The Seven-Step Ad Tech Guide

A step by step guide to address the privacy challenges of Real Time Bidding in programmatic advertising

Responsible Marketing

Joint Initiative

ISBA

DMA Data & Marketing Association

/ Contents

/ Executive Summary

The majority of digital advertising is delivered programmatically (through automation) via a variety of methods including Real Time Bidding (RTB). RTB is defined as the delivery of programmatic advertising by a real-time auction method.

To support this process, there are a myriad of technology solutions (Ad Tech) providers who enable advertisers to identify and target recipients of advertising delivered in real time.

The ICO (Information Commissioners Office) has identified a number of concerns relating to the protection of the rights of data subjects through the use of Real Time Bidding (RTB) in the programmatic delivery of digital advertising.

This document is written to support UK businesses actively engaged in the programmatic delivery of digital advertising to ensure they protect the rights of data subjects. It is a practical guide to the seven steps participants can take to ensure they adhere to the legal requirements and demonstrate their understanding of the regulator's concerns. We are grateful for the opportunity to consult with the ICO during the drafting of this document.

It is designed as a reference guide with clearly defined sections allowing readers to read the whole document or dip in as the need arises. Where suppliers are mentioned these are noted as examples and are not recommendations.

This guidance is divided into seven clear steps:

1. **Education and Understanding** – a comprehensive introduction to cookies and programmatic advertising with a detailed glossary of terms
2. **Special Category Data** – the ICO highlighted the importance of treating special category data with care and this section steps you through its definition and usage
3. **Understanding the Data Journey** – a key challenge is being able to track how data is captured and who processes it. This section explains how to complete a Record of Processing Activities as well as introducing the IAB's Transparency and Consent Framework.
4. **Conduct a DPIA (Data Protection Impact Assessment)** - the ICO noted the limited use of DPIAs in Ad Tech. This section sets out to explain what it is, when to use it as well as some pointers to what questions to ask.
5. **Audit the Supply Chain** – the ICO highlighted that you cannot rely on contracts to provide assurance around the use of personal data. This section provides audit check lists and questions you need answered when auditing suppliers.
6. **Measure Advertising Effectiveness** – the ICO have queried whether it's necessary to use all the data collected through Ad Tech platforms. This section provides links to reference materials for improving insights into advertising effectiveness to allow for a proportionate approach to using personal data.

7. **Alternatives to Third Party Cookies** – what does a post third-party cookie world look like? This section provides some suggestions about alternative methods of targeting including the adoption of contextual targeting. It also provides references to some industry initiatives which are exploring different ways of targeting in a less intrusive manner.

It's worth noting that some European DPAs interpret the law slightly differently hence the emphasis on the ICO in UK and their treatment and interpretation of GDPR and PECR. Therefore, the geographical scope is UK, and all references are to relevant UK law, UK regulatory guidelines and other UK centric materials.

/ Introduction

The ICO launched a review of Real Time Bidding (RTB) in programmatic advertising in February 2019. It started this process due to a concern regarding the complexity and scale of RTB, the risks it posed to the rights and freedoms of individuals and the concerns the ICO had received.

RTB is an area that has evolved and grown rapidly in recent years. It is underpinned by advertising technology (Ad Tech), allowing advertisers to compete for available digital advertising space in milliseconds, placing billions of online adverts on webpages and apps in the UK every day by automated means.

Since February 2019, the ICO has held two Fact Finding Forums (in March and November 2019) as well as publishing an Ad Tech Update in June 2019. In addition, the ICO has published a series of blogs which serve to reinforce their concerns about privacy rights in relation to RTB as well as highlighting progress achieved in engaging with the advertising, Ad Tech, media owner and marketing communities. The ICO's concerns are set out as follows:

> We have focused on RTB due to its complexity, the risks it poses and the low level of data protection maturity we've found through some of our initial engagements. Whilst we accept that RTB is an innovative means of advertisement delivery, our view is that, in its current form, it presents a number of challenges to good data protection practices.

The ICO further highlighted these key areas of concern:

- Methods for gaining consent are not transparent
- Opportunities to use legitimate interest are limited
- Special category data requires explicit consent for processing
- Widespread profiling is disproportionate and intrusive
- Soley relying on contracts for assurance is insufficient
- Lack of adequately developed DPIAs is a concern
- Appropriate and responsible data protection practices are crucial
- Queried whether data processing achieves the advertising outcome
- Collaboration with key players, such as Google and IAB Europe, is encouraged

Finally, the ICO concludes with:

> If you operate in the adtech space, it’s time to look at what you’re doing now, and to assess how you use personal data. We already have existing, comprehensive guidance in this area, which applies to RTB and Ad Tech in the same way it does to other types of processing – particularly in respect of consent, data protection by design and data protection impact assessments (DPIAs).

The purpose of this guidance issued by the DMA and ISBA is to provide a Seven Step Guide to help advertisers and marketers navigate their way through the complexity of RTB and to address the concerns highlighted by ICO. In particular our goal is to provide practical and easy to understand advice that is jargon free and accessible.

The two sponsors of this project are the DMA (Data and Marketing Association) and ISBA (Incorporated Society of British Advertisers). Between DMA and ISBA their membership is responsible for over £4 Billion of advertising and more than 3,000 brands.

/ Step One – Education and Understanding

Key Take-Aways

The Ad Tech sector is a complex ecosystem of technology providers who contribute to delivering programmatic advertising on behalf of advertisers via publishing platforms. This section discusses the following:

- Are you accountable? We explain how accountability not only means compliance with Data Protection law and guidance but also being able to demonstrate that compliance.
- Is your cookie policy compliant? We show how our checklists can help construct a strong cookie policy.
- We de-mystify the complexity of the Ad-Tech ecosystem
- We recommend that cookie preferences are managed in a Consent Management Platform (CMP)
- We provide a (non-exhaustive) checklist of places to go for Programmatic and GDPR training

Introduction

The Ad Tech sector uses many three letter acronyms and complex technology solutions. This complexity is compounded by the presence of a myriad of suppliers who support each stage of the Ad Tech food chain. All suppliers are taking a commission or cut from resulting revenue streams whilst many are not easily identifiable in the Ad Tech food chain.

The difficulties created by this complexity are compounded by limited consumer trust in how personal data is processed in the sector. A Harris Poll conducted by the ICO in 2019 shows that many consumers don't trust what happens to their personal data in the advertising and marketing ecosystem.

(https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf)

	2018	2019
NET: Low trust and confidence	**36%**	**38%**
1 – None at all	9%	10%
2	28%	28%
3	30%	30%
4	28%	27%
5 – A great deal	6%	6%
NET: High trust and confidence	**34%**	**32%**

Base: All Adults: 2018 (2131) / 2019 (2259)

Many marketers and marketing services staff may also have a limited understanding of what happens to the data they rely on to provide their services. As the provision of targeted, personalised advertising relies upon the use of personal data it's important that personal data is used responsibly and with due accountability.

There is a pressing need for information which will help the public reach informed decisions about where and how to share their data. This could be through codes of conduct and education from trade bodies or via communication directly from brands and advertisers.

In this section, our goal is to explain the importance of transparency and accountability in the context of Ad Tech. We aim to provide information which will shine a light on a technically complex issue and help advertisers and publishers become more transparent in their interactions with customers and readers.

The Role of Accountability and Privacy by Design

Accountability is a core theme throughout GDPR. It's designed to ensure that organisations are not only compliant with the GDPR but that they can also demonstrate that compliance has been achieved. One of the difficulties with the Ad Tech space is the lack of agreement around what might be acceptable as evidence to demonstrate this compliance.

The ICO states that an organisation

> Must put in place appropriate technical and organisational measures to meet the requirements of accountability.

In particular, it's important to focus on ensuring that customers' privacy rights are respected by organisations when processing data. In the context of Ad Tech, one would expect to see the following technical and organisational measures in place:

- Taking a "data protection by design and default" approach – putting appropriate measures in place to address data protection issues throughout the entire lifecycle of our processing operations, not just at the beginning
- Putting written contracts in place with organisations that process personal data on our behalf
- Maintaining documentation of how we process personal data which is under our control
- Implementing appropriate security measures to protect the personal data we control
- Carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests
- Adhering to relevant codes of conduct and signing up to certification schemes (where possible)

If it's not already in place, any major advertiser should consider creating a cross-functional governance group to develop and oversee a programme of sustainable activities that will deliver against this accountability goal. This should be linked to a dashboard of KPIs to ensure that compliance remains up to date.

Demystifying cookies

This section describes cookies and their usage. A cookie glossary is included in Appendix I.

What are cookies?

A cookie is a small text file that is stored by a browser on a user's device. Cookies don't 'do' anything - they are plain text and contain no executable code.

Cookies are like a memory aide for websites by acting as signposts to indicate your activity between visits, identify when you are using a site and record when you visit other sites.

The first time you visit a site, a cookie is downloaded onto your device, to record that you have visited the site. The next time you visit that site, the browser checks to see if your device contains a cookie that shows you have previously visited the site (that is, the cookie shows information containing the site name). If it finds the cookie with the site name, it sends the information contained in the cookie on your device back to the site. The site then 'knows' that you have been there before. In some cases, the site tailors what appears on your screen to take account of your previous visit (the display of a cookie banner specifically to first time visitors is an example of how a cookie might be used to differentiate between first time and subsequent visitors).

Cookies are also used to ensure the website functions in the way you would expect it to. They help understand how the website is being used. For instance, they can be used to store data about what is in your 'shopping cart', adding items as you click. They might record how long you spend on each page on a site, what links you click, or even record what are your preferences for page layouts and colour schemes.

Cookies are used to:

- Support website functionality
- Improve the user's experience e.g. by customising future visits
- Store a user's preferences
- Track website performance and operation - eg how quickly the page loads and refreshes its content
- Support display of information about how the content is viewed, in the form of analytics

Cookies from third party Ad Tech providers can be deployed when you move from one site to another. These cookies can be used to ensure that what is displayed to you (the content you are seeing on the website, including ads) is relevant to you. For this reason, cookies play a key role in Ad Tech.

Cookies are typically described under three headings:

- How long they last (duration)
- Who 'owns' them
- Their purpose

What does the law require?

When it comes to using cookies (or similar technologies) compliantly there are two laws which come into play:

- The ePrivacy Directive, implemented into UK law as the Privacy and Electronic Communications Regulations (PECR)

and

- The General Data Protection Regulation (GDPR) / UK Data Protection Act 2018

PECR

PECR gives people specific rights in relation to electronic communications and includes rules on:

- marketing calls, emails, texts and faxes (or any communication which is delivered using an electronic communication service)
- **cookies (and similar technologies) which place information on your device;**
- keeping electronic communications services secure
- maintaining customer privacy by controlling who can access the information generated when you use your device, such as traffic and location data, itemised billing, line identification, and directory listings

The reference to a **cookie law** is misleading. Consent is required to read anything from or write anything to a user's device. PECR does not refer to cookies directly, but Regulation 6 states:

6. *(1) ..., a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.*

(2) The requirements are that the subscriber or user of that terminal equipment—

(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

(b) has given his or her consent.

In other words, consent is required to

- read any information from the user's device

or

- write any information to the user's device

Note: these rules apply, even if you are not processing personal data.

GDPR

With introduction of GDPR in 2018, the underlying definition of consent changed:

GDPR Article 4(11) sets out that '*consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;*

Article 7 of the GDPR sets out further consent requirements:

- You must be able to demonstrate you have valid consent to use the user's data within a specified scope of use. If the scope is not wide enough to cover all uses, you must go back and get additional consent for this wider use.
- Your consent must be clearly distinguishable from other matters e.g. not bundled as part of your T&C's
- Your consent requests must be in an intelligible and easily accessible format, using clear and plain language
- Your consent mechanism must allow the individual to withdraw their consent at any time

Recital 32 of the GDPR:

- Specifically bans pre-ticked boxes - silence or inactivity does not constitute consent
- States that electronic consents must not be unnecessarily disruptive

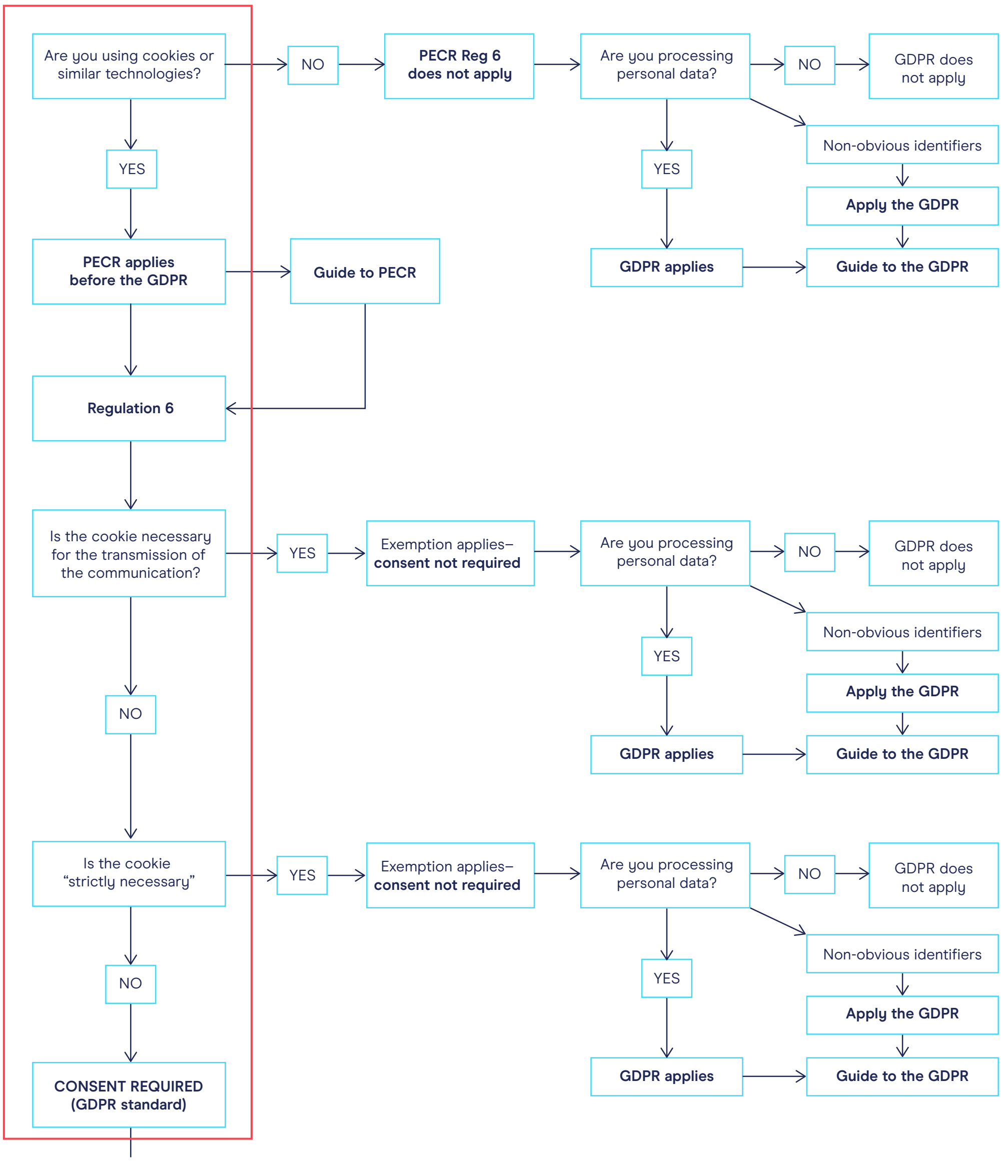
It's also important to note that the laws do not just cover websites...

> The use of cookies and similar technologies is not limited to traditional websites and web browsers. For example, mobile apps commonly communicate with websites and web services which can set cookies.
>
> **Ali Shah, ICO**

In the rest of this document any use of the term cookies should be taken to include cookies and similar technologies

The Intersection of GDPR and PECR

The ICO have provided a useful flow chart to help disentangle the two laws and their provisions relating to cookie 'notices':


Are you using cookies or similar technologies?
NO
PECR Reg 6 does not apply
Are you processing personal data?
NO
GDPR does not apply
Non-obvious identifiers
Apply the GDPR
YES
YES
PECR applies before the GDPR
Guide to PECR
GDPR applies
Guide to the GDPR
Regulation 6
Is the cookie necessary for the transmission of the communication?
YES
Exemption applies– consent not required
Are you processing personal data?
NO
GDPR does not apply
Non-obvious identifiers
YES
Apply the GDPR
NO
GDPR applies
Guide to the GDPR
Is the cookie "strictly necessary"
YES
Exemption applies– consent not required
Are you processing personal data?
NO
GDPR does not apply
Non-obvious identifiers
YES
Apply the GDPR
NO
GDPR applies
Guide to the GDPR
CONSENT REQUIRED (GDPR standard)

What Does a Good Cookie Notice Look Like?

The ICO's updated cookie guidance issued in July 2019 included the following section relating to cookie 'notices':

How do we tell people about cookies?

To comply with the information requirements of PECR, you need to make sure users will see clear information about cookies. In any case, doing so will increase levels of user awareness and control, and assist in gaining valid consent to cover the scope of the use of personal data you wish to make.

You need to tell people about the purposes of the cookies you place on their device and how long they will remain on their device.

You need to provide information about cookies in such a way that the user will see the information when they first visit your service. This is usually done within the cookie consent mechanism itself.

You should provide more detailed information about cookies in a privacy or cookie policy. This should be accessible through a link within the consent mechanism and also be reachable via a link at the top or bottom of your website.

You should consider how the design of your online service impacts on the visibility of the link to your policy. For example, a link at the bottom of a concise webpage which has no content "below the fold" will be much more visible and accessible than a link in the footer of a dense webpage of 10,000 words. In this case, a link in the header would be more appropriate.

Other ways of increasing the prominence of cookie information include:

- formatting – this might include changing the size of the link to the information or using a different font. The key is whether the link to this important information is distinguishable from "normal text" and other links.
- positioning – simply moving the link from the footer of the page to somewhere more likely to catch attention is an easy but effective thing to try
- wording – making the hyperlink more than simply "privacy policy"; this could involve a link through some explanatory text ("Find out more about how our site works and how we put you in control.")

You also need to ensure the information is clear so that your users understand it. Consider tailoring the language to your audience, and not using lengthy and overly complex terminology.

In summary, your cookie notice must be **prominent** and **understandable**. We have provided a detailed checklist in Appendix II

Cookie Governance

It is essential that bringing an organisation's cookie use into compliance is not regarded as a one-off exercise. Organisations must ensure they put in place appropriate processes to ensure their ongoing (and changing) use of cookies remains compliant. This could, for example, be achieved by incorporating cookie compliance into the scope of responsibility of your Governance team [group]

If any data captured via cookies is written back to your own servers, then it should be included in the scope of your data retention policy. If the data is personal, it should also be included in the scope of your response to Subject Access Requests.

Cookie Scans and Cookie Audits

Two terms which arise in the context of cookie governance are cookie scans and cookie audits. The terms have become blurred in their use so for the sake of clarity the following descriptions are provided:

- **A cookie scan:** A snapshot scan to determine what cookies are being used by a website or application. A cookie scan is a good starting point for understanding existing cookie usage and for carrying out an initial review and assessment of the cookies being used.
- **A cookie audit:** Provides assurance that an organisation is using cookies in accordance with the provisions of the law. An audit should evaluate the organisation's end to end cookie lifecycle by testing the design and operating effectiveness of controls and identifying any gaps/deficiencies, for example ensuring cookie choices made by users are being observed in practice.

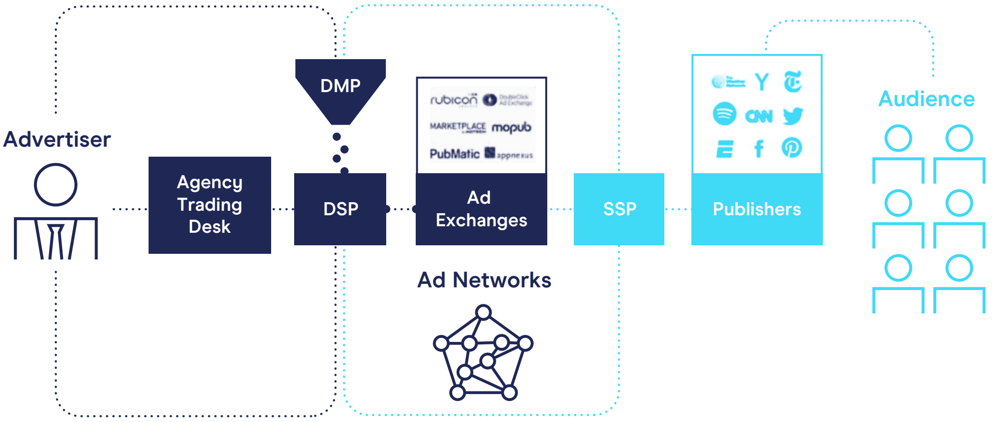
Cookie scanning and management software

There are several companies who provide cookie scanning and management software solutions. This software typically encompasses code to scan for cookies currently in use, code to categorise new cookies, code to generate the cookie banner and code to update the cookie policy (adding or removing cookies as relevant). Example suppliers include the Digital Control Room, OneTrust and Cookiebot.

Demystifying the Adtech Ecosystem

This section provides a description of the Ad Tech eco-system. A detailed glossary is contained in Appendix I.

This diagram is a high level representation of the different links in the lifecycle of a digital advertisement:



What is Programmatic Advertising?

An automated method of buying advertising space in digital media, where data is leveraged, often in real time, to make decisions on a per impression basis about things such as:

- whether this is the **right audience** and **environment** for a particular ad
- what **price** should be paid for the media (based on known data)
- what **creative/offer** this individual should be shown

In more technical terms:

Programmatic buying is the process of executing media buys in an automated fashion through digital platforms such as: exchanges, trading desks, and demand-side platforms (DSPs). This method replaces the traditional use of manual request for proposals (RFPs), negotiations and insertion orders to purchase digital media.

Source: IAB

It was projected that by 2020 Programmatic Digital Display Advertising will represent 88.9% of all digital display advertising.

The programmatic landscape from advertisers placing an advertisement on media platforms through to consumers responding to those advertisements is populated with a myriad of suppliers. Multiple data hand-offs occur with a high level of opacity around who processes which data and for how long.

Sell Side Platformm (SSP)

Sell Side Platform (SSP) is a company that provides technology for publishers to sell their advertising inventory through Real Time Bidding and other programmatic technologies. This virtual marketplace enables publishers to manage multiple and competing demands for advertising space within one platform. The intention is that publishers are able to auction their online marketing space (inventory) to the highest bidder. Example suppliers include: Index Exchange, OpenX, PubMatic, Rubicon Project, SpotX, Telaria (Merged with Rubicon Project), Xandr (formerly AppNexus)

Demand Side Platform (DSP):

A Demand Side Platform (DSP) is a company that provides technology for media buyers to purchase advertising through Real Time Bidding technology. Examples include: Adobe Media Optimizer (formerly Efficient Frontier and TubeMogul), Adform, Amazon A9, BrightRoll, Centro Basis, Criteo, Google Marketing Platform (DV360), Quantcast, The Trade Desk, Vertoz[3], Xandr (formerly AppNexus)

Data Management Platform (DMP)

Data Management Platform (DMP) is the backbone of data-driven marketing, and serves as a unifying platform to collect, organise, and activate first, second and third-party audience data from any source, including online, offline, or mobile. Using the cookie data that is collected as consumers move around the internet, a picture can be built up of which users can be grouped, by their behaviours, into audience segments.

On most DMPs, such audience segments are developed and refined through the platform using machine learning to identify ever more precisely users' repeat behaviours. Where once, DMP's were largely populated with third party data, they have evolved their role in the marketing mix away from third party data processing towards a greater focus on first party and CRM data. Best known are Lotame, Salesforce DMP (previously Krux), Adobe Audience Manager, OnAudience.com, Snowflake, SAS Data Management.

CPM (Cost per thousand)

The widely used pricing metric for trading digital advertising. Inventory is sold according to a cost per thousand price which will increase/decrease according to the level of targeting. A more highly targeted segment will have a higher price.

Real Time Bidding (RTB)

Real Time Bidding is the use of digital advertising technology to enable agencies and publishers to buy and sell advertising inventory in real time on an impression by impression basis. This will typically involve an auction pricing mechanism.

Open Market Place vs Private Market Place

Using cookies to help identify their target audience, buyers purchase media using Real Time Bidding auction method. Buyers are allowed to bid for airtime from a wide range of publishers in an unrestricted marketplace. This approach allows buyers to achieve scale as their ads are seen across many media platforms, usually at lower CPMs.

Buyers can also purchase media through a private marketplace (PMP). The difference is that agencies and/or advertisers will maintain a direct relationship with publishers using a “Deal ID” to transact.

Private marketplaces give publishers greater control, provide better transparency, can include exclusive inventory and access to publisher first party data. As a result publishers can achieve higher revenue levels (CPMs).

Programmatic Direct

Advertising which is delivered programmatically but is based on a direct deal between seller and buyer. This eliminates the need for ad exchanges and restricts the sharing of cookie data to only between seller and buyer, so no one sees the publisher’s audiences. The publisher will invite buyers, but no bidding is involved.

Deal ID

A Deal ID is an additional parameter that is passed in a bid request/bid response. In addition to things like timestamp, URL, IP address, cookie info, etc., many platforms can now also pass on the Deal ID with the transaction.

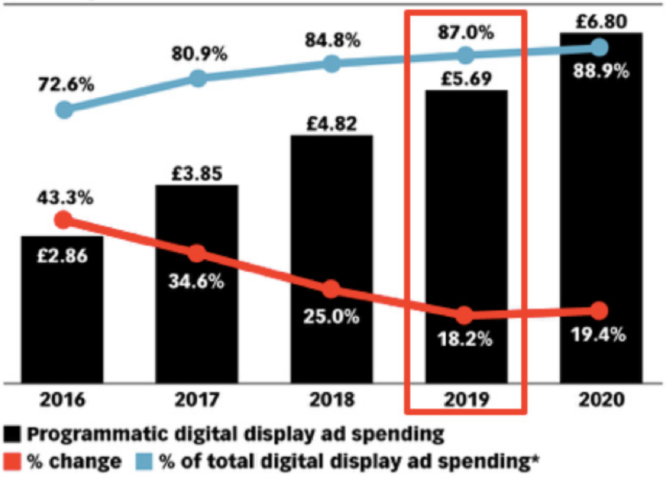
Deal ID is a unique string of characters that are used as an identifier for buyers and sellers. The buyer and seller will decide what is meant by that unique string of characters. Depending on what platform you are using, this could include things like priority, transparency, floor pricing or data. A Deal ID can usually be applied to any of the tactics that are executed through RTB process.

The Value of Programmatic Advertising

In 2019, it was projected that by 2020, Programmatic Digital Display Advertising will represent 88.9% of all digital display advertising. A market estimated to be worth £6.8bn. These projections have not taken account of the impact of Covid-19.

UK Programmatic Digital Display Ad Spending, 2016-2020

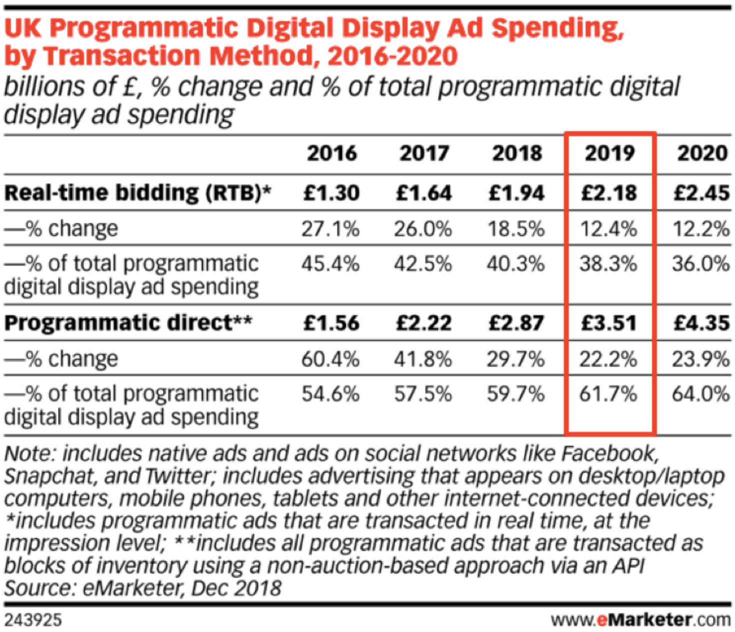
*billions of £, % change and % of total digital display ad spending**



*Note: digital display ads transacted via an API, including everything from publisher-erected APIs to more standardized RTB technology; includes native ads and ads on social networks like Facebook, Snapchat, and Twitter; includes advertising that appears on desktop/laptop computers, mobile phones, tablets and other internet-connected devices; *includes banners, rich media, sponsorship, video and other*
Source: eMarketer, Dec 2018

243924 www.eMarketer.com

Further, Real Time Bidding is projected to represent 36% of all programmatic advertising, a declining share against Programmatic direct.



UK Programmatic Digital Display Ad Spending, by Transaction Method, 2016-2020

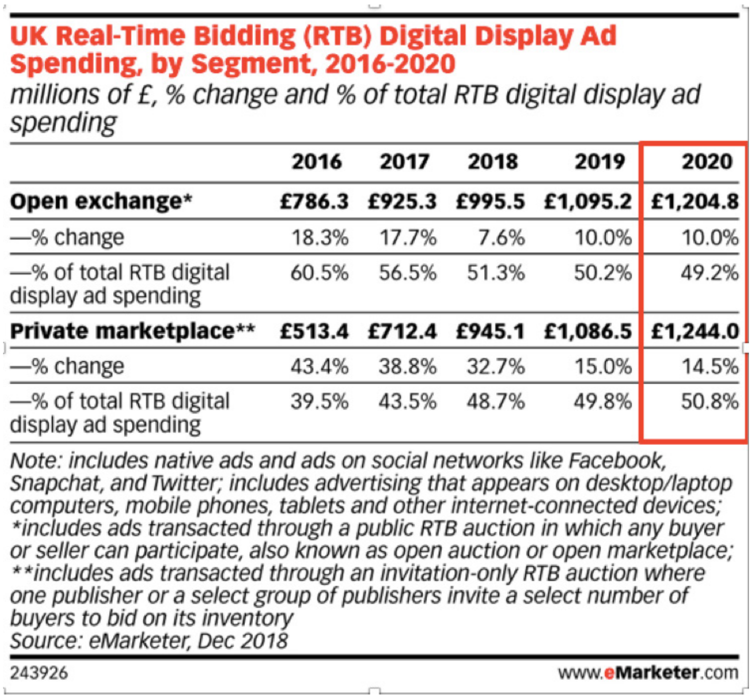
billions of £, % change and % of total programmatic digital display ad spending

	2016	2017	2018	2019	2020
Real-time bidding (RTB)*	**£1.30**	**£1.64**	**£1.94**	**£2.18**	**£2.45**
—% change	27.1%	26.0%	18.5%	12.4%	12.2%
—% of total programmatic digital display ad spending	45.4%	42.5%	40.3%	38.3%	36.0%
Programmatic direct**	**£1.56**	**£2.22**	**£2.87**	**£3.51**	**£4.35**
—% change	60.4%	41.8%	29.7%	22.2%	23.9%
—% of total programmatic digital display ad spending	54.6%	57.5%	59.7%	61.7%	64.0%

*Note: includes native ads and ads on social networks like Facebook, Snapchat, and Twitter; includes advertising that appears on desktop/laptop computers, mobile phones, tablets and other internet-connected devices; *includes programmatic ads that are transacted in real time, at the impression level; **includes all programmatic ads that are transacted as blocks of inventory using a non-auction-based approach via an API*
Source: eMarketer, Dec 2018

243925 www.eMarketer.com

When considering all Real-Time Bidding (RTB) spend, open exchanges represent a projected 49.2% share compared to 50.8% for private marketplaces. Again, this is a declining share.



UK Real-Time Bidding (RTB) Digital Display Ad Spending, by Segment, 2016-2020

millions of £, % change and % of total RTB digital display ad spending

	2016	2017	2018	2019	2020
Open exchange*	**£786.3**	**£925.3**	**£995.5**	**£1,095.2**	**£1,204.8**
—% change	18.3%	17.7%	7.6%	10.0%	10.0%
—% of total RTB digital display ad spending	60.5%	56.5%	51.3%	50.2%	49.2%
Private marketplace**	**£513.4**	**£712.4**	**£945.1**	**£1,086.5**	**£1,244.0**
—% change	43.4%	38.8%	32.7%	15.0%	14.5%
—% of total RTB digital display ad spending	39.5%	43.5%	48.7%	49.8%	50.8%

*Note: includes native ads and ads on social networks like Facebook, Snapchat, and Twitter; includes advertising that appears on desktop/laptop computers, mobile phones, tablets and other internet-connected devices; *includes ads transacted through a public RTB auction in which any buyer or seller can participate, also known as open auction or open marketplace; **includes ads transacted through an invitation-only RTB auction where one publisher or a select group of publishers invite a select number of buyers to bid on its inventory*
Source: eMarketer, Dec 2018

243926 www.eMarketer.com

Overall Open Exchange RTB is forecast to represent a shift from 27% in 2016 to 17.7% of all digital display advertising.

The Emergence of Consent Management Platforms (CMP)

Consent Management Platforms (CMPs) are a collection of Ad Tech tools which have emerged as a way to help media/advertising platforms collect user consent and pass that data to downstream advertising partners. There is a myriad of solutions available, whether from third party suppliers or bespoke platforms created by a publisher themselves. When selecting a CMP, it would be advisable to consider whether your chosen supplier has been verified by IAB Europe's CMP Compliance Programme. This list is interactive and is updated daily:

https://iabeurope.eu/cmp-list/

What are Browser Level Notifications?

Browser Level Notifications Definition

Web Push Notifications or Browser Notifications are clickable, rich content messages sent to an individual's device by a website or a web app. These notifications can be delivered to a device, mobile or desktop even when the user is not on the website. These notifications can only be sent to users who have opted-in to receive these notifications. Web Notifications are supported by Chrome, Firefox, Safari, Opera and Edge.

Web Push Notifications are often used to deliver time-bound content. For instance, retargeting following abandoned shopping carts, activating dormant users with offers or retaining users by displaying to them relevant new offers.

Users need to subscribe or opt-in to these notifications but do not need to download or install an application. Generally, they can simply subscribe to these notifications by clicking on the "Allow" button on the permission prompt.

Browser Level Notifications vs Native App Notifications

Native app notifications are only used in smartphones and tablets. Web push notifications are available on the websites displayed on any device, including desktop.

Native app notifications take full advantage of the device features including the camera, GPS, contact list whereas web push notifications are not able to tap into any of these features.

Native app notifications also support rich media including images, videos, gifs, audio and other interactive elements. Web push notifications only support large images.

Training Options

There are many training opportunities for marketers who wish to understand programmatic advertising as well as data protection related to digital advertising in more detail. Below is a (non-exhaustive) selection of organisations that provide training. The quality of the courses has not been tested and these are not recommendations:

Programmatic Advertising Training

https://www.emarketeers.com/training-courses/programmatic-advertising

https://www.circusstreet.com/our-process/

https://www.periscopix.co.uk/training/programmatic-training/

https://www.theidm.com/training-course/programmatic-marketing-essentials

https://digitalmarketinginstitute.com/en-gb/contact

https://iabeurope.eu/education/introduction-to-programmatic-advertising-course/

https://www.udemy.com/course/introduction-to-programmatic-advertising-digital-marketing/

https://www.simplilearn.com/

https://generalassemb.ly/corporate-digital-training/digital-marketing

https://academy.mediamath.com/faq-course/410534

Data Protection Training

https://dpnetwork.org.uk/data-protection-online-training-course/

https://www.theidm.com/gdpr-courses-qualifications

https://www.dqmgrc.com/services/gdpr-training

/ Step Two – How to Use Special Category Data

Key Take-Aways

- The ICO has highlighted the risks associated with handling special category data so any advertiser should handle such data with care
- The ICO has a clear definition of Special Category Data. This includes data relating to racial and ethnic origin, political opinions, health, biometric and genetic data as well as sexual orientation.
- It is also possible to infer Special Category Data by combining data from more than one source
- Handling Special Category data is high risk and you need to conduct a DPIA if you do decide you need to use it
- Processing of special category data is a very small part of advertising and marketing - ask yourself whether you really need to use any of that information

Introduction

A brand may end up capturing or processing special category data without intending to, from content consumption, product enquiry or purchases.

Special Category data can only be used if "Explicit Consent" is obtained in advance. Under existing statutory obligations, organisations need to be able to show how they have captured this higher standard of consent for the specific processing of that special category data. If brands never intended to capture special category data, it is important to explicitly exclude it from data being processed.

Definitions

The ICO has provided its own Special Category Data definition as well as a definition of when it can be used:

- personal data revealing **racial or ethnic origin**
- personal data revealing **political opinions**
- personal data revealing r**eligious or philosophical beliefs**
- personal data revealing **trade union membership**
- **genetic data**
- **biometric data** (where used for identification purposes)
- data concerning **health**
- data concerning a person's **sex life**
- data concerning a person's **sexual orientation**

This does not include personal data about criminal allegations, proceedings or convictions, as separate rules apply to use of such personal data.

The ICO states:

> Special category data includes personal data revealing or concerning the above types of data. Therefore, if you have inferred or guessed details about someone which fall into one of the above categories, this data may count as special category data. It depends on how certain that inference is, and whether you are deliberately drawing that inference.

What are the conditions for processing special category data?

Article 9 of GDPR explicitly lists the conditions for processing special category data:

- **Explicit consent for specific use**
- Employment, social security and social protection (if authorised by law)
- Vital interests
- Not-for-profit bodies
- Made public by the data subject
- Legal claims or judicial acts
- Reasons of substantial public interest (with a basis in law)
- Health or social care (with a basis in law)
- Public health (with a basis in law)
- Archiving, research and statistics (with a basis in law)

The only basis on which advertisers are able to process special category data is with Explicit Consent. This means that consent must cover any data processing, from data capture through to profiling to create customer segments.

Use of Special Category Data in Adtech

In its RTB update of June 2019, the ICO reports that special category data, which includes inferences of special categories, is widely used in the RTB context for targeting of adverts to individuals. The ICO has also been very clear in saying that 'consent' is the only condition that can be relied upon for processing special category data in a RTB context.

Given that there are risks associated with processing any Special Category Data in an AdTech environment, there is an expectation that this activity will require a Data Protection Impact Assessment (DPIA).

> You must do a **DPIA** for any type of processing that is likely to be **high risk**. This means that you are more likely to need to do a DPIA for processing **special category data**.

Our recommendation is that you should be conducting a DPIA in any situation where you are deploying Ad Tech solutions.

/ Step Three – Understanding the Data Journey

Key Take-Aways

- If a brand or supplier is using information that falls under the GDPR definition of personal data then they must ensure the data was originally captured in line with the requirements of the GDPR
- To understand a data and consent journey, a first obvious step is to develop a Record of Processing Activity (ROPA) which captures all processing activities in one document
- To help advertisers create a ROPA the AOP (Association of Online Publishers) has kindly provided access to their template, developed for publishers
- We have highlighted the importance of distinguishing between First Party Data (that which has been captured directly from your audience or customers) and Third Party Data (that which has been captured by a third party who does not have a direct relationship with the data subject)
- We recommend that third party data should be treated with caution as it will sometimes be difficult for advertisers to establish the source and provenance of that data
- We have previously discussed the use of Consent Management Platforms (CMPs) and here we describe the Transparency and Consent Framework (TCF) which has been developed by IAB Europe (Interactive Advertising Bureau) to standardise the provision of consent notices
- We highlight DAA Ad Choices as an alternative tool for managing Consent preferences with Ad Tech providers although awareness of it is low amongst data subjects
- There are other Consent frameworks provided by other Ad Tech platforms including Google and Facebook who process user data. Google have committed to adopting the TCF in 2020 which appears to strengthen the IABs desire to be developing an industry standard across Europe.

Introduction

A significant challenge in Digital Advertising is the need to identify all the participants who are processing personal data to deliver advertising. Because there are many hand-offs through the Ad Tech food chain, it is easy to lose sight of who is processing which data, when and under what circumstances. As a starting position, to untangle these activities, it is useful to capture, in writing, how this data is processed.

Record of Processing Activities (ROPA)

Article 30 of the GDPR states that it is necessary to record all your processing activities in writing. Essentially, it's an inventory of your data processing. You must maintain records which include details on processing purposes, data sharing and retention. It is likely that information audits or data mapping exercises will feed into the documentation of processing activities.

What do you need to document?

- The name and contact details of your organisation
- The purposes of your processing
- A description of the categories of individuals and categories of personal data
- The categories of recipients of personal data
- Details of any data transfers to third countries, including documenting the transfer mechanism safeguards in place
- Retention schedules
- A description of your technical and organisational security measures

What is useful but not necessary for you to document:

- Information required for privacy notices such as:
    - Lawful basis for the processing
    - The legitimate interests for the processing
    - Individuals' rights
    - The existence of automated decision-making, including profiling
    - The source of the personal data
- Records of consent
- Controller-processor contracts
- The location of personal data
- Data Protection Impact Assessments (DPIAs)
- Records of personal breaches
- Information required for processing special category data or criminal conviction and offence data:
    - The conditions for processing in the Data Protection Act
    - The lawful basis for the processing in the GDPR
    - Your retention and erasure policy document

This may seem like a formidable task but it is likely that some of this documentation exists already in your organisation. A first step is to establish how much documentary evidence has already been completed by your privacy team and how much you need to add.

It's also important to note that both Controllers and Processors have obligations to document their processing. The ICO has set out the specific requirements in their guidance documents:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/what-do-we-need-to-document-under-article-30-of-the-gdpr/#what1

The ICO has also published a generic ROPA template for Controllers and Processors which sets out the information that must be collected and could be collected.

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/documentation/how-do-we-document-our-processing-activities/

Publisher Specific Record of Processing Activities (ROPA)

The Association of Online Publishers has also created a publisher specific ROPA matrix which identifies the likely processing undertaken by most publishers.

https://www.ukaop.org/aop-news/aop-resources/aop-matrix?Preview=1

First and Third Party Data

First Party CRM Data

First party data is the information you collect directly from your audience or customers once a customer has been given adequate notice about what you collect and why and has given you consent to collect their personal data. This information about your customers can be collected from both online and offline sources, such as your company's website, apps, CRM, social media or surveys and is known as **first party data**.

First party data is considered to be highly valuable because:

- You know where it has come from and you know the scope of consent provided so can be confident in its use
- It's straight from the customer or prospect so highly relevant
- So long as the use is within the scope of consent, you can use it:
    - To gain an insight into how customers and prospects behave
    - To provide a direct insight into customer preferences
    - To see all interactions with the brand whether on or off-line
    - To link this data to customer transactional records in the CRM system, creating a data flow from advertisement to the P&L

It is becoming increasingly obvious that first party data will become more important for advertisers and marketers, as challenging questions continue to emerge regarding the ability to trace the provenance of third-party data.

Third Party Data

We recognise that a significant volume of third-party data has historically been collected offline. However, for the purposes of this document, we have focussed on digital / online sources.

Any data collected by an organisation which does not have a direct relationship with the data subject is categorised as third-party data. It can be a much more widely sourced set of information, including location-based information, online behaviour, activity on social networks.

The data may be derived from the browsing habits of individuals across a wide range of websites which can be amalgamated to create a user profile or segment. This data is typically processed through Data Management Platforms (DMPs) or other data aggregators which can use the variety of data sets to create comprehensive audience profiles, categorised into segments. In turn, advertisers can target audience segments, based on key behaviours or characteristics.

Since the introduction of the GDPR and the requirement to collect GDPR level consent for making use of cookies and the insight they provide into user's behaviours, it is increasingly difficult to trace the provenance of third party data and the necessary scope of the consent obtained which authorises the planned processing of that data in the first place. The challenge faced by data aggregators, is obtaining valid consent from the data subject to process their data within a desired scope, to track their journeys across the web.

The Transparency and Consent Framework (TCF)?

Sourced IAB Europe website and other IAB resources: https://iabeurope.eu/

What is the TCF?

IAB Europe have developed The Consent Framework as a means by which website publishers can tell visitors what data is being collected and explain the scope of such data use (how their website and partners intend to use it). The core goal is to provide a common standard and language to capture and communicate consumer consent for the online delivery of advertising.

There are a variety of resources available from IAB including:

- The Global Vendor List (GVL) managed by IAB Europe, captures and stores the registration of Vendors working with website publishers and advertisers, as well as Consent Management Platforms (CMPs) who work with publisher sites
- The CMP (Consent Management Platform) Validator is managed by IAB Europe and oversees the compliance process of CMP's participating in the TCF

So far, there have been two versions of the Framework TCF v1.1 launched on 25th April 2018 and TCF v2.0 on 21st August 2019. In terms of future developments, there is a clear commitment to continue to develop this framework and collaborate with ICO and other Data Protection Authorities around Europe.

How is TCF intended to work?

The Framework consists of open-source technical specifications managed by the IAB Tech Lab, and policies managed by IAB Europe. It has been designed to standardise the provision of information notices about the scope of personal data processing, and the transmission of 'signals' about user choices and transparency related to data processing. This will allow the digital advertising supply chain to continue to function in a way that aligns with GDPR requirements.

What is included in TCF v1.1:

A technical industry solution to allow website operators to:

- Understand privacy-related disclosures about their Ad Tech vendors
- Use those disclosures to make privacy-related disclosures to its users
- Disseminate the disclosure status through the online advertising ecosystem

https://github.com/InteractiveAdvertisingBureau/GDPR-Transparency-and-Consent-Framework/blob/master/CMP%20JS%20API%20v1.1%20Final.md

What's in TCF v2.0

- Revised definitions and descriptions of data processing purposes that combine greater granularity (now increased from 5 to 10 purposes with the addition of 2 special purposes, and 2 features and 2 special features) that will enable users to make more informed choices regarding the processing of their personal data
- The introduction of signals that allow CMPs to offer users a streamlined means for users exercising the "right to object" to processing on the basis of a "legitimate interest"
- A more complete accommodation of the "legitimate interests" legal basis for data processing that allows vendors to receive a signal about whether their legitimate interests have been disclosed

- New, granular controls for publishers about the data processing purposes permitted by them on a per vendor basis
- Greater support for the users of the framework in their application of the policies, terms and conditions and technical specifications with increased investment by IAB Europe in the resource to support compliance

https://iabeurope.eu/wp-content/uploads/2019/08/TCF-v2.0-FAQs-1.pdf

The intention was to transition all publishers and vendors to TCF v2.0 by June 29th 2020. Given the impact of the coronavirus pandemic this deadline has been extended to August 15th 2020. Whenever the transition is completed v1.1 will no longer be supported.

How many TCF Vendors are Registered?

The IAB has published a list of registered vendors both for v1.1 and v2.0. This list will continue to grow as more vendors are approved and is shown here:

https://iabeurope.eu/vendor-list-tcf-v2-0/

How many TCF Consent Management Providers (CMPs) are Registered?

The IAB has published a list of CMP providers who have passed the compliance checks required by IAB Europe's CMP Compliance Programme. That list is updated daily and is published here:

https://iabeurope.eu/cmp-list/

TCF Audit Plans

On 22nd January, IAB announced that a new iteration of IAB UK's Gold Standard would be launched later in 2020, bolstering the certification process and incorporating steps to address privacy concerns within the digital supply chain.

Gold Standard 2.0 will require companies to adopt IAB Europe's Transparency & Consent Framework version 2 (TCF v2.0). In addition, IAB UK plans to employ an independent third-party to audit the Gold Standard certification process, ensuring the robustness of the industry standard.

In its current form, the Gold Standard brings together industry programmes to combat ad fraud, increase brand safety and improve the digital advertising experience for users. There are currently 93 media owners, media agencies and Ad Tech companies certified and 11 registered to certify.

A wide range of resources and training materials are found at IAB Europe:
https://iabeurope.eu/

DAA Ad Choices

The Digital Advertising Alliance (DAA) is a consortium of the leading national advertising and marketing trade groups in USA that together deliver self-regulatory solutions to online consumer issues.

The Ad Choices service, provided by the DAA, gathers in one place the opt-out mechanisms provided by participating Ad Tech vendors, offering visitors a "one-stop" platform through which to opt out from the collection of Web-viewing data for interest-based advertising.

https://youradchoices.com/

Google Ad Manager

Google provides a variety of ways in which advertising is served to consumers, whether this is advertising on Google's own platforms or whether it is providing an ad serving solution for publishers who wish to manage advertising across their own inventory.

Google Ad Manager is the ad management platform for large publishers who have significant direct sales. It is a complete ad exchange platform that facilitates both the buying and selling of ads across multiple ad networks and locations, including AdSense and (the former) AdExchange.

Today, Google Ad Manager supports a wide range of distribution channels, including mobile, desktop, smart televisions, and video. The Ad Manager network is where you define your ad inventory and create, manage, and report on your advertising campaigns.

Google Chrome

Separately, Google Chrome announced, in January 2020, that it would cease to support third party cookies in its browser by 2022. This effectively spells the end of third-party cookies for ad targeting. The intention is to build out the Google Privacy Sandbox which will provide a set of tools for advertisers to deliver privacy friendly advertising campaigns. In general, this is seen as a positive move from the perspective of compliance with GDPR and PECR. Some concerns have been expressed about the likely increase in market dominance as a result of these changes.

Not enough is known yet about what might replace 3rd party cookies, as the Google Sandbox is not yet well developed and it's not clear how other operators may develop their solutions. Already Safari and Mozilla have acted unilaterally to block the use of third-party cookies without mirroring the 2-year transition phase applied by Google. It's worth noting that a fragmented market with a patchwork quilt of alternatives to cookies may not be a good outcome for advertisers.

Facebook Integrations

Facebook provide a variety of ways in which advertisers can reach and track audience behaviour. This may vary from the Audience Network, Instagram Platform, Messenger. Advertisers should be mindful of how user data is processed. Details can be found here

https://developers.facebook.com/docs/

Other AdTech Platforms

All advertising partners provide their own frameworks for capturing and managing personal data derived from cookies or other technologies across different formats. In advance of embarking on an Ad Tech/Martech project it's advisable to carry out a Data Protection Impact Assessment to understand the potential risks associated with using these products. Other suppliers include Adobe Advertising Cloud, Salesforce DMP, Freewheel and mParticle.

/ Step Four – Conduct a DPIA (Data Protection Impact Assessment)

Key Take-Aways

- It is best practice to evaluate proposed personal data use cases before the personal data is collected and used. This evaluation must include an assessment of the impact of the use of personal data on the individual.
- A DPIA (Data Protection Impact Assessment) provides a framework within which to assess the impact of the use of personal data to determine whether it is proportionate to the expected outcome
- The ICO has a DPIA template and the DMA (amongst others) provides guidance on how to conduct a balanced DPIA. It is critically important that these assessments are done with a degree of objectivity.
- The AOP has commissioned a specialist to draft a DPIA template questionnaire for the publishing industry. This provides a series of questions and prompts to help complete an Ad Tech DPIA.
- However, it needs to be remembered that every DPIA should be tailored to an individual companys' activities – there is no generic template or completed DPIA document

Introduction – what, why, where, when, how

A DPIA is a Data Protection Impact Assessment. As per ICO:

> It's a process designed to help you systematically analyse, identify and minimise the data protection risks of a project or plan. It is a key part of your accountability obligations under the GDPR, and when done properly helps you assess and demonstrate how you comply with all of your data protection obligations.

It does not have to eradicate all risk but should help you minimise and determine whether or not the level of risk is acceptable in the circumstances, taking into account the benefits of what you want to achieve.

DPIAs are designed to be a flexible and scalable tool that you can apply to a wide range of sectors and projects. Conducting a DPIA does not have to be complex or time-consuming in every case, but there must be a level of rigour in proportion to the privacy risks arising.

These are some of the conditions under which a DPIA should be conducted:

- Evaluation or scoring
- Automated decision-making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organisational solutions
- Preventing data subjects from exercising a right or using a service or contract

The ICO has made it clear that businesses involved in Ad Tech should be conducting DPIAs - it is hard to imagine any marketing activity in the ad-tech space that does not reach the threshold for completion of a Data Protection Impact Assessment.

Stages of a DPIA

The steps to follow when conducting a DPIA are as follows. You should be able to identify the nature, scope, context and purposes of what you are planning to do:

Step 1: identify the need for a DPIA
Step 2: describe the processing
Step 3: consider consultation
Step 4: assess necessity and proportionality
Step 5: identify and assess risks
Step 6: identify measures to mitigate the risks
Step 7: sign off and record outcomes

DPIA Templates

The ICO provides an example template, as does the DMA. Organisations can create their own, as long as all of the necessary questions are asked, and appropriate stakeholders consulted. The aim is to identify all risks associated with the processing of personal data as part of the project/initiative and describe how those risks will be mitigated.

The links below show examples of DPIA templates:

ICO DPIA template -

https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf

The AOP has also produced a template DPIA questionnaire for publishers to ensure all the key questions are covered:

https://docs.google.com/spreadsheets/u/1/d/1cIyX1CEs8sSqWu9IYrXLLuwJIK-OcQtoNqcS32bPceU/template/preview?urp=gmail_link

The AOP DPIA pre-qualifier Google sheet template provides a mechanism for establishing and recording when a full DPIA is required. *The link will provide access to a Google Sheets document that you can save locally by selecting the USE TEMPLATE option

Change Control Mechanisms

When implementing change involving the processing of personal data, it is essential to have a mechanism in place to ensure any risks identified through the DPIA process are properly mitigated.

Consider the creation of a regular report (ideally for discussion at a Governance meeting) covering the key risk areas with their latest status flagged as red, amber or green. It helps to have a detailed action list of all identified risks and remediation actions relating to functions, systems and third-party processors – along with any other data risks identified by other workstreams. Consider appointing a Project or Programme Manager to facilitate the process, chase people for progress updates, manage the budget asks, etc.

/ Step Five – Audit the Supply Chain

Key Take-Aways

- If at any point a brand loses sight of the personal data or takes another company's warranty about the scope of consent attached to personal data in Ad Tech chain then caution is needed
- The ICO has highlighted that much of the personal data used within digital advertising isn't audited or investigated in any meaningful manner. A contractual paper trail supporting the authorisation of use of the personal data is simply not enough to justify many use cases.
- In this section we have provided checklists to help advertisers establish whether their contracts include the necessary information to satisfy the ICO's criteria for compliant contracting
- Once a contract is in place, with the right of audit, then there is scope to carry out an audit of supplier activities on a periodic basis. Although we recognise that annual audits of all suppliers may not be possible, it is advisable to rotate audits and maintain an up to date record of their processing activities.
- Deciding on the frequency of audits is an inexact science and depends on the level of risk associated with processing the data. We have set out the likely factors relating to risk, volumes of data process etc that will need to be taken into account to determine the frequency.
- In the absence of an approved certification scheme, alignment with the recently published ISO 27701, the standard extending ISO27001 into privacy and personal data, is a good proxy for an approved scheme

Supplier Contract Due Diligence

When you negotiate a contract with any supplier in the Ad Tech supply chain it is good practice to consider the following factors:

- Does the contract set out what personal data is used for what purpose?
- Is the contracted partner a Controller, Joint Controller or Processor?
- Depending on the Controller/Processor relationship, have you included a Data Processing Agreement or a Joint Controller Agreement?
- Do you have the necessary Data Processing or Controller agreements in place?
- Does the contract highlight the importance of confidentiality?
- Does the contract provide for audits and inspections?
- Is it clear who is accountable and liable for different activities?
- Is there a provision to cover third party processing of data?
- What process exists for managing data when the contract ends?
- Is the personal data that is being processed detailed in their "Record of Processing Activities"?

Audit Frameworks

If you choose to audit an Ad Tech supplier, we have provided a checklist of some of the questions you should ask in Appendix III. The checklists are not exhaustive but provide a good starting point to help tease out issues.

The frequency of audits will depend on a variety of factors including the risk associated with working with that supplier. Factors to consider:

- How much data is handled?
- What type of data is handled – how risky is the process?
- What would be the impact if a data breach occurred?
- The quality of due diligence reporting at contract initiation
- Is the supplier accredited/certified?
- Have there been any complaints relating to privacy?
- Have there been changes in ownership?
- Have there been significant changes in processes and workflow?

Providing Assurance

Article 42 of the GDPR sets out that:

> The Member States, the supervisory authorities, the Board and the Commission shall encourage, in particular at Union level, the establishment of data protection certification mechanisms and of data protection seals and marks, for the purpose of demonstrating compliance with this Regulation of processing operations by controllers and processors.

No such certification has yet been approved in relation to Ad Tech or Martech.

In the absence of an approved certification scheme from ICO, alignment with the recently published ISO 27701, the standard extension ISO27001 into privacy and personal data, is a proxy for an approved scheme. It provides an indicator of good practice for those operating within the Ad Tech and Martech spheres as ISO 27001 has become around information security.

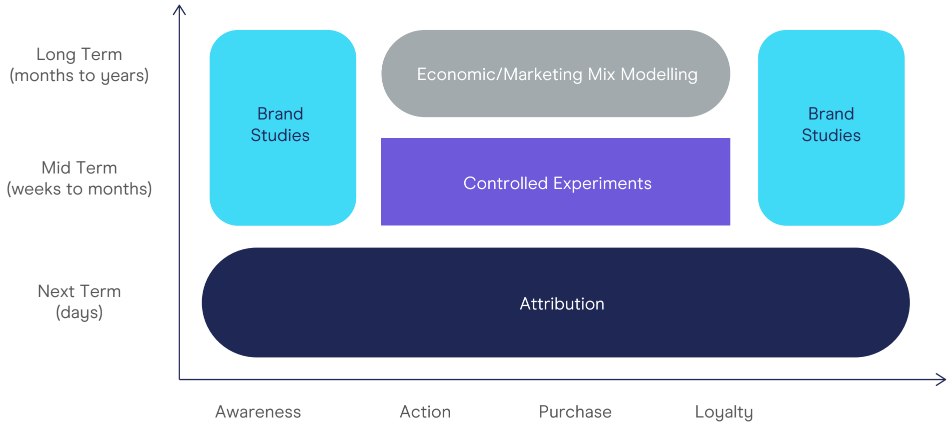
/ Step Six – Assess Advertising Effectiveness

Key Take-Aways

- As part of their close scrutiny of Ad Tech, the ICO queried whether large scale data processing activities achieve the advertising outcome
- Advertisers are striving to understand the benefits, risks and returns of their marketing activity. When these are understood the challenges associated with the use of personal data to buy/sell and target advertising can be viewed in the round.
- Modelling the value of marketing can be expensive, especially with econometric approaches, and this represents a challenge for smaller organisations. Article 25 of the GDPR stresses that, in implementing all the GDPR principles, the overall effectiveness of marketing could affect the actions and approaches being taken.
- A key benefit of programmatic advertising is the ability to understand the effectiveness and efficiency of advertising due to the comprehensive amount of data shared between systems. Regulation and changes to browsers and cookies means in the future much of this measurement data will be unavailable forcing new ways of thinking about how to measure advertising effectiveness. We have set out here other methods available.
- We have provided a (non-exhaustive) list of resources available, which provide guidance in the development of advertising measurement

Tools to measuring Marketing ROI and Performance

There are a variety of tools available to measure advertising/marketing effectiveness.



Reproduced from IAB Guide to Measuring Digital Advertising in a Multi-Media Context

Brand Studies

These studies are designed to measure and track brand awareness and salience over a long period of time. The main challenge from tracking the impact of targeted digital advertising is the difficulty in being able to isolate which variables have affected the branding metrics. Not only is it difficult to create any material shift in the metrics but there are likely to be a variety of other factors influencing brand health.

Econometric/Marketing Mix Modelling

Econometric modelling can be deployed to understand the impact of different marketing channels on the movement in key KPIs and financial performance over a long period of time. Rooted in the use of statistical analysis it requires a significant volume of data collected over a long period of time to derive meaningful results. It is also an expensive method of evaluating marketing performance and is therefore only really a viable solution for large advertisers with many data points.

https://en.wikipedia.org/wiki/Econometric_model

Controlled Experiments

Many direct marketing campaigns are rooted in the use of controlled experiments to understand the effectiveness of creative work and messaging as well as channel choice. It's necessary to have a control (your winning solution) against which you're able to test alternatives. In this scenario testing one variable at a time is critical to understand the impact of a change. If two variables are changed at once, it's impossible to isolate the impact of each change.

Attribution Modelling

This is a method of assessing the impact of different advertising/marketing actions on an outcome. In the context of advertising attribution there may be a variety of ways in which a brand is communicating to their customers/prospects and an effective attribution model will calculate the impact of the different touch points whether it is media, POS or digital advertising. The trick is to ensure that the full effect of the marketing is not attributed to the "last click" as there may have been other factors which contributed to the sale.

https://en.wikipedia.org/wiki/Attribution_(marketing)

Predictive modelling

This is a method of modelling data in order to predict outcomes. This may be a combination of data including transactions, conversion data, customer segmentation combined to create a model which allows you to predict future behaviour.

https://en.wikipedia.org/wiki/Predictive_modelling

Marketing Measurement Resources

IAB: Measuring Digital Advertising in a Multi-Media Context

https://www.iabuk.com/sites/default/files/public_files/IAB_Measurement_Toolkit_Online%20%284%29.pdf

IPA: Econometrics Explained

https://ipa.co.uk/media/4868/econometrics_explained_2_final_single_pages.pdf

ISBA: White Paper – Cutting Through the Clutter in partnership with Ebiquity

https://www.isba.org.uk/news/cutting-through-the-clutter-making-sense-of-the-hype/

Market Research Society: Courses to learn advertising effectiveness

https://www.mrs.org.uk/event/training-courses/effective-advertising-evaluation

Econsultancy: A guide to maximsing the ROI of Digital Marketing
(subscription service)

https://econsultancy.com/reports/a-short-guide-to-maximising-the-roi-of-digital-marketing/

/ Step Seven – Alternatives to Behavioural Advertising

Key Take-Aways

- There are signs that, in the long term, the third party cookie will no longer be the means by which we can deliver well targeted digital advertising. Arguably we will always struggle to track the data journey, understand the provenance of some data or be able to evaluate the effectiveness of our advertising.
- Contextual advertising is experiencing a resurgence and we have provided a (non-exhaustive) checklist of some providers of contextual targeting which avoids the use of personal data when creating targeting segments
- Edge Computing and Vertical Networks may help deliver different targeting methods
- There are also industry initiatives from IAB, Google and others which are considering how to target in a less intrusive manner

Other Means of Targeting

Contextual targeting

The announcement by Google Chrome that behavioural targeting based on third party cookies will become a thing of the past provides an opportunity for contextual advertising to reappear. Contextual advertising is targeting advertising based on the context for that advertising and would ensure that the advertising remained privacy compliant.

Instead of manually selecting individual sites which are contextually appropriate, technical solutions would be deployed which use machine learning to deliver contextual targeting and analytics solutions for publisher and advertisers. The publishers can create a more accurate picture of page content, ensure that it’s classified accurately and market inventory is created based on context. Advertisers can select an environment which is consistent with their brand and target based on context, whilst remaining privacy compliant.

Below is a non-exhaustive selection of companies that specialise in contextual advertising and marketing:

https://www.beemray.com/ - analytics company delivering personalisation through context

https://www.ozoneproject.com/ newspaper consortium delivering contextually relevant advertising campaigns

https://www.admantx.com/ - contextual advertising analytics and targeting tools https://www.comscore.com/Contextual-Targeting - programmatic provider deliver contextual targeting

https://entity-x.net/ - contextual analytics company

https://www.oracle.com/corporate/acquisitions/grapeshot/ - Grapeshot now part of Oracle Data Cloud a context based targeting tool

https://www.weareilluma.com/ - contextual targeting technology for advertisers

https://www.iris.tv/ - contextual ad targeting for video in partnership with Mediamath

https://www.precise.tv/ - Precise TV – contextual advertising company focused on YouTube advertising

https://www.silverpush.co/ - AI based contextual advertising in video

https://zefr.com/ - contextual targeting DMP platform for advertisers

Edge Computing

Edge Computing is a process by which you can process data on the device that generates the data rather than on a remote cloud server. This minimises the data leaving the user's device and thus protects their privacy. This is becoming a more widely used technique in advertising with some technical solutions leveraging this process:

https://brave.com/brave-ads-waitlist/ - an edge computing ad platform from Brave, the private web browser. It uses granular profiles that are maintained on the device and that the user controls.

https://permutive.com/ - a data management platform used by publishers where computations happen on the device where the data is generated, rather than in the cloud, using a combination of context and first party cookies.

Vertical Advertising Networks

These networks are designed to deliver advertising to a specific target audience based on their interests. Examples include travel, automotive, lifestyle. This is a more privacy friendly way of advertising, as you're relying on targeting the content context rather than individuals.

https://www.adnetworkdirectory.com/

Individual Industry Initiatives

Google Chrome Sandbox

In January 2020, Google Chrome announced that it would stop supporting third party cookies within 2 years. Even though Safari and Firefox had already stopped supporting third party cookies, this announcement from Chrome is a game changer because it represents more than 65% of all browser installations.
Google have further announced that third party cookies will be replaced with the Google Privacy Sandbox, although no dates have been set and the contents of the Sandbox have not been clearly defined. Essentially, it will be a secure environment for ad personalisation and measurement and could easily become the industry standard to follow.

https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html

https://www.chromium.org/Home/chromium-privacy/privacy-sandbox

IAB Project Rearc

IAB launched Project Rearc on 10th Feb 2020 which is a global initiative to help improve understanding of digital advertising. It is also setting up workgroups for different organisations to collaborate and participate in a project to identify future solutions for ad targeting, measurement and optimisation driven by the need to enhance consumer transparency and industry accountability.

https://iabtechlab.com/project-rearc/

The 5th Cookie

This is a collaboration between Anonos , Acxiom and Information Accountability Foundation to explore GDPR recommended technical and organisational safeguards to enforce greater accountability and ethics across the AdTech real-time bidding ecosystem. The 5th Cookie model supports the view that Legitimate Interest based Ad Tech processing is possible - described as "Pseudonymisation-Enabled Legitimate Interest Processing" - if the necessary safeguards in are in place when processing data.

https://www.5thcookie.com/

The World Wide Web Consortium (W3C)

The World Wide Web Consortium is an International community where member organisations, a full-time staff, and the public work together to develop web standards. Led by web inventor and Director Tim Berners-Lee and CEO Jeffrey Jaffe, **W3C's** mission is to lead the Web to its full potential.

https://www.w3.org/

Appendix I - Glossary of Terms

Cookies

#	Categorisation	Types	Description
1	**Cookie duration**	Session cookies	**Session** cookies are stored in a browser's memory until the browser is closed. These are typically used for essential site functions such as quickly loading a page.
		Persistent cookies	**Persistent** cookies are set with a specific expiration date, meaning that they will survive in a browser's memory beyond a single session.
2	**Cookie owner**	First-party cookies	A first party cookie is set and collected by the website you're browsing and only used by that site when a user is visiting it. These are usually critical to providing key functionality such as allowing you to add items to a shopping basket.
		Third-party cookies	These cookies are set and collected by third parties (other than the website itself) including advertisers, analytics providers or social media providers.
3	**Broad Cookie Categories**	Essential cookies	There are two scenarios where consent is not required: • Cookies enabling the transmission of the communication. • Cookies which are defined as 'strictly necessary' to provide the service requested by the user. For instance, remembering goods in a basket or load balancing to ensure a page loads efficiently.
		Non-essential cookies	All other cookies are non-essential cookies and require consent. This includes analytics which may be helpful or convenient, but are not essential.

3	**Cookie purpose / function** *(These are the four categories of cookies originally published by the International Chamber of Commerce when the cookies law first came into effect in 2012)*	Strictly Necessary	**Strictly Necessary** the use of the cookie must be related to a service provided on the website that has been explicitly requested by the user. For example, without these, a service like shopping baskets cannot be provided.
		Performance (Analytics)	**Performance** cookies collect info about how visitors use a website (e.g. which pages visitors go to most often or if they get error messages from web pages). The information collected is aggregated and is used to improve how a website works.
		Functional	**Functional** these cookies allow the website to remember choices you make (like username, language, region) and provide more enhanced personal features.
		Targeting or advertising	**Targeting or advertising** these cookies are used to target ads based on your profile and your interests. They are also used to limit the number of times you see an ad and measure the effectiveness of advertising campaigns.

Conditions for Consent

Unambiguous	Clearly explain what people are consenting to in a way they can be easily understood.
Freely given	The individual must have a genuine choice over whether or not to consent to marketing.
Explicit	Consent must be explicit - Implied consent is no longer valid under GDPR.
Informed	Consent needs to be specific and informed. Informing the data subject, at the time they give their consent, must cover the controller’s identity, the purposes of the processing, the processing activities, the right to withdraw consent at any time.
Positive affirmative action	Clear affirmative action means someone must take deliberate and specific action to opt in or agree to the processing.
Unsubscribe	Where an individual has given their consent, it must be as easy for them to withdraw that consent as it was to give it.

Ad Tech

Ad blocking	Technology that allows consumers to block ads whilst browsing the internet.
Ad Choices	AdChoices is a self-regulatory program for digital advertising vendors in USA, Canada and Europe. On a case by case basis it allows you to opt out of receiving advertising based on behavioural targeting.
Ad Exchanges	An ad exchange is a digital marketplace that enables advertisers and publishers to buy and sell advertising space, often through real-time auctions. They're used to sell display, video and mobile ad inventory.
Ad Tech company	Ad Tech companies provide the underlying technologies that help marketers and their agencies create, plan, target, buy, serve, measure and/or optimise ads.
Advertising arbitrage	When an advertising agency buys advertising inventory for one price, packages it up and sells it on to clients for another price, thus making a margin.
ASA	Advertising Standards Authority - the advertising regulator who reviews advertising against their code of practice. In short, is the ad legal, decent, honest and truthful.
Automated guaranteed	A model that enables a programmatic buyer to match an audience with a publisher through device ID or cookie. Price can be fixed in advance, dependent on the correct match being established. Sometimes referred to as programmatic reserved or programmatic guaranteed.
Browser level preferences	Consent derived from settings of the browser.
Certification	Certification is a way of demonstrating that your processing of personal data complies with the GDPR requirements, in line with the accountability principle. When they are available, the ICO will encourage the use of data protection certification mechanisms to enhance transparency and compliance with the GDPR.
CMP	Consent Management Platforms – used by any website that needs to manage the permissions gathered to use cookies for advertising or other means. It allows data subjects to manage their consent preferences in a standardised environment.
CPMs	Cost per thousand impressions – the usual pricing metric used. The more targeted an ad the higher the CPM.

Creative optimisation	Highly automated and rules-driven approach to tailored advertising creative work.
Data aggregation	Data aggregation is the compiling of information from databases with intent to prepare combined datasets for data processing.
Data governance	Data governance is a structured way for organisations to proactively manage data held and processed.
Data management platform (DMP)	The DMP is the technology which allows for the organisation and activation of first and third party audience data into segments to enable better targeting of advertising. Examples include Oracle BlueKai, Mapp Digital, Lotame, Salesforce DMP, Adobe Audience Manager.
Deal ID	A unique string of characters that are used as an identifier for buyers and sellers.
Demand side platforms	Software used by advertisers to buy publisher inventory via a marketplace. This can be used for mobile, search and video ads. The platform facilitates management of advertising across multiple real-time bidding networks.
DPA	Data Protection Authority - DPAs are independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law. In UK this is ICO (Information Commissioners Office).
DPIA	Data Protection Impact Assessment - required in some circumstances under GDPR, to assess the potential risks of processing individuals' personal data.
First party data	Information about the customer directly flowing from the customer to the company. Web browsing, purchase history, spend, product choice, etc.
Horizontal ad networks	A horizontal ad network is a platform for advertisements that don't need a specific audience and covers a wide audience across several industries. It is suitable when wishing to appeal to a global market and can be used for targeting based on demographics.
IAB (Europe)	The Interactive Advertising Bureau is the industry body for digital advertising and has a Europe wide remit. There is also a UK branch. The Transparency and Consent Framework (TCF) initiative is driven by IAB Europe.
IAB Framework	An open-source technical specification management by IAB Tech Lab. It is designed to standardise the transparent collection and transmission of user preferences relating to cookie consent. The IAB have created an approved registry of CMPs and Vendors. Many CMP's (Consent Management Platforms) are embedded in IAB Framework.

IAB Tech Lab	The IAB Technology Laboratory (Tech Lab) is a non-profit consortium that engages a member community globally to develop foundational technology and standards that enable growth and trust in the digital media ecosystem.
Insertion orders	The agreement between publisher and advertiser to run a campaign.
Manual RFPs	Now rare, manual RFPs or requests for proposals, involved human negotiations and manual insertion of orders.
Martech	Martech is the use of technology to achieve marketing goals and objectives. CRM, Analytics, Customer Journey Mapping, DMPs are all part of Martech stack.
Media planning	A service that is usually outsourced to agencies. It involves planning and selecting media to promote brands. The aim is to determine the best combination of media to achieve the marketing objectives.
Mobile ads	Advertising that appears on mobile devices such as smartphones and tablets. Ads are adapted for smaller screens and are usually more concise.
Native ads	Adverts place within the publisher's content to improve relevancy and improve results for advertisers.
Non-auction based approach	Referred to as a preferred deal which makes it possible for publishers to sell their premium media inventory at a fixed price to selected advertisers. This removes the uncertainty of an auction environment.
Open auction	An open auction allows any buyers to openly bid against other buyers for available inventory in real-time targeted against a specified audience. A publisher will allow any buyers to participate in accessing their advertising space through this mechanism. Publishers may exert some control over what adverts they publish by setting a floor price that they know to be too high for some advertisers or by blocking them (through a blocklist) from the auction.
PII	Personally identifiable information. Often referred to as personal data.
Pre-bid decisions	Tools that allow advertisers to evaluate the quality of individual publisher impressions and influence decisioning before bidding. Quality is evaluated largely against viewability, brand safety a nd/or fraud.
Preferred deal	A preferred deal bypasses programmatic auctions altogether. It allows publishers to sell their premium media inventory at a fixed price (or higher dependent on bids) to selected advertisers. The benefit to advertisers is access to more exclusive advertising space and less volatility in pricing.

Price floor	Minimum accepted bid price in a preferred deal, open or private auction.
Private auction	A private, or closed auction allows publishers and buyers to bid in real-time, as in an open auction, but advertisers can only bid if they are invited to by the publisher. The highest bidder will win the advertising space.
Private marketplace (PMP)	Advertisers are selectively invited to participate in a closed marketplace using a “Deal ID” to transact. PMPs give publishers greater control, provide better transparency, can include exclusive inventory and access to publisher first party data and can achieve higher CPMs.
Programmatic Advertising	Programmatic advertising is the method by which digital advertising is delivered to an audience. It is an automated method of media buying where data is leveraged, often in real time, to make decisions on a per impression basis about the target audience, the environment, the price and selection of creative/offer.
Programmatic Buying	The process of executing media buys in an automated fashion through digital platforms such as exchanges, trading desks and demand side platforms (DSPs).
Programmatic direct	An automated process where an advertiser buys advertising space directly from a publisher matched against the advertiser’s own segmentation of data sets.
Programmatic eco-system	Programmatic advertising leverages a technology eco-system to automatically buy and sell targeted online advertising in real-time. The eco-system includes Demand-Side Platforms (DSPs), Supply-Side Platforms (SSPs), Ad Exchanges, Ad Servers and Data Providers.
Programmatic guaranteed	Enables a programmatic buyer to match an audience with a publisher through device ID or cookie. Price can be fixed in advance, dependent on the correct match being established. Sometimes referred to as programmatic reserved or automated guaranteed.
Programmatic premium	Where advertising is sold directly to the publisher. The advertiser chooses in advance premium publisher websites where its adverts will be placed.
Publisher ad serving	Software to manage advertiser creative tags and delivery priority amongst many advertisers.
Retargeting	Allows you to target previous visitors to your site with display ads as they browse the web.

RTB	Real Time Bidding - The use of digital advertising technology to enable agencies and publishers to buy and sell on an impression by impression basis. This will typically involve an auction pricing mechanism.
Second party data	Data owned by one organisation that is sold directly to another, for that organisaations' exclusive use.
Sell side platform (SSP)	A platform for publishers to sell digital advertising to multiple buyers in one environment. It enables Real Time Bidding and other programmatic methods. Examples include OpenX, Rubicon Project, PubMatic, BrightRoll.
Tag management	A tag is a short snippet of javascript (code). In the context of marketing/advertising tags and pixels collect information about the visitor to a website and their behaviour. Tag management is the ability to manage tags (also known as pixels, categories, taxonomies or folksonomies) within collaborative software.
Third party data	Data that has been collected by a third party about your customer and allows you to enhance/grow targeting segments. In context of GDPR, compliantly sourcing this data has become problematic.
Trading desks	Trading Desk is an agency team that executes online media buying. They use either proprietary technology or a demand side platform (DSP) to buy and optimise media campaigns on ad exchanges, ad networks, and other available sources of ad inventory.
Unreserved Fixed Rate	This type of transaction is similar to Automated Guaranteed except that there is not a guarantee that inventory is available to match the criteria specified. It's not an auction either in that the price is agreed in advance.
Vendors	Suppliers of solutions/systems/platforms within the advertising ecosystem.
Verification	3rd party technology intended to measure on target delivery, viewability, brand safety, or fraud. Often, but not necessarily, the same provider of pre-bid and post-bid tools.
Vertical ad networks	A vertical ad network is a platform for delivering to a specialised audience. Examples include food and travel.

Measuring Advertising Performance

Conversion rate	The proportion of website visitors that complete a desired goal (a conversion). A high conversion rate is indicative of successful marketing and web design
CTR	Click-through rate (CTR) is the measurement of individuals who click through on a single advertisement. The higher the click-through rate, the more successful the ad has been in generating interest.
Personalisation	Marketing personalisation is tailoring the marketing of products or services based on their preferences and previous browsing habits.
ROI	Return on investment. Often used to measure the financial return on a campaign
Value exchange	A 'value exchange' between consumer and brand is defined as a balanced exchange of data for better experiences. Deployed well, it facilitates commercial transactions and improved engagement

/ Appendix II – Cookie Information Requirements

#	Requirement
1	Users must see your cookie notice when they **first** visit your service
2	Users must be told about cookies **before** they are dropped
3	**Consent** is required for all but strictly necessary cookies
4	**Strictly necessary** is a tightly defined term (and the ICO does not consider analytic cookies to be strictly necessary)
5	Where consent is required, the **GDPR standard of consent** applies
6	You must be able to **demonstrate** that you have valid consent
7	The user must be able to **withdraw** their consent at any time
8	The consent mechanism presented must not **'nudge'** or influence the user
9	Consent is required, **regardless** of whether the cookie contains personal or non-personal data
10	Users must be provided with information on the **duration** of the cookies
11	Users must be told if **third parties** will have access to the cookies
12	Cookie information must be kept **up to date**
13	'Terms and conditions' cannot be used to gain consent for cookies

Appendix III - Ad Tech Audit Checklist

- Have they appointed a DPO (Data Protection Officer)?
- Is a suitable data governance framework in place?
- Do they hold robust and documented policies and processes to show they handle personal data within the authorised scope granted by the customer?
- Can they demonstrate robust records management?
- Are robust and appropriate security and access arrangements in place?
- Have DPIAs been carried out and logged for any new/high risk projects?
- Have they provided appropriate data and privacy training for employees?
- Do they hold any certification or accreditation relating to the storage of data?
- Do they have clearly defined processes for reporting a data breach? Have any breaches occurred?
- Are clearly defined retention policies in place? Is there evidence of compliance?
- Are non-EU data processing arrangements/agreements in place?
- Are there clear processes for managing the rights of data subjects?
- Have they clearly defined the scope of third-party organisations processing personal data?

Supplementary Ad Tech Data audit

Beyond the standard supplier questions it is important to understand how data in Adtech and RTB especially, is being used by a supplier. These audits extend beyond a standard data protection audit as you will be focusing on the use of personal data within the adtech platforms. The data could be first party data that is being collected from your website, or it could be 3rd party data that is being used to target your advertising:

- Does the supplier have a detailed “Record of Processing Activities” for their processing activities and any other sub processors in the supply chain?
- Can the supplier demonstrate where any data collected from your site is going to be processed?
- Can the supplier identify the sources of any 3rd party data being used to target your advertising?
- Can the supplier clearly demonstrate the legal basis for the processing they are carrying out?
- Can the supplier demonstrate robust consent for the processing of 3rd party personal data?
- Can the supplier demonstrate processes for managing the rights of data subjects?
- Can the supplier identify special category data within their processing?
- Can the supplier provide a full list of the sub processors in the supply chain?

/ Further Reading - ICO Documents and Guidance

We've provided some links to the material which is most relevant to this guidance:

A summary of the ICOs Ad Tech work is kept here:

https://ico.org.uk/about-the-ico/what-we-do/tech-and-innovation/our-work-on-adtech/

Simon McDougall's blog relating to Ad Tech is here:

https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/06/blog-ico-adtech-update-report-published-following-industry-engagement/

Guidance on Accountability and Privacy by Design is here:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/

Guidance on Data Protection Act 2018:

https://ico.org.uk/for-organisations/guide-to-data-protection/introduction-to-data-protection/about-the-dpa-2018/

Guidance on Cookie is here:

https://ico.org.uk/media/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies-1-0.pdf

Special Category data:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd7

Age appropriate design code of practice:

https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/

Guidance on the use of DPIAs (Data Protection Impact Assessments) is here:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/

(https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when6)

Guidance on the responsibilities of Controllers is here:

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/contracts-and-liabilities-between-controllers-and-processors-multi/responsibilities-and-liabilities-for-controllers-using-a-processor/

/ Acknowledgements

This guidance would not have been possible without the contribution of the following organisations and individuals:

Data and Marketing Association (DMA) – co-sponsor and trade body for the data driven marketing community.

https://dma.org.uk/

ISBA – co-sponsor and the only body representing leading UK advertisers.

https://www.isba.org.uk/

DPN (Data Protection Network) – author and privacy publisher of views, analysis, practical resources and supportive guides. Our content (aimed at experts and non-experts) is written, developed and edited by data protection and privacy specialists.

https://dpnetwork.org.uk/

PWC – contributors Fedelma Good and the team from PWC have provided invaluable advice to the project including contributing comprehensive guidance on the use of cookies.

https://www.pwc.co.uk/issues/data-protection.html

AOP (Association of Online Publishers) – contributors AOP are advocates for quality original digital content. It provides research, events and opportunities to discuss and agree key policies for its publisher membership.

https://www.ukaop.org/

Brave – contributors Brave are the private web browser and edge computing ad platform. Brave developed some of the original thinking around the articulation of the privacy challenges facing Ad Tech companies.

https://www.brave.com

IAB (UK) and IAB (Europe) – contributors IAB represents and supports the digital advertising community and have developed a wide range of resources to support the open and transparent evolution of the delivery of digital advertising.

https://iabeurope.eu/

ICO (Information Commissioners Office) – the ICO have produced a wide range of advice and guidance to support marketers and advertisers. The DMA and ISBA are grateful for the opportunity to consult with ICO whilst researching this guidance.

https:www.ico.org.uk

The DMA/ISBA joint digital marketing committee: Catherine Dunkerley (PWC) Charles Ping (Winterberry Group), Chris Combemale (DMA), Clare O'Brien (ISBA), Damon Reeve (Ozone Project), Fedelma Good (PWC), Graeme Adams (BT), Julia Porter (DPN), Mathilde Fiquet (FEDMA), Nina Barakzai (Facebook), Peter Farrell (Unilever), Phil Livingstone (The Body Shop), Phil Smith (ISBA), Stephen Chester (ISBA), Tim Roe (Redeye)

/ About ISBA

ISBA (The Incorporated Society of British Advertisers) is the only body representing leading UK advertisers.

Speaking with one voice on behalf of over 3,000 brands, we champion an advertising environment that is transparent, responsible and accountable; one that can be trusted by the public, by advertisers and by legislators.

Our network of senior marketing professionals works together with ISBA to help members make better decisions for the future.

www.isba.org.uk

/ About the DMA

The Data & Marketing Association (DMA) comprises the DMA, Institute of Data & Marketing (IDM) and DMA Talent.

We seek to guide and inspire industry leaders; to advance careers; and to nurture the next generation of aspiring marketers.

We champion the way things should be done, through a rich fusion of technology, diverse talent, creativity, insight – underpinned by our customer-focussed principles.

We set the standards marketers must meet in order to thrive, representing over 1,000 members drawn from the UK's data and marketing landscape.

By working responsibly, sustainably and creatively, together we will drive the data and marketing industry forward to meet the needs of people today and tomorrow.

www.dma.org.uk

/ Copyright and Disclaimer

Although the greatest care has been taken in the preparation and compilation of this report, no liability or responsibility of any kind (to extent permitted by law), including responsibility for negligence is accepted by the DMA or ISBA, its servants or agents. All information gathered is believed correct at April 2020. All corrections should be sent to the DMA for future editions.