# Direct marketing and privacy: striking that balance

***Nicola Flannery, Deloitte Risk Advisory Ireland,*** ***discusses the often conflicting relationship between direct marketing practices and evolving privacy legislation, and addresses what steps can be taken now to be prepared for the ever looming GDPR implementation date***

Nicola is leading a workshop on 'Privacy by Design – How to Implement an Effective Framework' at the 12th Annual Data Protection Practical Compliance Conference—Preparing for the GDPR. See the website for further details: www.pdp.ie/conferences

The days of 'traditional' forms of direct marketing are numbered. Customers are more interested in their privacy nowadays, and do not always want to hear about targeted offerings. For organisations, the safe advice seems to be this: delete all the personal data from your CRM systems and focus on aggregated non-identifiable data to produce generic marketing campaigns. Do this now, or be subject to extortionate fines and the loss of brand and reputation.

This advice is all well and good, except that in reality, what has happened is quite the opposite. There is in fact a growing desire for, and pressure on, marketers to use personal data in new, creative and personalised ways. This is — at least in part — a response to consumers' increasing sharing of more personal data than ever across publicly available platforms, resulting in the availability of new and unique data sets, analytics and insights.

The challenges lie with striking the balance between meeting customers' expectations and creating an innovative brand, while also complying with legislation. A position complicated by the incoming General Data Protection Regulation ('GDPR') and the proposed changes to European Directive 2002/58/EC ('e-Privacy Directive'), each of which will change the direct marketing landscape significantly. This article looks at the key things marketers need to consider when looking at the legislative changes ahead. The GDPR changes regarding consent are perhaps more well-discussed, but what about the e-Privacy Regulation?

## Proposed e-Privacy Regulation

The new e-Privacy Regulation, currently going through the legislative process, is intended to complement, add to, and underpin the requirements of the GDPR. Its territorial reach is the same as the GDPR in terms of extending wider than the EU to include any data gathered from data subjects in EU countries by international organisations, and it applies to all direct marketing through electronic means.

Under the proposed new rules, business recipients of direct marketing are as protected as individual consumers. Whilst postal marketing does not fall under the scope of the e-Privacy Regulation, it does fall under the scope of the GDPR.

The fines and sanctions for non-compliance also align with the GDPR. The Article 29 Working Party has welcomed this approach in its recently issued opinion on the proposed new e-Privacy Regulation (see page 18). The Opinion also welcomes the fact that the new instrument is a Regulation as opposed to a Directive, meaning it will, like the GDPR, have direct effect in Member States, and Data Protection Authorities across the EU will be responsible for its enforcement.

It is key that organisations involved in electronic communications and currently focused on implementing the GDPR give adequate consideration to the e-Privacy Regulation. Not only do the two Regulations strengthen and complement each other, but the implementation date for the e-Privacy Regulation is currently proposed to also be the 25th May 2018.

Set out below is a discussion of the changes being proposed in both Regulations around direct marketing rules.

## Consent and transparency

A key element of any direct marketing campaign is having adequate prior consent. The enhanced rules around consent in the GDPR and the proposed new e-Privacy Regulation support a stricter standard and higher threshold for marketers to meet before they have gained consent.

As well as these stricter standards, the scope of the consent rule has widened to incorporate more technologies, such as the sending of personal messages through social media (In-platform or In-App messaging), instant messaging, web mail or unmanaged VoIP, collectively known as Over-the-Top ('OTTs') communication services. Marketers may have previously relied on implied consent for these kind of in-

(Continued on page 12)

(Continued from page 11)

app campaigns, or may have used WhatsApp etc. as a means of sending direct marketing without the need for consent, but consideration must now be given to whether adequate consent is in place.

According to the new standards, consent must be freely given, specific, informed and an unambiguous indication of the individual's wishes. There must be a clear, affirmative action that signifies agreement for the processing of personal data.

An individual must 'opt-in' to direct marketing as opposed to 'opting-out'. New accountability requirements means that there is a need for stricter controls around records of consent, including being able to demonstrate that an individual has consented and that the consent is clearly distinguishable from other matters.

One caveat which still remains is where an individual has provided their email details as part of a sale or service. An organisation may send them marketing emails in relation to the product or service (i.e. soft 'opt-in'), but there must be a clear means of opting out included in each marketing communication.

The 'informed and unambiguous' requirement strengthens the need for transparency in the collection of consent from individuals. Clearly stating what 'types' and means of direct marketing an organisation plans to carry out must form part of this. An individual must know exactly how they will be marketed to, on what subject and by whom, including any marketing affiliates/ partners. Catch-all, high level statements left open to interpretation will no longer be sufficient.

> ***"An individual must know exactly how they will be marketed to, on what subject and by whom, including any marketing affiliates/ partners. Catch-all, high level statements left open to interpretation will no longer be sufficient."***

## Right to object

Hand in hand with new rules on consent is the right to withdraw consent. This is not a new requirement by any means, but the GDPR specifically refers to direct marketing in the right to object in Article 21(3). When an individual objects to processing for direct marketing purposes, then their personal data must no longer be processed in this way.

The need to include a specific opt-out in every marketing message to allow an individual to withdraw their consent at any time still stands. The key challenge for organisations is processing these opt-outs in a timely manner, in order to comply with the GDPR's requirement of maintaining internal records of processing and processing data subject requests 'without undue delay'. Fulfilment of such objections (to the processing of personal data for direct marketing) requires careful thought, as it may have an impact across a number of systems in an organisation. Consideration should be given to technical measures ensuring the interoperability of systems, data lineage, and data discovery where feasible. In the absence of such measures, clearly defined policies and processes must be implemented to ensure that no 'opt-out' slips through the cracks.

## Profiling and analytics

In this era of the Internet of Things and Big Data, innovation is top of any organisation's agenda. Being able to use personal data in innovative ways to build brand and add value is key to business growth.

The use of marketing insights, which at an aggregate level are valuable but nothing short of game changing where data are individually identifiable through profiling and analytics, is where innovation can happen for an organisation.

Developers of new technologies and products that allow customers' banking apps to tell them where they spend most of their money, and serve offers based on this, or geo-targeted offers delivered directly to their phones, provide huge opportunities. Provided the GDPR and proposed e-Privacy Regulation is assessed prior to the implementation and roll-out of these, there is no reason that these can't continue to be ways for organisations to provide direct marketing and add value to their brand.

When it comes to marketers carrying out these kinds of profiling or analytics to tailor marketing campaigns specifically to individuals, consideration again needs to always be given to adequate consent, full transparency and the individuals' right to request not to be profiled.

## Affiliate marketing

Whether organisations share their own customer marketing lists with affiliates/partners, procure and use a third party marketing list, or engage an affiliate/partner to carry out direct marketing on their behalf, the proposed e-Privacy Regulation and the GDPR very much applies in all scenarios.

Data controllers procuring any of these kinds of services from a third party must do so with adequate measures in place to ensure compliance with the Regulations. Again, consent and transparency is key, and a consumer must not be surprised to receive direct marketing from an organisation or from a third party on behalf of an organisation. Due diligence before engaging with such third parties must be carried out and an organisation must be comfortable that the third party's direct marketing practices are compliant with the Regulations before contracting with them.

Contracts with third parties must adequately reflect the requirements under the Regulations, including around the security of sharing of any personal data. Organisations must be satisfied that the third party has all the necessary consent records for any marketing list they are using. The requirements on organisations to ensure compliance apply regardless of whether organisations engage third parties as data controller or as a data processer.

## Practical steps

While the e-Privacy Regulation is still at proposal stage, the European Commission is encouraging the European Parliament and the Council to work towards an adoption date in line with the GDPR of 25th May 2018. With this in mind, organisations involved in electronic communications should be looking at what steps they are taking now to implement the GDPR and how these will align with the e-Privacy Regulation. Some key steps that can begin now are outlined below.

**Governance and accountability**: Are the GDPR and proposed e-Privacy Regulation requirements adequately governed under the organisation's privacy framework? Organisations should appoint a data owner within their marketing teams responsible for ensuring implementation and compliance with a direct marketing policy.

**Consider a consent review**: Organisations should look at how they currently manage consent in general and specifically in relation to direct marketing campaigns, and the management of this consent. They should identify consent mechanisms and ensure they have adequate consent for all personal data with clear distinguishable records of consent. An individual must be able to accurately state that they know exactly what kind of marketing they are opting-in to when they provide consent.

**Managing Opt-outs:** How are opt-outs managed across the organisation? Include opt-outs in every direct marketing message. Organisations should assess whether they have the technical and/or manual means to process an opt-out across all systems where personal data are stored without undue delay.

**Profiling and analytics and new technologies**: Organisations should implement a privacy by design approach at the beginning or re-design of any processing of personal data via a new product, process, project, third party or system. They should ensure that Privacy Impact Assessments are carried out on any large scale processing of personal or sensitive personal data.

**Affiliates/partners**: Are adequate due diligence processes in place prior to engaging with marketing affiliates? Organisations should ensure that their contracts with marketing affiliates are updated to reflect the stricter requirements under both the GDPR and the proposed e-Privacy Regulation, including regular auditing of affiliate practices. Plus, they should ensure there are measures in place if an individual complains directly to them regarding a marketing campaign carried out on the organisation's behalf.

**Training and awareness:** Key risk training and awareness to an organisation's marketing teams is important to ensure that compliant direct marketing practices are embedded into business operations.

## Other considerations under the e-Privacy Regulation

The proposed e-Privacy Regulation does not focus solely on direct marketing by electronic means, but also enhances and changes the rules around cookie consent, other tracking technologies, the use of content and metadata of any electronic communications as well as call blocking, rules on public directories and caller identification. It is important to point out again that all these changes underpin, add to and complement the GDPR, and should be considered during the planning stages of a GDPR implementation programme.

While the changes in this area can seem insurmountable to organisations at the moment, the GDPR and the proposed e-Privacy Regulation should be considered as business enablers, leading to a transparency with consumers that builds trust which in turn strengthens brand and leads an organisation towards innovation.

The secret is in the balancing act.

**Nicola Flannery**
Deloitte
niflannery@deloitte.ie