

# Adtech and transparency: an area of focus for regulators

---

**Joanne Vengadesan, Partner, and Michael Ridge, Associate, Penningtons Manches LLP, perform a whistle-stop tour of the recent action of Supervisory Authorities in respect of data processing practices in the adtech industry**

---

**W**hilst online targeted advertising has been around for almost as long as the internet itself, its scale and sophistication has exploded in recent years. This growth has been driven by the ever larger and richer pools of personal data being processed either directly by vendors or on their behalf by third party marketing agencies, data brokerage firms and data aggregators.

In the push to better understand their customers, businesses are processing more data than ever before, from browser and purchasing histories, to demographic information such as age, race, sex, estimated income level, employment status and level of education, to details of an individual's lifestyle and interests.

There has been much commentary in recent years regarding the tension in the space where adtech meets data protection rules. Consumers are now used to seeing highly personalised, real-time advertisements on a range of platforms, including online, via mobiles and through so-called 'smart' TVs, and through personalised or profiling-based digital marketing. However, it is less clear whether they have a genuine understanding of the volume of their data being processed to enable these interactions, or the number of businesses in the supply chain with whom those data are shared, or the type of profiling that might be being applied to them.

Adtech businesses still have work to do to build consumer understanding of and trust in this developing sector and bake-in a 'privacy by design' approach. Recent events have highlighted the cost to businesses of getting things wrong in this area.

Armed with increased powers and potential sanctions under the General Data Protection Regulation ('GDPR'), regulators across the EU are taking an increasing interest in the data processing practices in the adtech industry, with a particular focus on promoting transparency for consumers. A number of European regulators have been active in this area in recent months, including the UK Information Commissioner's Office ('ICO'), the French data protection regulator ('CNIL') and Poland's Personal Data Protection Office ('UODO'), as well as

the European Commission. We consider a few of these developments and their implications below.

## France: Enforcement action

In January 2019, the CNIL fined Google €50m for breaches of GDPR in how it collects and processes personal data in order to serve its personalised adverts. Google's breaches fell into two categories: breaches of the transparency requirements arising from deficiencies in Google's privacy notices; and failure to establish a valid legal basis for processing individuals' personal data for the purposes of ad personalisation.

Interestingly, although the necessary information regarding the data being processed, the purposes for processing, storage periods etc. was provided in Google's privacy notices, the CNIL criticised Google for disseminating the information across multiple documents, requiring users to have to take 'up to 5 or 6 actions' to access all of the information.

The information was also found to be neither sufficiently 'clear nor comprehensible', as it was not possible for users to fully understand the extent of Google's processing activities (in particular, the number of Google applications and services that were involved in sharing and exploiting users' data — some twenty in all).

Given these transparency failings, the CNIL held that Google could not rely on individuals' consent as a valid basis for processing, as the consent was not sufficiently informed. Moreover, Google's attempt to rely on a single action by a user as constituting consent to all of Google's processing activities (that rely on consent) was also found to be invalid. As consumers were unable to give a granular consent, specifying which of Google's processing activities they were consenting to, the consent was insufficiently 'specific' or 'unambiguous'. Google was also criticised for the use of pre-ticked boxes.

The case reiterates the importance of providing privacy notices that genuine-

*(Continued on page 12)*

[\(Continued from page 11\)](#)

ly explain to users, in granular detail, how and why their data are used, especially when seeking to rely on consent as the basis for processing. It is also a reminder of the need to obtain a separate consent for each processing activity, rather than simply bundling all consents into a single tick box without giving data subjects the ability to decide to which activities they wish to consent.

## UK: Consultation

Adtech is increasingly on the ICO's radar. In March 2019, the regulator held an adtech fact finding forum, focusing on programmatic advertising and real-time bidding. The topics being examined by the ICO touch on many of the same issues highlighted by the Google case: how can genuine transparency be achieved in such a complex advertising system, and what is the most appropriate legal basis for processing.

The ICO highlighted the inconsistency between the legal bases relied upon by different organisations in the adtech ecosystem.

What form the ICO's next steps will take is not yet clear, but what is clear is that it does not regard the status quo for targeted advertising as being fully compliant. Further regulatory action is likely in the coming months.

## Poland: Enforcement action

In March 2019, Poland's regulator, the UODO, issued its first penalty under the GDPR, fining an information brokering company PLN 943,000 (approximately €220,000) for breaches of the information requirements under Articles 14(1) and (2) of the GDPR.

The company processed the data of several million sole traders, but only fulfilled its information obligations to notify data subjects under Article 14 where it held the individuals' email address in its records. It placed a privacy notice on its website, but claimed that sending out the required information by post where no email address was held would involve a

'disproportionate effort' per Article 14(5)(b). The UODO rejected these arguments, making clear that the financial burden of compliance was not sufficient (on its own) to permit the company not to comply with Article 14, in particular where the collation and brokering of data was a core part of the company's business.

The decision has caused controversy in some circles and is subject to appeal. However, in light of this decision, organisations should consider carefully what steps they are taking to comply with their information obligations under Article 14, especially where they have not obtained the information directly from the data subject. This is an often-forgotten or dismissed requirement. It is not likely to be sufficient simply to place a privacy notice on your website, if the data subjects involved would have no reason to look there or to expect you to be processing their data in the first place. Organisations should also be able to show more than simply a financial burden if asserting that meeting their information requirements would involve 'disproportionate effort'.

## European Commission: New guidance on AI

In April 2019, the European Commission issued new ethics guidelines on building trustworthy artificial intelligence. These guidelines aim to promote the development of AI within an ethical and lawful framework to ensure the development of robust AI that has public confidence.

Although not a legal document, the guidance is a useful indicator of the Commission's approach to this fast-emerging area. The guidance promotes the development of fair and transparent AI systems that can provide those directly and indirectly affected by its decisions with a readily-understandable explanation. As would be expected, the guidelines accord with the existing rules in the GDPR on profiling and other forms of automated decision-making. They also emphasise the importance of ensuring the accountability of AI systems through enabling systems to be audited and individuals to be able to obtain redress where unjust adverse impacts occur.

## Key points:

All the above underline that with tightening rules is coming increased regulator scrutiny and oversight in the adtech space.

To achieve genuine transparency, information about the categories of data being processed, the purposes for processing, storage periods etc. should be presented in a clear and readily-understandable form, and should not be disseminated across multiple documents requiring data subjects to take several steps to access the information.

The correct legal basis to rely on for processing personal data in the adtech ecosystem is coming under increased scrutiny. Organisations should ensure they are relying on the most appropriate basis in their specific circumstances.

Transparency should be specifically addressed when using AI technologies and profiling, particularly where this could impact the nature of marketing directed at an individual. If marketing consents are being collected, it is important to be transparent within the consent collection process, to ensure that consents are sufficiently informed to meet the GDPR standard.

Remember the obligations under Article 14 to inform data subjects about the nature and purposes of the processing etc., especially if the information has not been collected directly from the data subject.

If collecting consents, ensure that the consents are stored in a manner capable of verification (including as to time and date that the consent was given and the specific language in response to which the consent was given).

---

**Joanne Vengadesan and  
Michael Ridge**

Penningtons Manches LLP

joanne.vengadesan

@penningtons.co.uk

michael.ridge@penningtons.co.uk

---