this assessment out in the course of a detailed Privacy Impact Assessment (PIA). In the course of our PIA, we have

01

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

02

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

03

Assessed the purpose and legal basis of each processing activity

04

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

05

Identified safeguards necessary to protect the data

06

Minimised 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 extremely unlikely to result in a high risk to individuals.

We will only be detailing the tracking activity through which personal data is processed.

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 can 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.

The data Awin tracks is all pseudonymous, non-sensitive, largely technical and not related to behaviour, 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 as 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 data should be processed

How it should be processed to achieve the intended purpose, *or both*.

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

Networks and publishers; processors or joint controllers with the advertiser?

Awin's position is that Awin is a joint controller with the advertiser, and with publishers. There is, in fact, a tripartite joint controller relationship. 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.

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

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.

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 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 chose 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 tech 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 provisions are Awin making?

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 text of the arrangement and are not required to include the GDPR level obligations of a processor.

For advertisers, Awin is providing a joint controller data processing agreement upon request. Awin is also updating the advertiser terms and privacy policy to include the sections around data processing as a fall-back scenario for when there is no data processing arrangement in place.

For publishers, we are adding new terms to our standard publisher agreement so that we are clear on which joint controller 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, (advertisers and) 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 can 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 the 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:

Consent	Contract	Legal obligation	Vital interest	Public task	Legitimate interest

All publicly issued statements from networks have indicated one of two legal bases will be used. Two have said they will use consent as a legal basis, the remainder legitimate interest.

When assessing Awin's legitimate interest, the interests of the full affiliate ecosystem were considered. A balancing test was then carried out in which it was confirmed that tracking carries no risk or 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, as part of its tracking services under GDPR.

It was confirmed that tracking carries no risk or a very low risk of undue negative impact on the data subjects'

12

Why not consent?

It's initially important to state that there is 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 (commonly referred to as the Cookie Directive).

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. If data privacy is considered, think of the GDPR Regulation as being all-encompassing and broad on all aspects of data. ePrivacy by contrast is specifically concerned with Direct Marketing and the functions of online tracking.

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 many 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.

Under the 2012 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 a 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.

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 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 a pureplay 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.

13

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 based on 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 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.

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.

Cookie Consent is back under discussion because, in most EU member states, laws implementing the ePrivacy Directive rely on the definition of consent in local data laws for the Cookie Consent definition.

So, when GDPR replaces local data laws, the definition used for Cookie Consent is also replaced.

It is significant because the standard of consent necessary for GDPR is higher than under existing local data laws; the key difference being that consent must be unambiguous.

15

How does GDPR impact Cookie Consent?

The outcome 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 unlikely to be 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 to indicate their agreement. You may be familiar with a growing focus on universal consent tools; a piece of technology that serves up a message when a user arrives on a website and seeks permission to track that consumer's onsite activity.

The individual must do something to indicate their agreement

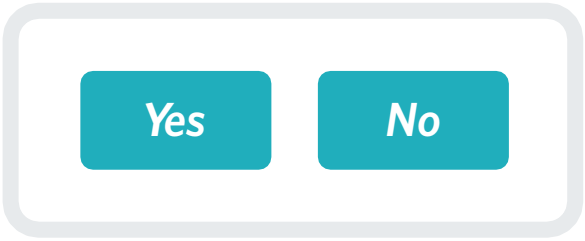
Therefore, publishers may choose to use consent tools, but consent could also be obtained, for example, by continuing to navigate a website by clicking internal or external links (provided that cookies aren't set before this point).

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 for cookies.

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.



16

How does this change the way publishers work with Awin?

We recognise that, because of this change in the definition of consent, complying with existing obligations has been made harder for publishers. This is unless they operate in a jurisdiction like the Netherlands, which already requires individuals to indicate their consent to cookies.

Complying with existing obligations has been made harder for publishers

Cookie Consent will continue to be required by Awin for its publishers to obtain Cookie Consent both for themselves and for the cookies set by Awin's domain.

We will also be continuing to review publishers' compliance with these requirements and asking 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.

Awin will be offering a consent tool which may be used for Cookie Consent, but we are also happy for publishers to use other consent tools, or to obtain valid consent in other ways. For example, it will be sufficient in most cases to change existing cookie notices to explain that an individual will be giving his or her consent to an affiliate tracking cookie if they click an external link without changing their browser cookie settings. Awin's approach will follow this methodology.

We recognise GDPR is not straightforward, especially for smaller publishers, and we are trying to minimise the burdens of compliance for our publishers 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 to obtain any Data Consent for us. This is not an option for Cookie Consent; if a business does not need to set the cookie to deliver a service requested by an individual, Cookie Consent cannot be avoided. However, as Cookie Consent is more straightforward than Data Consent to cookies, we can at least be flexible in the methods of lawful Cookie Consent that are acceptable to us.

17

Awin's consent tool

Awin's consent tool has been designed to be used by publishers who are seeking to obtain cookie consent under current ePrivacy guidance.

It is a simple banner that can be easily installed and is designed to be instructional for consumers, but not intrusive or disruptive.

The technology is similar to that issued by Awin in 2012 when the ePrivacy Directive was passed into law and sought to obtain 'informed' consent from consumers. In its updated version the banner will seek explicit consent, linking the consent to the action of clicking on an advertisement.

Cookie consent requirements, as mentioned, have been strengthened. Awin believes serving up a notice on a website when the visitor arrives that informs them that by clicking on a link they will be served with tracking cookies,, allows users to make a considered and clear decision should they then continue to click on affiliate links on the page. If a user chooses to click on a link, but wishes to opt-out from tracking, this will of course still be possible by changing the browser settings to switch off cookies should they choose to do so.

Please note, publishers will need to obtain cookie consent for other cookies they may be dropping. The banner is not integrated with the IAB Consent framework at present, due to the focus of this tool on programmatic and personalised activity.

More information can be found here. Further instructions are also available when logged into the user interface.

Publishers will need to obtain cookie consent for other cookies they may be dropping

18

Awin's position in short

01

Awin is a joint controller with advertisers and most publishers

02

This negates the need to sign data processing agreements

03

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

04

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

05

Awin is not requiring affiliates to seek consent for GDPR, offering a flexible approach (also recognising that some affiliate models will be better suited to different legal bases)

06

Awin will require all affiliates to seek Cookie Consent under existing data laws; this is unchanged since 2012 but consent has been strengthened and now must be freely given and unambiguous

07

Publishers are free to obtain consent in whichever way they see fit, however, Awin will be offering an easy to install consent tool

19

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, as a publisher working with Awin you will 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 after 25 May:

01

Check whether you are required to register with your local data protection authority

02

Update your terms and conditions and privacy policy for GDPR

03

Enter into agreements or arrangements with all third parties with whom you process data; accept any updated terms to make sure they apply post 25 May

04

Make sure you have contact details where individuals can contact you with privacy related queries

05

Make sure you have a legal basis for all processing activities

06

Gather consent for cookies where ePrivacy requires you to do so and make sure your consent mechanism covers all your activities

20

Where do I find out more?

Awin is updating its GDPR portal, found here. The network will also be publishing further guidance and a whitepaper on all these topics and themes.In the past few months 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? How did Awin prepare for the GDPR?

Yes, Awin is compliant with the provisions of the GDPR. In the past few months a cross-departmental working group has been working to ensure Awin's GDPR compliance for the May deadline. Projects including the creation of a Privacy Impact Assessment (PIA), a review of all contractual relationships around data privacy, internal data minimisation and policy review have been carried out. Although we consider ourselves compliant, we will continue seeking improvements as the GDPR requires businesses to keep data privacy at the forefront of their operations and to continuously improve data processing practices wherever possible. May 25th is considered the starting point for future data privacy provisions, as well as the deadline for compliance.

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

Yes, Awin has appointed a team of data protection officers to ensure there is sufficient local representation within our core markets. You can reach the DPOs 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.

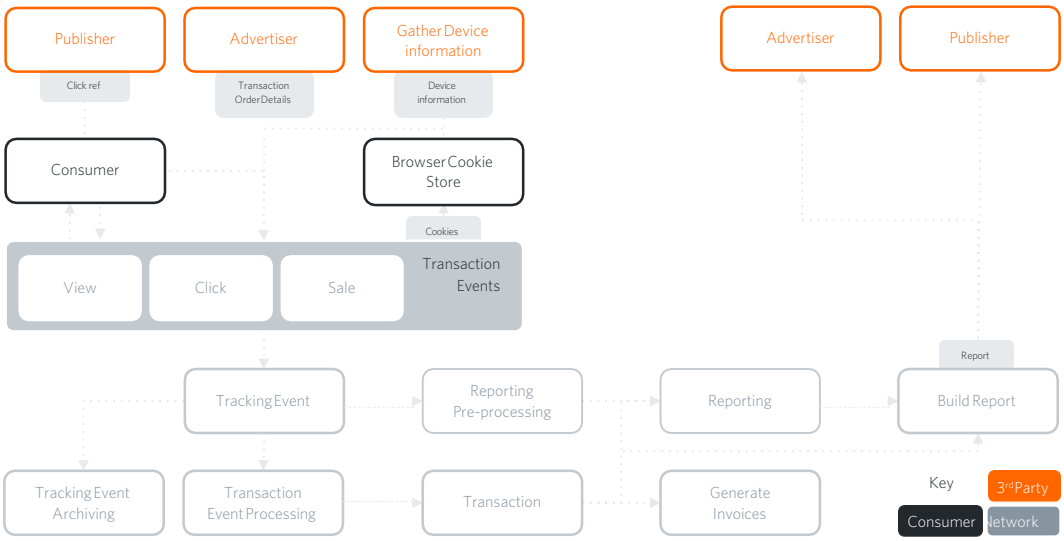
A tracking cookie would, for example, collect the following bits of data:

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.

Are there any secondary/backup sites?

Locally backed-up data is encrypted and stored offline in an offsite AWS cloud storage.

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

Yes, Colt Technology Services (Berlin), Equinix (London/Slough) which are our co-located data centers. 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 has reviewed and updated its data retention policy. Unless otherwise specified in the policy (and permitted by law), personal data is deleted after 36 months.

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

Yes, Awin uses a number of processors; a can be shared upon request. These service providers have undergone a review 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 meassures you have in place to safeguard the data.

In preparation for the GDPR our technical and organisational measures have been reviewed and a number of additional safeguards have been implemented. As a result, 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's 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 will be reviewed annually and in the unlikely event of any security or data breach.

How is IT security organised in terms of roles and responsibilities?

The Chief Technical Officer (CTO) takes overall responsibility for IT security. Our IS policies are set at a global level by our Group Systems and Architect Director. They are then implemented in each local market by the IT directorate with full support from the management teams. Network security is the responsibility of the Head of Network and Security, corporate security is the responsibility of the Head of Internal IT, application security is the responsibility of the Group Systems and Architecture Director. The Legal team support and assist with compliance in each of these areas.

Do you encrypt, anonymise or pseudonymise 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 (utilising SSL 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 center) is 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 approved personnel within the IT teams. Access to these locations is logged.

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, internal firewalling further segregates 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?

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 two-factor authentication

Do you have security breach notifications in place?

Breaches are handled and reported in line with our incident report plan. In case of a personal data breach (or an unlawful disclosure of confidential information) the impacted advertisers, publishers will be informed as soon as reasonably possible, prior to the disclosure to the data protection authorities and impacted individuals wherever possible.

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 local Awin Data Protection Officer (DPO) immediately. This is a critical element in ensuring the 72-hour deadline is met and is emphasised in all employee training materials and policies. Once the information has reached the Awin DPO, they will take care of the notification requirements. The DPOs are trained on the requirements of notifications.

How do you ensure the rights of individuals?

Awin has reviewed its processes around the rights of individuals and is confident that it will be able to comply upon request. All requests should be addressed to global-privacy@awin.com where the local DPOs will respond to the requests in the language of the individual request.

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

Yes, Awin has implemented a training programme for employees in both areas.

Please provide a link to your privacy policy.

www.awin.com/gb/legal/privacy-policy

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, please request a copy of the data processing agreement for joint controllers from your account manager (or the account management team).

Can we sign a data processing agreement as a publisher?

This is not necessary as all relevant provisions are to be included in the publisher terms. Please review and accept these terms when you access the Awin user interface.

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 DPOs directly, you can email global-privacy@awin.com

AWIN