GDPR: A Plain English Guide to the Implications for Middle East Marketing Activities

The advertising marketing world is becoming more reliant on data secured from online sources. All of the entities that are involved in the delivery of advertising content to consumers are able to receive, store and use data about consumer's likes and dislikes, with the aim of ultimately understanding buyer preferences.

Some entities are scrupulous in collecting and maintaining the integrity of that data, not revealing or providing it to third parties for any reason. Other entities are less likely to exhibit this level of behaviour and, taking advantage of some less prescriptive laws in some parts of the world, may take a less ethical approach to the receipt, storage and use of data. The recent scandals that have engulfed the use of Facebook data has shown that there can be unexpected failures, even by entities that proclaim compliance to high standards in using data from the general public.

Into this world of data reliance and scrutiny, the European Union has been long debating, and now finalising, the General Data Protection Regulation, known as the GDPR. The GDPR is intended to protect the data of residents of EU countries but in doing so, there are claims that it has the capacity to extend beyond the jurisdiction of the European Union to the operations of entities outside that region.

The intention of this article is not to provide an in depth analysis of the GDPR – we will leave the EU lawyers to drill down on the small print. However, the publicity being given to the GDPR has meant that many local entities are focussing on data issues. We are receiving many queries about data, with entities often not understanding the complexity of their own data collection and storage protocols. Very often they do not realise that the operation of these protocols potentially give rise to a requirement to comply with the GDPR.

In this article, we will pose some simple questions for companies to consider when analysing their protocols and, whilst the article does focus on issues of compliance for marketing industries in particular, it will certainly guide other industries in this analysis. All companies need to properly review their data collection and storage protocols and must properly consider whether they need to alter those protocols in order to ensure that they are not placing themselves, their clients or their EU affiliates in a position where they are in breach of the GDPR.

Getting the consent

The cornerstone of the GDPR is the consent that has to be acquired from all subjects – consent to the collection and use of their data. However, the manner in which the consent can be obtained is not ambiguous. There are three critical areas that are to be considered when consent is given under the GDPR.

First, the notice that is provided to the data subject at the time the consent is obtain must be phrased in such a way that the data subject is going to be "informed" at the time that consent is provided. On this basis, the current view is that all aspects of storage and use of material should be clearly laid out – how long it will be stored for, what will it be used for, what rights will the data subject have, will data be transferred to third party countries, and of course the all-important question: what will the data be used for? In marketing, this might be when the person signs up for a newsletter, or adds their name to a competition database.

Getting the consent: properly

The second key component that must be reviewed and properly undertaken is the method by which the consent is obtained. To simplify this aspect of the GDPR, the most important thing to know is that consent requires affirmative action from the data subject. It is no longer acceptable to assume opt-in from conduct. Further, it would not be acceptable to have a pre-ticked box that already accepted that the data will be used on specific terms. The GDPR indicates that the data subject must actively do something – tick a box for example, or choose a setting from a drop box or perhaps type some wording into a form.

Consent cannot be bundled with other issues. So for example it is ineffective to have a tick box that said "I agree to receive newsletters and for the company to use my data". This separation permits the data subject to choose to agree to some aspect of data use without having to agree to all of them. In the case cited above for example, the subject may agree to receive newsletters but does not agree to the general use of the data. Marketers that are, for example, using a social media competition to create a targeted mailing list, will have to consider whether the simple act of 'liking' the post will be sufficient for these stringent requirements.

Reiterating the first point, however the consent is obtained, the wording and meaning should remain clear and unambiguous at this second stage. General commentary on this point agrees that uncertainty or lack of clarity at this stage may cause difficulties under the GDPR. It is also advisable to ensure at this point that the data subject is reminded that they are able to withdraw their consent at any time. The data subject should also be informed about the manner in which they can get access the information if they wish to do so.

It should be noted that there are some special cases where consent must be specifically and explicitly provided. This would include cases where the data will be transferred internationally, which could prove to be extremely important for companies that are part of larger global operations.

Recording and filing the consent

Finally, in relation to consent, it is important that the company collecting the data is able to demonstrate that they have received a valid consent by way of appropriate records. All details of the record of consent must be maintained as a complete record. The record must include at least the following: who consented, what they were consenting to, when they provided the consent and the manner in which they provided the consent.

We note that consent is not the only legal basis upon which the data can be collected as a process but it is likely to be the most common for the marketing industry. If a company wishes to bypass consent and utilise other methods, specific legal advice should be sought regarding the particular position.

Rights of the data subject

Under the GDPR, the data subject has various rights that are particularly relevant to entities undertaking marketing activities. For example the data subject has a right to access any data that has been collected and they have the right to rectify any data that is incorrect. Even further, they have right to have their data records erased completely at any time and for no reason. They may also come back at a later date to request restrictions on processing of their data – they literally can alter the consent that was originally given.

Territoriality

The concept of territoriality – a fundamental issue when considering whether or not GDPR will apply to you or your organisation – is complex. What is clear is that entities with an EU presence will be covered by the GDPR and any entities that are targeting residents of the EU will also have to comply. On this basis, there are some scenarios that could mean that a company from the Middle East may also have to comply with the GDPR.

For example, a social media marketing firm that is directly targeting businesses that wish to expand into the Middle East by speaking at various conferences in Europe and providing materials for European based business publications could find that the GDPR considers them to be targeting European residents. In fact, it seems highly likely that they would be. Despite the fact these European residents may only make up small percentage of their target client based, the outcome remains the same: they are targeting EU residents for the purposes of their business. The question remain is to whether they only need to maintain this data standards just for those few data subjects that they encounter during EU targeted activities, or whether they have to upgrade their entire database to GDPR standards. In other words, can they keep two databases with differing standards?

But this can get even more complex. If a media agency, for example, is undertaking a multimedia buy for a client, there is a strong possibility that some of those publishers will be subject to the GDPR. In undertaking this media plan, does that media agency utilise databases that are or could be held by its European counterparts or otherwise targeting EU residents? When we look at the complex chain of relationships between the brand and the consumers, including agencies, publishers, various DSPs and others, the client cannot guarantee that all of these links do not expose the transaction to databases that are subject to the GDPR.

Conclusion

So in the end, a brand or marketing manager must ask themselves the following questions: Who is touching the data in my chain? What data is being collected and where is it being collected? And how it is going to be used within this transaction? These questions should provide answers in relation to the need for compliance with the GDPR.

Of course none of this is simple. The GDPR itself is already raising difficulties in interpretation before it has been put into place. Perhaps a small data breach in the Middle East may not be initially noticed, or if it is it may not give rise to the high fines that have been often discussed in GDPR articles – the maximum fine is set at 4% of global revenue or € 20 million. However as we have seen on so many occasions, when consumer data is used in a way that was unintended or beyond the acceptable scope the result is often a legal issue, accompanied by a large public relations issue. Once EU and global consumers become used to having extra protection in relation to their data and accustomed to seeing complex consent and detailed description of use cases, we will no doubt start to see a new brand of informed and diligent consumer who will be very comfortable in generating publicity against a brand that does not provide that protection.

Whilst, in the face of it, GDPR may not obviously apply to all businesses, we suggest that marketing companies and related businesses undertake a thorough audit of their processes, partners and data points so that compliance can be assessed and, where necessary, assured.