IN BRIEF

▶ ICO guidance is helpful, but without clarity on the e-Privacy Regulation the rules remain in a state of flux.

Mind the GDPR (Pt 5)

In the fifth of this special series on the GDPR, Rollits LLP provide a post-implementation review

On 25 May 2018 the UK's data protection regime was shaken up amidst much hullabaloo by the introduction of the General Data Protection Regulation (GDPR). As the dust begins to settle, we take a look at the impact the GDPR has had so far, focusing on marketing activities.

Marketing activities

Whenever an organisation sends out marketing material to an identifiable individual, GDPR will apply and the organisation will need to ensure that it has a lawful basis for doing so: typically the consent of the individual is required, but where it is not the organisation may be able to rely on its own legitimate interests.

In the run up to 25 May 2018 one of the biggest consequences of the GDPR felt by the general public related to the stricter requirements controllers had to abide by in order to process personal data based on an individual's consent. Almost simultaneously marketing departments all over the country (and further afield) appeared to wake up to the fact that they may need to refresh their consents in order to ensure that they were GDPR compliant, and suddenly inboxes were awash with the same request to 'click here to indicate that you would still like to hear from us'.

It is not surprising—given the public exposure of the topic—that since the GDPR took effect we have seen an increase in the number of complaints clients have been receiving in relation to their direct marketing practices. Many complaints are founded on the basis that the individual did not consent to receiving the relevant message. To add an extra layer of complexity, such complaints are often accompanied by a subject access request.

Additional guidance has recently been published by the Information Commissioner's Office (ICO's) on the rules that apply to sending our marketing material. Key points include:

1. The rules are different depending whether the organisation is sending unsolicited direct marketing to an individual subscriber or to a corporate subscriber. An individual subscriber includes individual customers (including sole traders) and some partnerships. A corporate subscriber includes companies and other corporate bodies (and also comprises employees that have personal corporate email addresses such as *firstname.lastname@company.co.uk*).
2. If sending unsolicited direct marketing by electronic means (which includes email, text (SMS) messages, mobile pictures, video messages and voicemail messages) to an individual subscriber, the individual's consent to receiving that marketing material is required and such consent must be GDPR compliant regardless of whether the consent was obtained pre or post GDPR (for further guidance on consent requirements, see 'Mind the GDPR (Pt 2)').
3. Notwithstanding our comments in 2 above, organisations can send direct marketing by email *without consent* if: the individual's details were obtained in the course of a sale or negotiations for a sale; the direct marketing is in respect of similar products or services; and the individual is given a right to object at the time of collection and each time a message is sent. This is known as the 'soft opt-in'. If an organisation is relying on soft opt-in to send unsolicited direct marketing by email, it will have to demonstrate that it is in its legitimate interests to send such emails (see our comments below in relation to relying on legitimate interests).
4. If sending unsolicited direct marketing by email to a corporate subscriber with a personal corporate email address, consent is not required if the sender can demonstrate that it is in its legitimate interests to send such marketing messages and can satisfy the legitimate interests test. If the message is being sent to a generic corporate email address, such as *info@company.co.uk*, which does not identify an individual then it is not personal data and so it falls outside the scope of GDPR (although the relevant subscriber should still be given the option to object to receiving the marketing).
5. Consent must be obtained before making 'live' phone calls to numbers registered on the Telephone Preference Service (TPS), the Corporate Telephone Preference Service (CTPS) and to anyone that has previously objected to receiving marketing calls from the organisation. Organisations may be able to rely on their legitimate interests, rather than consent, if the organisation wishes to make live phone calls where there is no TPS/CTPS registration of objection.
6. Consent must be obtained for automated phone calls.
7. Organisations may be able to rely on their legitimate interests, rather than consent, for sending out marketing material by post.

The specific rules regarding direct marketing are predominantly contained in the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)—GDPR's often overlooked dancing partner—and they are in the process of being updated to ensure that they are consistent with GDPR. The e-Privacy Regulation (which will eventually replace PECR) is still under review and it is unclear what the final text will say. At the time of writing we

can surmise the following:

- The requirements in relation to soft opt-in will be tightened so that organisations can only rely on soft opt-in if the individual's details were obtained in the context of the sale of a product or service (under PECR an organisation can rely on the soft opt-in if the individual's details were obtained during negotiations for a sale, whether or not the sale actually took place).
- If making live marketing phone calls to individuals, the default position is that consent is required. Member states can opt out of this. Whether or not the UK will decide to opt out and retain the status quo is yet to be revealed.
- The e-Privacy Regulation does not distinguish between corporate subscribers and individual subscribers in the same way as PECR and it is unclear how this will be resolved.

Legitimate interests

Legitimate interests can potentially be relied upon as a lawful basis for processing personal data in a number of different circumstances, including for certain marketing activities as detailed above. If an organisation is seeking to rely on legitimate interests as the lawful basis for processing personal data it should undertake a three stage test and document the outcome:

1. Purpose test: identify a legitimate interest for processing.
2. Necessary test: identify whether processing is necessary for the purpose identified in 1 above.
3. Balancing test: balance the individual's interests, rights and freedoms against the organisation's legitimate interest. For example, does the processing provide a clear benefit to the organisation or others? Is there a limited privacy impact on the individual? Would the individual reasonably expect you to use their data in that way?

The above test is not new and should have been carried out by organisations relying on their legitimate interests under the previous data protection regime. Applying the three part test, direct marketing may—but will not always — constitute a legitimate interest. Whether or not it can be relied upon will depend on the circumstances.

Here are some examples to illustrate how it might work in practice:

A) If an organisation is relying on soft opt-in to send unsolicited direct marketing to an individual subscriber by email then (assuming the organisation can satisfy tests 1 and 2 above) whether or not the balancing test favours processing is likely to depend on how broadly the organisation interprets the soft opt-in requirements. If an individual purchases a DVD from an organisation and the organisation (having given the individual an opportunity to object, which is not taken) considers whether to send out a marketing email to that individual with information in relation to similar DVDs. The organisation determines that sending such email is likely to have a limited impact on the individual and that the individual would reasonably expect their data to be used in this way. As a result the organisation takes the view that the balance favours their processing and that it can send the email on the basis of its legitimate interests.

B) Keeping with a similar theme as set out in A) above, but in this case the individual does not purchase the DVD but merely enters into negotiations in relation to it (for example, by placing it in their online shopping basket). The organisation considers whether to send out a marketing email to that individual with information in relation to DVDs, CDs and other electrical goods. While some of the goods may be similar in nature, the organisation determines that the individual would not reasonably expect their data to be used in this way and that the balance does not favour their processing. The organisation takes the view that it cannot rely on its legitimate interests in this instance (and under the e-Privacy Regulation the lack of a sale will likely be an additional barrier to marketing).

C) The organiser of a business event collects business cards from some of the attendees and wishes to add them to her database in order to send information about future events. The organiser determines that she has a legitimate interest in networking and growth of her business and that collecting attendee details is necessary for this purpose. The organiser assesses whether the balance is in favour of processing and determines that attendees handing over business cards would reasonably expect their business contact details to be processed and that the impact on them will be low. The organiser therefore decides that it can rely on its legitimate interests for sending marketing information to the attendees about future events.

D) The organiser of the business event in C) considers whether to send event information by email to business contacts she has found online. The organiser has had no contact with the individuals and does not know whether the events will be relevant to the individuals' businesses. As a result, the organiser determines that the balance does not favour processing.

You may disagree with the decisions reached above, but the important point is to carry out the exercise and document the outcome should the decision to process ever be challenged.

Summary

Organisations relying on their legitimate interests for sending any form of direct marketing will always face the risk that the individuals they are targeting will view their marketing practices as excessive and unwarranted and that a complaint may ensue. The guidance from the ICO to date is helpful, but, until there is clarity on the e-Privacy Regulation, the rules remain in a state of flux with no current end date in sight. It will be interesting to monitor over the coming weeks and months the extent to which an organisation's determination of the three-stage test is challenged and, if so, what we can learn from the ICO's subsequent decisions. NLJ

David White, senior solicitor; **Tom Morrison,** partner, Rollits LLP (*www.rollits.com*). 'Mind the GDPR': Pt 1, 167 *NLJ* 7762, p8; Pt 2, 167 *NLJ* 7774, p11; Pt 3, *NLJ* 13 April 2018, p12; & Pt 4, *NLJ* 25 May 2018, p11).