DATA PROTECTION, ADTECH INDUSTRY AND DIGITAL ADVERTISING: THE CHALLENGES TO COME.

Gemserv

3

In 2018 and 2019, Data Protection Authorities in Europe have launched different initiatives around digital advertising with far-reaching consequences for all organisations, especially the AdTech industry.

From the focus by the Commission Nationale de l'Informatique et des Libertés (CNIL) and the UK Information Commissioner Office (ICO) on Real-Time Bidding and AdTech to the new rules around collection of consent for cookies and other tracking technologies, the recent changes should be a wake-up call for many advertisers and publishers in the EU. The massive fines issued against Google in France, Facebook in the U.S., and the investigations on Facebook and Quantcast by the Irish Data Protection Commission confirm the shift of landscape for targeted advertising activities.

In this paper we aim at presenting and summarising the practical changes for the AdTech industry and, more generally, any organisation using digital advertising. Any organisation involved in digital advertising is accountable for the online targeting solution they use. Today, most organisations have some form of digital advertising activities and work, to some extent, with advertisers. Very few organisations are able to conduct their own digital advertising campaigns from A to Z.

4 COOKIES AND OTHER TRACKING TECHNOLOGIES

In the past months, many Data Protection Authorities have issued updated guidance on cookies, other tracking technologies, and consent collection, especially the UK ICO,[1] the French CNIL,[2] the Irish Data Protection Commission (DPC)[3] and the German Conference of the Data Protection Authorities (DSK).[4]

While these different documents converge on many points, it is also noticeable that the Data Protection Authorities diverge in some places.

The most important point is that it is now widely stated that GDPR standard consent is applicable to online tracking technologies, and that legitimate business interest is not a lawful legal basis for tracking and profiling users online.

In short, a compliant cookie banner must fulfil the following conditions:

- No pre-ticked boxes except for strictly necessary processing
- Purposes must be separated and explicit (necessary, website preferences, audience measurement, advertising...)
- A link to the cookies policy must be provided
- The list of third parties used for audience measurement and advertising purposes must be provided

In this regard, it is important to note that:

- You cannot rely on implied consent for the use of cookies, you need express opt-in as per General Data Protection Regulation (GDPR) standards.
- Analytics cookies cannot be considered as strictly necessary and you must seek consent for such cookies as well.
- You cannot use a cookie wall to restrict access to your site until users' consent.
- You cannot rely on legitimate interests to set cookies, consent is always required for non-essential cookies, such as those used for the purposes of marketing and advertising.

Consent must be freely given, specific, informed, unambiguous, by a statement or by a clear affirmative action, opt-out is simply not acceptable. A bundled or global consent box is not considered as consent. Emphasising the consent option over the decline option would be deemed as influencing users towards consent. This would be the same if the option to decline consent were located in a second layer with the option to agree were in the first layer.

However, some interesting discrepancies arise when it comes to analytic cookies or cookie walls. For the CNIL and the DSK, using analytics cookies is permitted on the basis of legitimate interest when no data is transferred to third parties to be matched with additional data sets. For the ICO, their usage requires consent, although the ICO explained that a breach would unlikely result in a formal enforcement action. However, in both cases, it must be noted that these statements do not give a blank cheque to use the analytics solutions provided by Google and Facebook, since these services will inevitably match the data collected with their own sources.

Another interesting disparity is regarding cookie walls. For the CNIL and the DSK, they are strictly prohibited, where the ICO provides that if an acceptable alternative to tracking is offered to the data subject – such as a paid subscription – cookie walls could be considered acceptable. This will certainly delight the Washington Post website!

Finally, the positions issued by the different Data Protection Authorities are not only applicable to cookies, but to any technology that stores or accesses information on the user's device. This is aligned with the last ePrivacy Regulation draft, and includes, but is not limited to:

- Pixel beacons
- Tracking scripts
- Tags
- Software development kits in mobile applications
- Unique identifiers (UIDs)
- Local objects
- Browser fingerprinting technologies

Any website publisher must determine how their cookie banner will collect consent from their visitors, meaning that they are responsible for this technical solution. There is no doubt that many websites are yet to be compliant with these rules.

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

2. https://www.cnil.fr/fr/cookies-et-autres-traceurs-la-cnil-publie-de-nouvelles-lignes-directrices

3. https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190612%20Guidance%20on%20Cookies%20and%20Similar%20Technologies.pdf

4. https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

5 THE DATA PROTECTION AUTHORITIES FOCUS ON ADTECH

It is important to note that both the ICO and the CNIL have stated they will start enforcing their new positions early 2020.

On 20th June 2019, the ICO published their updated report into AdTech and real time bidding,[5] with findings affecting the whole online advertising industry. The ICO focused specifically on the processing of special categories of data, and the widespread data sharing across the AdTech sector. They are currently investigating the industry and online advertisers are strongly encouraged to review their practices in light of this report.

Simon McDougall, ICO, said: '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 AdTech 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.'[6]

In a later interview with the Financial Times on 29th August, Mr McDougall said the ICO had been 'unsatisfied' by the answers offered by the AdTech industry before it issued its warning in June. 'We're digging and digging, [and] we're still not happy' for the reason that the industry has so far given 'vague, immature and short answers'. Especially, 'What we're seeing is a blind reliance on contracts and no real attempt to assess whether the counterparty you're using is likely to have controls in place around security, retention. That's just not how the rest of the world works'.[7]

The French Data Protection Authority (CNIL) adopted a similar action plan[8] for 2019-2020 on 28th June 2019, making investigating online targeting practices in the industry a priority.

This does not only target ad brokers and advertisers, but also any publisher (i.e. website editor) relying on such providers. A website editor (publisher) determines the means and purposes of the processing for the personal data of users visiting their website, and it will be considered as a controller under the data protection legislation.

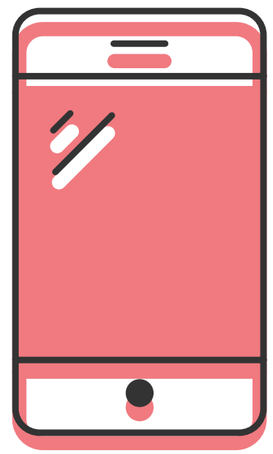
A publisher is not only responsible for designing a compliant cookie banner, but also to select a compliant advertising provider for their targeted advertising. There is no doubt that the AdTech industry will face increasing questioning of their practices from their clients in the next months.

5. https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf

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

7. https://www.ft.com/content/ff7af558-c5b8-11e9-a8e9-296ca66511c9

8. https://www.cnil.fr/fr/ciblage-publicitaire-en-ligne-quel-plan-daction-de-la-cnil



6 A STRICT ENFORCEMENT IN PLACE AND TO COME

Many spectacular enforcement actions happened in the past months and it is interesting to focus on the few of them relating to digital advertising.

One of the most noticeable was Google France being fined €50 million in January 2019 on behalf of Google U.S. by the CNIL for its data protection practices. Several lessons can be drawn from this case:

- There was a breach of transparency and of the right to information: the information provided by Google about the purposes, the retention periods, and the categories of data used for personalised advertising were scattered amongst many privacy notices, through hidden links and buttons to activate to get complementary information, with sometimes the relevant information only accessible after 5 or 6 steps.
- There was a lack of legal basis due to Google's uncompliant consent mechanisms: the consent provided to personalised advertising by Google's users could not be considered specific and unambiguous, since it was not sufficiently informed and moreover enabled by default.
- Finally, and most interestingly, Google Ireland was not considered a proper representative for GDPR purposes as it did not have any decision making power on the determination of the collection, purposes, and legal basis for Google products. In a serious blow to U.S. tech giants' forum shopping for more relaxed jurisdictions in Europe, the CNIL held that nearly all European Supervisory Authorities have jurisdiction over Google U.S.

Let's also not forget that Facebook had been fined £500,000 by the ICO in October 2018 over the Cambridge Analytica scandal (the previous maximum amount possible under the Data Protection Directive) for the misuse and permissiveness over its users' personal data.

But the most striking example on Facebook is the $5 billion fine pronounced by the Federal Trade Commission (FTC) in the U.S., for the following reasons:

- Facebook violated previous order requirements
- Facebook repeatedly used deceptive disclosures and settings to undermine users' privacy preferences
- Facebook had unsatisfactory overview of third-party apps and data disclosure.

However, many experts have countered that the new privacy settings and structure imposed to Facebook by the FTC are only cosmetic and would comfort Facebook in its current business model. Ultimately, the FTC ruling had been pronounced on the basis of unfair practices with consumers, and not on data ethics and privacy perspectives, which is making such critic arguable. However, many investigations opened against Google, Apple, Facebook, Amazon and Microsoft (GAFAM) by competition regulators in Europe focus on anti-competitive practices, rather than data protection. This approach seems to be equally effective, as we have seen a number of significant decisions taken by the European Commission, the Italy or German competition authorities in the past years.

In parallel, the Irish DPC is currently investigating Google[9] and Quantcast [10] on their digital advertising practices, to find out:

- Whether the processing of personal data carried out by Google at each stage of an advertising transaction is compliant with GDPR transparency, data minimisation, and data retention standards
- Whether Quantcast's processing and aggregating of personal data for the purposes of profiling and utilising the profiles generated for targeted advertising is compliant with GDPR transparency and data retention standards

Another valuable lesson can be learnt from the CNIL Vectaury case in October 2018, named after a small French online advertising agency. The ruling was critical for all actors involved in digital advertising, including publishers: data brokers cannot rely solely on contractual arrangements to demonstrate that they have lawful consent from end users, and must be able to demonstrate the reality of the existence of such consent. In summary:

- Contractual provisions are not enough to demonstrate consent
- Writing in a contract that publishers must collect proper consent is not sufficient, advertising providers can still be challenged to prove they have compliant and proper consent from the publishers
- Publishers must be able to demonstrate to their advertising providers that they have collected proper consent from their visitors and customers

All these various cases are preparing the ground for the future investigations and massive fines to be expected in 2020 in Europe. Data Protection Authorities have been very clear on the next steps of their enforcement actions.

9. https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-google-ireland-limited

10. https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-opens-statutory-inquiry-quantcast

7 THE CONSEQUENCES FOR THE ADTECH INDUSTRY

While there is an undeniable shift in the landscape for the AdTech industry, the silence from the industry is absolutely compelling. Most of the large companies are based in the U.S., meaning they do not seem to take the issue seriously. However, interestingly, a Federal Data Protection law in the U.S. could be expected in the next few years, but to which extent American AdTech companies (SMEs and Big Tech Companies alike - GAFAM) are ready for a regulation remains unanswered. It would be interesting to monitor the developments after the California Consumer Privacy Act comes into effect in 2020. Over time, there may a be convergence.

While it is undoubtedly necessary to put an end to the misuse of personal data in the AdTech sector, the new rules are leading to a poor consent rate from cookie banners. This will mean tracking becoming ineffective to profile users and serve targeted advertising. However, one question has been left out the current debate about the way to keep the digital economy mostly free without digital advertising. Beyond this complex question, is it even realistic to have the whole AdTech industry compliant in six months' time when all tracking technologies, even the stealthiest ones, are in scope?

There are mixed reactions across the industry with certain actors challenging the law whilst others are waiting. This problem seems to be compounded by the fact that a number of suppliers are based in U.S. where the privacy regime is rather different. The IAB Europe has just upgraded their consent framework and there is an expectation that this will address a number of the concerns raised by ICO. A further update towards the end of the year may encourage further action. Some inconsistencies across Data Protection Authorities in Europe regarding their cookie guidance is not encouraging a fast response. It is also worth noting that there are a significant number of AdTech organisations who do not scrutinise the regulations or who might believe this does not affect them.

Little by little, it seems that there is a necessity for the AdTech industry to switch to other business models, supposing such flexibility is possible. Could we imagine a shift from targeted advertising to contextual advertising, with scripts not profiling users' behaviour anymore, but adapting the ads served to the content of the pages visited? The ICO and the CNIL have, to an extent, acted unilaterally and ahead of the ePrivacy regulation draft, meaning there may be future changes in the guidance they have issued.

Finally, this new regulatory landscape seems to have a counter-productive impact by encouraging economic concentration in the AdTech industry. Indeed, the new rules would mostly be beneficial to the GAFAM since they could be the only actors robust enough to survive a complete change of business model with thorough obligations to comply with around collecting and demonstrating proper consent. Getting an accreditation could become an important asset which might be too costly for some players. Some consolidation in the industry can be expected, with bigger tech companies pivoting their business models. Programmatic as a means of delivering advertising is not going to disappear but the way it is deployed may change.

SAMUEL PLANTIÉ PHD, CIPP/E,
PRINCIPAL DATA PROTECTION CONSULTANT

JULIA PORTER,
SENIOR ASSOCIATE, OPT-4 DATA PROTECTION CONSULTANCY

LONDON OFFICE

8 Fenchurch Place

London, EC3M 4AJ

Telephone: +44 (0)20 7090 1091

bd@gemserv.com

IRELAND OFFICE

Fitzwilliam Hall Business Centre

Fitzwilliam Place, Dublin 2

Telephone: +353 (0) 1 669 4630

bd@gemserv.com

DATA PROTECTION WORLD FORUM

PRIVACY | TRUST | RISK | SECURITY

Telephone: +44 (0)345 319 4377

info@dataprotectionworldforum.com

Gemserv

INVESTORS IN PEOPLE | Gold Until 2020

bsi. ISO/IEC 27001 Information Security Management

GlobalGROUP ISO 14001 UKAS MANAGEMENT SYSTEMS 0039

LLOYD'S REGISTER LRQA ISO 9001 UKAS MANAGEMENT SYSTEMS 001

CYBER ESSENTIALS PLUS