About ID5

ID5 is the first centralised ID synchronisation platform for the ad tech industry.

User IDs are key to the monetisation of audiences and inventories in a programmatic world. ID5 matches user IDs between publishers, data providers and ad tech platforms to enable efficient and privacy-compliant transfer of user-level data along the advertising value chain.

Created in 2017 by seasoned ad tech professionals, ID5 services clients across Europe from offices in London and Paris. For more information about ID5 and cookie synchronisation, please visit: https://www.id5.io/
Introduction

Since the beginning of the “commercial” Internet in the late 1990s, advertising has enabled providers to deliver content and services to consumer for “free”. Internet users enjoy access to premium news outlets, on-demand TV shows, social networking and communication services, unlimited search capabilities, global weather forecasts, booking services, and consumer reviews - all in exchange for their attention and sometimes personal information.

This business model has funded an unprecedented revolution in access to information and services, even sparking more “offline” political revolutions in the Middle East and elsewhere. The advertising industry has been revolutionised as well by digital technologies. Digital advertising originally started as a copycat of offline advertising where brands would reserve real estate on websites to reach users in affinity with the content of these websites. The interactive nature of the Internet and the ability to track individual users' behaviours enabled advertising to evolve into a more data-driven process, where brands would reach individuals based on what they had observed or what they knew of their preferences and intents.

This evolution culminated with the advent of programmatic, a technique based on software enabling impression-level decision making to buy and sell advertising individually and in real-time. Introduced in the mid-2000s, programmatic has quickly taken over display advertising (banners) to represent over 50% of all display ad buys across the main European markets and as much as 75% in countries like the UK and France.
Programmatic solutions rely on several data points to inform a brand’s decision to buy (or a publisher’s decision to sell) an ad impression:

- **Contextual**: is the user on a website or on a page that I want to associate my brand with? Is the ad format impactful? Is it the right time of the day / day of the week to talk about my product or service?

- **Situational**: is the advertiser running a campaign on TV at the same time? Has the temperature dropped below a certain level? Is my product still in stock?

- **User-level** (behavioural and socio-demographic): is the user a client or a prospect? Has she been to my website before? Does she belong to my core target audience?

Programmatic relies heavily on the 3rd category of data: user-level. Advertising has become more about who brands want to reach than about where, when, and how to reach them. User-level data is now the cornerstone for digital advertising.

This reliance on user-level data and the excesses of some digital advertising vendors have sparked a consumer backlash over protection of personal data. Politicians have tackled the subject and the European Union has developed the General Data Protection Regulation (GDPR) which imposes new levels of transparency and acceptance for personal data to be collected and processed for advertising purposes.

Given the importance of user data in the advertising process (and therefore the balance of the digital ecosystem), the GDPR has changed the rules of the game for the entire industry.

In this White Paper, ID5 explores the key success factors of programmatic monetisation for publishers, analyses how the GDPR changes these strategies, and offers recommendations and guidelines to help publishers thrive in this new context.
What are the keys to maximizing programmatic revenue for publishers?

Programmatic advertising relies heavily on user data to make impression-level bidding and valuation decisions. There are two key elements that impact the value of user data, and therefore the value of the ad impressions it informs: **audience qualification** and **audience matching**. Audience qualification refers to the quantity and quality of information about a user that is available to buyers and sellers of programmatic ads. Audience matching refers to the ability for two discrete platforms to effectively communicate who the user is to each other.

As illustrated in the Audience Value Matrix, audiences that are highly qualified and have high match rates with buyers are the most valuable in the ecosystem. On the other hand, low match rates or low qualification de-value audiences and can hurt publishers’ monetization and buyers’ ability to reach their target audience.

**Audience qualification**

Audience qualification criteria are critical to estimate whether a user falls into the target audience of a campaign or PMP (private marketplace) and to estimate the likely outcome of the ad impression (i.e. whether the user will interact with the ad, convert, etc.). This information is key to determining the value of an ad impression and the price buyers are ready to pay for it (or the minimum price sellers are willing to sell it for).
In order to qualify audiences, advertisers and publishers rely on data from several sources. First party data comes directly from users’ input and provides buyers and sellers with direct access to their users’ interests and demographic data. Advertisers, especially those with online retail storefronts, can also use behaviour and intent predictions from their own website to better target a user, attempting to bring them back to their site to complete their purchase. Much like in search, retargeting data is explicitly based on a users’ stated intent (e.g. they browsed a product or added something to their shopping cart), which makes it highly accurate and effective. Another source of 1st party data for buyers is a user’s historical interactions with ads from previous campaigns. An advertiser’s buying platform may leverage this data to predict the likely outcome of a future impression and determine its bid price. Data that can be leveraged includes clicks, conversions, and ad interactions (time in view, hovering on an ad, playing a video, etc.).

First party data is considered highly accurate and valuable because it comes directly from a user and not derived from patterns or extrapolated from a sample of users. It also doesn’t have an explicit price tag since advertisers don’t have to buy it from a third party - which doesn’t mean that it is free, but makes its cost less obvious and its ROI easier to justify.

However, first party data is often limited to a few pieces of information collected by the advertiser or publisher. In order to get a more complete picture of a user, advertisers and publishers can work with other vendors, known as Third Party Data Providers, to collect and aggregate from more sources of data. These companies can analyze the behavioral patterns of a user to predict their interests, intent-to-purchase, and basic demographics (like age or gender).

The longer a user retains his or her browser cookies, the more data advertisers and publishers can aggregate, thus increasing the value of this user. This means that users with “older” cookies are generally more valuable and publishers can earn more revenue for them.

Audience data and data management solutions have become key success factors for publishers, as the more they understand their customers the better they can monetise their ad inventory, personalise their content and find new customers. By organising their own data on user profiles (subscription details, on-site or in-app behaviours) and leveraging external data sources (2nd and quality 3rd party data), publishers are in a unique position to create a 360 degree view of consumers to maximise internal and external value from these insights.

Chris Hogg, Managing Director, EMEA
LOTAME
Programmatic is an ecosystem in which several ad tech platforms need to interact with each other to execute campaigns. If a given user is well qualified by one advertising technology platform, they need to ensure this information can be passed on to other platforms when this user is available to receive an ad for the system to work - in other words, they need to match users with their partners. The value gap between a matched and an unmatched impression can be 2 to 3x, which illustrates the huge impact match rates can have on publishers’ revenues.

To ensure users are always matched between buyers, sellers, and data providers, all platforms would ideally refer to the user with the same pseudonymous user identifier (“UID”). However, due to the way browsers work and how the advertising technology industry grew and developed, this is not the case today. Instead, every platform has its own UID for the same user. In order for these platforms to exchange information about a user, they must synchronise their UIDs with every other platform they work with.

**IN FOCUS - USER SYNC**

All advertising technology platforms operate on their own web domain. To individualise users (for measurement or profiling purposes), they create a unique pseudonymous identifier and store it in a cookie in the user’s browser. This cookie is only accessible to read and write by the web domain that initially wrote it. This means that the same user will have a UID for Platform A (e.g. 123) in a cookie attached to a dsp.com, and another UID (e.g. ABC) for Platform B attached to b ssp.com. For Platform A and Platform B to share information about this user, one or both of them must build a match table that links ID 123 to ID ABC. This process, known by several names (cookie syncing, user syncing, or user matching...), is done by exchanging calls to invisible images (known as “pixels”) to and from the user’s browser, passing one platform’s UID as a variable that the other platform can read, along with their cookie containing their UID, and write to a database with the match.
The current user syncing process is inefficient and not entirely effective, in large part due to its decentralized nature. When talking to SSPs, DMPs, and DSPs, match rates often range from 40 to 70%, with some as low as 20%. This means that a large portion of impressions or audience will not be well monetized, hurting revenue for publishers. Additionally, to even reach these poor match rates seen today, hundreds, or even thousands, of pixels must be dropped for every user in order to map the various platform identifiers with each other. ID5 has conducted dedicated research on this topic and discovered that each web page had to support an average of 35 user sync pixels (68 for News sites) and that this process took an average of 6 seconds (12 seconds for News sites) to complete.

![Measuring the Footprint of User Syncing per Page](image)

More details and findings from the research will be made available on our website (id5.io) in the near future.
How does the GDPR impact programmatic advertising?

Since May 25, 2018, all companies have to comply with the EU’s General Data Protection Regulation (GDPR), which governs collection, storage and usage of data subjects’ personal data.

By principle, the legislation is designed to give data subjects in the EU control over their personal data: how and what data is being collected, stored, used, and most importantly, shared with others. Companies that have poor data-handling practices or that breach the legislation will be heavily fined: up to 4% of annual turnover or 20€ million, whichever is higher. Although the regulation is limited to personal data of data subjects in the EU, it applies to any businesses handling, transmitting, or storing that data, regardless of whether their physical location is in the EU or elsewhere in the world.

Unsurprisingly given the risks, some American companies decided early on to completely close their European branches, with some publishers blocking their websites from any incoming traffic from EU countries, to avoid GDPR and its implications. In January 2018, 4 months before the implementation deadline, 60% of European companies surveyed by Californian tech outfit Senzing said they were “unprepared” for the new regulation, including 24% who considered themselves to be “at risk”.

The GDPR was not specifically designed with digital advertising in mind. Several requirements from the GDPR were even already considered “best practices” by digital advertising regulatory bodies and implemented by many ad tech companies (ability to “opt-out”, restricted processing for sensitive data, etc.) However, the GDPR has introduced new topics that dramatically impact the industry:

1. **Pseudonymisation**

   The GDPR creates the new category of “pseudonymous data”, which covers some information that was previously considered to be “Non Personally Identifiable Information” (NPII). Under the GDPR, anonymous identifiers such as unique alpha-numerical codes stored in cookies (“user IDs”), fall under this category because they may lead to re-identification of an individual if combined with additional data points (such as post code, gender, date of birth, etc.) NPII wasn’t covered by privacy regulation, but pseudonymised data is, causing data-driven advertising to fall under the GDPR.

2. **Purpose & legal ground**

   Under the GDPR, data controllers must have a legal ground to collect and process personal data for a given purpose. These two dimensions (legal ground and purpose) are pivotal to the GDPR and force publishers, marketers, and ad tech vendors to clearly define the purpose (or purposes) for which they collect and process data, and to justify their reasons for doing so. The main legal grounds applicable to digital advertising are explicit consent (users freely and explicitly consenting to their data being used for advertising) and legitimate interest of the controller (a “softer” justification balancing interest of the controller versus interest of the data subject).

3. **Co-responsibility**

   The third element of the GDPR which profoundly impacts digital advertising is the notion of co-responsibility. By default, all parties involved in the data collection and processing chain are responsible in case of a security breach or misuse of that data. Given the nature of digital advertising in general, and programmatic in particular, and the fact that it involves multiple stakeholders (publishers, advertisers, and various ad tech vendors in between), co-responsibility is a huge challenge for the industry that has led to several parties strong-arming their “partners” to take the blame in case of problem.

The following practices that have been conducted by publishers, marketers, and ad tech vendors to “optimise” placement of digital ads, now require new levels of transparency and acceptance under the GDPR:

- **User profiling** - collecting behavioural data on a user for the purpose of estimating his or her characteristics, preferences, or intents
- **User targeting** (including retargeting) - using personal (user-level) data to display a personalised advertising message
- **Cookie matching** - because user identifiers are considered personal data, sharing that information between ad tech platforms is a process that must be disclosed under the GDPR
These practices are not forbidden by the GDPR, but those who engage in them need to provide transparency to users about them, and provide users with the means to accept or refuse them. In some cases, data controllers responsible for these processes do not have a direct relationship with users, which makes these constraints more difficult to respect.

In order to help the industry achieve the level of transparency and control required by the law, IAB Europe has supervised the definition of a standard to collect, encrypt, and share information related to the right for each stakeholder to process data for a given purpose. The IAB’s proposed “Transparency & Consent Framework” is a way to standardise communication of purposes and vendors involved in personal data collection and processing, and to share their ability (or inability) to do so along the value chain, in order to operate programmatic advertising campaigns at scale under these new obligations. More information about this framework is available at www.advertisingconsent.eu.

While the GDPR could make it seem impossible for traditional programmatic advertising to continue as it has, there are ways for publishers to make the most of the opportunity the GDPR presents by re-evaluating strategies and partnerships.
How can publishers maximise their programmatic revenue under the GDPR?

The first opportunity is for publishers to combine access and context to maximise audience qualification capabilities. Secondly, publishers need to protect their audience by ensuring there is no “backdoor” access to it. And finally, they must increase their match rates to maximise audience monetisation capabilities.

Improve first party audience qualification

Publishers are uniquely positioned to qualify audiences. Their direct relationship with users enables them to collect personal data through subscription mechanisms (email address, socio-demographic characteristics, household income, etc.) in a GDPR compliant way. Because they have this direct access to users, publishers can completely control the experience, including the consent collection process, and ensure awareness of usage and reasons to use personal data. Publishers’ rich context and high frequency of contact with users provide unparalleled abilities to understand users’ preferences, interest, and intent, which can prove invaluable for marketers eager to understand their client’s path to purchase. They also allow for extension of audiences by applying look-alike modelling algorithms to very granular behavioural data.

Thanks to a preferred relationship with consumers and a rich context to analyse their behaviour, publishers can create multi-dimensional profiles enabling them to accurately identify marketers’ target audiences, engage with them, and deliver efficient messaging to support brands’ marketing goals. Publishers can accomplish this by creating PMPs with their buyers. Publishers, who are more likely to receive consent for the collection and analysis of users’ data than ad tech platforms, can provide buyers with the insights they need while still maintaining the efficiencies and benefits that programmatic advertising offers.
It is estimated that programmatic direct and private marketplaces will amount to 80% of the total programmatic transaction volume in 2019. The impact the GDPR will have on these estimates is still unknown, but with buyers and sellers needing to better control the value-chain, it’s possible the industry will move even more towards these channels.

Publishers are well-suited to leverage their data in a GDPR-compliant way to enable buyers to reach their goals without the need for their own data (and therefore, buyers’ own consent across several Purposes).

Close back-doors to their audience and protect against data leakage

Most publishers suffer from data leakage, but very few do something about it. Sharing and insights tools, bid listeners, 3rd party tracking solutions, and cookie matching are some of the many holes in publishers’ ships through which valuable audience data leaks to the outside world, diminishing the uniqueness of that information and therefore its value.

With the GDPR making user-level data more scarce and therefore more valuable, pressure on publishers’ audience data will increase. Publishers need to hold their ground and demand transparency when considering integrating a new technology solution on their site or opening access to their inventory to a new buyer. Best practices on this topic can be found at most large walled gardens where ad tech vendors need to be certified (and in some cases need to adapt their data management practices) to be allowed to run tags on the sites. For publishers who can’t command this type of practice, ongoing analyses using services like Evidon or The Media Trust provide much needed visibility on vendors getting in touch with their audiences through indirect channels.

Audience data are publishers’ most valuable assets, but they don’t maximise yield from these assets because they rely on third parties to monetise for them, or because they don’t protect them well enough. Publishers need to rely on credible, open, and data-protective tech platforms to really regain control of their destiny and make sure their core assets are protected. We see publishers being very successful by creating “private gardens” and finding the right balance between a healthy scarcity of inventory; best-in-class user experiences; a focus on quality over quantity; and a respect for user privacy.

Michael Nevins, Chief Marketing Officer
Smart
Control ID matching to maximise audience monetisation opportunities

Advertising technology platforms operate on different web domains. For that reason, they need to match UIDs with each other to be able to share the user-level information that fuels programmatic advertising.

The quality of this matching process has a direct impact on a publisher’s ability to monetise audiences and inventories. Sell-side platforms and DMPs usually present match rates in the 40-70% range, leaving at least 30% of inventory and audiences under-monetised. Based on a conservative 2x uplift in eCPMs for matched users, publishers have the potential to significantly increase their programmatic revenue if user matching is improved.

By controlling and monitoring user matching more closely, publishers can leverage it in sales negotiations with buyers. Raising the user matching priority to certain buyers can guarantee better access to a publisher’s inventory, which is very valuable for most marketers. Publishers can bundle this with higher CPMs or larger annual spend commitments.

While publishers are often not directly involved in the user syncing process\(^6\), their website hosts the entire process and their revenues are directly impacted by its effectiveness. Therefore, publishers should demand transparency and control of the process from their partners to ensure their users are not impacted negatively and they can monetize as many impressions as possible.

While publishers are often not directly involved in the user syncing process, their website hosts the entire process and their revenues are directly impacted by its effectiveness.
Below, ID5 illustrates how publishers can take steps to understand the impact user syncing has on their site and better control the process with their partners.

**Types of Match Rates**
Make sure you understand the difference between user match rates and impression match rates. Impressions with matched users are most important when it comes to monetization.

**Apply Uplift to Match Rates**
Once you know your match rates with various buyers and the uplift from a cookieed users, you can calculate your opportunity cost of unmatched users across your supply.

**Ask for Avg. Match Rates per Buyer**
Ask your ad server and SSPs to provide you with average match rates per DSP on your inventory.

**Calculate Uplift of Matched Users**
Run your own analysis, or ask your partners, to compare the average monetization for users with a known UID compared to those that don’t.

**Control Who Syncs on Your Website**
Work with your ad server and SSPs to prevent unknown platforms from user syncing on your site.
Conclusion

The GDPR presents new challenges to the programmatic advertising ecosystem, but given their long-standing relationships with consumers, publishers are in a favourable position to take advantage of these disruptive times. Transparency about data being collected and for what purpose, and control over these processes, are key elements of the regulations. They will also be key arguments for the development of a trust-based relationship between publishers and their consumers going forward.

To make the most of this opportunity, publishers need to invest in audience qualification. By organising their content as a way to understand consumer preferences, they can provide marketers with much needed insights into consumer journey and path to purchase. Because data is more difficult to access, it is also more valuable. Publishers must therefore protect this increasingly valuable asset and ensure appropriate levels of protection against data leakage, closing all “back doors” to their audiences and inventory. Finally, after maximising the value of their assets and ensuring that they retain all of it for themselves, publishers need to maximise access to their audience data for preferred buyers, by ensuring that it is well matched with buyers’ platforms.

Following these recommendations will ensure that publishers maximise their revenue from programmatic advertising and benefit from the GDPR disruption to thrive as preferred partners for brands and marketers.
APPENDIX 1: Sources and Footnotes

1. Through conversations with publishers and sell-side platforms, ID5 estimates that publisher revenues increase 2 - 3x when a user is properly matched between platforms.

2. Match Rates definition: the percentage of one platform’s users identifiers that can be mapped to another platform’s user identifier.

3. On May 25, several websites including the Los Angeles Times and the Chicago Tribune, were unavailable to EU-based users (the company have used IP location services to determine traffic origin).


6. Publishers aren’t generally responsible for calling DMPs or DSPs directly, instead they put ad server or SSP tags on their page. These tags give platforms access to their own cookies and user identifiers and the ad server or SSP must match user ids with DMPs and DSPs during the auction process.