Data protection and adtech in Europe: where next?

Julia Kaufmann, Partner, and Joanna de Fonseka, Senior Associate, with Baker & McKenzie,
discuss the impact of recent developments in adtech for industry, advertisers and publishers

A lot has happened in the world of data protection and adtech recently. At EU level, the Court of Justice of the European Union ('CJEU') issued its decision in the *Planet49* case in October 2019 (Case C-673/17), confirming that consent for cookies cannot be obtained via a pre-ticked checkbox. The CJEU also confirmed in that case that a valid consent for cookies requires, among other things, prior information on the storage period of the cookie and whether third parties have access to the cookies. A number of EU Supervisory Authorities ('SAs') have also issued guidance on how to use cookies and similar technology in compliance with European data protection law. Additionally, we are starting to see first enforcement actions by SAs in this field.

This article discusses the impact of these recent developments for the adtech industry, as well as for advertisers and publishers.

What is adtech?

'Adtech' refers to technologies used for online targeted advertising, meaning personalised advertisements on websites or mobile apps which are specifically selected for a particular user, based on their characteristics or interests. Most internet users will be familiar with seeing personalised advertisements appear on the websites and apps they visit, but much less aware of the complex process behind the scenes that enables this to happen.

There are a number of different permutations of the basic business model, but one of the most common (and one that has attracted particular attention) is 'real-time bidding' ('RTB'). In RTB, while a website is loading, the website operator (the 'publisher') auctions the available advertising space on its website for advertisers (i.e. brands) to purchase. Typically, the advertiser does not purchase the ad space directly from the publisher, but does so through a series of intermediary providers of adtech services, which might include demand-side platforms ('DSPs') on the advertiser side, supply-side platforms ('SSPs') on the publisher side, and ad exchanges.

The RTB process itself typically relies on the use of cookies or similar technologies (such as pixels, plugins or device fingerprinting) to track the user when they visit a website or app. This then triggers a real-time bid request containing information about that user, which is typically sent, via an SSP, to an ad exchange and to hundreds of DSPs, thereby allowing advertisers to assess and bid on the request, based on the types of users they want to reach. The winning bidder's ad is then placed on the website or app by the advertiser's ad server, which also tracks its performance. In practice, the process is highly complex and is underpinned by a sophisticated technical ecosystem, often involving hundreds of different parties. The bidding process is also entirely automated, and typically happens in milliseconds.

Adtech has many advantages. It allows advertisers to reach a new audience with their advertisements and publishers to increase the revenue by selling website advertising space to the highest bidding company. However, the industry also faces a multitude of privacy issues, not least because of the complexity of the underlying ecosystem and the numerous actors involved.

How does data protection law apply to adtech?

From a data protection law perspective, there are two distinct but overlapping regimes to consider.

Firstly, the EU Privacy and Electronic Communications Directive 2002 ('e-Privacy Directive', which contains rules on the use of cookies and similar technologies) and the Member State laws that implement it need to be considered, because adtech typically relies on the use of cookies, pixels and other tracking technologies to collect information about the user. It is important to note here that the e-Privacy Directive is technology-neutral, meaning it applies not only to cookies, but also to any technology used to store or access information in a similar way. In addition, the e-Privacy Directive's scope is not limited to personal data, but instead applies to any use of tracking technologies to collect information from a user's

device, regardless of whether that information is personal data or not.

Furthermore, because online targeted advertising almost always involves processing personal data, the GDPR is also relevant, both in relation to the initial collection of the data, and any subsequent processing of that data by the various actors involved.

Cookies and adtech

Requirements for non-essential cookies: notice and consent — The usage of cookies is governed by Article 5 (3) of the e-Privacy Directive under which it is only permitted to store or gain access to information stored on the terminal equipment of a user, where the user concerned: (i) has given their consent; and (ii) has been provided with clear and comprehensive information, including information about the purpose of the processing. As such, the placing of a cookie on a user's device, or using other technology to gain access to information stored on the user's device, usually requires consent under the e-Privacy Directive. There is an exception for cookies which are essential to provide a service requested by the user, but cookies used for the purposes of targeted advertising will not normally be considered essential.

The EU Member States were required to transpose Article 5 (3) of the e-Privacy Directive into national law. The UK, for example, implemented Article 5 (3) of the e-Privacy Directive through Regulation 6 of the Privacy and Electronic Communications Regulations 2003 ('PECR'). The current rules on cookies under the e-Privacy Directive were originally intended to be replaced by a new e-Privacy Regulation in May 2018, alongside the GDPR. However, nearly two years on, the e-Privacy Regulation is still not finalised, so the local laws implementing the e-Privacy Directive remain applicable for the time being.

The delays to the e-Privacy Regulation initially led to considerable uncertainty regarding the interplay between the e-Privacy Directive and the GDPR, in particular in relation to the standard of consent required to set cookies. However, more recently, a number of EU SAs, such as the Data Protection Commission in Ireland and the CNIL in France, have issued fresh guidance on cookies to help clarify the situation, and it is now fairly clear that SAs will expect cookie consents to meet the GDPR standard. That is, the consent must be freely given, specific, informed, unambiguous, and confirmed by a statement or positive action (and a pre-ticked box or equivalent, such as a slider defaulted to 'on', will not suffice). Although the UK is technically no longer an EU Member State, the UK Information Commissioner's Office ('ICO') also issued new guidance on cookies in July 2019 in which it took a similar position. The ICO and the CNIL have also confirmed that implied consent formulations such as 'by continuing to use our website you agree to our use of cookies' will not constitute valid consent — which is broadly in line with the position taken by the CJEU in its *Planet49* decision.

> ***"The GDPR transparency and consent requirements (and current interpretations of those requirements from courts and SAs) therefore raise numerous practical difficulties, not least because the number of advertising companies involved in the adtech ecosystem can easily run into the hundreds."***

Uncertainty in Germany: what are the cookie rules? — Unusually among Member States, in Germany, Article 5 (3) has not been explicitly implemented into national law, as German lawmakers took the view that the existing provisions of Sections 12, 13 (1) and 15 German Telemedia Act already sufficiently reflected the cookie requirements under the e-Privacy Directive. The German SAs, however, have been demanding a national implementing law for Article 5 (3) of the e-Privacy Directive for years. In their view, the rules of the German Telemedia Act are insufficient to implement the cookie requirements under the e-Privacy Directive.

In light of the GDPR, the German SAs have stated publicly that the German Telemedia Act, to the extent it relates to data protection, shall no longer apply as of 25th May 2018 due to Article 95 of the GDPR. Consequently, the German SAs currently apply only the general GDPR requirements for data processing activities involving cookies, and no additional cookie-specific rules.

Interestingly, despite the pronouncements of the German SAs, the German Supreme Court still appears to consider the German Telemedia Act good law in relation to data protection, and applied certain data protection-related provisions of the German Telemedia Act in a recent decision in September 2019. However, this decision was concerned with the provisions of the Telemedia Act relating to the disclosure of personal data for the purposes of establishing and exercising legal claims, rather than the provisions on cookies. Therefore the position on cookies in Germany remains unclear.

Where does the GDPR fit in?

As stated above, the use of cookies in the adtech context generally involves processing of personal data. The data shared by the website operator with the various advertising companies through the RTB process can result in very detailed profiles being created about the users concerned. These profiles consist of data collected by the website operator or by third parties through cookies and similar technologies, and might include data such as IP address, type of device, country,

(Continued on page 12)

(Continued from page 11)

websites visited and search queries on search engines. Taking the broad definition of personal data under the GDPR into account, this information will qualify as personal data. As such, the initial collection of personal data through the use of cookies, the sharing of those data with the advertising companies, and the further processing by those companies as part of the adtech ecosystem, is subject to the GDPR's requirements, in addition to the e-Privacy requirements discussed above.

Legal basis for processing

A number of SAs have recently confirmed that consent will generally be the most appropriate legal basis for processing in the adtech context.

For example, the German SAs take the view that processing activities relating to tracking pixels for advertising purposes require consent; in their view, legitimate interests does not work, because the user has an overriding legitimate interest against such tracking. Furthermore, the SA in Baden-Württemberg has confirmed that website operators using cookies relating to advertising networks require consent.

In the UK, the ICO has taken a similar position, and has stated in its recent report on adtech and RTB (copy at www.pdpjournals.com/docs/888050) that consent will generally be the appropriate legal basis in this context, for both the initial placing of the cookie and for any subsequent processing performed by the various actors within the ecosystem. The ICO also observed in its report that there is currently a general lack of clarity and understanding in the industry around what the correct lawful basis for processing should be, as at present many companies offering adtech services or engaging with adtech providers rely on legitimate interests for processing, rather than consent. Like the German SAs, however, the ICO considers that legitimate interests will generally not be appropriate in the RTB context in view of the intrusiveness of the processing and the fact that most individuals are unlikely to expect it.

Given the high standard of consent set by the GDPR, the SAs' position on legal basis creates considerable practical challenges for the industry. We explore these further below.

What does 'good' consent look like?

Firstly, as stated above, an active indication of consent (opt-in) is required, as confirmed by the European Court of Justice in the recent *Planet49* decision. Opt-out consent solutions, or solutions which rely on the user's silence or inactivity, such as pre-ticked boxes in a cookie banner or statements that the user confirms their agreement 'by continuing to use our website', will not be sufficient. The opt-in consent must also be obtained before any processing activities are commenced, i.e., before any non-essential cookies are placed on the user's device and before data about the user are collected and shared with the various third parties in the ecosystem, i.e. before the RTBF process starts.

Secondly, the consent text must provide sufficient detail on the processing activities to which the user is asked to consent, including details of any third party recipients of the data. The *Planet49* decision confirms that the consent text must not only specify the controller and the processing purposes but also the recipients or categories of recipients (to address the GDPR requirement of fairness), and how long the cookies are in operation.

With respect to the recipients, the Article 29 Working Party stated in its guidelines on transparency (WP 260, now adopted by the European Data Protection Board) that the recipients should be identified by name, rather than referring merely to categories of recipients. Again, this is fundamentally about the principles of fairness as well as transparency, and is intended to ensure that data subjects know exactly who has their personal data. Further, the Article 29 Working Party stated in its guidelines on consent (WP 259) that all recipients receiving the data as controller and relying on the consent must be identified by name in the consent text.

In the UK, the ICO has indicated that it shares this view, and that this interpretation of the requirements (i.e. that the recipients of the data should be individually named) applies equally in the adtech context. When these transparency and consent requirements are applied in the adtech sector, the consent text would need to mention: (i) the identity of the website operator as initial controller; (ii) the categories of personal data to be collected and shared in the adtech ecosystem; (iii) the purpose of the processing (for example, analysing the data, matching it with other datasets or sharing with third parties to serve targeted ads); (iv) the lifespan of the cookies used; and (v) each of the advertising companies as a recipient of the personal data.

The GDPR transparency and consent requirements (and current interpretations of those requirements from courts and SAs) therefore raise numerous practical difficulties, not least because the number of advertising companies involved in the adtech ecosystem can easily run into the hundreds. Following a strict interpretation of the requirements, such detailed information on (potential) recipients, together with the other information required, would likely entail an extremely lengthy consent text, which in practice most users are unlikely to read or understand. Paradoxically, this may ultimately result in a lack of transparency and in a lack of sufficiently 'informed' consent from the users, as well as being detrimental to the user experience. One possible solution might be a 'layered approach' providing users with consent language in a banner or pop-up that summarises the aspects (i) to (v) above with links to a second layer setting out the required information in more detail. However, formal guidance from the SAs on this issue is currently very limited, and so it is by no means certain that this approach would be considered satisfactory.

Finally, consent must be freely given. This means users must have a genuine choice and must have the freedom to refuse consent; in addition, the user must be able to withdraw consent in the future. Website operators and other players will also need to respect the user's choices, and not

place cookies on the user's devices or present tailored advertising to the user if the user has not given their consent. 'Cookie walls' (which require users to 'agree' or 'accept' the setting of cookies before they can access an online service's content) are also unlikely to represent a compliant approach, because the user is effectively forced to accept the cookies in order to access the service.

Impact for advertisers, publishers and adtech providers

A number of SAs, most notably the ICO, have expressed concerns about the current level of data protection compliance in the adtech industry. In its June 2019 report on adtech and RTB, the ICO stated that organisations involved in the RTB ecosystem should adjust their current data protection practices and in particular will need 'to re-evaluate their approach to privacy notices, use of personal data and the lawful bases they apply'. More recently, the ICO has also stated that organisations that have not addressed the issues identified in its report risk being in breach of data protection laws, and has expressed disappointment that while there has been a positive response from some parts of the industry, other organisations 'have their heads firmly in the sand' and are 'ignoring our message'. Furthermore, the ICO has warned that it is prepared to use its wider powers if organisations do not engage with its recommendations, which could include enforcement action.

At the time of writing, neither the ICO, nor any EU SA, has issued formal guidance for the adtech industry specifically. However, the ICO's June 2019 report and subsequent pronouncements are still a useful measure for the compliance challenges, and ultimately serve as a warning to the entire industry subject to EU or UK data protection law. As such, there are a number of actions that those involved in the industry should consider taking now:

- cookie audits — organisations should review both first-party and third-party cookies that they currently use. This will be an essential first step in ensuring that privacy and cookie notices are sufficiently transparent and that cookie consents are genuinely informed;
- contracts — all organisations involved in sharing or receiving data within the adtech ecosystem will need to ensure their contracts contain appropriate data protection clauses. Contracts will need to clearly define the roles of the parties (as controller, processor or joint controller) and set out the parties' respective responsibilities, in particular with regard to notice and consent requirements;
- review current consent mechanisms — current cookie consent mechanisms should be reviewed, and if necessary updated, to align with the legal requirements under the GDPR and e-Privacy Directive, and with SAs expectations. In practice, this is likely to require a collective effort from advertisers, publishers, and the wider adtech industry, as well as action from organisations on an individual level;
- review legal basis for processing, both for initial placing of cookies and other subsequent processing activities such as profiling, third party sharing, data augmentation and targeting;
- review privacy and cookie notices to ensure they accurately describe which cookies are used, what data is collected, how that data is processed, and who it is shared with; and
- undertake due diligence on data received from third parties. In particular, it will be important to ensure that data subjects have been provided with appropriate notices and that consents obtained are sufficient to cover the proposed processing.

Outlook

There is no question that the adtech industry is currently in the regulatory spotlight when it comes to privacy compliance, as illustrated by the ICO's recent report on adtech and RTB and its subsequent pronouncements.

The industry is also attracting scrutiny from a number of other SAs around the EU. As such, data protection compliance is increasingly seen as a key risk area for the adtech industry and, given the maximum fines that can be levied under the GDPR, this is a risk the industry will need to take seriously. However, as we have seen, data protection requirements (particularly around transparency and consent) can be challenging to comply with in practice, largely because of the sheer number of actors involved.

Where does this leave adtech? While it is still relatively early days, one possibility is that advertisers may begin to move to other models, such as contextual advertising, which carry a lower privacy risk. Long-term, we might also start to see the industry consolidating so that there are fewer actors in the data supply chain, which would go some way towards mitigating the data protection risks (though it would not eliminate the risk entirely, and a change on this scale is likely to take time). In the meantime, the adtech industry will need to reconsider its current approach to data protection compliance and in particular the requirements on transparency and consent discussed above.

Julia Kaufmann
Baker & McKenzie
julia.kaufmann@bakermckenzie.com