LEWIS SILKIN

Introductory guide to using data to market to customers

LEWIS SILKIN

Executive Summary

The development of new technologies has significantly enhanced the ability of organisations to collect and process information about individuals, often with wide-reaching benefits. From a marketing perspective, it is now far easier to know more about your customers. This has also highlighted the importance of safeguards being put in place, particularly given concerns about that information being used in unwarranted and intrusive ways.

As direct marketing involves the processing of personal data, marketers need to comply with the Data Protection Act 1998 (DPA) – the key law in this area; as well as the Privacy and Electronic Communications Regulations 2003 (PECR) – containing the rules about electronic marketing and cookies. The DPA and PECR aren't the only rules though and, when using data for marketing purposes, you may need to also consider the Direct Marketing Association's (DMA) Code of Practice and the UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (CAP Code) if relevant.

Introduction

If personal data is being used for marketing purposes, compliance with the eight Data Protection Principles under the DPA is essential. The first principle requires "fair and lawful processing" and ensures that data is only processed either with the consent of the individual, for a purpose that the DPA regards as "necessary" or if it's in the legitimate interests of the organisation doing the marketing.. Marketers usually, but not always, need consent to process personal data for marketing purposes, as the "necessary" purposes in the Act are narrowly defined and rarely applicable in the marketing context and even if legitimate interests can be relied on, you still need to tell individuals you are going to use their data for marketing so it's often easier to ask for consent up front so there are no surprises.

The obligation to comply with the DPA falls on the data controller, that's the person that determines the purpose for which and manner in which personal data is to be processed. So it's up to the data controller to explain to individuals the marketing use that will be made of the data once collected (this is typically explained through a fair processing notice), and ensure that it is clear how the data controller will market to the individuals (typically by including opt-in choices on data collection).

Using data for marketing

Consent

When obtaining consent from individuals to process their personal data for marketing purposes, the consent must be

freely given - there has to be a genuine choice; consent can't be a condition to using the particular services the individual is signing up for

specific – be clear on both the type of marketing communication you're going to use (e.g. postal, email, SMS, telephone calls) and who will be doing the marketing (e.g. you and/or your subsidiary companies)

informed – the fair processing notice (required by Principle 1), often known as a "privacy policy", should set out clearly, and in plain English, what the data will be used for; and

given by an action from the individual – a positive indication is required and can't be inferred simply by someone not responding to a communication

Marketers need to ensure that collection of data for marketing purposes is accompanied by a suitable privacy notice and appropriate data capture language (for example "by submitting this form you consent to Company using your data to send you details about our products" or "Tick here if you consent to Company sending you marketing communications").

Note that asking individuals to fill in a form and then telling them that by submitting the form the individual will give consent to the marketing (unless they tick a box to object) is known as "form-based consent" and is currently a valid way of evidencing a positive indication although this may no longer be the case under the new European General Data Protection Regulation (GDPR) which will come into force with effect from 25 May 2018.

Third parties

Collecting data to use for your own marketing is a more straightforward issue, but often companies within a group might want to share data between group companies to market the group's products or services. The consent obtained when collecting the data needs to make it clear who you're sharing the data with and what marketing they'll be doing. That notification requirement applies whether you're passing the data to another company in the same group or to a completely independent third party.

The Information Commissioner's Office (ICO) requires data controllers to be as specific as possible when collecting data for third parties to use and suggests that you consider whether or not the marketing action would be "expected" by the individual receiving it. Simply asking an individual to "tick here" if you agree to us passing your details to "specially selected third parties" is no longer specific enough. The ICO currently asks you to identify at least the class of organisation you're sharing the data with and their latest guidance goes further and under GDPR they may expect you to name the individual organisation.

Buying in marketing lists

If you're on the receiving end of personal data and intend to use it for marketing, you'll want to be sure that the organisation providing the details collected it properly in the first place – and, ideally, identified your organisation as the recipient of the data and one of the companies that would be sending marketing materials.

Clearly, where you want to buy a list of details from a third party, you'll need to be even more careful and ask searching questions and ask for evidence about what consent was given by the individuals and, preferably, obtain contractual protection from the seller in your purchase agreement.

Electronic marketing

In addition to the DPA, PECR sets out a set of rules about electronic marketing. If you're marketing using phone calls (automated or live), fax, SMS, email or voicemail, PECR will also apply and you need to comply with these rules in addition to the DPA.

PECR sets out rules about whether you can send unsolicited marketing messages to individuals without their consent and treats "individual subscribers" differently from "corporate subscribers". If you're undertaking B2C marketing, you need to take care because a single email sent in breach of PECR can incur liability. There's no need for the ICO to prove that your marketing communication actually caused distress or harm.

The table below sets out a summary of the rules in PECR:

Mode of contact	Prior consent needed?
Mail	No, but check the Mailing Preference Service (see below)
Email and SMS, and also voicemail and answerphone messages, (all known as "email" for the purposes of PECR)	Yes for individual subscribers – unless you rely on the soft opt-in (see below). No for corporate subscribers – provided you give an opt-out in every communication.
Fax	Yes for individual subscribers. No for corporate subscribers – provided the subscriber is not registered with the relevant Fax Preference Service (see below) and hasn't previously objected.
Automated calls	Yes
Live calls	No – provided you don't call anyone who is registered with the Telephone Preference Service (see below) or has previously objected to phone calls.
Cookies or similar technology	Yes – prior to placing cookies or similar technologies on an individual's device, unless the cookies are strictly necessary (e.g. to keep content within a shopping basket – unlikely in a marketing context).
Location data	Yes

Preference lists

The DMA maintains a number of preference services that allow consumers (and in some cases businesses) to register their wish to opt out of unsolicited marketing communications via phone, mail, fax or email. These include the Mail Preference Service (MPS), the Telephone Preference Service (TPS) and the Fax Preference Service (FPS). These services allow marketing organisations to screen their own databases and potential marketing lists against the relevant preference service's list so as to remove those people who are listed. As noted above, in a number of cases it is a legal requirement for marketers to screen their contact lists in this way and the ICO is responsible for enforcement. Note too that there's a new preference list being introduced by the Fundraising Regulator in respect of marketing by charities.

Soft opt-in

An often-used alternative to obtaining prior consent from individuals to email marketing is to rely on the soft opt-in. This applies only where:

you have obtained an individual's details in the course of a negotiation or sale;

the same legal entity that collected the data sends further marketing materials about their similar products or services; and

you gave individuals the ability to opt out of marketing communications on collection, and in every subsequent communication.

All three conditions have to be met in order to be able to rely on the "soft opt-in", and you need to ensure that you keep a record of any individual who objects at any time – and put them on your suppression list to avoid sending further communication. As explained in the ICO's Direct Marketing guidance the soft-opt in won't apply to charities as details collected in the course of a donation won't qualify as "in the course of a negotiation or sale".

Enforcement

The ICO is responsible for enforcement of both the DPA and PECR and offers a "report spam" button on their website where they collate complaints from members of the public. It's advisable to follow their direct marketing guidance as breach of either set of rules is punishable by fines of up to £500,000 and, as you can check on the ICO's own website, they regularly issue monetary penalties for breach of PECR. In addition, the Direct Marketing Guidance is soon to be put on statutory footing allowing a failure to comply with it to be taken into account should your breach be taken to the tribunal.

Once the GDPR comes into force, these fines could increase up to €20,000,000 or 4% of its global annual turnover for the previous year, whichever is the highest. In addition, the UK government is looking at introducing personal liability for directors of companies who send spam marketing to ensure companies can't avoid fines by putting their companies into liquidation.

Spam marketing is a key area of focus for the ICO and they are taking a harder line on enforcement. Changes pending within the GDPR such as obtaining 'unambiguous' consent and ensuring transparency will only become more important. The original European E-Privacy Directive (the basis for PECR in the UK) is also under review and changes are expected shortly to ensure those rules match up to the new requirements under the GDPR.

The proper use of data for marketing can help build up better customer relationships and improve brand loyalty, but failing to comply can result in unwanted publicity and fines. The subsequent loss of trust, and customers, will be something that all marketers will want to avoid.

For further information, contact:

Olivia Savage
Managing Asscoiate

+44 (0) 20 7074 8231
olivia.savage@lewissilkin.com

Bryony Long
Senior Asscoiate

+44 (0) 20 7074 8435
bryony.long@lewissilkin.com

LEWIS SILKIN

5 Chancery Lane – Clifford's Inn
London EC4A 1BL
DX 182 Chancery Lane
T +44 (0)20 7074 8000 | **F** +44 (0)20 7864 1200
www.lewissilkin.com