

## AdTech and Data Protection – A Collision?

The Information Commissioner's Office (ICO) has confirmed that it has resumed investigating the Adtech Sector and warns all UK media companies involved in this sector that many are breaking the law. Considering this, ClearComm advises that organisations should urgently review how they use personal data.

Simon McDougall, ICO Deputy Commissioner, said:

In May 2020, we paused our investigation into real-time bidding (RTB) and the AdTech industry, as we prioritised activities responding to the COVID-19 pandemic. We have now resumed our investigation.

"Enabling transparency and protecting vulnerable citizens are priorities for the ICO. The complex systems can use people's sensitive personal data to serve adverts and requires people's explicit consent, which is not happening right now.

"Sharing people's data with potentially hundreds of companies, without adequately assessing and addressing the risk of these counterparties, also raises questions around the security and retention of this data.

"The investigation is vast and complex, and, because of the sensitivity of the work, there will be times where it won't be possible to provide regular updates. "All organisations operating in the AdTech space should be assessing how they use personal data as a matter of urgency.

### AdTech and Data Protection – Overview

When a website owner/operator sells AdSpace on their website for targeted online advertising, the website owner/operator shares the personal data processed for the above purposes, with online advertising companies. There is a lack of sufficient understanding between the requirements set out in the Privacy Electronic Communications Regulations ('PECR') and other applicable data protection laws in the AdTech industry.

PECR regulates the privacy in electronic communications, imposing precise rules on cookies and related technologies on an end user's device. In most cases, using cookies and associated technologies involves processing personal data, meaning that both the GDPR (among other legislation) and PECR rules will simultaneously apply:

#### 1. Lawful basis for processing personal data

Personal data is processed by a real-time bidding participant (the auction process that occurs in real-time to sell visual advertising to digital channels), a lawful basis as required by Article 6 of the GDPR. Therefore, due to the nature of the processing, consent of the end-user is the only lawful basis that can be relied on to process personal data for the real-time bidding auction process. Additionally, the lawful basis relied on personal data processing in connecting with auxiliary activities within the real-time

bidding process, (e.g. Advertising), so also needs to be carefully considered. Moreover, those engaged in real-time bidding processing also need to comply with consent rules of granularity and the PECR rules which require consent for using advertising cookies.

To put this in practice, real-time bidding participants should document the lawful basis used, and ensure that consent is used is: granular, freely given, specific, and unambiguous.

#### 2. Special Categories of Personal Data (Article 9 GDPR)

For any processing of special categories of personal data (e.g., health information, political and religious beliefs), GDPR requires that explicit consent be sought from the end-user. Since real-time bidding processes sometimes involve processing personal data, after a series of investigations the Information Commissioner's Office found after a series of investigations, that the consent requests did not meet the GDPR's standards for explicit, freely-given, unambiguous consent.

To ensure that the standards are met, the real-time bidding participants should first: identify whether special categories of personal data are to be processed concerning real-time bidding activities and then consider whether the processing is necessary for the

activity's scope. Ensure that explicit consent is obtained from the end-users. Consent must also be recorded as this falls under a Data Controller's accountability requirements.

### 3. Transparency

One of the data protection principles is transparency. This is about the processing of personal data. Transparency is a difficult topic for real-time bidding participants, mainly due to the complex processing involved, including automated processing for various purposes, including targeting and analysis. Besides, PECR requires clear and comprehensive information to be provided using cookies and similar technologies.

In practice, real-time bidding organisations should make sure that their Privacy Policies and Notices are up to date and that they reflect what the processing involves. Moreover, auditing the use of cookies should ensure that the Notices and the Banners are accurate, and identify the purpose and duration of the cookies used.

### 4. Identify and block intrusive and unfair processing

During the real-time bidding process, the collection of data creates a profile of an end-user. Therefore, this may constitute unfair and intrusive processing if the quantity and nature of the personal data being processed depart from the initial purpose of the processing, which is delivering targeted advertising.

To identify and block this unfair and intrusive processing, the real-time bidding participants should carry out a Data Protection Impact Assessment to determine whether the purposes match and the security and regulatory risks posed to such processing.

### 5. Establishing the correct title and responsibility

There are no set criteria to decide the Data Controller and Data Processor in the digital advertising business. It is impossible to say that the supply-side platforms are Data Controllers always or sometimes Data Processors. In some cases, there is no substitute for a factual, case by case analysis, to designate the Data Controller/Data Processor role. However, there are a few patterns that can be drawn out to help with this analysis:

- a. The website owner/operator is a Data Controller, as it is the one selling AdSpace on its website for targeted online advertising.
- b. The advertising organisation is also a Data Controller, as it is deciding to bid to serve ad impressions on the website owner/operator's website.
- c. Ad networks are usually Data Controllers. This can be inferred from Online Behavioural Advertising Opinion 2/2010 (of the Article 29 Working Party), highlighting that when behavioural advertising entails processing personal data, ad network providers also play a Data Controller role.
- d. The data management platforms that collate the incoming data from multiple sources to support targeted advertising are usually Data Processors.
- e. The consent management platforms enable website owners/operators to manage their user consents. The Consent Management Platforms process personal data on behalf of the Data Controller. Therefore, they will be Data Processors.
- f. The providers of website analytics services and products are also defined as Data Processors.

**Delivering global Data Privacy, Information and Cyber Security solutions.**

#### CONTACT US

Call: **+44 (0) 20 7566 4000**  
Email: **info@clearcomm.org**