A DATA PROTECTION CHECKLIST FOR DIRECT MARKETING

This data protection checklist should be useful for companies wishing to be sensitive to European data protection legal requirements but needing guidance on practical implementation of data protection principles.

This checklist is drawn from the UK's Advertising Association's (AA) Code of Practice Covering the Use of Personal Data for Advertising and Direct Marketing Purposes (see page 10). Although the code was drawn up in the UK, it nevertheless, took into account the Council of Europe's Direct Marketing Recommendation (see page 16). Therefore, the checklist will be particularly useful for companies based in countries, like the USA and Canada, without data protection legislation covering the private sector, which are seeking Europewide guidance in this unfamiliar area. This code of practice also offers a valuable insight into what may be expected from the self-regulatory codes being planned to enable companies to comply with Finland's new law (PL&B May'87 p.14) and the Netherlands bill (PL&B May'87 p.18).

In each case, the data protection principle is followed by an extract from the relevant section of the AA code:

* Information shall be collected fairly: "If in the course of acquiring personal data from data subjects, data users materially misrepresent to these data subjects the purposes for which the data are to be held, used or disclosed, those data will be regarded as having been unfairly obtained."

* A data user should seek a guarantee (warranty) that data has been collected fairly and lawfully: "The warranty from the list owner should include undertakings that -

a. he is registered as a data user;

b. the data were fairly and lawfully obtained;

c. the list was updated on a specified date or during a specified period. This undertaking should be accompanied by a statement of the respects in which the data have been updated;

d. requests from data subjects for the correction or deletion of data have been complied with;

e. received and disputed data have, where appropriate, been so marked;

f. the purpose or purposes for which the data are registered are compatible with their disclosure to the intending user and his proposed use of them;

g. the data have, where applicable, been collected, held and processed in compliance with this Code;

The warranty should also state whether the list has been Mailing Preference Service cleaned (that is, checked against the industry's own list of those individuals who do or do not wish to receive certain categories of data), and if so during what period this was last done.

The list supplier should also require from the prospective user guarantees that:

a. "the data will be used only for the purpose or purposes authorised by the supplier;

b. where the prospective user is required to be registered under the Act, those purposes are within the terms of the prospective users' registration;

c. no disclosure will be made to any third party, except as expressly permitted by the supplier, and provided always that such disclosure is covered by the terms of the prospective user's registration;

d. any request for access, correction or deletion received by the prospective data user from a data subject will, when appropriate, be referred to the supplier."

* Personal data held for any purpose or purposes shall not be used or disclosed in any manner incompatible with that purpose or those purposes.

"In any case where harm of any kind is likely to result from disclosure, such disclosure should not be regarded as acceptable unless the data subjects have been asked whether they object to such disclosure and have not objected."

* Personal data held for any purpose or purposes shall not be kept longer than is necessary for that purpose or those purposes.

"Data users should regularly review the data they hold with a view to ensuring that they do not hold personal data in breach of this principle. The frequency of such reviews will be related to the use that is made of the personal data, but only in exceptional circumstances will a period exceeding a year between reviews be acceptable."

* Data subjects access to records on themselves.

"Data users should acknowledge subject access requests as soon as possible, which other than in exceptional circumstances should not exceed 10 days after they have been received, and should at the same time indicate what delays, if any, might occur in supplying a copy of the information requested." (The law provides for a maximum delay of 40 days).

* Mediation

"When the data user and the data subject are unable to agree as to the correction or erasure of personal data, the data user should advise the data subject of the circumstances under which the Data Protection Registrar may investigate an individual complaint."

* Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

"Data users whose marketing lists contain sensitive personal data should,

where appropriate, include access-markers to facilitate the investigation of suspected breaches of security."

* Sensitive data

Sensitive data is defined as information on the racial origin of the data subjects, their political opinions, religious or other beliefs, their physical or mental health, their sexual life, or their criminal convictions. "Where sensitive personal data of this nature are collected, used or disclosed, data users should consider whether it is appropriate to seek express consent from the data subjects concerned."

* The Council of Europe Recommendation on Data Protection and Direct Marketing

Even though the UK Act does not state that data subjects have a right to have their names excluded from mailing lists, the above Recommendation proposes that such a facility should be made available. Accordingly, data users should comply with the Mailing Preference Service's Code of Practice and should "where possible, use the recommended method of not erasing the name, but of retaining it on file with a suppression marker."

* Revealing the source of personal data

"Data users should reveal the source of personal data (if they consent) in response to enquiries from data subjects."

* Causing offence

"Data users should avoid including in advertising material references to age, economic status, education, purchasing behaviour, employment status, bereavement, marital status or children in the family, where such references would be likely to cause alarm, distress or legitimate offence to recipients."

* Protecting privacy

The goods and services offered and the messages transmitted should be presented in such a form and manner as not to prejudice the privacy of addressees (eg. confidential information showing through window envelopes).

For further information on the impact of data protection rules on direct marketing, see Norway's new regulations (page 5).

The Code of Practice Covering the use of Personal Data for Advertising and Direct Marketing Purposes (1987) is published and available from The Advertising Association, Abford House, 15 Wilton Road, London, SW1V 1NJ, UK, Telephone (44) 1 828 2771.