The changing landscape for digital marketers

Author: Steve Wilkson

Not a day goes by where there's a news headline about brand owners not doing what they should to protect the rights, freedoms and interests of their customers, clients, supporters and employees. And what we're witnessing right now is the impact EUGDPR is having across the globe. Whilst EUGDPR was conceived within the EU, it can be said that many countries around the world have been looking at their own data protection, privacy and security laws specifically following the Facebook/Cambridge Analytica scandal. Such international reviews will cause specific hot topic for marketers working on an international and country specific basis.

Many commentators have described the EUGDPR as the biggest shake up in data protection, privacy and security standards for over two decades. In many respects, the UKGDPR and the DPA18 is an evolution of best practices gained from Europe.

The consequence for marketers is that they must re-boot their thinking by putting the rights, freedoms and interests of their customers and clients at the centre of their thinking. The UKGDPR places a higher global standard on data protection, privacy and security for the digital age. There's now a higher degree of transparency and accountability required by brand owners in respect top the way in which they process personal data and that control over this data must be replaced into the hands of customers and clients. This series of articles will address 6 hot topics around UKGDPR that are causing most interest amongst marketers., the article has also been written with the view of the implementation of the United Kingdom General Data Protection Regulation (UKGDPR) which will come into force on Brexit.

Article 1:

Re-wiring the contractual and legal relationship between the Data Controller and the Data Processor in the Value Chain

In the past, outsourcing could be strategic or tactical, such as IT or payroll processing. However, over time, it's become much more a strategic issue, not simply one based on cost savings.

Under the UKGDPR, the data controller – the client in this relationship that makes decisions as to purposes and means for processing personal data - is responsible for data protection, privacy and security at every point of the value chain[1].

There are a raft of duties and responsibilities to data subjects whose personal data it processes. This includes, for example, how it will collect personal data, how it will later deal with this personal data across many types of processing and how it provides access to the personal data for data subjects.

Appropriate technical and organizational measures must be in place, including a data protection policy, in order to ensure compliance with the UKGDPR.

And this also means that the data processor contracted to carry this out on behalf of the client must commit to maintaining the highest standards expected and act only in accordance with the written instructions of the data controller[2].

The stakes have been raised by the UKGDPR in that both the data controller and the data processor are jointly and severally liable in law for any personal data breach as a result of their joint activities. It's no longer a matter of contract where liability now falls as both are held to account.

Pre-UKGDPR

Under an outsourcing contract, the FMCG client contracts with a fulfilment house to process customer personal data from a variety of sources for an international marketing campaign. Any non-performance of the data processor is a contractual matter and not one regulated by law. Responsibility for compliance with data protection rules is a matter for the client.

Post-UKGDPR

The data processor must provide the FMCG client with sufficient guarantees that it will meet the requirements of the UKGDPR and ensure protection of the rights of data subjects whose data it's processing on behalf of the client.

[1] Art. 24, UKGDPR
[2] Art.28, UKGDPR

This outsourcing contract can't be entered into by the client unless there's clear agreement on the following points:

- The data processor will only process and transfer personal data upon express written instructions
- Commit staff to keep personal data confidential
- Ensure appropriate security is in place to protect the personal data
- Get explicit agreement from the data controller before engaging with another third party (sub-data processor such as cloud service provider)
- Get any agreed third party to comply with the same responsibilities as imposed by the data controller under the UKGDPR
- Support the FMCG client to achieve compliance with respect to data subject rights
- Support the FMCG client to achieve compliance with respect to the use and retention of personal data
- Support the FMCG client in evidencing compliance under the UKGDPR.

The contract should also provide that the data controller should manage all incidents and report all personal data breaches for their part of the value chain to the DPO and, if required, to the supervisory authority within 72 hours of finding out about them[3].

The UKGDPR lays down that the data processor has to inform the data controller without 'undue delay'. In simple terms, this means within two hours of any personal data breach[4]. There will be some push back from data processors, who will argue that this is impossible, and they need more time.

[3] Arts.33-34, UKGDPR
[4] This is in accordance with best practice as taught on her UKGDPR Programme, Henley Business School (UK)