10

DATABASE PRACTICE

Background

CAP is currently consulting on changes to its rules on the collection and use of data for marketing. These changes are intended to ensure that its rules cover data protection issues most relevant to marketing, and that they are aligned with the standards introduced by the General Data Protection Regulation (EU 2016/679, the GDPR). The consultation will close at 5pm on 19 June 2018.

From 25 May 2018, when the GDPR is enforceable, until CAP introduces new rules, the ASA will not administer the existing rules in section 10 and Appendix 3 of the CAP Code. If the ASA receives complaints during this time, it will make advertisers aware of the complaint and issues raised, and ensure that they are aware that they must be complying with the GDPR. CAP encourages members of the public and businesses to find more information about their legal rights and obligations at www.ico.gov.uk .

Marketers must comply with all relevant data protection legislation. Guidance on that legislation is available from the Information Commissioner's Office. Although data protection legislation has a wide application, these rules relate only to databases used for direct marketing purposes. The rules should be observed in conjunction with the legislation; they do not replace it.

Responsibility for complying with the database practice rules may rest directly not with marketers but with data controllers. Those responsible are expected to comply.

Definitions

A "data controller" is an entity that determines the purposes for which, and the manner in which, personal information is to be processed. It may be an individual or an organisation and the processing may be carried out jointly or in common with other persons or organisations.

A "preference service" is a service that, to reduce unsolicited contact, enables consumers and businesses to have their names and contact details in the UK removed from or added to lists that are used by the direct marketing industry.

Electronic mail in this section encompasses e-mail, Short Message Service (SMS), Multimedia Messaging Service (MMS) and other data transfer methods.

(See also CAP Help Notes on Mobile Marketing and Viral Marketing.)

Rules

10.1 Personal information must always be held securely and must be safeguarded against unauthorised use, disclosure, alteration or destruction.

10.2 Any proposed transfer of a database to a country outside the European Economic Area must be made only if that country ensures an adequate level of protection for the rights and freedoms of consumers in relation to the processing of personal information or if contractual arrangements provide that protection.

10.3 Marketers must do everything reasonable to ensure that, if asked in writing, consumers or the ASA (with consent of the consumer concerned) are given available information on the nature of a consumer's personal information and from where it has been obtained.

10.4 Marketers must not make persistent and unwanted marketing communications by telephone, fax, mail, e-mail or other remote media. To avoid making persistent and unwanted marketing communications, marketers must do everything reasonable to ensure that:

10.4.1 marketing communications are suitable for those they target

10.4.2 marketing communications are not sent unsolicited to consumers if explicit consent is required (see rule 10.13)

10.4.3 anyone who has been notified to them as dead is not contacted again and the notifier is referred to the relevant preference service

10.4.4 marketing communications are not sent to consumers who have asked not to receive them (see rule 10.5) or, if relevant, who have not had the opportunity to object to receiving them (see rule 10.9.3). Those consumers should be identifiable

10.4.5 databases are accurate and up-to-date and that reasonable requests for corrections to personal information are effected within 60 days.

10.5 Consumers are entitled to have their personal information suppressed. Marketers must ensure that, before use, databases have been run against relevant suppression files within a suitable period. Marketers must hold limited information, for suppression purposes only, to ensure that no other marketing communications are sent as a result of information about those consumers being re-obtained through a third party.

10.6 Marketing communications sent by electronic mail (but not those sent by Bluetooth technology) must contain the marketer's full name (or, in the case of SMS messages, a recognisable abbreviation) and a valid address; for example, an e-mail address or a SMS short code to which recipients can send opt-out requests.

10.7 Fax and non-live-sound automated-call marketing communications must

contain the marketer's full name and a valid address or freephone number to which recipients can send opt-out requests.

10.8 Marketers are permitted, subject to these rules and to database rights, to use published information that is generally available if the consumer concerned is not listed on a relevant suppression file.

10.9 Unless it is obvious from the context, or if they already know, consumers must be informed in a clear and understandable manner and at the time personal information is collected:

10.9.1 who is collecting it (and the representative for data protection queries, if different)

10.9.2 why it is being collected

10.9.3 if the marketer intends to disclose the information to third parties, including associated but legally separate companies, or put the information to a use significantly different from that for which it is being provided; if so, an opportunity to prevent that from happening must be given.

10.10 The extent and detail of personal information held for any purpose must be adequate and relevant and should not be excessive for that purpose.

10.11 Personal information must not be kept for longer than is necessary for the purpose for which it was originally obtained.

10.12 If after collection they decide to use personal information for a purpose significantly different from that originally communicated, marketers must first get the explicit consent of consumers. Significantly different purposes include:

10.12.1 the disclosure of personal information to third parties for direct marketing purposes

10.12.2 the use or disclosure of personal information for any purpose substantially different from that which consumers could reasonably have foreseen and to which they might have objected.

10.13 The explicit consent of consumers (see rule 10.4) is required before:

10.13.1 processing sensitive personal data, including information on racial or ethnic origin, political opinion or religious or other similar beliefs, trade union membership, physical or mental health, sex life, criminal record or allegation of criminal activity

10.13.2 sending marketing communications by fax

10.13.3 sending marketing communications by electronic mail (excluding by Bluetooth technology) but marketers may send unsolicited marketing about their similar products to those whose data they have obtained during, or in negotiations for, a sale. Data marketers must, however, tell those consumers they may opt out of receiving future marketing communications both when they collect the data and at every subsequent occasion they send out marketing communications. Marketers must give consumers a simple means to do so

10.13.4 sending non-live-sound marketing communications by automated calling systems.

10.14 Explicit consent is not required when marketing business products by fax or by electronic mail to corporate subscribers (see III j), including to their named employees. Marketers must nevertheless comply with rules 10.4.5 and 10.5 and offer opt-outs in line with rule 10.13.3.

Children

Background

Please see Section 5: Children

10.15 Marketers must not knowingly collect from children under 12 personal information about those children for marketing purposes without first obtaining the consent of the child's parent or guardian.

10.16 Marketers must not knowingly collect personal information about other people from children under 16 unless that information is the minimum required to make a recommendation for a product, is not used for a significantly different purpose from that originally consented to, and the marketer can demonstrate that the collection of that information was suitable for the age group targeted.

Data about third parties collected from children must not be kept for longer than necessary.