**WORLD MEDIA GROUP – THE IMPLICATIONS OF GDPR FOR THE ADVERTISING INDUSTRY**

This month's World Media Group Breakfast Briefing – Everything You Need to Know about GDPR - was one of our best-ever attended sessions. It seems that with just over eight months to go until GDPR comes into practice, advertisers, agencies and publishers alike are realising that there is not much time to get their houses in order. There is still a lack of clarity around the directive and its implications are both broad and complicated – but it is going to be part of all our lives.

GDPR is a legal directive relating to anyone using or processing personal data so its reach and implications extend across many industries. The aim of the report below is to provide a review of the advice and thinking covered on the day regarding the implications of GDPR that are most pertinent to *advertising practitioners.* This is not a legal report and is intended for guidance only, if you are in anyway responsible for personal data for your company or any other, we advise taking proper legal counsel.

Key take outs below cover:

- Who will the new law apply to?
- Why have GDPR rules changed?
- GDPR overview
- What is the definition of a Data Controller versus a Data Processor and why do we need to know this?
- Contracts and paperwork
- Consent can be king.....
- .....but legitimate business interests are better
- Targeting
- Retargeting and frequency capping
- Analytics
- The GDPR opportunity

**What does GDPR stand for?** General Data Protection Regulation which will come into force on 25th May 2018.

**Who will the new law apply to?** While it applies to organisations who operate within the EU, it also applies to operations outside the EU that offer goods and services to EU citizens. The UK government has already indicated that, post-Brexit, GDPR rules will still apply within Great Britain.

**Why have GDPR rules changed?**

The first data privacy laws came in almost 30 years ago when the technology we take for granted today didn't exist – no mobile phones, no social media, no biometrics etc. Advancements in technology move so fast that the law tends to have to play catch up. Hence why we are now seeing a long overdue overhaul in data privacy to reflect the reality of how we collect personal information, how we use it and also the behaviour of consumers today.

However difficult it is going to be for advertising practitioners to get compliant, there is no denying that the reasons behind the changes makes sense. As Sue Elms, Co-Founder at BE Insight, commented, "If what I heard today is correct, GDPR will rein in the data and digital targeting practices of agencies; and thankfully curb the communications pollution that has been choking off consumer receptivity to advertising."

**GDPR overview**

While it's worth looking in detail at the Information Commissioner's Office website for their detailed documents on the GDPR, here is a summary of some of the key changes advertising practitioners need to know about:

*Consent:* GDPR requires 'unambiguous consent' if consent is the lawful basis you are relying on. This means that pre-ticked boxes, opt-out boxes or default settings as a means for collecting data will no longer be allowed – consumers will need to proactively affirm that they are giving their consent to their data being processed.

*Transparency:* It is imperative that organisations are very clear with consumers about why they are collecting data, who will use it, how it will be used etc. E.g. Privacy notices on websites will need to be changed to include information such as what third party organisations it will be shared with.

*Defined roles:* Contracts will need to be made clearer to define processes and responsibilities around data so that every part of the supply chain that 'touches' data understands their role as seen within GDPR. In particular, are they a 'Controller' or 'Processor'.

**What is the definition of a Data Controller versus a Data Processor and why do we need to know this?**

Under current data privacy laws, only Controllers are liable. However, GDPR means that both parties now become liable under the law. Controllers and Processors are therefore both open to regulatory fines if there are breaches of GDPR laws – and these can be huge: for each party the maximum fines are up to 4% of annual worldwide turnover or €20m, whichever is greater, plus the potential for damages claims from data subjects.

Hence it is vitally important to understand the definitions of each role. A Controller is someone who '*alone or with others determines the purposes and means of processing personal data'*. The Processor is the entity that '*processes data on behalf of the Controller*'.

While there will be some crossovers, for the most part, this means that the roles of advertisers, agencies and media owners are as follows:

*Clients* = Controllers

*Agencies* = Processors

*Media owner* = Both Controllers and Processors as they manage and process their data for their own communications, but also on behalf of their advertisers.

**Contracts and paperwork**

Whereas under current laws Processors are just required to have adequate security measures in place under their contracts with Controllers, there will be many more stringent requirements they must adhere to PLUS they must only act on the written instruction of the Controller. Controllers and Processors therefore need to work together within clearly prescribed contracts that make roles and allowable processes clear.

Controllers need to consider what data they and their processors hold, why they hold it, where it is being held, who is using it, how it is being used etc and have paperwork in place that makes this unambiguous. In asking these questions, it will then be possible to document everything and find the holes in the business that need to be plugged in order to be GDPR compliant.

Similarly, when Processors are asked to process data they should be able to check that Controllers have *their* compliance processes in place that gives them the right to do that.

Industry bodies such as the IPA and ISBA are in discussions to try and create industry standards for contractual clauses. This should help both parties in defining their roles and creating contracts that are fit for GDPR.

**Consent can be king.....**

There are a number of lawful grounds for processing personal information under GDPR, including: to fulfil a legal obligation, if you have clear, unambiguous consent from the data subject or if it is necessary for the purposes of your legitimate interests (provided those are not overridden by the interests of the individual).

To get consent, advertisers will need to provide individuals with a clear picture of why they are collecting the data, how it will be used and who will use it.

When asking for consent, it is worth marketers thinking of their WIFM strategy – what's in it for me – offering some kind of value exchange that provides real benefit to the individual in return. Indeed, some organisations, such as Lloyds Bank, are using the shift to GDPR compliance as a valuable reason to ask consumers about what they want. This enables the rejigging of marketing strategy to ensure that communications all offer relevance and value. The positive for advertising practitioners here is that by being GDPR compliant they will build greater trust with their customers – who are likely to spend more with them as a result.

**.....but legitimate business interests are better**

As consent can be withdrawn by the data subject at any time – at which point you have to stop processing their personal data – marketers should also look at the other lawful grounds for processing personal data if the circumstances allow.

Ann Silla, Senior Counsel at the Economist Group, suggested, "In particular, it's worth understanding whether processing is necessary for the purposes of an organisation's 'legitimate interests' (which don't override the interests or fundamental rights and freedoms of the data subject) – although this is a balancing act that needs to be assessed carefully."

A legitimate interest may involve an online retailer collecting and maintaining someone's name and address so that they can send them the item they have ordered. Similarly, if you need to email customers to tell them about a new customer service phone number then that may be a legitimate interest. However, you could also argue that an email to inform a regular customer about a new product section on your website is a legitimate business interest. Indeed, the new act says that direct marketing *may* be a legitimate business interest. As with anything to do the law, unless you are 100% clear, it's best to check with lawyers to get their point of view.

It is worth noting that there are some types of personal data processing where you *have* to have consent. For media practitioners, this particularly relates to the fact that data subjects have the right not to have a decision made about them solely through automated processing, including profiling, unless they give their explicit consent.

**Targeting**

Under GDPR, third party data is predicted to be less available and less rich compared to what is available now as a result of the need for explicit consent. As a result, DMPs and new technologies called CDPs (customer data platforms) will develop interesting new roles as they start to onboard data, which not only will activate digital marketing activity, but also help manage consent and the way customer data is removed.

David Pandit, Digital and Data Analytics Leader at Appraise, explained, "Overall, companies are likely to shift to more 'upper funnel' activity (content targeting) but decrease 'lower funnel' activity (behavioural targeting), especially as in the short-term advertisers will not be able to target user segments."

**Retargeting and frequency capping**

Retargeting campaigns use individual device IDs or cookies to track and reach relevant individuals. Under GDPR there will be a requirement for consent to be given by the data subject to any third party wanting to carry out retargeting campaigns. This could have huge implications which are likely to much diminish retargeting's within digital advertising. Interestingly, the inability to track people across various platforms also has implications for sequential and frequency capping, which could be detrimental to consumers who may see an ad far more often than before.

**Analytics**

Companies will have to start analysing anonymous data rather than PII or pseudonymous data (data that can be linked to other data to unlock a personal profile). This means that attribution models are predicted to be treated with care as they are likely to be "freakishly wrong" in the short term. As a result it will be necessary to do resampling and identify other ways to improve analytics going forward e.g. experimental design.

**The GDPR opportunity**

GDPR needs to be seen as more of an opportunity than a challenge. There will undoubtedly be losers as a result of the regulations becoming law, but for the industry as a whole it is a good thing. Data should be better quality which should lead to greater ROI for advertisers – potentially leading to bigger budgets going to premium publishers in particular. Overall, it should create better, deeper, more respectful relationships for both advertisers and publishers with their consumers. Essentially, any industry player with a focus on best practice is likely to benefit from GDPR in the end, even if it means hard work right now.

Indeed, for many it has the potential to create a favourable business position. Deborah Dillon, EU GDPR Executive Consultant at ATOS, said, "GDPR can be seen as adding a competitive advantage in that it encourages organisations to be transparent with the customer and also allows for effective digital transformation by making sure that personal information is accurate, available and has the correct security controls in place for the future."

What is clear is that organisations need to start putting their house in order *now,* identifying the changes that need to be made and creating a roadmap of how to get to compliance by May 2018.

Jon Chase, Chair of the Media Agencies Council at EACA, added, “All of the major media agency groups have appointed experienced data specialists to lead their strategic preparations. This includes reviewing and implementing the required changes within their internal data and analytics divisions, right through to ensuring the appropriate contractual clauses and checking procedures are in place with all external businesses from whom they access data.”

Emma Winchurch-Beale, International Sales Director at The Washington Post and President of the World Media Group (WMG), concluded, “At the World Media Group we felt it was important to take the initiative to provide insights on the impact and implications that the new GDPR regulations will have on current business models. There is clearly going to be a need to change and evolve, but WMG members are well placed, as first party data and contextual advertising will become increasing important. Due to further demand, we will be hosting a follow up session in Q1 ahead of the 25th May launch date.”

**Thanks go to the panellists at this World Media Group Breakfast Briefing** (from left to right):

- Sue Elms: Co-Founder at BE Insight
- Deborah Dillon: EU GDPR Executive Consultant at ATOS
- Jon Chase: Chair of the Media Agencies Council at EACA
- Ann Silla: Senior Counsel at the Economist Group
- Richard Lindsay: Director of Legal and Public Affairs at IPA
- David Pandit: Digital and Data Analytics Leader at Appraise