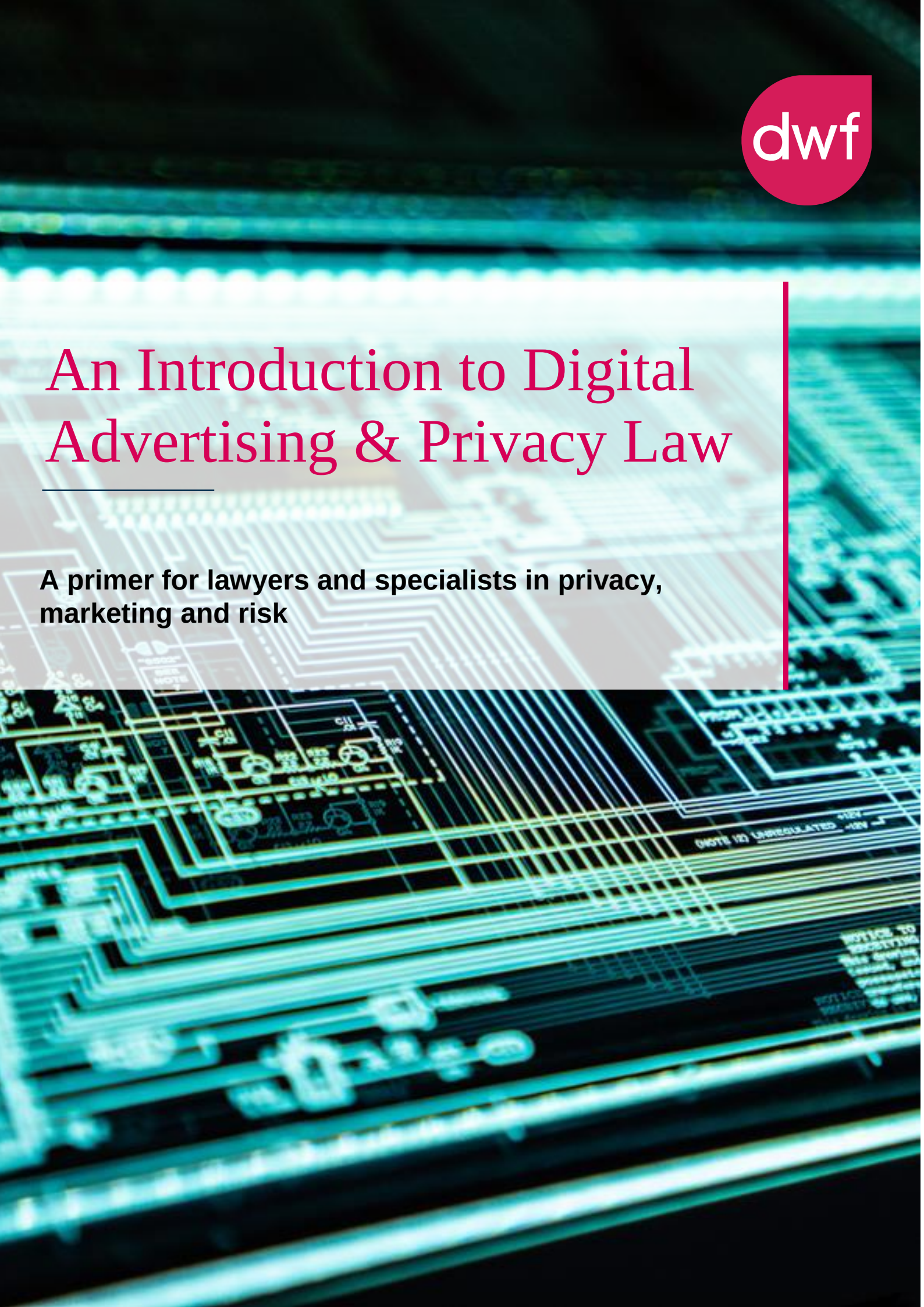


An Introduction to Digital Advertising & Privacy Law

A primer for lawyers and specialists in privacy, marketing and risk

Contents

dwfgroup.com

linkedin.com/company/dwf

@DWF_Law

1. Introduction

Digital advertising has become an essential part of many organisations' marketing strategy. It brings businesses the opportunity to reach a wide audience with personalised and targeted messaging. All of which is designed to increase conversions and drive sales.

This paper aims to provide an overview of the digital advertising ecosystem, explore key issues relating to digital advertising and data protection, analyse the current regulatory landscape and highlight the challenges faced by advertisers, publishers, data subjects, regulators and policymakers alike.

By shedding light on these complex issues, we seek to provide insights to legal counsel as well as data protection, risk and marketing specialists who navigate the interplay between online advertising activities and privacy.

We hope this paper will aid you to support innovation and growth within your respective organisations while balancing the needs of privacy requirements.

While the issues discussed in this paper generally reflect the requirements of UK and EU law, many of the topics and issues covered have relevance beyond those jurisdictions.

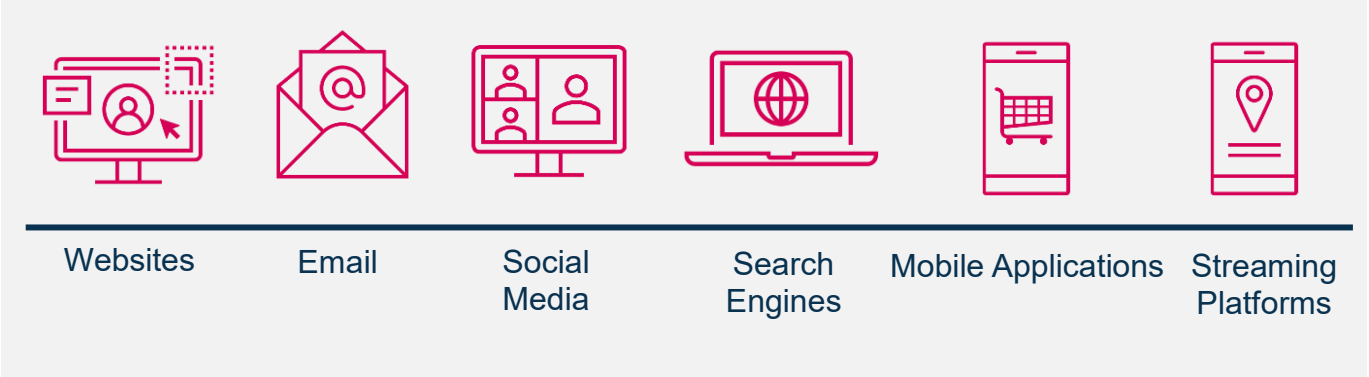
In sections 1 to 7 of this paper, we delve into the complexities of the digital advertising ecosystem, providing technical insights that will help you to offer informed advice to your business.

In sections 8 to 12, we explore the legal framework governing digital advertising from a data protection perspective. We also discuss relevant themes from case law and enforcement activities that can provide guidance for the use of advertising technologies.

Finally, in sections 13 and 14, we draw conclusions by examining the practical implications of online advertising.

2. What is digital advertising

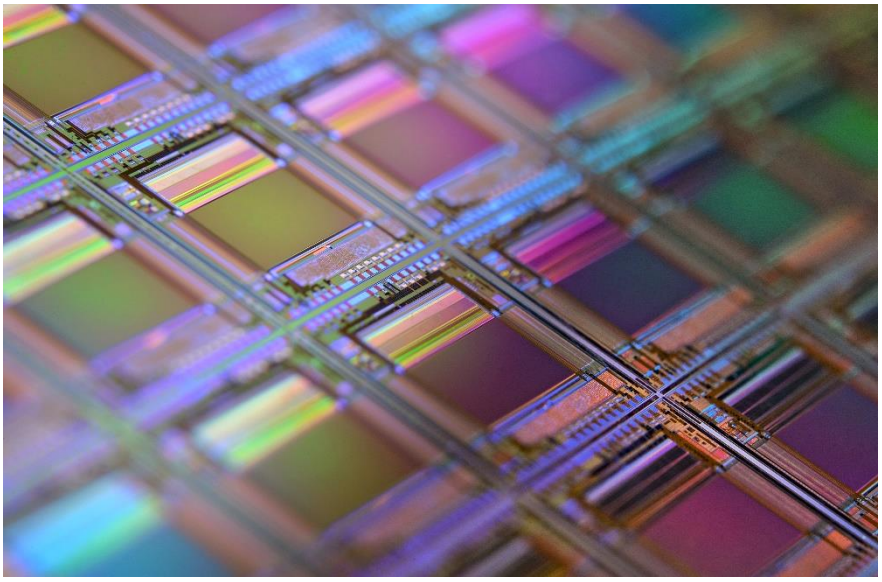
Digital advertising, also known as online advertising, involves the promotion of products and services through digital channels such as websites, email, social media, search engines, mobile applications (including messaging apps) and streaming platforms.



Digital advertising is delivered through a variety of formats, including display ads, video ads, social media ads and search engine ads.

Digital advertisers can use digital advertising technologies to target individuals within specific demographics, who have specific behaviours or interests, or to retarget individuals who have previously interacted with a particular online service or ad.

Digital advertising technologies, also known as adtech, are often seen as offering a cost-effective and efficient means of reaching large audiences. They can also be used to build marketing campaigns, measure the performance of those campaigns (often in real-time) and change advertising strategy accordingly.



3. What are the different types of online advertising?

Digital advertising can take various forms including text-based, image-based, video-based, or sound-based ads. Some of the commonly used channels for delivering these different forms digital ads are described below.

Search advertising

This is advertising that appears within the search results on a search engine webpage. Search advertising is typically displayed to users who search for keywords. Advertisers pay to display their adverts when a user undertakes a search using keywords that are associated with the advertiser's product or service.

Social media advertising

This is advertising that appears on a social media platform's website or app. It usually takes the form of banner ads or video ads that appear in a user's content feed on the platform, or before or during the playing of video content on the platform.

Display advertising

Refers to the use of banner, image or video ads on websites and apps, excluding search and social media advertising. This form of advertising can be found on various platforms, including streaming services, online newspapers, large e-commerce platforms and other publishers.

Classified advertising

Refers to advertising placed on online market places where the platform provider does not set the terms of sale or take a fee from the sale (other than a listings fee).

Native advertising

Involves the creation of ads that blend in with the content of the platform they appear on. Such ads are usually designed to look like regular content and are less intrusive compared to traditional banner ads.

Email and SMS marketing

Involves the sending of promotional materials to a recipient via email or text message. These materials can include offers, promotions or information about new products and services. Advertisers may also be able to use push notifications on a user's mobile device to deliver similar messaging.

In this paper, we focus on digital advertising delivered through display advertising.

4. How can online display advertising be purchased?

Online display advertising is commonly purchased through programmatic advertising processes. These processes involve the use of automated technology to buy and sell "ad inventory", which is a reference to advertising space that is available for purchase on websites or in apps.

There are different forms of programmatic advertising, these include:

Real-time bidding (RTB)

RTB is the most common type of programmatic advertising. It uses a combination of IT systems and algorithms to deliver a real-time and automated process for the buying and selling of ad inventory online.

Programmatic direct

Whereas RTB usually involves many parties and intermediaries in the process of purchasing ad inventory, programmatic direct allows advertisers to purchase ad inventory directly from publishers using an automated platform.

Private market place (PMP)

In a PMP setting, publishers offer ad-inventory at auction to a limited number or selected group of advertisers.

A publisher and advertiser will typically sell and buy on this basis where the publisher has a premium audience that the advertiser wants to target.

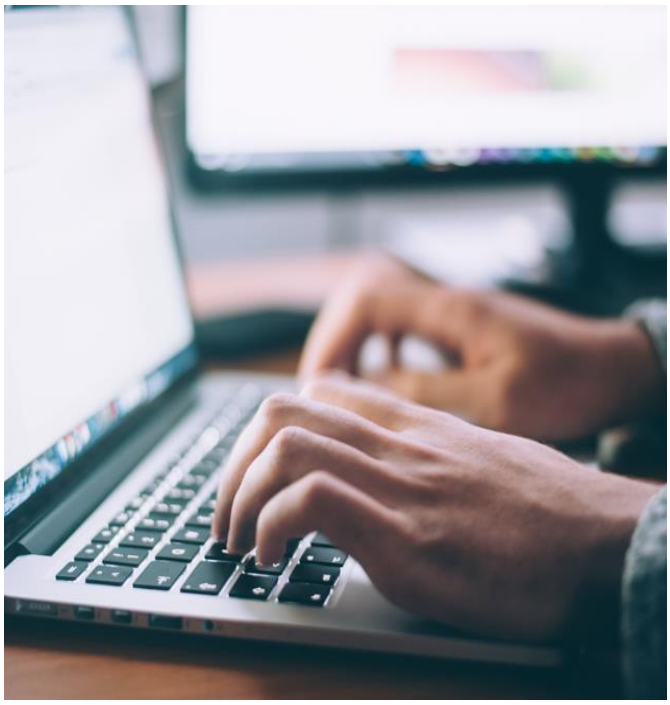
Guaranteed deals

Guaranteed deals involve an advertiser reserving ad inventory in advance at a fixed price with a publisher, which in return guarantees delivery and placement of the ad within its ad inventory.

Contextual advertising

Contextual advertising is advertising that is targeted at users based on the content they are viewing.

Advertisers choose specific keywords, topics or user categories to reach audiences that may be interested in their products and services.

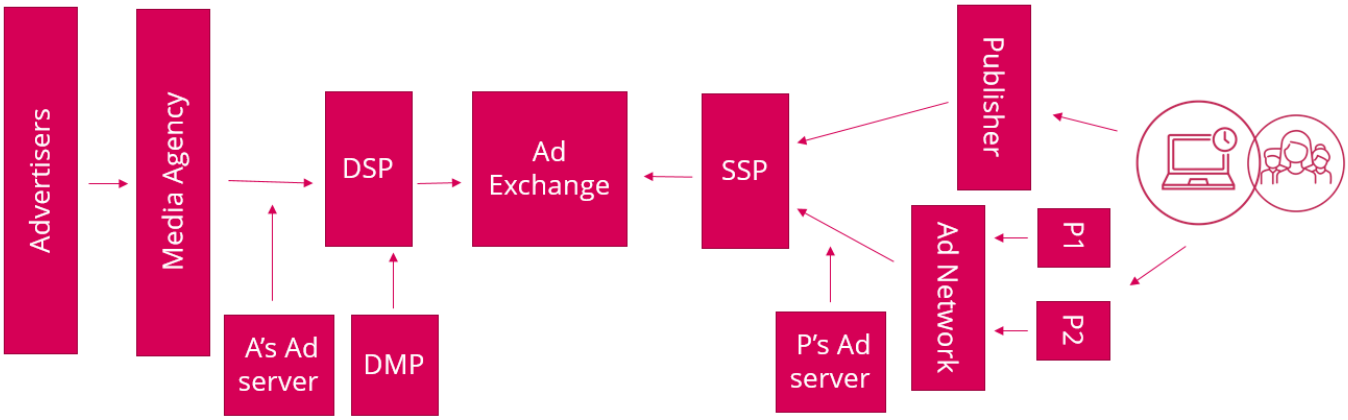


All forms of programmatic advertising can raise data protection concerns. RTB, in particular, is subject to significant scrutiny and criticism because it involves vast data processing operations.

In the remainder of this paper, we focus on RTB, but many of the issues we discuss will be relevant to other forms of programmatic advertising.

5. An overview of RTB

RTB involves multiple parties and technologies combining to deliver the sale and purchase of ad inventory through an online auction process. The diagram below shows a simplified but typical RTB ecosystem.



The parties and technologies involved in RTB and the activities they are involved in are described in the table below.

Party	Role and activities
Advertisers	Advertisers are organisations that want to place ads on publishers' websites or apps. They will buy ad space from publishers either directly or through a media agency.
Publishers	Publishers are organisations that make advertising space available on their websites or apps. Publishers include online broadcasters (of TV and radio), online newspapers, online magazines, streaming platforms, gaming platforms and e-commerce sites. Publishers sell ad space to advertisers.
Media Agency	A media agency works with advertisers to manage and execute advertising campaigns through digital channels. Tasks they undertake on behalf of advertisers include developing advertising campaigns and content, selecting marketing channels, buying ad inventory (on behalf of advertisers), monitoring and optimising campaigns, and using and supplying access to various forms of adtech.
Demand-Side Platforms (DSPs)	DSPs are technology platforms that allow advertisers to bid on and purchase ad inventory programmatically. DSPs analyse data from ad exchanges about users and ad impressions to make decisions whether and how to bid. DSPs can be used for campaign management. They provide tools for creating and managing advertising campaigns, including setting criteria for targeting users, bidding budgets and strategies. They provide reporting and analytics in relation to campaign performance and return on investment. They can also ingest first-party data, third-party data and data from data management platforms to determine targeting and bidding decisions.
Supply-Side Platforms (SSPs)	SSPs are technology platforms that allow publishers to sell their ad inventory programmatically. SSPs are used to pass information about ad impressions to ad exchanges. SSPs are used for inventory management and aggregating ad inventory from multiple publishers. They can supply publishers with reporting and analytics in relation to sales and

Party	Role and activities
	ad inventory revenues. They can also adjust pricing and ad inventory availability in response to market trends.
Ad Networks	Ad networks purchase ad inventory from publishers. They aggregate ad inventory from multiple publishers and sell it onto advertisers typically through an ad exchange.
Ad Exchanges	An ad exchange is a platform providing a market place where ad inventory from publishers can be bought and sold through real-time bidding in an auction process.
Data Management Platform (DMP)	A DMP is a technology platform that collects and organises data from different sources, including first-party and third-party data, to inform decisions in relation to bidding on ad inventory. DMPs provide advertisers with information that can improve and optimise their advertising campaigns. DMPs can be used to segment data based on user attributes, such as demographics, interests and behaviours, allowing advertisers to target their advertising more effectively.
Advertiser's Ad Server	An advertiser's ad server is a technology system that is used to deliver digital ads to websites and apps. Ad servers store and serve ad content to publishers. Ad servers are also used to track ad impressions (i.e. the calling of the ad to be placed on a browser), interactions (e.g. clicks) and conversions.
Publisher's Ad Server	A publisher's ad server is a technology system that is used to manage the display of digital ads on websites and apps. The ad server is used to configure ad content sent to it by advertisers and deliver it to ad spaces on the publisher's website or app. Ad servers are also used to track ad impressions, interactions and conversions. This information informs the publisher's advertising strategy and allows it to optimise ad placement and pricing.

In the diagram at the start of this section, you can see that an advertiser (shown on the left side of the diagram) is attempting to deliver advertising to a website (shown on the right side of the diagram). The steps that are typically taken to achieve this through RTB are described below.

Summary of the RTB Process

1. The user visits a publisher's website.
2. The publisher's server will send content to the user's browser in the form of HTML (HyperText Markup Language), which the browser interprets to display the content on the user's screen.
3. Within the HTML code is an instruction to retrieve ad content from the publisher's ad server to be displayed within the ad inventory on the website. The user's browser will connect to the publisher's ad server.
4. The ad server will determine whether the ad opportunity has been reserved for a specific or premium buyer or whether it is to be made available for auction on the open market.
5. If the ad opportunity is available for the open market, the ad server will connect to an SSP.
6. The SSP will analyse the ad opportunity and may add new information to the ad opportunity to enhance its prospects when bid on. It will then send the ad opportunity to an ad exchange.

7. The ad exchange will make the ad opportunity available to advertisers by connecting to DSPs, ad networks and other ad exchanges.

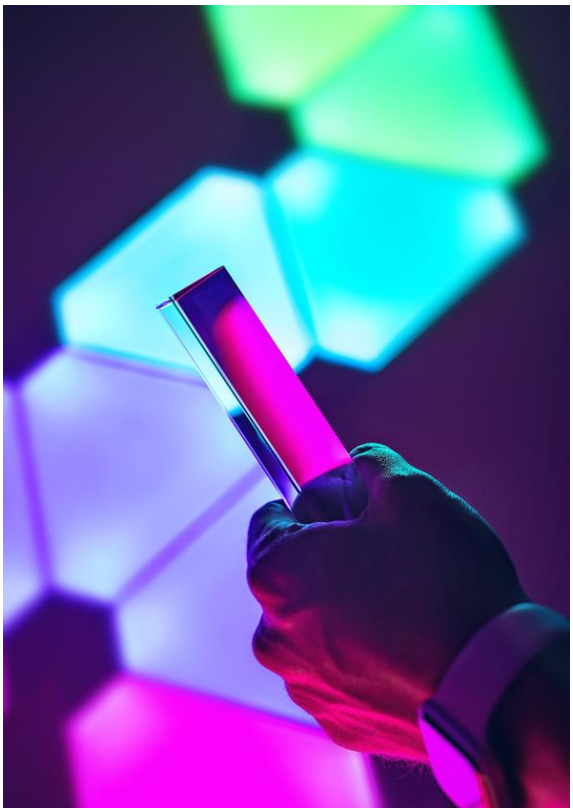
8. The DSPs, ad networks and ad exchanges will then provide the ad exchange with pre-cached bids. Pre-cached bids are instructions from advertisers that they will buy x impressions, at x price (for example, £1 per 1000 ads) when certain criteria are met (e.g. the user's profile has certain demographics).

9. If there are no pre-cached bids the ad exchange will start a bidding process. Advertisers will then make their best bid on the ad opportunity.

10. The winning advertiser, potentially working through its media agency, uses its DSP to pass instructions for retrieving the advert to the ad exchange, which passes those instructions to the SSP, subsequently passing those instructions to the publisher's ad server.

11. The publisher's ad server then informs the user's browser, through the HTTP connection, to go to the advertiser's ad server to retrieve the ad, which is then placed on the browser.

12. The DSPs, ad networks and ad exchanges will then provide the ad exchange with pre-cached bids. Pre-cached bids are instructions from advertisers that they will buy x impressions, at x price (for example, £1 per 1000 ads) when certain criteria are met (e.g. the user's profile has certain demographics).



The entire process described above takes place in fractions of a second.

6. What data is used in a bid request?

A bid request is a communication from a publisher to an ad exchange or ad network requesting ads to display on the publisher's website or app. The request will contain information that advertisers can analyse to determine whether to bid to acquire the available advertising space for their advert and how much they are prepared to bid.

Information types that typically included in a bid request are described in the table below.[1]

Information type	Overview
Bid request unique identifier	A bid request unique identifier is a unique code assigned to a bid request. It is used to track a bid request and ads served in response to the request through the ad serving process.
Internet protocol (IP) address	An IP address is a unique number given to an electronic device by an Internet Service Provider or network administrator when the device connects to the Internet. The IP address is used to direct communications between the device and other devices and servers on the Internet.
Cookie IDs	A cookie ID is a unique identifier assigned to a browser and stored in cookies (small text files) on the browser. They can be set by a browser connecting to a server via HTTP or JavaScript on a web page read by a browser. Cookies are used to collect information including browsing history and information about the ads a user has seen or interacted with.
Mobile advertising IDs	A mobile advertising ID, also known as a MAID, a mobile device ID or an IDFA (Identifier for Advertisers), is a unique identifier assigned to a mobile device by its operating system or by the device manufacturer. A mobile advertising ID performs a similar function to a cookie ID, allowing a user to be tracked across websites and apps.
User IDs	A user ID is a unique identifier that is associated with a specific user account or profile. It is typically generated by a website or app when a user creates an account or signs in, and is used to track that user's activity across different devices and platforms.
User-agent string	A user-agent string is a piece of text that describes the software/browser that is connecting to a website or server. Typically, it will include information about a device's operating system, browser type and version, and any plugins or extensions that are installed. The user-agent string is important for website and server administrators, as it allows them to optimise their content and services for different devices and software platforms. For example, a website might use the user-agent string to detect if a user is accessing the site from a mobile device and serve a mobile-optimised version of the site.
Location	The degree to which actual location is shared will depend on numerous factors. For example, the location of a mobile device could be gathered using precise GPS data where a user gives a website or app permission to collect this information e.g. when using a location based service. Relatively precise location data could also be determined from an IP address where the IP address is fixed

[1] This list has been developed from the information types that the UK Information Commissioner's Office described in its report dated 20 June 2019, "*Update report into adtech and real time bidding*".

Information type	Overview
	and publicly associated with a location. Alternatively, the IP address may only allow the determination of a city or area within a city where the user is situated.
Time zone	The time zone the user is situated in.
Detected language	Detected language is the language associated with the user's system.
Device type	Device type is information about the user's device such as whether it is a desktop or mobile device, the brand, the model and the operating system.
Audience segmentation	Information relating to the audience segmentation(s) that the user is associated with.
Referring site	Information about the site the user came from before reaching the publisher's website.
User journey on the site	Information about the pages the user visits and activities on the site, which may include mouse cursor movement.
Events	Information about scrolling, clicking, highlights and media views on the publisher's website.
Search queries	Search query data is information about the specific terms and phrases a user enters into a search engine. This can include data from searches undertaken on specialist search sites (such as comparison websites or special interest sites) and on e-commerce sites and platforms. This is in addition to searches undertaken using commonly used search engines. Search query data is valuable to advertisers as, in addition to providing information about a user's interests, it may also demonstrate a user's actual intent to make a purchase.
Session time	Session time data is information about the amount of time a user has used a particular website or app for, or the amount of time a user has engaged with particular content.
Site behaviour	Site behaviour data refers to information collected about a user's behaviour on a particular website or across multiple websites. This data can include contextual and thematic preferences, such as the types of pages a user visits or the topics they are interested in. It can also include interactions such as clicks on links and advertisements, downloads, form submissions and purchases. In addition, site behaviour data can include information about how long a user spends on a particular page, how they navigate through a website and whether they return to the site at a later time. This data can be used by online advertisers to create targeted ad campaigns based on a user's specific interests and intentions.
Demographic data	Demographic data is information collected about a person's characteristics, such as their gender, age, education level, income, geographic location, purchase history and personal preferences.

A key component of digital advertising is the collection and use of online identifiers to facilitate the targeting of individuals. Online identifiers include user IP addresses, cookie IDs, mobile advertising IDs and user IDs.

Online identifiers are used in conjunction with other information, including the information listed in the table above, to place users into what are called "segments". Segments are groups of online users that share common characteristics, such as shared needs, interests, lifestyles or demographics (e.g. women, aged 30 – 45, interested in technology, located in London). Segments can also be used for retargeting campaigns, where ads are shown to users who have previously interacted with a particular product or service but did not make a purchase.

The aim of placing users in segments is to increase the likelihood of those users seeing ads online that are relevant to them, in turn resulting in a higher click-through rate and ultimately, more conversions.

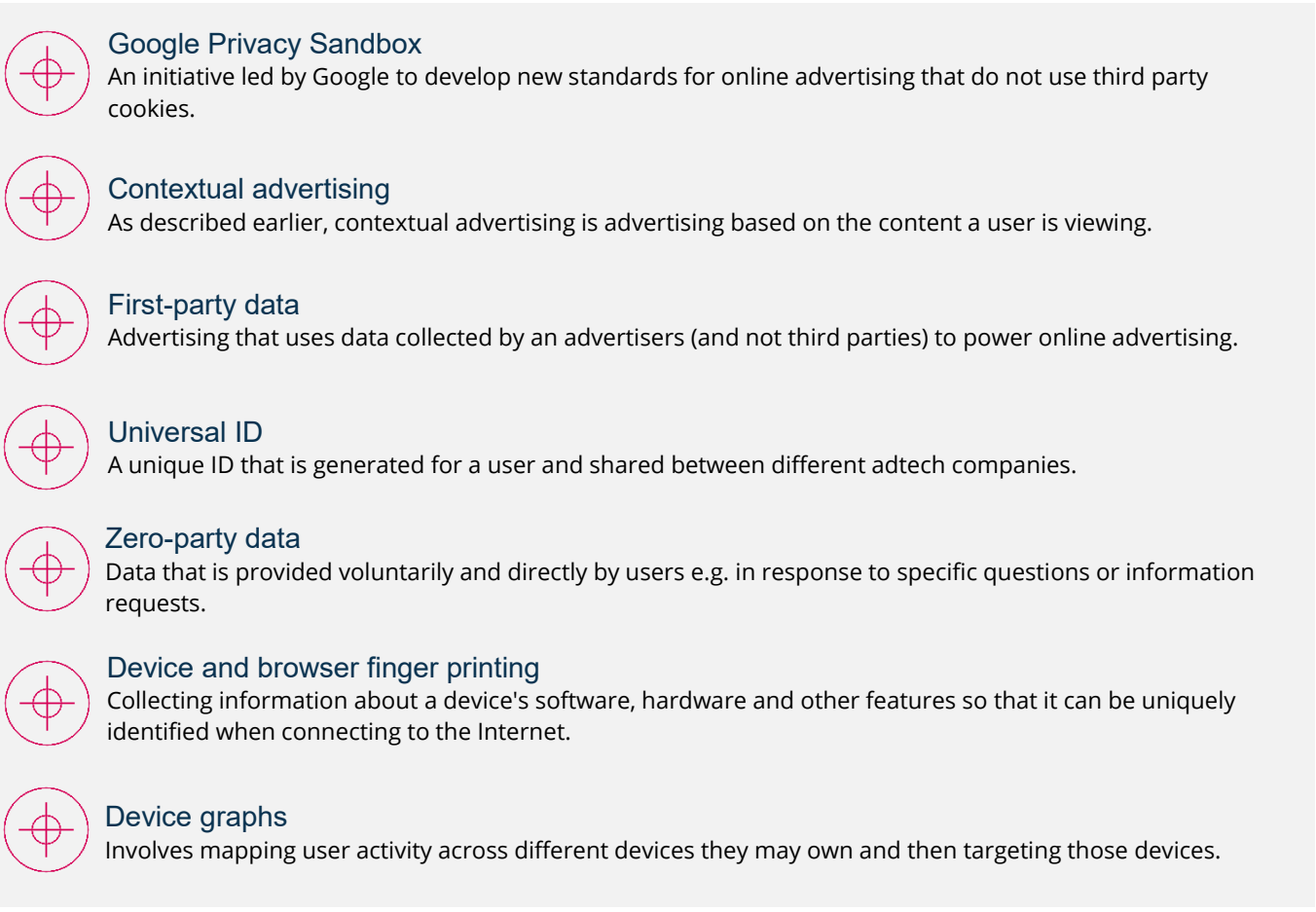
7. A cookieless future

Presently, cookie IDs play a significant role in digital advertising. However, their future is less certain. Google plans to phase out third-party cookies (i.e. cookies placed by third parties) in its Google Chrome browser by the end of 2024, and since 2020, Apple has blocked third-party cookies by default.

In addition, Google has announced that in the future it will not use mobile advertising IDs on its Android operating system. Further, Apple's App Tracking Transparency (ATT) framework, established in early 2021, which requires apps to ask for user permission to track them before collecting their Apple's IDFA, has seen a rapid decline in information passed to advertisers from Apple devices.

The results of the above are likely to mean that the use of cookie IDs and mobile advertising IDs in online advertising will reduce significantly over the coming years. This it is sometimes referred to as a "cookieless future" or even the "cookie apocalypse".

Digital advertising in a cookieless future could be supported by some of the alternative mechanisms below:



It is too early to predict which alternative targeting mechanism(s) will prevail. However, for those involving the tracking of devices or the exchange of personal data between parties involved in digital advertising, the data protection and privacy issues discussed in the remainder of this paper will continue to be relevant. In addition, at least in the immediate future, RTB will remain an important constituent of the digital advertising ecosystem.

8. The legal framework

In the UK and Europe, the legal framework that applies to digital advertising derives from and is primarily governed by the General Data Protection Regulation (GDPR) and the ePrivacy Directive.

In the UK, the GDPR was incorporated into UK law following Brexit as the UK General Data Protection Regulation[2] and the ePrivacy Directive was implemented into UK law through the Privacy and Electronic Communications Regulations[3].

At present, the UK and European legislation described above remain broadly aligned with respect to the requirements for online advertising. References in this paper to the GDPR or ePrivacy Directive should therefore be read as references to the respective UK implementation.

Together, the GDPR and ePrivacy Directive establish a framework for the collection, use and protection of personal data in the context of online advertising. The GDPR sets out rules for processing personal data. The ePrivacy Directive sets out rules that apply to the use of electronic communications for direct marketing purposes, and to the access and storage of information on electronic devices using cookies and similar technologies.

8.1. ePrivacy Directive

The ePrivacy Directive establishes rules governing the use of cookies and similar technologies that are commonly used in digital advertising. By referring to "similar technologies" we mean a shorthand for any technology that stores or accesses information on a user's device. This could include, for example, HTML5 local storage, Local Shared Objects, scripts, tracking pixels and plugins. When we refer to "cookies" in this paper, it should be read to include similar technologies.

The ePrivacy Directive contains provisions requiring that before storing or gaining access to information on a user's device, the user is provided with clear and comprehensive information about the purposes for storage or access, and provides their consent to such storage or access. The transparency and consent standards under the ePrivacy Directive must meet the requirements of the GDPR.

Website and app operators typically comply with the transparency requirements of the ePrivacy Directive by providing users with access to cookie notices, privacy notices, and consent management tools. This is often achieved through the use of banners or pop-ups that are displayed to users when they first access a website or app, informing them of the use of cookies and giving them the option to consent or decline.

Consent is not defined in the ePrivacy Directive, instead the GDPR definition of consent applies. This requires that a user's consent must be a freely given, specific, informed and unambiguous indication of their wishes, which they signify by a statement or clear affirmative action. Furthermore, the GDPR requires that, website and app operators must be able to demonstrate that they hold valid consent and that users can withdraw their consent at any time.

The requirements mentioned above do not apply in cases where the storage of or access to information by cookies is solely for the purpose of transmitting a communication over an electronic communications network, or is strictly necessary to provide an information society service that has been explicitly requested by the user. Cookies that are utilised for these purposes are typically referred to as "essential cookies" or "strictly necessary cookies." On the other hand, all other types of cookies are often referred to as "non-essential cookies".

[2] This was by virtue of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

[3] The Privacy and Electronic Communications (EC Directive) Regulations 2003 as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011.

Overall, the requirements described above mean that for non-essential cookies, website and app operators must:

- tell users that they use cookies;
- explain what cookies they use and why;
- set out on a named basis any third parties who may also process information stored in or accessed from the user's device;
- detail the duration that any storage or access will last for;
- before using cookies, get user consent for storing the cookies or gaining access to information stored on the user's device; and
- provide users with controls over any non-essential cookies.

Additionally, they must not:

- bundle consent to the use of cookies into terms and conditions for using the website or app;
- use pre-ticked boxes or sliders that are defaulted to "on" or rely on other forms of inaction from users to demonstrate consent;
- prevent access to websites and apps if users do not consent to the use of non-essential cookies; and
- place cookies or access information before the user has given consent.

8.2. General Data Protection Regulation

Where the setting of cookies involves the processing of personal data, in addition to the complying with the ePrivacy Directive, the requirements of the GDPR must also be addressed.

Many forms of digital advertising will involve the processing of personal data, particularly where such advertising utilises online identifiers.

Online identifiers are specifically stated to be "personal data" under Article 4(1) of the GDPR. Further, Recital 30 of the GDPR recognises that online identifiers provided by devices, applications, tools and protocols (such as internet protocol addresses, cookie identifiers or other identifiers) may leave traces which, when combined with other information received by servers, create profiles that can identify natural persons.

The combination of online identifiers with the other information that is shared as part of a bid request is likely to constitute personal data. The ICO states in its guidance on the use of cookies and similar technologies:

"A single information element may not be personal data on its own, the combination of multiple elements makes it more likely that the information will constitute personal data. This is particularly the case when the information enables you to single out, make inferences or take specific actions in relation to users (such as identifying them over time or across multiple devices and websites, even if you don't know the name of those users)."

Similar to the requirements of the ePrivacy Directive, where the GDPR applies to data processing for online advertising purposes it is essential that users are provided with transparent information about the personal data collection and use, and that there is a lawful basis for processing the personal data. This is in addition to meeting the other requirements of the GDPR such as those relating to purpose limitation, data minimisation, respecting data subject rights, putting in place data sharing and data processing agreements, international data transfers, data security and accountability.

Although the UK GDPR provides six lawful basis for processing personal data[4] , if you are already relying on consent for compliance with the ePrivacy Directive's requirements, consent will also be the appropriate lawful basis for processing personal data related to the use of cookies. Data protection regulators are unlikely to accept the use of another lawful basis, such as legitimate interests, for the processing of personal data when consent has already been gathered to meet the ePrivacy Directive's requirements.

The requirement for the lawful basis of processing to be consent is made necessary by the nature, extent, context, and purpose(s) of the processing operations. This is in addition to the fact that the data is gathered using cookies. In particular, the complexities of the data sharing, analysis, tracking and profiling that take place within digital advertising, are likely to make consent the most applicable lawful basis for the associated personal data processing.

[4] Excluding the lawful bases of processing that relate to the processing of special category personal data

9. The challenge: transparency and consent

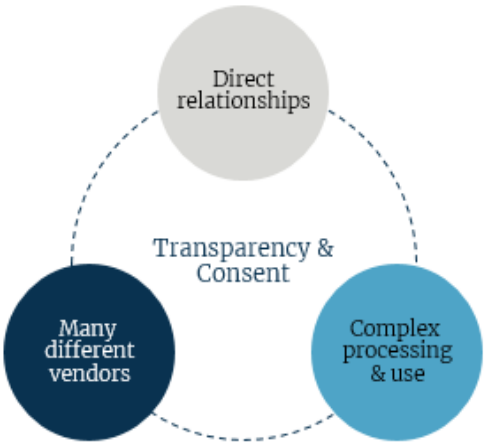
At the heart of the legal framework governing digital advertising is the requirement to be transparent with users and gain their consent to the connected data processing. However, this presents significant challenges.

How can GDPR-level transparency be achieved when digital advertising often involves complex processing operations using personal data?

How can users be made aware of all the parties that may access their personal data within the digital advertising ecosystem?

How can parties that lack direct relationships with users fulfil their obligation to be transparent about how they use personal data?

Moreover, if transparency is insufficient, how can valid GDPR consent be obtained from users for the processing of their personal data for digital advertising?



Addressing the challenge

To address the challenges to transparency and consent in digital advertising, parties involved in the process typically rely on a range of responses. Advertisers, publishers and other parties that have direct relationships with users provide privacy notices and cookie notices that explain to users how their personal data will be collected, processed and shared for online advertising purposes, as well as how cookies and similar technologies will be used for these purposes.

Consent management tools are also often used by advertisers and publishers to obtain consent from users.

These tools allow users to give or withhold consent, as well as enable them to withdraw their consent at a later date. Consent management tools aim to give users control over the collection of their personal data, the use of cookies, and help advertisers and publishers to comply with their requirements under the GDPR and ePrivacy Directive.

Industry frameworks have also been developed to address the challenges of transparency and consent in digital advertising. These frameworks provide guidelines and may include standards for protecting data and privacy online.

One commonly used industry framework is the Interactive Advertising Bureau (**IAB**) Europe's Transparency and Consent Framework (**TCF**). However, as you will see in section 10, the TCF is under substantial scrutiny from data protection regulators, which poses a risk to compliance levels within organisations that rely on it.

Dark patterns – impact on transparency and consent

Dark patterns are mechanisms used to influence user behaviours and actions. The European Data Protection Board (**EDPB**) has identified 6 categories[5] of dark patterns:

Overloading
Giving the user too much information.

Skipping
Encouraging the user to overlook certain aspects.

Stirring
Influencing user decisions through more positive or negative language or different visual styles.

Hindering
Making it difficult for the user to find the information they are looking for.

Fickle
Providing users with inconsistent privacy information or locating it on a page that is unrelated to data protection.

Left in the dark
Leaving users unclear on how their personal data is processed.

The use of dark patterns can undermine consent by coercing individuals into providing personal data and similarly reduce transparency by making information difficult or impossible to find.

[5] The 6 categories are described in the EDPB's *'Guidelines 03/2022 on deceptive design patterns in social media platform interfaces: how to recognise and avoid them'*, Version 2.0, adopted 14 February 2023.

10. The Transparency Consent Framework

The TCF, developed by IAB Europe, aims to support online advertising ecosystem participants (such as publishers, consent management platforms and other adtech vendors) to comply with the GDPR and e-Privacy Directive. It does this by providing an operational framework of guidelines, policies, technical specifications, and rules and conditions designed to give online users transparent information and secure their informed consent.

TCF Version 1.0 was released in 2018 before being modified again shortly after in 2019. The second version was published in August 2019 following considerable consultation with the online advertising industry.

The TCF relies on the use of consent management platforms (**CMPs**) to collect, document and manage a user's consent to the use of cookies and the collection and use of a user's personal data. Typically, as an integrated part of a publisher's site, the consent management platform will provide a user with an interface that supplies transparency information and allows the user to accept or reject their data being used for certain specified purposes.

In order to participate in the TCF, CMPs and other adtech vendors must register with IAB Europe, which will require that they can satisfy the technical specifications and other requirements of the framework. Once registered, IAB Europe will add them to the publicly available Global Vendor List (**GVL**).

Some of the information that vendors provide for the GVL include:

- the legal name of the vendor, company website and contact details;
- a link to the vendor's privacy policy;
- the vendor type e.g. CMP, DSP, SSP or DMP;
- the purposes for data processing;
- the legal basis for processing, such as consent or legitimate interest; and
- the adtech vendors or other partners that they share personal data with for advertising purposes.

The TCF provides a list of 12 predefined data processing purposes that CMPs and other adtech vendors can select from to describe the purposes that personal data is processed for - see the list opposite.

The list offers a degree of standardisation to allow publishers and CMPs to make disclosures, and give choices to users about who their personal data is disclosed to and how it is used.

- Purpose 1 — Store and/or access information on a device

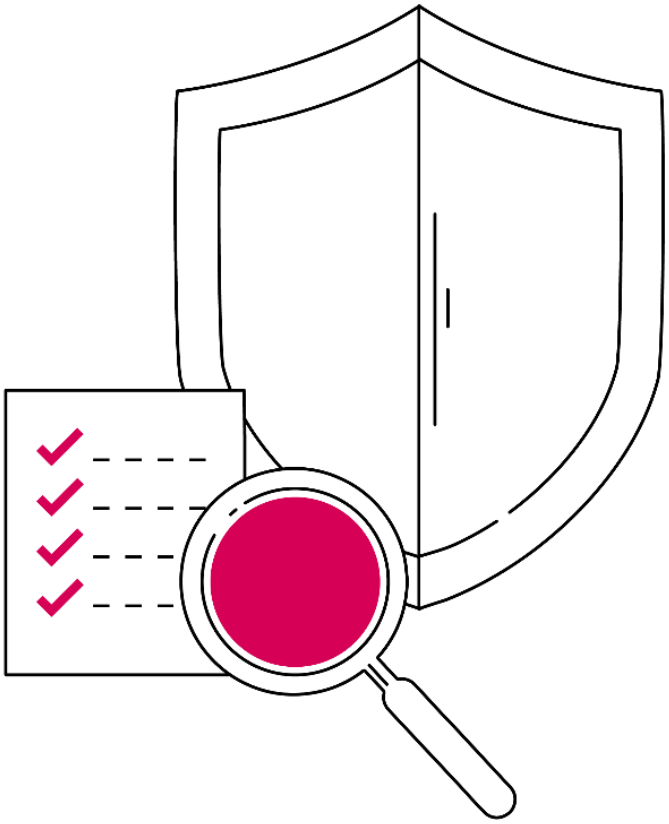
- Purpose 2 — Select basic ads
- Purpose 3 — Create a personalised ads profile
- Purpose 4 — Select personalised ads
- Purpose 5 — Create a personalised content profile
- Purpose 6 — Select personalised content
- Purpose 7 — Measure ad performance
- Purpose 8 — Measure content performance
- Purpose 9 — Apply market research to generate audience insights
- Purpose 10 — Develop and improve products

- Special Purpose 1 — Ensure security, prevent fraud, and debug
- Special Purpose 2 — Technically deliver ads or content

Importantly, CMPs can package this information up into a text string, called the TC string, that contains information about a user's consent choices for online advertising purposes and pass that information to other adtech vendors in the ecosystem.

Adtech vendors can read the TC string and use it to determine whether they are authorised to process a user's personal data for online advertising purposes.

The TCF offers a number of benefits to various stakeholders. Publishers can use it to ensure that they are engaging technology partners that are taking steps to comply with the GDPR and ePrivacy Directive. CMPs can use the framework to capture and communicate information about a user's choice through the online advertising ecosystem. Adtech vendors have a single standard they can follow and implement across thousands of websites, apps and platforms. Advertisers can manage the legal basis for sharing personal data and provide information to users regarding their preferred vendors. Lastly, users benefit from knowing who is processing their personal data and for what purpose.



11. Challenge to the TCF

On 2 February 2022, the Belgian Data Protection Authority (APD) issued an administrative ruling against IAB Europe concerning the TCF.

The decision was composed of four elements:

1 The APD found that the TCF is inadequate in providing transparency to data subjects. It states that the twelve standard purposes are too broad and lack specificity, making it difficult for data subjects to understand who is processing their personal data. Additionally, the large number of vendors makes it impossible to provide effective transparency.

2 The APD concluded that the current version of the TCF is inadequate for obtaining valid consent from data subjects. The consents provided by the TCF are not specific enough and lack sufficient information, and given the number of vendors, it is disproportionate to expect users to read this information. The APD also found that users cannot withdraw their consent as easily as they provide it.

3 The current form of the TCF does not provide sufficient information on specific legitimate interests relied upon for processing data subjects' personal data, making it insufficient to establish legitimate interests as a lawful basis for processing (which was asserted in some cases). Due to the large number of vendors, the balancing test requirements for legitimate interests were not met.

4 The APD deemed IAB Europe, CMPs, publishers, and vendors as joint data controllers for collecting and processing data subjects' consent preferences. As a result, IAB Europe was found to be non-compliant with the GDPR's controller obligations, such as the failure to designate a DPO, implement a GDPR Article 30 Record of Processing Activities or conduct a data protection impact assessment.

The Belgian DPA gave IAB Europe until 2 April 2022, to submit a remedial action plan following the APD's decision. However, on 4 March 2022, IAB Europe appealed the APD's decision to the Belgian Market Court, challenging several points. On 7 September 2022, the Belgian CA issued a judgment dismissing most of the grounds of appeal but stayed the decision until the Court of Justice of the European Union (**CJEU**) resolves questions about the TC string and whether IAB Europe is a joint data controller. There likely will be no further judgment until 2024.

In the meantime, IAB Europe has submitted the required remedial action plan, which was approved by the APD on 11 January 2023. IAB Europe had until July 2023 to implement the changes due to the six-month implementation period that the APD allowed. However, IAB appealed the six-moth implementation period due to the impact the CJEU's decision may have on remedial action plan. The appeal is before the Belgium Market Court.

In the interim, IAB Europe has released TCF Version 2.2, which it states are designed to bring "*meaningful changes in an attempt to better meet the expectations of regulators…*". This includes removal of the legitimate interest basis for advertising and content personalisation, updates to the information provided to end-users, and requirements to facilitate users' withdrawal of consent.

12. Themes from case law and enforcement activity

In recent years, there has been a significant increase in enforcement activities related to digital advertising and cookie use by data protection authorities. There are examples from across Europe of enforcement action being taken, including fines ranging from hundreds of thousands to hundreds of millions of Euros.

Privacy activists have also added fuel to the fire by filing complaints directly with data protection authorities in relation to alleged non-compliances with the GDPR and e-Privacy Directive. Case law of the CJEU has also added additional scrutiny to practices that are relevant to online advertising.

Key themes that can be discerned from the case law and enforcement activity include the following:

Transparency and consent

Repeatedly, data protection authorities have brought enforcement action against organisations for failing to provide users with adequate information in their consumer-facing privacy and cookie policies about the use of their personal data for advertising purposes and not obtaining their valid consent. In particular, big tech has been the focus of multimillion Euro fines in this respect. Consumer-facing businesses have also been subject to significant fines and other enforcement action.

Joint controllership

The Fashion ID ruling of the CJEU and the Belgian DPA's decision in relation to the TCF has shown both judicial and regulator willingness to find joint controllership between participants in the online advertising ecosystem.

The Fashion ID case demonstrates that website operators can be held responsible for the collection and transmission of personal data by third-party plugins. This means that website operators need to ensure that they have a legal basis for the collection and transmission of personal data to third parties, provide users with transparent information about the disclosure and obtain their consent where necessary.

Active consent

Pre-ticked checkboxes for consent to the use of cookies are invalid. As found by the CJEU in the Planet49 case, and subsequently followed by data protection authorities, website operators relying on consent must obtain a user's active consent, which requires a user to perform a positive action (such as ticking a box).

Cookie walls

Blocking access to a website unless non-essential cookies are accepted should be approached with caution. If a cookie wall is used to require or influence users to agree to their personal data being used by third parties for the purposes of online advertising, it is unlikely that their consent will be considered valid.

Nudge behaviour and dark patterns

Designing user interfaces that guide users towards certain actions, such as consenting to cookies (nudge behaviour) or being intentionally deceptive/misleading (dark patterns), are likely to invalidate consent. Both nudge behaviour and dark patterns can be used to influence user choices related to cookies and online advertising. In doing so, they undermine the requirement for consent to be freely given.

13. Practical considerations when engaging in digital advertising

Many organisations use data and digital advertising for the benefit of their business. This use of data to achieve a business gain is common but is under increasing scrutiny and threat from enforcement.

It is therefore vital to understand the background and technological context we have outlined earlier in this paper when assessing your use of digital advertising. It is also important to consider the steps you can take to meet the requirements of the GDPR and ePrivacy Directive.

In this section, we provide practical guidance for engaging in digital advertising, meeting your GDPR and ePrivacy Directive obligations and managing associated risks.

13.1 Data protection impact assessment

The appropriate starting point for all complex or potentially high-risk projects involving personal data should be the undertaking of a data protection impact assessment (**DPIA**).

Article 35 of the GDPR mandates that a DPIA should be undertaken when processing is likely to result in a high risk to the rights and freedoms of natural persons. Many digital advertising initiatives are likely to meet this threshold, particularly as they may involve the use of personal data for evaluation or scoring, systematic monitoring, processing data on a large scale or matching and combining datasets.

Even if the digital advertising initiative does not trigger the mandatory requirement for a DPIA, you may still decide to undertake one. We would recommend this for two reasons. Firstly, it acts as a central record of risk identification, assessment and mitigation for the purpose of complying with GDPR's accountability principle; and, secondly, as many of the GDPR's principles and requirements will be engaged by the use of digital advertising, it can provide a methodical framework for working through and considering how each should be addressed.

It should also be noted that as digital advertising will usually engage the ePrivacy Directive, if your DPIA does not presently consider the requirements of the ePrivacy Directive, they should be expressly addressed in the assessment.

Finally, from our experience, it is common for discussions with a preferred provider of digital advertising services to be well progressed before legal and privacy teams are involved. We advocate for the early engagement of legal and privacy colleagues so that they have time to understand the proposed technology and data use. In turn, they can facilitate the successful deployment of relevant technologies and prevent delays. In particular, they can help ensure that the technology deployment is underpinned by relevant assessments that support contract drafting and help to determine the updates that may be required to websites and apps.

13.2 Determine the roles of the parties (controller, processor, joint controller)

When considering the steps required to lawfully pass data between two or more parties, it is necessary to determine their role as defined under data protection law. Before any data sharing takes places, you should therefore take steps to ensure you have clarity on how each party will use the personal data they have access to.

Historically, advertisers have been classified as a controller and other parties supporting the advertiser's digital advertising activities classified as processors. Many contracts for digital advertising services still reflect this. However, in-line with the case law and enforcement activity trends highlighted earlier in this paper, the position is changing.

While some digital advertising providers remain relatively fixed on their status as a processor, others are now willing to move away from this. We typically see this come about in a couple of ways:

(a) at the point of negotiating the contract, the digital advertising service provider accepts that it is an independent or joint controller (at least in relation to some data processing activities); or

(b) while the digital advertising service provider is not willing to agree it is an independent or joint controller immediately, it is willing to concede that there is the possibility, in the future, that one or more data protection relationships may be applicable to the service. That is a controller-processor, independent controller-independent controller and/or joint controller relationship may apply at a later date.

13.3 Drafting and negotiating agreements

In addition to the typical points of contractual negotiation (such as payment and liability terms), we recommend considering the following issues, which we have found are specific to digital advertising agreements:

Certainty regarding which services are being provided

What is the nature of the services that will be provided under the agreement? This seemingly simple question can be complex to answer but you must aim to have certainty over it.

Digital advertising services providers often offer a range of services and provide a draft contract setting out all of them. However, the customer's marketing or digital media team will not always know the service(s) they wish to obtain, or at least won't be certain whether they may want to use all or a subset of the services at some future point.

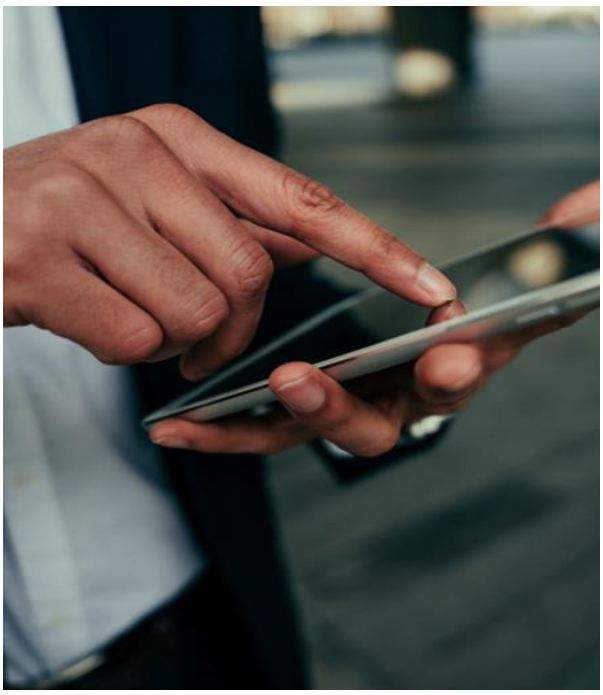
This leaves the pre-contract assessment and contract drafting in a difficult position. The assessment and the contract may need to address all the different data protection relationships, data sharing and associated requirements before you know all the services that will be used.

Ideally, you will be able to identify at least one or more of the services that will be used from the commencement of the agreement. This will allow an assessment to be performed and the contract to be negotiated with those services at the forefront.

However, you may need to prepare the contract to cater for the business taking a number of different services in the future, which may entail the service provider(s) having different statuses as controller, processor or joint controller depending on the nature of the service in question.

Drafting for the relationship status

Depending on the relationship status of the different service providers involved in delivering the digital advertising services, your contract may need to include: (a) controller-processor; (b) independent controller - independent controller; and/or (c) joint controller terms.



Taking each in turn, controller-processor terms must address the Article 28 GDPR mandatory requirements, they should also include relevant commercial terms e.g. in relation to audit rights, allocation of compliance costs and liability.

For independent controller - independent controller relationships, the GDPR does not prescribe mandatory terms as such, however, the parties should make it clear in the contract what types of personal data are shared between them and the purposes the data is shared for. In particular, the advertiser may wish to put contractual limits on what, why and for how long data can be used for by recipients.[6]

Lastly, in joint controller arrangements, Article 26 GDPR sets out mandatory requirements that must be met. In general, Article 26 requires joint controllers to allocate controller responsibilities between themselves. This requires active dialogue between the parties to agree how the allocation of responsibilities will work in practice under the service.

Across all three types of relationship there will need to be appropriate consideration of liability limits. Often these are not found in the data protection terms but in the main terms of the service agreement. Proportionment of liability will need to be checked and appropriate limits set based on the risk profile of the services, the parties involved and matters such as the supplier's insurance cover.

Often we find that digital advertising arrangements are set up as master services agreements, i.e. a framework under which services can be acquired via the completion of orders or statements of work. There is a benefit to this approach, in that it allows the parties to agree the terms that will apply to different relationship statuses in advance without those terms necessarily applying to the services from day one (depending on the nature of the services initially taken). This potentially allows terms to be agreed when the parties' negotiating positions are better matched and the advertiser is under less pressure from within its business to quickly agree to terms in order to acquire a service.

Compliance with the ePrivacy Directive

Digital advertising contracts are sometimes presented for review by service providers which include very simple data protection terms. Amongst other issues this creates, you may find that the terms focus on compliance obligations under the GDPR. It is therefore important to review the terms to ensure that they also create obligations to comply with the ePrivacy Directive.

Review of privacy notices, cookie notices and consent management tools

We recommend an obligation is placed on the parties to collaborate in the review of relevant privacy notices, cookie notices and any consent management tool notices (e.g. those relied on by the service provider) to ensure they appropriately reflect personal data collection and use (including data sharing) under the proposed services.

---

[6] Additional considerations in relation to sharing data between controllers can be found in the ICO's Code of Practice on Data Sharing.

Mandated terms from digital advertising supply chain partners, due diligence and overseas transfers

If you are acting for an advertiser, when the digital advertising service provider provides you with details of its supply chain, it is important to check it and to understand the various supply chain parties' relevance to the services that are to be provided.

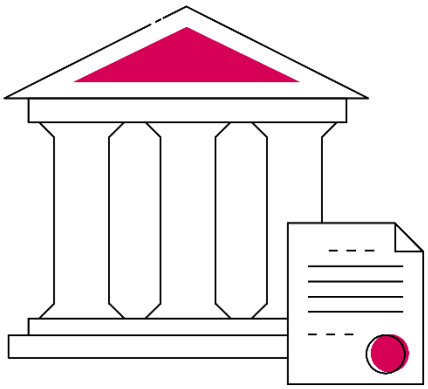
It is not uncommon for a digital advertising service provider to list all of it supply chain together, without fully distinguishing the roles the parties undertake or the data they have access to in that role. However, it is important to push for clarity on these point so that it can be determined, amongst other points:

- the entities that will be involved in the delivery of the services;
- whether they are acting as a sub-processor, independent controller or a joint controller;
- how obligations will pass down from your service provider into its supply chain and its liability for its supply chain;
- when international data transfers will take place, and the appropriate transfer mechanism and safeguards that will need to be in place to facilitate this; and
- the extent to which you will have audit rights to conduct appropriate due diligence on the supply chain.

Some of the large providers of digital advertising services will have standard terms, which are often presented as non-negotiable and offer limited due diligence opportunities. Where this is the case, it is still important to examine the points set out above. Failure to do so is likely to mean you will be operating with unascertained risk. The inability of a service provider to be able to provide adequate responses to the questions above can also be a significant red flag.

13.4 Automated decision making – Article 22 GDPR

Care should be taken when assessing the nature of the services. You should consider whether the technologies used will result in automated decision-making being applied that is subject to Article 22 GDPR i.e. that the technology will, without human interaction or final decision, make a decision that has a significant impact on an individual.[7]



Very often automated decision-making includes profiling. Both topics are heavily regulated by the GDPR (and subject to significant guidance). Where Article 22 applies, individuals who are subject to the automated processing or profiling should be informed that the processing is taking place and their consent gained to such processing unless it is required in relation to a contract between an organisation and that person, or specifically required by law. The controls are tighter if special category personal data is involved (most frequently this is health information in the digital advertising context) where explicit consent will usually be required or such processing can be justified on substantial public interest grounds. It is difficult to imagine a scenario where the requirements for explicit consent or satisfying public interest will be met in a digital advertising context.

If Article 22 GDPR applies, it will need to be appropriately addressed in the contract with the service provider e.g. through obligations to implement appropriate safeguards to protect the rights of the data subject. Privacy notices, cookie notices and consent management tools will need to be reviewed to ensure they adequately address the requirements of Article 22.

[7] Article 22(1) GDPR states that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

13.5 Identifying the legal basis for processing – Article 6 and 9 GDPR

Article 6 GDPR regulates the legal basis for processing of all personal data other than special category personal data (e.g. health, religious beliefs, sexual preferences, etc.), which is regulated by Article 9 GDPR. From the legal bases available for processing personal data under Article 6 GDPR, generally only legitimate interests or consent are considered relevant in the online advertising context and, of the two, the use of legitimate interests is most open to challenge.

Data protection authorities are likely to accept only the consent of the data subject as an appropriate legal basis for delivering online advertising. Flowing from the enforcement action against IAB Europe, we have seen that the role of legitimate interests has be reduced in the TCF framework.

We have set out in sections 8.1 and 8.2, that the GDPR sets stringent conditions for achieving valid consent, including when and how it can be used, and the rights of individuals to withdraw it. It will therefore be important that privacy and cookie notices clearly set out how consent is being relied on for digital advertising and how individuals can withdraw consent.

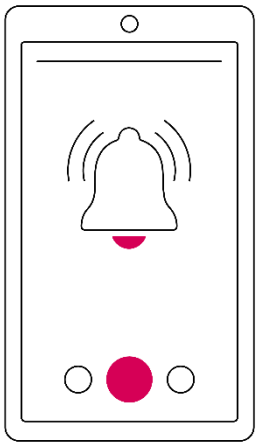
Consent statements and consenting functionality used by consent management platforms should be reviewed to ensure they meet GDPR requirements for transparency and valid consent. In particular, they should be reviewed to ensure they are not deploying dark patterns or nudge behaviours.

13.6 Privacy notices and cookie notices

In order to meet the transparency requirements under both the GDPR and ePrivacy Directive, it is important to ensure that individuals are informed about their personal data being used for digital advertising purposes, the cookies that are used and the controls and rights they have over both. This will typically be achieved through privacy and cookie notices, which should be reviewed to ensure they accurately reflect the digital advertising being deployed.

In relation to the privacy notice, this should describe:

- the types of personal data used for online advertising;
- the different purposes personal data is used for in the context of online advertising;
- the legal basis of processing;
- the entities with whom the personal data is shared, including details of any international data transfers;
- data subject rights, including the existence of any automated processing and/or profiling, and the ability to object; and
- the right to withdraw consent.



The cookie notice should name the cookies that are used for digital advertising, their role or function in delivering the digital advertising, the period of time they will remain on a user's device for before expiring and identify whether the cookie is a first or third party cookie (including the third party source where relevant).

13.7 Use of consent management tools and platforms

These tools are often incorrectly configured for the site they are deployed on, hence they will require the parties and the tool provider to work together to ensure that the technology, the privacy and cookie notices, and the consent management tool all align to present the individual with complete and accurate information.

13.8 Regular review and monitoring

Once the contract has been signed and the services started, the use of digital advertising is likely to remain a live data protection issue, which will require regular monitoring.

Any future changes to the digital advertising services being delivered will need to be assessed to identify GDPR and ePrivacy risks. For example, changes to the service may require updates to privacy notices with new information about data collection, updates to cookie lists in cookie notices or adjustments to settings in consent management tools.

Processes should be developed to ensure that changes to websites or apps (for digital advertising purposes) do not take place without an appropriate data protection assessment. Processes will also need to be in place to ensure the digital advertising contract and any orders or statements of work under it are kept up-to-date to reflect the actual nature of the processing being undertaken.

Regular monitoring for regulatory changes should also take place. For example, in the EU, there is significant regulatory activity regarding digital advertising, both in terms of the technologies used (and their compliance with privacy laws) and in relation to related international data transfers. In the UK, the Data Protection and Digital Information (No.2) Bill, if passed into law, will significantly increase the highest fine for non-compliance with cookie requirements from £500,000 to £17.5 million or 4% of global group annual turnover - whichever is greater. At the same time, it may also create a more permissive regime for analytic cookies.

14. Concluding comments

In this paper, we have explained the background and operations of digital advertising, the legal requirements for undertaking it, as well as setting out a range of practical steps to address those requirements.

Digital advertising is a pervasive part of our lives, seen by many of us every single day. This pervasiveness is a double-edged sword. It provides businesses with an unparalleled ability to reach their intended audiences but this ability also means that scrutiny will never be far away. Without undertaking the correct assessments and putting the correct controls in place, organisations will operate with unascertained risk. However, for those that take the proper steps, risks can be managed and the benefits of digital advertising truly realised.

If you need our support, we are here to help. Please get in touch with our Data Protection & Cyber Security team should you wish to discuss any aspect of this paper or the impact of digital advertising on your business.

DWF is a leading global provider of integrated legal and business services.

Our Integrated Legal Management approach delivers greater efficiency, price certainty and transparency for our clients. All of this, without compromising on quality or service. We deliver integrated legal and business services on a global scale through our three offerings; Legal Services, Legal Operations and Business Services, across our eight key sectors. We seamlessly combine any number of our services to deliver bespoke solutions for our diverse clients.

dwfgroup.com