Contents

[6] What's in store for global marketers over the next 24 months?

Growing importance of data ethics in global digital marketing

The storm clouds gathering over many social media sites and app developers worldwide as well as brand owners that traditionally followed a strategy of 'big data' is now a matter of concern.

Simple, adapt to survive, there's no doubt that GDPR is going to shake up the digital marketing landscape. Therefore it is important for businesses to ensure they have implemented the changes necessary to comply. With the possibility of a slow-down in the progression of marketeers must ensure their business is ready to adapt and shift in order to tackle this. Don't just accept it, do what you can in order to drive business development and sales. Plan ahead. The troubles facing Facebook and Google[1] post-GDPR are just the tip of the iceberg when it comes to privacy under threat on a global basis.

[1]Google hit with €4.3bn Android fine from EU https://www.bbc.co.uk/news/technology-44858238

It's now time to re-boot marketing thinking in light of the legal challenge against 'surveillance capitalism' as well as the higher standards now expected from brand owners, post-GDPR.

And what's more, marketeers knew this was coming appearing and coming down the line.

The lack of awareness regarding peer-dependent privacy is one way that London-based Cambridge Analytica Ltd. was able to collect the personal information of more than 71 million Facebook users, even though only 270,000 of them agreed to take the now-bankrupt company's app-based personality quiz.

"Cambridge Analytica reportedly knew what it was doing[2], but any company that accesses customer data, such as contacts, call logs, and files, can unknowingly breach peer privacy. Blame apps. Virtually all large companies offer apps to their customers, and most of those apps access and collect customer data[3]. Often, that includes peer data, which also is collected even though the app's owner may have no direct relationship with the user's peers," say the authors of this article that recently appeared in MIT Sloan Management Review.[4]

Regulator enforcement actions over the next 12 months

The drive for enforcement of data privacy principles must be a key factor for governments and supervisory authorities. The UK's ICO is making it clear to businesses it will not tolerate non-compliance and marketing is a prime target. As part of their investigations to political manipulation through 'marketing' the ICO served its first enforcement notice since the GDPR came into force on 25 May 2018. The notice was served on AggregateIQ Services Ltd, an online behavioural advertising service provider, which is based outside the EU in Canada. The notice is in connection with online political messages sent to UK citizens during the Brexit campaigns by Aggregate IQ.

[2] https://www.wired.com/story/whistleblowers-on-cambridge-analytica-and-the-question-of-big-data/

[3] https://www.nytimes.com/2017/05/03/technology/personaltech/how-to-protect-your-privacy-as-more-apps-harvest-your-data.html

[4] Your Customers May Be The Weakest Link In Your Privacy Defenses by Kolah, A; Kamleitner, B; Mitchell, V and Stephen, A (2018), MIT Sloan Management Review https://sloanreview.mit.edu/article/your-customers-may-be-the-weakest-link-in-your-data-privacy-defenses/

The enforcement notice requires Aggregate IQ to "*cease processing any personal data of UK or EU citizens obtained from UK political organisations or otherwise, for the purposes of data analytics, political campaigning or any other advertising purposes*".

New rules on claims management cold calls

New rules entered into force from 8 September 2018, by way of amendments to PECR under Section 35 of the Financial Guidance and Claims Act. These rules require that marketing calls by claims management services can now only be made with the prior opt-in consent of the recipient. These rules also apply where the calls made relate to advice, financial services, representation of people or making introductions or inquiries.

Holding individual directors to account

Regulations amended PECR and give the ICO increased powers to impose direct fines of up to £500,000 on rogue individual directors. Directors will be personally liable for PECR breaches relating to the use of automated calling systems and unsolicited direct marketing where they have consented to or connived in the breach or the breach is attributable to their neglect. The Regulations came into force on 17 December 2018.

The ICO will monitor the number of complaints it receives about marketing by a particular organisation, to gauge the level of action. A single badly managed campaign resulting, for example, in a number of complaints from recipients, could be enough to trigger investigation by the ICO. Another factor likely to lead to ICO action is an organisation's failure to take appropriate remedial steps as directed by the ICO.

Investigations will be thorough and penetrating.

There will be no getting away with anything, marketers can expect to be asked to answer detailed questions on and provide evidence for the source of the marketing data they use, the lawful basis for the marketing e.g. LIA's, the total numbers of different marketing communications sent or made to individuals over the course of the past year, as well as about the number of opt-outs and complaints received and how these where handled. Further questions are likely to focus on the policies, procedures and training within the company.

Leave UK fined £135,000 in Feb 2019.

More than 1 million emails were sent to Leave.eu subscribers contained marketing material raising concerns with the ICO regarding personal sensitive data being gathered for political purposes. The ICO are investigating how personal data was processed as well as staff training. The directors will also be investigated, along with senior managers and the Data Protection Officer.

Use of alternative legislation for custodial sentences

Many marketing companies will be aware the GDPR, DPA18 and PECR do not have custodial options for the courts to pursue. This thought should have changed recently following the sentencing of an individual. A motor industry employee has been sentenced to six months in prison in the first prosecution to be brought by the Information Commissioner's Office (ICO) under legislation which carries a potential prison sentence.

Mustafa Kasim, who worked for accident repair firm Nationwide Accident Repair Services (NARS), accessed thousands of customer records containing personal data without permission, using his colleagues' log-in details to access a software system that estimates the cost of vehicle repairs, known as Audatex.

People who think it's worth their while to obtain and disclose personal data without permission should think again.

Impacts of regulatory actions

Marketers who face impending investigations or financial penalties from the ICO will find trading in the future difficult as customers will tend to migrate to competitors who, may have suitable data protection systems or just have not been highlighted yet. Cambridge Analytic (CA) will be remembered in history as the example of when marketing gets it wrong. As soon as the ICO published their requests for information, CA's customers began to turn away, contracts cancelled or terminated mid research. The main data brokers removed their services and the company was left high and dry.

The large press coverage and political involvement also drove clients away and following the removal of all company assets by the ICO, the company had no way of contacting anyone – basically a dead company. What this demonstrates is that when the ICO investigates a company the damage

is enormous. But ask yourself, has CA been fined for a breach of data protection? – no, the only fines have been for LeaveUK whilst AggregateIQ received a 'stop processing' notice.

Loss of new customers

Marketing companies who have a fine imposed on them will find it very difficult to attract customers as all the company's details will be posted on the ICO's website, which would be the first calling point for any prospective client. Again this was a key factor for Cambridge Analytic whose customers left in droves.

Loss of existing clients

As CA proves, clients will distance themselves as soon as they become aware of any potential regulator involvement, clients will also ask the company to remove data from servers. Marketing companies must be very careful in completing this request as it would give the ICO additional investigatory requirements e.g. why did you delete the data? Fortunately for CA they did not allow a potential new client to send data from the US to CA servers, as this data was gained from facebook and breached facebooks privacy code.

Marketers and Brexit

The UK government indicated it will permit data to flow from the UK to EEA (European Economic Area) countries, the legislative binding for this will be section 17A of the DPA18 but organisations that have data flows from the EEA to the UK will be affected.

The EU (Withdrawal) Act 2018 (EUWA) retains the GDPR in UK law (identified as the UKGDPR). The fundamental principles, obligations and rights that organisations and data subjects have become familiar with will stay the same. To ensure the UK data protection framework continues to operate effectively when the UK is no longer an EU Member State the Government will make appropriate changes to the GDPR and the DPA18 using regulation-making powers under the EUWA.

As a result, the ICO recently issued a statement to recommend standard contractual clauses for all transfers of personal data to any country outside the EEA, (specifically section 17A of the DPA18). Organisations that rely on binding corporate rules will receive further information from the ICO in due course.

The new regulations and detailed guidance will:

- Place the EUGDPR in local law, this will be known as the UKGDPR;
- Confirm that the UK will transitionally recognise all EEA countries (including EU Member States) and Gibraltar as 'adequate' to allow data flows from the UK to Europe to continue;

- Preserve the effect of existing EU adequacy decisions, including the EU-US Privacy Shield, on a transitional basis;
- Preserve EU standard contractual clauses and binding corporate rules authorised before Exit Day;
- Maintain the extraterritorial scope of the UK data protection framework; and
- Require non-UK controllers that are subject to the UK data protection framework to appoint a representative in the UK if they are processing UK data on a large scale.

Marketers that do not have the UK as their lead supervisory authority to review the structure of their EU operations and assess whether they will continue to be able to have a lead authority and benefit from the one-stop-shop mechanism. Marketers will have to deal with both the ICO and the supervisory authority in the other EEA state where they are established, according to the ICO. Marketers must consider **now** which other EU and EEA supervisory authority will become lead authority on Exit date (if any) and approach them closer to the exit date.

ENDS