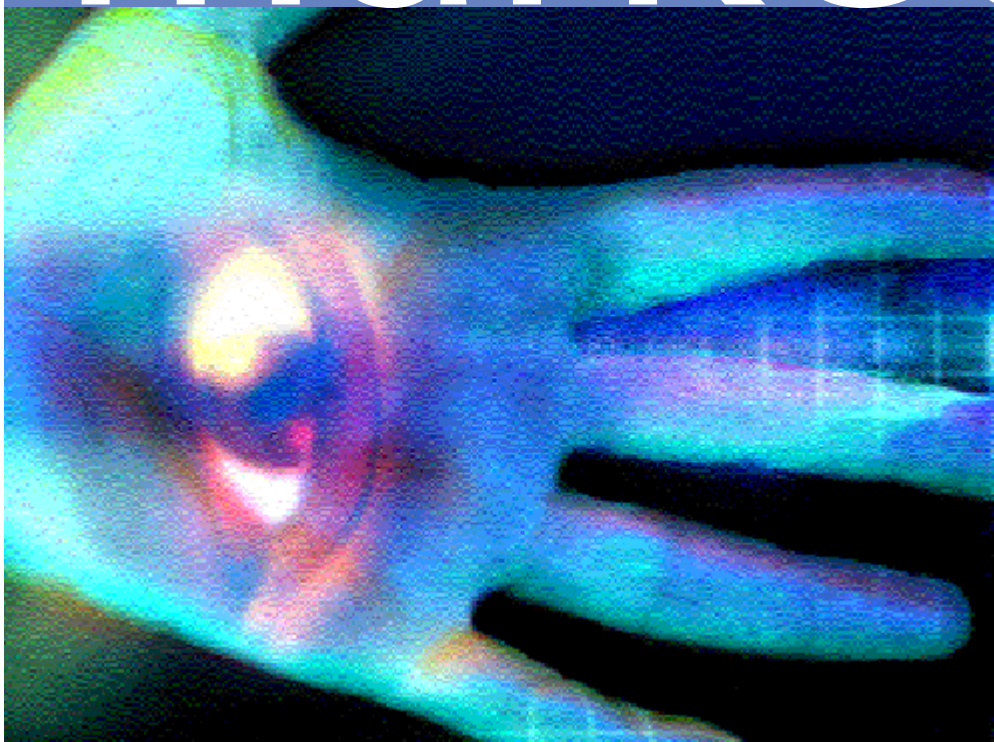


data protection and privacy practice marketing



Comment from the author

In February 2000, I spoke at a DMA meeting in New York which focused on the relationship between Europe's approach to data protection (e.g. as found in the UK's Data Protection Act 1998) and its impact on the use of personal data for a direct marketing purpose. This event encouraged me to produce a more detailed write up of that presentation which included all aspects of direct marketing as regulated by UK data protection law.

If any reader has any comments please contact Dr. Chris Pounder

Tel (DDI): +44 (0) 20 7490 6605

Fax: +44 (0) 20 7490 2545

E-mail: chris.pounder@masons.com

Marketing: The Key Issues

Introduction

Access to a global market-place, the increasing use of electronic means of payment and other e-commerce related activities has intensified a problem. On the one hand, for instance, the use of this technology has provided each organisation performing marketing (the "Data Controller" to use the correct jargon) with the ability to track its customers' behaviour and monitor shopping habits in great detail.

This has permitted new ways of exploiting such data and increased the effectiveness of targeted marketing. For example, it is a relatively straightforward matter to track domestic use of the Internet and record which web-sites have been visited. The analysis of these visits and pages scanned

provides intelligence as to what goods and services a particular individual may be seeking and hence provides the potential to customise marketing offers based on recorded patterns of behaviour. In the USA, for instance, it is possible to tailor marketing offers which are displayed on a web-site to match the known use of the Internet from a particular machine (e.g. by tracking the Internet Protocols used).

On the other hand, such use of personal data by a Data Controller is viewed by some customers ("Data Subjects" in jargon-speak) as a gross invasion of individual privacy. Viewed from this perspective, the technology which improves targeting, is considered as facilitating unwarranted surveillance which even intrudes the sanctity of the home. How can "an Englishman's

home be his castle" when each electronic foray over the ramparts is recorded, analysed and digested by others?

This article explores the main rules which apply to the processing of personal data for a marketing purpose. There are several broad headings to consider, for example: the kind of information which needs to be provided to customers at the time of obtaining personal data; the circumstances when it is advisable to seek consent of the customer for a marketing purpose, and the need for Data Controllers to abide by procedures set out in important Codes of Practice. In Part I, these and other topics are explored in the context of the Data Protection Act 1998 which gives effect to the Data Protection Directive (95/46/EC). In Part II, these topics are further considered in

the context of the "Telecommunications (Data Protection and Privacy) Regulations 1999" (SI. 1999 No. 2093); the Regulations which give effect to the Data Protection Directive (97/66/EC) and its provisions relating to telemarketing.

It is important to understand that the stakes can be high. If a Data Controller, for example, processes personal data either unfairly or unlawfully then there are powers in the Act which could cause that processing to cease - and that embargo could extend to all Data Subjects affected by the same problem as the single complainant. In worst case scenarios, this could result in the destruction of entire databases, or the expense of seeking consent of all Data Subjects for the marketing purpose, or re-collecting the personal data, or the enforced abandonment of an important marketing campaign. Note in this scenario, nobody is prosecuted or fined - however, the commercial value of the marketing campaign is reduced to a big round zero.

In this article the phrase "marketing purpose", unless specified in the text, has been used as a convenient shorthand for **all** marketing related activities in **all** its guises (e.g. by e-mail, post, phone, fax) **including** host mailing for the benefit of Third Parties or list rental.

The Principles and direct marketing

The two Principles which are of particular relevance to this analysis of the marketing purpose are the First (especially the fairness of the processing for a marketing purpose) and the Second with respect to disclosure of data to Third Parties for a marketing purpose. The consideration of the lawful processing arm of the First Principle is also important; this will primarily focus on the application of the law of confidence, and whether prior consent of Data Subjects for the marketing purpose has to be obtained

(e.g. to legitimise the processing in terms of Schedules 2 and 3).

However, other Principles can also become important. For example, in this latter regard, a breach of the lawfulness arm of the First Principle can also lead to a breach of the Seventh Principle which contains an obligation for Data Controllers to take appropriate organisational measures "against unlawful processing". So, for example, the Seventh Principle could be breached if a Controller's senior management fails to arrange for the appropriate organisational measures to protect personal data from, for example, that processing which could infringe copyright. Additionally, the Eighth Principle could apply to any transfer of personal data outside the European Economic Area pursuant to a marketing purpose. Failure to satisfy a Data Subject's right to object to the processing of personal data for a marketing purpose would also constitute a breach of the Sixth Principle.

Fairness

However, in the context of marketing, it will be the fairness requirements of the First Principle which will be the most familiar; these are similar to the fairness obligations under the First Principle of the 1984 Act. Under the latter Act, sources of personal data, usually each individual customer concerned, had to be notified of any marketing purpose **prior** to the obtaining of the personal information. Usually such choices were presented to customers at the time of collection of personal data (e.g. on an application or web-site form) by means of a familiar fair processing notice and "opt-out" combination (e.g. "Please tick the box if you do not want your data to be used by us or selected Third Parties for a marketing purpose? []").

We remind readers that in our last issue (DPPP 2) we noted that the Commissioner

has stated in a letter that "I am minded to take the line, once the new law comes into force, that the provisions of an opt out box by those collecting personal data for direct marketing as a secondary use will be mandatory".

Although many of these fair obtaining statements associated with the 1984 Act will also satisfy the requirements of the First Principle of 1998 Act, compliance cannot be taken for granted. As will be seen, data protection officers should consider the fairness obligations of the First Principle afresh, in the context of a revised interpretation of the First Principle. This states (in Schedule 1, Part II), that if a Data Subject (e.g. customer) is providing the personal data, the Data Subject must at the point of contact with the Data Controller be made aware, before any personal information is provided to the Data Controller, of:

- "the identity of the data controller" (i.e. the person who is collecting the personal data for use in its marketing purpose). This normally does not create a problem as often the identity of the Data Controller is clearly described as providing the service being offered or advertised. In practice, this identifying information usually takes the form of a name (e.g. of the company providing the goods or services) which the Data Subject can use, if need be, to make contact with the Data Controller (e.g. to register an objection to the marketing purpose). Where this obligation can create confusion is where the Data Controller cannot be clearly identified because the identity has been associated with a strong brand name; for example the use of the brand name "Virgin" in the UK does not immediately identify the particular Data Controller in the Virgin Group, because this brand covers a number of diverse companies offering a wide range of services. Occasionally, there might be

issues of recognition if a Data Controller uses a service provider (i.e. a Data Processor) to collect personal data. In such circumstances, it is important to insist (e.g. in a contract with the Data Processor) that the Data Controller is specifically identified. It is the Data Controller's responsibility to check that the procedures for collecting personal data adopted by the Data Processor provide for an appropriate and complete description of the Controller's marketing objectives

- **"if he has nominated a representative for the purposes of this Act, the identity of that representative"**. Note that if the Data Controller is based outside the European Economic Area (e.g. in the USA) and is performing the processing for a marketing purpose in the UK, the Data Controller **must** still be identified as such. In addition, the representative **must** be identified as acting on behalf of that Controller and it is important to avoid any confusion in the minds of Data Subjects as to who is the representative and who is the Data Controller. Failure to identify this clearly could also result in a breach of the Eighth Principle if the personal data were to be transferred outside the EEA. Note that if a Data Controller is based outside the EEA, it is advisable to identify, in any fair processing notice, the country or territory where that Controller is established. If there is a properly constructed fair processing notice which includes the description of the location of the Data Controller, and if a Data Subject consents to the Controller's marketing purpose, then there would be no need to assess the adequacy of the Third Country to which personal data are transferred, as the consent to the marketing purpose would also carry with the consent criteria which is required by Schedule 4 of the Act
- **"the purpose or purposes for which the data are intended to be processed"** (e.g. if the personal data are to be disclosed to other Third Parties for their marketing purposes). This obligation is reinforced by the provisions of the Second Principle which calls on a Data Controller to have regard "to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed". Thus, a Data Controller should know **before any disclosure** to a Third Party whether that Party will process the Controller's personal data for a marketing purpose. It then follows that the issue before a Data Controller is whether it should inform Data Subjects as to the identity of each specific Third Party performing the marketing (e.g. "your details are disclosed to Acme Heating Ltd for its marketing purpose"), or whether a general description of the Third Parties will suffice (e.g. "your details are disclosed to selected companies in the energy retail sector for their marketing purpose"). In practice, it could be either; it all depends on the nature of the personal data processed, the products marketed and the Data Controllers performing the processing (factors which are discussed later in this analysis)
- **"any further information which is necessary"**, having regard to the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair". To put it bluntly, in data protection terms, this opens a Pandora's Box, as the phrase is unspecific and its meaning will be dependent on the circumstances of each Data Subject. Given that most marketing campaigns are intended to involve thousands of Data Subjects, an approach based on providing the **minimum** information to customers will always run the risk of **not** complying with this Principle with

respect to those Data Subjects whose specific circumstances require further information to be provided. In short, a Data Controller will need to collect all relevant information about the processing and select what needs to be provided to Data Subjects; in short anything which would raise the eyebrows of that proverbial man on the Clapham Common Omnibus

Finally, in relation to fair processing, Data Controllers will need to consider how the fairness rules with respect to the marketing purpose relate to the other information which will need to be provided to Data Subjects. For example, personal data collected by a financial institution will probably be processed for the financial service on offer as well as for fraud prevention, credit scoring, debt tracing and other administrative purposes; such purposes will have to be described in the fair processing notice. In addition, there will be other "non-data protection" information to give on such forms; for example, with respect to the Controller's distance selling obligations or to consumer rights. It is not an understatement to say that the message conveyed by a fair processing notice about the processing of personal data for a marketing purpose, if it is to remain fair, **must not be submerged**.

What "further information?"

It is worth exploring the nature of this "further information". For example, suppose a Data Subject provides a name and address and agrees to a fair obtaining statement which said "we wish to contact you to provide you with information concerning the excellent goods and services provided by Acme Heaters Ltd"; is that Data Subject expecting a home visit from the sales-force or some sales literature sent, in the mail, to the home address? Given that the general expectation would be the latter, the "further information" which is

necessary to guarantee fair processing will be that information which clarifies the particular marketing approach that an individual can expect if personal data are provided; for instance, in the example, that contact is to be made by home visit. In general terms, therefore, the mode of contact will be important (telephone, fax, email or post) and if this mode is not specified, it will be that which is most obvious (e.g. if a Data Subject provides a home address, then the expected form of contact will usually be 'by mail').

This separation of mode of contact is very important on other grounds. Failure to specify contact by telephone, for example through the use of a generally phrased opt-out, might mean that under the specific Regulations that such contact cannot be made without seeking the prior consent of the customer (however, more of that in Part II). Even the stance adopted by the Data Protection Registrar (under the Data Protection Act 1984) relating to telemarketing was beginning to settle on the firm position that such prior consent was needed.

A problem then arises as to the popularity of the different modes of contact for the marketing purpose as there is a considerable body of research which indicates that telemarketing is the least popular (especially when the phone called is ex-directory). The reason for this can be explained easily: direct marketing by post is less intrusive because a Data Subject can decide when (or whether) to open the marketing communication; with a phone call, the Data Subject has to interrupt current activities to answer the phone (merely in order to silence the ringing tone). So if such customers are presented with a choice of "we wish to contact you by phone and mail" they may decline the choice of both because they do not want to be phoned, even though they would not object to communications sent by mail.

Does this mean that the First Principle is requiring a separate "opt-out" box for each mode of communication? Answer "No" - data protection considerations only require the provision of information about the mode or modes of contact. How this is presented to Data Subjects is currently a matter of choice for the Data Controller - but as can be seen, it is important to consider the consequences of a choice which combines options. Note that Data Controllers who rely on list brokers for the personal data to support their marketing promotions should always ensure that any list rental warranty covers the envisaged the type of marketing, the method of contact and of course the type of product to be marketed (but more of this latter point later). Note that if the mode of contact is not mentioned, it will default to the obvious one - and if an name and address is held, this usually means post.

Fair and Prominent

When an opt-out is presented on a fair processing notice, it must be located in a prominent position with a reasonably large font size so that there can be no possible claim that the opt-out has been constructed so that it could be easily overlooked. In addition, the language describing the opt-out must be simple to understand yet comprehensive; application and web-site forms should also be designed so that they specify what information is to be used for the marketing purpose.

These requirements were established in the Linguaphone Tribunal Decision ("*Data Protection Registrar v. Linguaphone Institute Limited*" (case reference DA/94 31/49/1)) under the 1984 Act. This and other Tribunal Decisions remain relevant because **all** the fairness elements of the First Principle of the 1984 Act are also found in the First Principle of the 1998 Act.

In looking at the text of fair processing notices which were appearing in newspaper advertisements promoting Linguaphone's products, the Tribunal was "concerned that the opt-out box appears in minute print at the bottom of the order form". The Tribunal concluded that "the position, size of print and wording of the opt-out box **does not** amount to a sufficient explanation to an enquirer that the company intends or may wish to hold, use or disclose that personal data ... for the purpose of trading in personal information" (our emphasis).

Such an opt-out must be provided in all forms of marketing methods employed, including TV and radio advertising if need be. This was established in the Innovations Tribunal Decision ("*Data Protection Registrar v. Innovations(Mail Order) Limited -Case DA/92 31/49/1*"). Here the Tribunal noted that "Whilst there may be some difficulty in communicating a comprehensive warning in radio, television, satellite or telephonic advertisements we did not consider these sufficient to justify excluding these forms of promotion from the general obligation to give a warning prior to obtaining.... We concluded that it was possible to contain within any form of advertisement currently available a statement informing of the purpose to trade in names and addresses".

Finally, on this topic, further information might relate to the right to object to the marketing purpose. In the Commissioner's letters obtained by DPPP (and reported last issue), the Commissioner also notes that "We take the view that in order to process personal data fairly, a data controller **must** make the individual aware of the right to object to processing of the data for direct marketing" (our emphasis) and that "If the individual is returning a form to the data controller but the data controller requires the individual to write separately to exercise the right to object rather than simply tick a box on the form, we find it difficult to come to any conclusion other than that the data controller is deliberately putting an obstacle

in the way of the individual exercising the right to object". To make the point, the letter adds that, in the Commissioner's view, the Data Controller "is thereby processing personal data unfairly".

Provision of information to new customers

It's worth summarising the approach taken above by analysing a worked example - a draft data protection notice for a web-site for a normal, unexceptional, small to medium sized enterprise which undertakes routine "boring" processing.

In explaining the elements of the fair processing notice below, note that the phraseology has to be carefully parsed to tease out any inferences. It is **very important to do this**. Any ambiguity could render the notice unreliable as a fair processing notice with the effect that the personal data could not be processed for a marketing purpose without further action (e.g. processing must halt until all existing customers have been contacted to seek their consent to an unambiguous marketing purpose). Note that this could render the personal data unusable and cause the "death knell of a marketing campaign" (with a P45 for that "very special person", perhaps?).

The following draft web-site fair processing notice contains a number of options in square parenthesis and uses the personal pronoun "I" to address the Data Subject. The notice reads as follows:

"I am willing to allow details which relate to my use of this web-site to be processed by Acme Heaters Ltd (AHL) in order to improve the efficiency and effectiveness of this site(1). In addition, I agree that these details and my contact information can be used by AHL and [forwarded to(2)] [or used by(3)] selected Third Parties [within the

domestic energy home-heating sector(4)] [including Parties based outside the European Economic Area(5)]. I understand that these Third Parties may contact me by [phone, fax, e-mail or mail(6)] in relation to goods and services which may interest me, and that I can choose not to be contacted by ticking the box? []".

The comments, which relate to the superscript numbers in the fair processing notice, are as follows:

- 1 This phrase permits the use of personal data so that a Data Controller can, for example, monitor traffic/transaction data in order to improve **only** the site visited (i.e. no other web-site). Note there is no opt-out offered to Data Subjects with respect to this "improvement" purpose; it could be that the Data Controller considers that such monitoring is essential in ensuring that contracted service levels are met (e.g. response times at the web-site), or that the offering of an opt-out is inappropriate for other reasons (which can be justified if challenged). If the Data Subject agrees, such traffic/transaction data can be also used as a selection criteria with respect of marketing (established by the first clause of the second paragraph.) Finally, note how other Principles can relate to the processing of personal data for the purpose of improving "the effectiveness of the site"; this does not mean the personal data can be retained indefinitely for this purpose (breach of Fifth Principle), as such processing can also be excessive for the purpose (breach of Third Principle)
- 2 This phrase covers the situation where there is a disclosure of personal data to a Third Party for its marketing purpose (e.g. by a sale of a list). It is clear that the Third Party then has the capability to make contact and send out the mailing
- 3 This phrase would cover the situation where there is no direct disclosure as described by (2) but where there is a host-mailing by AHL on behalf of the third party for a marketing purpose. Care may be needed with respect to "indirect disclosure" - a matter which is discussed later
- 4 This phrase would limit the types and goods of services marketed to those within the domestic energy heating sector; it would not permit the processing of personal data to support the marketing of other goods and services (e.g. car insurance)
- 5 This phrase covers the situation where the Third Party processing the personal data for a marketing purpose is based outside the European Economic Area (EEA). If this text is removed, there would be an implication that there is no direct disclosure of personal data to a Third Party outside the EEA. Also, if transfers were to arise, there is an implication that there is nothing exceptional or "dodgy" about the country outside the EEA (i.e. there is no transfer of personal data to a country which offers an inadequate level of protection). If the latter case arose, we would expect that 'inadequate' countries could well need to be identified (i.e. the transfer to specific processing locations would constitute "further information" which was necessary to give Data Subjects in order to guarantee fair processing)
- 6 The mode of contact with the customers has to be specified and in this case four modes have been linked to

itself. Note that the general nature of the Third Party implies that there is no specific Third Party who by reason of identity, location, or goods and services should be drawn to the attention of Data Subjects

one opt-out box. Note that the wider the scope of the marketing purpose described by the notice the less attractive it might appear to some Data Subjects - which of course minimises revenue from list usage. In this case, for example, a Data Subject who hates the idea of telemarketing has no choice but to opt-out of all marketing.

Marketing own products to existing customers

Does one need to contact each customer and obtain consent for the marketing purpose in every instance? Quick answer "No - but read the following carefully".

The main problem with respect to the marketing purpose does not arise from obtaining permission for the marketing purpose from **new** customers (who can be readily informed of this purpose when they provide their personal data) but from **existing** customers who were **not** informed of the marketing purpose at the time of obtaining. The stark problem often facing data protection officers is offering advice on a simple question: "Can we use our personal data for a marketing purpose?".

The first key point is that the Data Protection Act **does not** require consent for a marketing purpose in **all** circumstances. This was established under the 1984 Act by a Tribunal Decision ("*Data Protection Registrar v. British Gas Trading Limited (BGTL)*"), where the Tribunal noted that with respect to goods and services traditionally provided by BGTL, it was **not unfair** for BGTL to process (but "not to disclose to" Third Parties for its marketing purpose) personal data in order "to promote such goods as are from time to time stocked for retail sale in shops and showrooms". Similarly, the Tribunal did "not find that BGTL unfairly processed personal data" in order to send letters to customers about its plans to supply electricity. However, such processing was only fair "on

the basis that BGTL will continue to offer customers an opportunity to 'opt-out' from receiving direct marketing mail" (e.g. customers can object to such processing at any time, and that this decision must be respected).

This position can be substantiated under the First Principle of the 1998 Act if a Data Controller wants to use customer data to market its own range of products and services even if its customers are unaware of this purpose. For instance, assume that there is nothing special about the personal data (e.g. the data do not comprise Sensitive Personal Data) which are intended for use for this limited marketing purpose, **and** further assume that the product sold is of a similar nature to that which Data Subjects have already ordered, then this marketing purposes could be legitimised in terms of paragraph 6 of Schedule 2, on the grounds that the processing was "in the legitimate interests of the Data Controller" (e.g. to maximise revenue). The Controller can take into account the "legitimate interests of the Data Subject" by offering an opt-out at any time; and the fairness processing issues would be satisfied if the Data Controller wrote to the Data Subject 30 days or so **before** commencement of the processing for a marketing purpose. This fair processing notice would specify the limited nature of the marketing purpose, the identity of the Controller and offer customers an easy way of objecting to, or opting out of, the purpose.

Note that the assumptions associated with this procedure are important; a Data Controller **could not** rely on this mechanism if there was something "unusual" about the Data Controller (e.g. if the Data Controller was a monopoly supplier), or the processing (e.g. if confidential personal data were to be processed) or the product sold (e.g. if the products marketed were significantly different to the products which Data Subjects had already obtained from the Controller).

The meaning of "consent"

"Consent" in some circumstances will be needed to legitimise a marketing purpose. Unfortunately consent is not a defined term in the Data Protection Act; however, since it is defined in the Directive (in Article 2(h)), the Data Protection Commissioner will be guided by this definition if an interpretation is needed (e.g. as in relation to the use of consent in Schedules 2 to 4). In further detail, "*Data Subject's consent*", as defined in the Directive, means:

"any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

The BGTL Tribunal adjudication (referred to previously) came close to this definition of "consent", in particular, "consent" having to be expressed in terms of a positive indication of the Data Subject's wishes. However, the Tribunal noted that this positive indication can be expressed with a negative statement (and in many circumstances it is often normal to express consent negatively; for instance, as in "No. I do not want this to happen."). The Tribunal noted that "we do not consider that it is sufficient merely to send to the customer a leaflet providing them with an opportunity to object to their personal data being processed for purposes beyond those gas related purposes". If, however, "the customer returns a document to BGTL, or by other means of communication received by BGTL indicates consent" or "by not filling in an opt-out box, or other means, indicates no objection" then the processing will be fair because the informed consent of the Data Subject had been obtained.

The amended text of the Enforcement Notice, approved by the Tribunal, which was finally served on BGTL makes clear what will **NOT** suffice for consent: "consent shall not be inferred from the failure of any person to

return any leaflet or other document containing an opportunity to opt out". Therefore, sending a leaflet which says "we wish to use your personal data for a marketing purpose; if we do not hear from you we assume you have consented" **is not consent**. However, the return of a form by the Data Subject which contains an opt-out can be considered a valid positive indication of the negative wishes of the Data Subject, so long as the opt-out is also fair (e.g. the use of the opt-out is connected to a properly constructed, fair processing notice which is located in a prominent position on the form).

As an aside, there is an important inference which arises from the Tribunal statement (quoted above) which we have italicised: "we do not consider that it is sufficient merely to send to the customer a leaflet providing them with an opportunity to object to their personal data being processed for purposes beyond those gas related purposes". In other words, such an approach (i.e. sending a leaflet) **could** be fair in the case of "gas related purposes". This reinforces our "similar products" observations which have been presented under the paragraphs associated with "Marketing own products to existing customers" (see above).

In the context of a marketing purpose, it should be anticipated that some Data Subjects who have consented to a marketing purpose will withdraw that consent at some later stage. If this happens, a Data Controller should always take this to mean that the Data Subject concerned has exercised his right to object to the marketing purpose.

Finally, two comments on English law. Consent has always been considered as requiring a positive action on the part of the person who is consenting. Second, where there is doubt as to whether an individual has consented or has withdrawn consent (e.g. a Data Subject who consents in

January, withdraws consent in February, consents in March etc), the last indications of wishes will prevail. Note that this position has meant that the notion of "implied consent" has always rested on difficult legal grounds.

Consent and the marketing purpose

There are a number of areas where the prior consent of the Data Subject would be advisable if a Data Controller was planning to process personal data for a marketing purpose (especially a marketing purpose which involves list rental, host mailing and the marketing of dissimilar products).

Firstly there are the circumstances which have already been identified by previous Tribunal Decisions under the 1984 Act as requiring consent (e.g. Linguaphone and Innovations; references above). In both these cases, the companies concerned knew that personal data would be processed for a list trading purpose **before** obtaining personal data from Data Subjects. However their procedures notified Data Subjects of this purpose **after** collection (e.g. in a notice given to Data Subjects which was enclosed with the product they had purchased). In the Linguaphone case the Tribunal was especially severe with respect to those personal data which were subject to the company's procedure of providing notification **after collection**. It wholly rejected the argument that it was fair to require "a person not making an order and who does not wish their name to be marketed ... to send a blank form back to the company". It concluded such a procedure "places upon the Data Subject the responsibility for taking positive action whereas the Tribunal holds that the responsibility rests upon the Data User to obtain **the Data Subject's positive prior consent**" (our emphasis).

Thus, if Data Subjects are **not** informed of a non-obvious marketing purpose which involves list rentals or host mailing so that Third Parties then the prior consent of the Data Subject has to be obtained before the personal data can be processed by the Data Controller for a marketing purpose. Such consent **must** involve some positive indication of the Data Subject's wishes although that positive indication can be by means of an opt-out (e.g. when the Data Subject returns a form containing the fair processing notice to the Data Controller). Attempts at "implied consent" where the Data Subject takes no action **will generally fail** (e.g. a letter which says "if you don't respond within 30 days we shall assume you agree to the use of your personal data for the marketing purpose" **cannot** be relied upon to mean consent).

Confidential data

Explicit consent of each Data Subject will be needed if Sensitive Personal Data (e.g. medical records, religious beliefs) are to be processed for a marketing purpose. This is because the processing of such Data have to be additionally legitimised in terms of the categories listed in Schedule 3 of the 1998 Act and the most likely option, in the context of the marketing purpose, is that processing has to be legitimised in terms "explicit consent". Much as marketing departments would like, it is **not** in the "vital interests" of the Data Subject to receive promotional material!

Consent will also be needed where the personal data to be processed for a marketing purpose are subject to a duty of confidence (e.g. personal data relating to an individual's financial affairs). Under the 1984 Act (and the 1998 Act is no different), the First Principle requires personal data to be processed "lawfully", in particular, in accordance with the common law of confidence. According to well-established advice issued by the Data Protection

Registrar with respect to the 1984 Act, this generally means that the processing of personal data has to be justified in terms of one of three criteria:

- **first** that the processing is required because the Data Controller is under a statutory obligation to process (e.g. a particular disclosure of personal data is required by law)
- **second** that there is a public interest in the processing which should outweigh a duty of confidence (e.g. the processing of personal data is necessary to prevent serious crime, or to safeguard national security, or to prevent serious physical harm to any individual); or
- **third** that the processing has the fully informed consent of the Data Subject.

Since it is unlikely that the processing of personal data for a marketing purpose will be justified in terms of a statutory obligation or in the public interest. It follows that processing must be made lawful by obtaining consent.

In the BGTL case, the Tribunal reinforced this view. It concluded that such a duty of confidence "may in appropriate situations inhibit use as well as disclosure" (e.g. for a marketing purpose) and provided examples of personal data where such a duty of confidence applied (e.g. "information relating to crime, tax, benefits, health and welfare"). We would add that most people expect personal data describing their financial affairs (e.g. data relating to income, problems with late repayments) to remain confidential - an important consideration if a marketing initiative uses such personal data (e.g. collected from a web-site which monitors financial activity).

However, in the case of BGTL, the Tribunal added an important clarification: it stated that "a duty of confidentiality is unlikely to arise generally from the ordinary relationship

of the supplier of goods and services and his customer, although there may be special circumstances in which this might arise with particular customers". This is an important statement if Data Controllers are considering using personal data stored in run-of-the-mill accounting systems for a marketing purpose. Here, the Tribunal is saying that consent is **not** an automatic prerequisite on the grounds of confidentiality unless of course, there are specific grounds for considering the personal data to be considered as being subject to a duty of confidence.

Unfortunately, the sting in the Tribunal's statement is the use of the qualifying phrase "special circumstances" - what does this mean? For instance, suppose a Data Controller is deciding whether or not to process basic personal data (e.g. from a billing database) for a marketing purpose how can it be sure that, lurking in a general customer database of thousands of names, there are no cases with "special circumstances" to which a duty of confidence could apply? Unfortunately the Tribunal was not expansive on this issue, and this can lead to uncertainty. However, we can suggest that the main "special circumstances" will be case-by-case considerations which are associated with, for example, personal data relating to well known public figures or celebrities, or data which reveals phone numbers of customers known to be ex-directory, or marketing activities which are based on patterns of consumption of goods and services which could infer a specific lifestyle or medical condition.

Common sense consent

Plain "common sense" (a dangerous phrase often used by politicians) indicates that consent for the marketing purpose is likely to be a prerequisite in the following circumstances:

- **if a code of practice** which applies to the Data Controller requires consent to be obtained. For example, the Banking Code of Practice (1998 revision) states that "Unless you specifically request it, or give your express consent in writing, we will not pass your name and address to any company, including other companies in our group, for marketing purposes". The point being made here that it is irrelevant that consent might be required on grounds of confidentiality - here the Code is setting out circumstances when consent **must** be sought - otherwise the Code is breached
- **if other legislation or if another regulator** requires the seeking of consent to the processing of personal data for the marketing purpose
- **if the Data Controller is providing a monopoly service** as is often the case where personal data are processed by the privatised public utilities. The point here is that the provision of information to Data Subjects about the marketing purpose is to provide Data Subjects with a choice, in effect, allowing them to decline to provide their personal details and to walk away from the Data Controller's service offerings. However, in the case of a monopoly supplier, the Data Subject cannot decline to provide personal data (or to walk away from the Controller). For example, a monopoly supplier (e.g. in the water industry) cannot satisfy the fair processing requirements by providing a notice to Data Subjects which effectively says: "we wish to use the information you provide for a marketing purpose, and if you don't like this purpose, you can always get your water from someone else".

Seriously considered consent

Consent for the marketing purpose will need serious consideration in the following circumstances:

- **if the personal data is linked to products or events which could cause offence or embarrassment** (e.g. marketing of condoms or incontinence pads, or processing which could reveal certain confidential information in foreseeable circumstances). Problems in this latter category, one should add, are not uncommon and many revelations are often made inadvertently in the name of “offer a friendly face to the customer”. For example, a marketing letter from a Hotel Group might commence: “we hope you enjoyed your stay in our London Hotel in September and, as a valued customer, we want to offer you a special discount on another double room”. Unfortunately this sort of letter can sometimes get in the hands of the “the other-half” who might enquire of the Data Subject “can you explain your stay in Hotel X when you said you had to go on a business trip abroad?”
- **if the marketing initiative involves the promotion of products to children;** in which case the consent of a parent or guardian must be an important consideration. The issue often arises with sports and fan clubs which often obtain personal data from youngsters (e.g. under sixteen). For example, it would be embarrassing to say the least, if such young Data Subjects were to obtain information on cigarettes, credit cards, alcohol, loans etc, when the recipient of the marketing communication is not old enough to drink, smoke or enter into a contract for a financial service.

“Give me five” for consent

There are five other important considerations associated with Data Subject consent. These relate to the following circumstances:

- **consent to the marketing purpose only ensures compliance with the First Principle.** In the BGTL case (under the 1984 Act), the Tribunal considered a hypothetical case in which “excessive data was held in breach of the fourth data protection principle, or inaccurate data in breach of the fifth data protection principle”. The Tribunal concluded that “this would not absolve the Tribunal from examining whether when particular processing was undertaken using excessive or inaccurate data it was unfair”. Expressing this ruling in terms of the 1998 Act: to process excessive personal data in breach of the Third Principle can also be a breach of the First Principle in terms of holding (i.e. unfair processing) of such data. The corollary will also true: even if personal data are processed fairly (e.g. with the consent of the Data Subject), this does not absolve the Data Controller from complying with the other obligations and Principles (e.g. security obligations; applying Codes of Practice dealing with updating personal data; relevance of the personal data to the marketing purpose). In short, all the Principles are separate entities and must be considered in the context of the processing
- **consent does not legitimise the processing in every case.** For example, if the law does not expressly permit the processing of personal data for a marketing purpose (this is often the case faced by Data Controllers within the public sector), then obtaining consent for this purpose does not make the processing lawful. This position was agreed by the BGTL Tribunal who said

that: “If we had found that the British Gas Corporation had done acts beyond its statutory powers then we would, for the purpose of deciding if there had been a breach of data protection principles, have regarded such acts as unlawful”. In other words, consent cannot make up for a lack of statutory powers

- **registration (or notification) is not a substitute for consent.** Some Data Controllers (believe it or not) still cling to the myth that if a marketing purpose which involves list trading and host mailing is registered with the Data Protection Commissioner, then that purpose can proceed on a legitimate basis. This fallacy was debated before the BGTL Tribunal which noted that “The fact that processing when undertaken could be used for a registered purpose does not in our view render the processing fair when it is established it was not in fact carried out for a purpose to which a data subject had agreed”. The same arguments will apply under the 1998 Act
- **when consent should be refreshed.** The Banking Code (1998 revision), for example, provides for this kind procedure; it states that “when you become a customer, we will give you the opportunity to say that you do not wish to receive this (marketing) information” and that “We will remind you, at least once every three years, that you can ask not to receive this information”. For example, fair processing notices are often prominently stated on application forms which are returned to the Data Controller - so how can the Data Subject remember the extent to which consent has been given? The general question thus posed to Data Controllers is “when a Data Subject consents, is that consent for ever and ever amen - and if not, what is to be done?”. A

prudent Data Controller should thus anticipate that a failure to refresh consent might, over time, invalidate consent; perhaps Data Subjects could be periodically reminded that they can exercise their right to object to the marketing purpose at any time. Note that procedures like this are very easy to design into a system, especially when the Data Subject has regular contact with the Data Controller (e.g. home banking)

- **where indirect disclosures associated with a marketing purposes need to be brought to the attention of Data Subjects.** An example of indirect disclosure will be helpful. Suppose an organisation approaches a Data Controller to perform a promotion on its behalf (e.g. mail out a leaflet), and suppose further that the organisation identifies particular criteria to target those who are to receive a particular mailing; such an organisation might say “our targets are single women, no children, under 35, employed with a salary over £30,000”. Note that in our illustrative example, the Data Controller **does not directly disclose** personal data to the organisation wanting the mailing; all the Controller does is select qualifying Data Subjects from its personal data and mails them with the marketing material in the post. However, in this case, any woman who responds to this targeted mailing (because the response is sent to the organisation requesting the mailing) will be also identifying her salary range, age, marital status and family circumstances **(the indirect disclosure)**- probably without knowing it. In the BGTL Tribunal’s view, fair processing required that “where any marketing or promotion is undertaken on behalf of a third party based on selected criteria, the data subjects so circulated are sufficiently informed of the basis of selection”. In this way the

Data Subjects will become aware “of what information arising from the relationship of gas supplier and customer, may be disclosed to a third party if they respond to the marketing or promotion”. **Note:** this comment from the Tribunal is made in the context of providing an opt-out for the marketing of similar products and services. Consequently, where other factors could be involved (e.g. where an indirect disclosure could reveal personal data subject to a duty of confidence), then seeking the consent of the Data Subject to the marketing activity becomes, in our view, **essential**.

Right to object

From October 24th next year, Data Subjects will have a right to object, on request, at any time and at little cost (other than a postage stamp), to the processing of personal data for any marketing material directed at them (Section 11 of the Act). This right to object extends to **any** kind of marketing (e.g. package inserts with bills, promotional material stapled to pay slips) and Data Controllers will be well advised to alert Data Subjects to this right as part of the appropriate fair processing notice. This right is an absolute right; there is no exemption and a Data Subject does not have to give a reason for objecting. If a Data Controller receives a request to cease processing for direct marketing purposes, he must comply as soon as reasonably practicable. This will require Data Controllers to have systems and procedures in place to flag all requests as soon as they are received. These “stop lists” **must** then be used subsequently and thus be accessible to all staff preparing personal data for use in a future marketing campaign. Stop-lists of objectors should always be compiled in a form which facilitates their use in conjunction with other stop-lists, such as those organised by the Preference Services (see below).

The right to object has to be exercised formally in writing and this may occur in many ways. For example, an individual might scribble on the envelope “don’t send me any more of this guff” or may even resort to more colourful or even rustic phraseology. Such objections should be treated as valid - they have been received in writing. Occasionally, an objection will be lodged by phone or be received from a person who is not the Data Subject. For example, if a Data Subject has “gone away” and the new occupiers of an address want to stop “junk mail” not addressed to them, or if the objector is acting on behalf of the Data Subject (e.g. a grandson objecting on behalf of his granny). In these circumstances, although the right to object might **not** have been formally exercised by the Data Subject, the application of the general fairness rules of the First Principle can have the same effect: it is unfair to process personal data for a marketing purpose (e.g. to send items of mail) when the Data Controller knows that there has been an objection to this purpose. In other words, the fair processing position established under the 1984 Act is maintained: thus **any objection** to the to the processing of personal data marketing purpose, **irrespective** of how it is received, should be subject to the standard procedure which has to be established to deal with objections directly from Data Subjects.

Although the right to object to the processing of personal data for a marketing purpose is specific to one Data Controller, difficult decisions will have to be reached as to whether a right to object to the marketing purpose received by **one** Data Controller relates to **other** Data Controllers in the same group of companies. If a group of companies promote themselves by using a strong brand image, trade-mark or rely on brand-name recognition, it will minimise the risks if an objection is treated as one which has been sent to “the brand” (i.e. extending to all companies associated with the brand).

Finally decisions will need to be taken as to the relationship between an “opt-out” which has been exercised and subsequent “opt-outs”. For example, suppose a Data Subject completes a form for a service from the Data Controller and ticks the no marketing “opt-out” box; the next month the Data Subject completes the same form again for repeat business and this time the “opt out” is not ticked. What takes precedence? Has the Data Subject said with the second unticked opt-out “I’ve changed my mind, please send me marketing material” or could it be “I’ve already opted out, so I have no need to opt-out again”.

Although the legal position is that the last specified wishes will prevail, it is safer to err on the side of caution, especially if it is ambiguous as to what those last wishes are. This is because there is always the data protection argument that any foreseeable ambiguous circumstances which relate to the processing of personal data can easily be resolved if “further information” is provided (i.e. in a fair processing notice). For example “Tick the box, **again if necessary**, if you do not want your personal data to be used to send you marketing material which we think you may be interested in”. If Data Subjects cannot be informed in a notice (or other method) a safe rule of thumb will be that a Data Subject who has “opted out” of the marketing purpose should need to positively “opt-in” at a later stage if a change of mind to the marketing purpose is to be substantiated by the Data Controller.

Can you seek consent for a marketing purpose?

The processing of personal data in order to send out a leaflet to seek the consent of the Data Subject for a marketing purpose is not, in itself, unfair. For instance, the BGTL Tribunal commented on the processing of personal data which is necessary to send Data Subjects a leaflet to alert them to the proposed use of their personal data for a

marketing purpose. It concluded that “The specific processing to achieve distribution of this leaflet could not in our view be said to be unfair processing, even if its content indicated that a firm intention had already been formed to send out marketing material promoting non-gas related supplies and services”. In other words, the processing of personal data to seek Data Subject’s consent for a marketing purpose cannot be treated as part of the marketing purpose. This position is logical; if processing to seek the consent of Data Subjects for a marketing purpose is part of the marketing purpose, this would require the prior consent of Data Subject; but then it would be impossible to approach Data Subjects for such consent!

This point was also discussed in a different guise by the Appeal Court in the case of Source Informatics Ltd (see DPPP No 2) who wanted to use anonymised data, extracted from confidential information contained in prescription forms, for a marketing purpose. The Court noted that “the processing required to render the personal data anonymous was clearly intended not to constitute processing operations which were subject to the principles” (of the Directive as the 1998 Act was not in force at the time). The Court concluded that “the anonymisation of data is in my judgement unobjectionable here under domestic law”, a clear hint that with respect to the 1998 Act, Source’s processing to render personal data anonymous so that they could be used for a subsequent marketing purpose is **not** part of the marketing purpose.

Note that if the Court had come to a contrary view (i.e. the anonymisation of personal data for use in a subsequent marketing purpose was part of the marketing purpose), then this step would require the application of the First Principle. Thus, in the case of the anonymisation of Sensitive Personal Data (e.g. health data), the Data Controller would have to obtain the explicit consent from Data Subjects (as required by Schedule 3).

One warning on this topic: the argument that one can process personal data to approach Data Subjects to seek their consent to a marketing purpose should **not be stretched too far**. For instance, a Data Controller might argue that Data Subjects should be fully informed as to the products which a Data Controller intends to market, and the best way to do this is to send them all the actual promotional material (in the name of “fully informed consent” - of course!). We believe that such procedures will be doomed - the processing described by the BGTL Tribunal relates to sending the customer a letter or leaflet containing a general, brief description of the range of marketing initiatives- not to the sending of a comprehensive marketing bundle about the products! Similarly, a Data Controller who bombards Data Subjects with repeated consent requests will have difficulty; it is unfair to process personal data in an attempt to harass Data Subjects into changing their minds.

Codes of Practice

There are two Codes of Practice which are relevant to the marketing purpose; the first is produced by the Direct Marketing Association and the second is the British Codes of Advertising and Sales Promotion, produced by the Advertising Standards Authority. This latter Code contains “List and Database Practice” rules which set out detailed procedures which are **in addition** to those that arise expressly from compliance with the Data Protection Act.

These rules, some of which are summarised below to give a flavour of content, apply to personal data held by:

- **List owners, brokers and users.** These persons should, for instance “ensure that their lists are run against the most recent quarterly Mail Preference Service Suppression File” or “be able to identify anyone who has

objected in the last five years, or who has not had an opportunity to object, to their inclusion on any list that is to be disclosed to others"

- **List users** In addition to the above, list users should "not use lists or selections from lists that are more than six months old unless they have been updated", "inform the list owner of any requested corrections", and "if asked, give the sources of names on their list".
- **List owners.** List owners should also "make corrections or suppressions themselves, or ensure that list users do, if mailing is delayed by more than six months", "require list users to inform them of requests for corrections", and "demonstrate their compliance with this Code".

The Codes are very important as they provide details as to when other Principles should be taken into account; for example, the rules which relate to "gone-aways" describe procedures which will also keep personal data "up to date". It is **very likely** that the Commissioner will be guided by these Codes, when assessing a Data Controller's approach to these Principles in the context of a marketing purpose.

Preference Services

The direct marketing industry has long recognised that to send marketing material to those who don't want to receive it is a waste of resources and a source of aggravation. That is why the industry, in the early 1990's set up a Mail Preference Service (MPS) and later a Telephone Preference Service (TPS); this has been augmented by Fax Preference Service (FPS) and an E-mail Preference Service (EPS). All these Preference Services offer the same simple function; they provide organisations, at moderate additional expense, with a list of those who don't want "junk mail" or "junk calls". If it

came to an investigation, failure to use these readily available Services could count against the Data Controller, and make it harder for the Controller to argue that the processing of personal data was fair; this is especially the case since the Codes of Practice identified above recommend the use of such Services. As will be seen in Part II of this analysis, there are specific statutory rules which relate to telephone and fax for any **unsolicited** direct marketing activity; and that in some cases, these rules apply to legal persons (e.g. companies which object to their fax machines being used to receive **unsolicited** marketing material). **Note:** statutory rules with respect to marketing by e-mail are a distinct possibility.

In further detail, the "Telecommunications (Data Protection and Privacy) Regulations 1999" impose upon the Director General of Telecommunications (OFTEL) an obligation to maintain a record of the fax numbers and telephone numbers of those subscribers who have indicated an objection to receiving **unsolicited** marketing material by fax or telephone. The Direct Marketing Association, which was providing these FPS and TPS services on a voluntarily basis, became the chosen provider of these services on a statutory basis. The Regulations impose **a legal obligation** upon every organisation sending **unsolicited** marketing material by fax or telephone to screen its lists against the FPS or TPS (as appropriate). Currently there is **no** statutory obligation to use MPS or EPS.

There are statutory time periods involved. For example, if a caller screens its lists at the start of the month and a subscriber subsequently registers with the TPS a week later, a call made to that subscriber will not be in breach of the Regulations because they provide a 28 day grace period to cover this kind of situation. If, however, the subscriber is contacted the following month - after the expiry of the 28 day period - the caller will be in breach.

Finally, the emphasis on the word **unsolicited** provides a clue as to the resolution of the data protection problems associated with the application of the Regulations: the Regulations do not apply if the marketing approach is **solicited**. And how is an approach solicited? By providing full information in a fair processing notice of course!

Summary of common problems

Unfair or unlawful processing of personal data for a marketing purpose usually arises under the following set of circumstances:

- if a Data Controller has issued a fair processing notice which does not fully describe the marketing purpose or has otherwise processed personal data which have been unfairly obtained (e.g. from a Third Party)
- if the personal data are confidential or comprise Sensitive Personal Data and the personal data are processed for a marketing purpose without the consent of the Data Subject concerned
- if a Data Controller continues to process personal data for a marketing purpose despite an objection to the purpose or has failed to use the relevant Preference Service; such processing can also constitute a breach of the Sixth Principle as being processing which does not respect the Data Subject's right to object to processing for a marketing purpose
- if a Data Controller claims adherence to the set of marketing rules outlined in a Code of Practice and does not comply with the Code
- if the personal data are processed unlawfully (e.g. in breach of copyright); many organisations think that because a list is in the public domain (e.g.

published in a directory, listing or Year Book) that the information contained therein is freely available for use for a marketing purpose

- if the personal data cannot, by law or other regulation, be used for the marketing purpose.

Key actions at a glance

Data Protection Officers should review all fair processing notices on application forms and on web-sites in the light of the requirements of the First Principle under the Data Protection Act 1998, as further information may have to be provided in order to ensure that processing is fair in all the circumstances.

Where there is an existing relationship between supplier and customer, consent of the Data Subject is not always a prerequisite to legitimise the processing of personal data for a marketing purpose which only involves the products produced by a Data Controller. However there are some circumstances when prior consent of Data Subjects will be needed to legitimise other forms of marketing.

Data Controllers are well advised to use the Telephone, Fax and Mail Preference Services and to adhere to all relevant Codes of Practice which are associated with the

processing of personal data for a marketing purpose.

Failure to comply with the First Principle (in particular) could result in serious delay to, or the termination of, a direct marketing campaign; personal data collected for a marketing purpose might become unusable for this purpose.

All the rules established by the Data Protection Tribunals with respect to the First Principle of 1984 Act will apply to the First Principle of the 1998 Act; the Data Subject's right to object to the processing of personal data for a marketing purpose in the 1998 Act will strengthen these rules.

Concluding thought

If a Data Controller is processing personal data unfairly or unlawfully, and if that Data Controller is "caught", the worst case scenario, from the business perspective, will not be the fines, enforcement provisions, investigations or even prosecution; the main effect is that personal data cannot be used for the intended (and usually immediate) marketing purpose. It is essential therefore to anticipate the need for a little contingency - just in case. For example, a prudent Data Controller, when planning a marketing campaign, would arrange matters so that it could identify the personal data which have been processed in relation

to that campaign. Thus, if there is a serious complaint about the processing, the personal data affected can be "ring fenced" and any remedial action limited to those data.

Mind you, if a Data Controller is processing personal data unfairly or unlawfully, and if that Data Controller has "not been caught" (yet) then it has some time on its hands to amend its procedures quietly and hope the breach will not be noticed. But be quick though, that market-busting complaint could arrive at any time.

Contact pointers

Contact with the Preference Services can be made by phoning **0207 766 4410** (MPS), **0845 070 0707** (TPS) and **0845 070 0702** (FPS). The DMA web-site, which has links to the Advertising Standards Authority, the DMA Code of Practice, and all the Preference Services, is "www.dma.org.uk".

Direct Marketing: Telecommunications

Introduction

Part II of this analysis considers the impact, on the marketing purpose, of the "Telecommunications (Data Protection and Privacy) Regulations 1999" (SI No 2093) which give effect to the European Union Telecommunications Directive (97/66/EC). The Articles of this Directive which relate to marketing were brought into force on May 1st 1998 through the enactment of the "Telecommunications (Data Protection and Privacy) (Direct Marketing) Regulations 1998" (SI No 3170); these were worded to mesh with the provisions of the Data Protection Act 1984. With the commencement of the 1998 Act (and the consequent demise of the 1984 Act), the 1998 Regulations had to be replaced; hence the 1999 Regulations which came into effect on 1st March 2000 to coincide with the commencement of the 1998 Act.

In the context of this analysis, the 1999 Regulations are very important because they impose restrictions upon the use of **unsolicited** telemarketing communications for marketing purposes. The fact that a "subscriber" is defined as a person who is a party to a contract with a telecommunications service provider for the supply of publicly available telecommunications services means that some data protection practices which apply to natural persons are extended to protect legal persons. This too could lead to some interesting "non-data protection" issues: for example, if a Data Controller has to have regard to an objection from a legal person with respect of telemarketing, why should an objection from that person be ignored in the case of marketing by mail? In summary, Part II deals with the essential effect of this legislation in the context of marketing; the analysis concludes with some "frequently asked questions" which brings together the sometimes complex relationship between the Regulations and the Act.

Since some readers may be aware of the content of the 1998 Regulations in detail, it is important to reassure them that, although the wording is different, the key effects of the 1999 Regulations are the same as the 1998 Regulations with just a few minor adjustments.

Meaning of "direct marketing"

There are two definitions of "direct marketing" to consider; one lurks in the Act and the other in the Regulations; it is important to determine whether none, one or both applies to any processing. In further detail:

- **Section 11 of the Act** defines direct marketing as "the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals". Since the Act applies to personal data this definition will apply if marketing calls are made to telephones used by particular customers, employees, contacts, sole traders, and partnership members (but not corporate subscribers)
- **The Regulations** define direct marketing as "the communication of any advertising or marketing material on a particular line". If the marketing is directed down "a particular line" to a Data Subject, it can be seen that the definition in the Regulations is contained with the Section 11 definition described above. It follows, that the main impact of the definition in the Regulations is apply to circumstances when personal data are not processed (i.e. the data processed relate to corporate subscribers).

The Commissioner has already expressed her view that any communication which is intended to enhance the image of the caller can be viewed as a marketing call; this "will apply not just to the offer for sale of goods

or services, but also the promotion of an organisation's aims and ideals" (from her Interim Guidance on the 1998 Regulations). This view means that the Regulations will apply to some "customer care calls" but, which when deconstructed as to the reason behind the call, are marketing calls in all but name (e.g. "we are phoning you to obtain your views on the current world-wide widget shortage, and by the way, would you want to buy some widgets at our fantastic reduced quantity discount rates"). An example of a customer care call which does not fall within this category would be one which relates to an unsafe product recall.

Finally, a warning. If personal data are processed for a tele-marketing purpose then both the Regulations **and** the requirements of the 1998 Act have to be satisfied.

Automated calling systems and faxes

The Regulations apply to any system which, when activated, make unsolicited telemarketing calls through the use of an automatic calling system (i.e. without human intervention) and to the sending of unsolicited faxes which are sent for a marketing purpose.

In relation to automated calling systems, the Regulations require a caller, using such a system for an unsolicited direct marketing purpose, to obtain the prior consent of the individual or corporate subscriber whose line is to be called. The Data Protection Commissioner's view is that predictive diallers would not fall within the definition of an automated calling system because the called subscriber speaks to an individual, even though the telephone number is initially dialled automatically.

With respect to unsolicited faxes there are three main provisions:

- **first**, a caller may not send unsolicited direct marketing faxes to an individual or corporate subscriber where the caller has been notified not to do so by the subscriber
- **second**, the caller cannot send such an unsolicited fax to a fax number which has been registered as objecting to the marketing purpose with the Fax Preference Service ("FPS")
- **third**, a caller must not send unsolicited direct marketing faxes to an individual subscriber unless that subscriber has previously notified the caller that he consents to such communication.

Note that these provisions protect corporate subscribers (e.g. companies) and individuals (e.g. sole traders, partnerships, employees of a corporate subscriber) and that if a subscriber registers an objection to the unsolicited marketing purpose (e.g. with a Preference Service), then that objection will be valid for all users of the subscriber's communications equipment thus registered.

There also seems to be an apparent contradiction between the three provisions described above which is, at first, not easy to understand. The first two provisions allow unsolicited marketing faxes to be sent to individual subscribers (unless they have "opted out" by registering with the FPS or by notifying the caller directly); thus, for example, if a number is registered with the FPS then the fax should not be sent. However, the third provision does not allow such faxes to be sent to individual subscribers for a marketing purpose unless they have consented; there thus seems to be no need to use the FPS because such subscribers have to "opt-in".

One reason for this apparent contradiction is that, in practice, both options might be needed. For example: a subscriber might be approached for consent to receive a marketing fax; the subscriber might then

register an objection which is then valid only for the particular calling subscriber; however, not wanting to be bothered by other approaches for consent, the called subscriber might then contact the FPS so his wishes can be communicated to all those who market by unsolicited fax. In addition, there is an issue where it may be difficult to identify, among a list of small businesses, those which belong to sole traders or partnerships and which, therefore, enjoy the rights provided to individuals under the Data Protection Act; to avoid confusion, every individual or corporate subscriber is free to register with the FPS.

So "can an organisation send a fax to an individual seeking consent for the marketing purpose?". Following the arguments presented in Part I, (under the heading "Can you seek consent for a marketing purpose?") there seems to be no objection to this **so long as** the information sent to the subscriber (so that any consent is fully informed) is not abused (e.g. as an excuse to send the marketing material itself). In addition, if a subscriber has registered its number with the FPS, then the caller knows that an approach seeking consent is likely to be futile and a waste of time; such numbers **should not** be faxed with a request for consent. Finally, the non-registration with FPS **should not** be taken as an excuse to repeatedly fax individuals to seek their consent.

Telephone

The provisions in the Regulations relating to the making of unsolicited direct marketing calls apply **only** to individual subscribers (i.e. not to corporate subscribers). They require a caller not to make an unsolicited direct marketing telephone call to an individual subscriber where the caller has been notified not to do so by the subscriber, or where the telephone number has been registered with the Telephone Preference Service ("TPS"). This set of options seems to raise the same

contradiction mentioned in connection to fax; so its resolution (explained previously) is also applicable.

The Regulations, however, make it clear that a call will not be treated as an unsolicited call falling within the Regulations if the individual subscriber has notified the caller that he does not object to such calls being made on his line. Since details about individual subscribers will also be personal data, Data Controllers should ensure that fair processing notices contain explicit details describing the mode of contact (i.e. phone, fax, mail). Additionally, if the worst happened, the existence of an opt-out (or opt-in) demonstrates that the subscriber has had the opportunity to object; this provides further evidence as to the solicited or unsolicited nature of a particular call, and provides evidence that the fairness rules associated with the 1998 Act have been satisfied.

Finally, in the case of a known individual using the phone of a corporate subscriber (e.g. as in the case of a direct line used by a particular employee), one might be tempted to argue that since the Regulations do not apply (the line relates to a corporate subscriber) nor do the marketing rules. However, since these data relate to a direct line used by a particular individual, the data will also be personal data, and the fairness processing rules of the Data Protection Act will apply. As has been noted in Part I of the analysis, the fairness rules will require the provision of an opt-out of the processing of personal data for a marketing purpose (and this includes telemarketing).

"Further information" requirements

The Regulations require certain information to be provided by the caller undertaking the unsolicited telemarketing which assist subscribers to exercise the right to object to the telemarketing purpose; such

information can easily be incorporated in fair processing notices given to subscribers who are individuals.

In further detail, the caller must provide the subscriber with:

- **where contact is made using automated calling systems or faxes**, his name and address or “freephone telephone number” where the caller can be reached. This should be prominently included in any marketing material (which normally it is, as the point of sending a marketing communication is to sell goods and services from a particular supplier). It follows that these points of contact for sales will also, from the subscriber’s perspective, be the natural place to deal with “objectors” to the marketing purpose (i.e. make sure such staff know how to deal with objectors)
- **where contact is made using the telephone**, his name (e.g. “I’m speaking on behalf of Acme Heaters Ltd”) and, if **requested** to do so by the subscriber, his address or freephone telephone number where the caller can be reached. Since there is no obligation placed on the caller to provide all of these details (unless asked) one assumes that there will be some campaign to educate subscribers of the fact that they can demand such information. Some Data Controllers may wish to be proactive and to pre-empt such requests by providing all the relevant details as part of the marketing communication.

Note that compliance with **both** the Regulations and the Act **is obligatory**. For example, a Data Controller who checks a telephone marketing list against his own objectors list and that of the TPS is compliant with the Regulations. This action does not, in itself, satisfy all the requirements of the First Data Protection Principle; if, for example, the Controller (or

his list broker) failed to give the appropriate fair processing notice when the personal data relating to individual subscribers were first collected.

Finally a reminder of an important point raised in Part 1 of this analysis. With respect to telemarketing there is likely to be additional rules (e.g. associated with distance selling) which will require the provision of information to callers. Do not let this information drown the data protection messages that need to be given.

Enforcement

The Commissioner has power to enforce the provisions of the Regulations if they relate to the processing of personal data. This means that all the powers granted to the Data Protection Commissioner under the Act may be used to enforce the Regulations. These include the power to issue Information Notices (requiring certain information to be provided within certain time periods), the power to issue Enforcement Notices (preventing, restricting or in some way affecting the processing of personal data by the Data Controller) and powers of entry and inspection. Failure to comply with an Information or Enforcement Notice can constitute a criminal offence. It is also an offence to intentionally obstruct, or to fail to provide reasonable assistance in, the execution of a warrant. In the case of breaches which do not involve personal data, the Director General of OFTEL has similar powers.

The criminal sanctions under the Act are limited to a fine (maximum £5,000 in the Magistrates’ Court and unlimited in the Crown Court). However, the real sanction for organisation is that they may be prevented from further using personal data which they may have spent tens of thousands of pounds to collect. Furthermore, a person (e.g. individual or corporate subscriber) who has suffered

damage (or damage and distress) by reason of a breach of the Regulations could claim compensation from the caller. The Regulations provide a defence in these circumstances if the caller can demonstrate that all reasonable care had been taken to prevent the breach.

Summary at a glance

It can be unlawful to make an unsolicited phone call, or send an unsolicited fax, to a Data Subject for a marketing purpose if that Subject has not consented, or has lodged an objection, to receiving such a call or fax.

Companies can also object to the receipt of unsolicited faxes sent for a marketing purpose. In addition, companies can object to unsolicited marketing calls if these are made through the use of an automatic calling system.

There is a statutory requirement to use the Telephone or Fax Preference Services when undertaking telemarketing campaigns where the calls made are likely to be unsolicited.

There is a statutory obligation to provide further information with respect to some aspects of telemarketing, or to provide such information on demand; such information should be contained in a Data Controller’s fair processing notice.

The statutory rules with respect to telemarketing should be integrated with the general approach described in Part 1 of this analysis.

Direct Marketing: Case studies

Can a business telephone existing customers for direct marketing purposes?

Where telephone numbers are obtained directly from Data Subjects with the intention that they will be processed for a marketing purpose, those individuals must be made aware of this purpose as part of the procedures associated with data collection. If individuals are unaware, they may have to be notified and possibly consent will need to be obtained; the exact nature of the contact (as described in Part 1 of this analysis), depends on a number of factors (e.g. the nature of the Data Controller, the personal data processed, and the products to be marketed).

In most cases, however, Data Subjects will be given a fair processing notice which identifies the Data Controller, describes the marketing purpose and provides any further information which is necessary to guarantee fair processing (e.g. the fact that marketing contact may be made by telephone); individuals should also be given the opportunity to opt-out at this stage. If the source of the personal data is a Third Party (e.g. a list broker), warranties should be obtained which cover the above requirements.

However, there may be some circumstances in which it is obvious that telephone contact will be made and this does not have to be specifically addressed in a notice. One such example might be where an individual completes a coupon requesting additional information about a product which requires him to provide only his telephone number and name; in this example the only method of approach in these circumstances is by telephone. However, such a respondent will only be giving permission with respect to the product advertised; this permission cannot be extended to the promotion of dissimilar products into an indefinite future. For this reason, it is often safer to describe the marketing purpose completely as "silence"

can introduce ambiguity - and ambiguity can lead to uncertainty with respect to compliance with fair processing requirements.

The Regulations with respect to direct marketing state that unsolicited calls to individuals for direct marketing purposes may not be made where the called line is that of an individual who has previously notified the caller that such unsolicited calls should not be made, or the telephone number is one which is registered with the TPS. So if an individual has done either, it will be unlawful to make an unsolicited call to the Data Subject (unless a Data Subject has registered with TPS **but** has also given the organisation specific permission for contact for the marketing call). Note that this means, for example, that where an existing customer of an organisation has registered with the TPS, the organisation might not be able contact that customer for the purpose of making an unsolicited marketing call - even though the phone is used to communicate information about other aspects of service delivery.

However, a telephone call will not be treated as an unsolicited call if the individual has "notified" the caller that he does not object to calls being made by the caller for direct marketing purposes (e.g. in a fair processing notice on a form which has been returned to the Data Controller). In some circumstances, it could be that a Data Subject may be genuinely inviting a marketing call (e.g. where the individual contacts the supplier and asks for information knowing that this will be provided by telephone). However, in such circumstances, be careful to ensure that the position is clear; as with the coupon case above if the Data Subject makes contact in order to receive a marketing call specific to one service that does not mean that subsequent marketing calls relating to others product are solicited (unless of course, the Data Subject is informed of this).

Note that if a Data Controller does **not** use an adequate fair processing notice (e.g. the notice is silent in respect of the telephone approach) then clearly individuals cannot "notify" their objection to being contacted by telephone. If such Data Subjects have registered with the TPS so that seeking of consent will prove problematic (e.g. it will be possible to seek consent by mail), it follows that the business could be prevented from calling those customers as the marketing call can be deemed to be unsolicited. **And that, in a nutshell is why those fair processing notices are crucial.**

How can an organisation cold contact individuals?

Assume that a Data Controller who wishes to cold call individuals first obtains personal data (e.g. name, address, phone number) from a marketing list sold by a list broker, or from a publicly available source which can be legitimately be used for a marketing purpose. After obtaining the list, the organisation must then consider the application of regulations and the data protection principles.

In general, there are four overlapping questions to ask: "Is the intended contact solicited or unsolicited?"; "Has a registration with a Preference Service been made?"; "Has the Data Controller received an objection to receiving marketing communications which is specific to the Controller?"; and "What is the fair processing situation".

For example, when starting a telemarketing campaign, the first step is for the Data Controller to consider the Regulations. These provide that an individual may be called if he has not previously notified the organisation that he does not wish to receive marketing calls, or if he has not registered with the TPS. Thus, the prime check is to see whether the individual has registered his phone number with the TPS; if

so, then he **cannot** be called. However, marketing campaigns are often broad brush affairs which sweep in personal data from a number of sources, this will always bring in the prospect that personal data may relate to existing customers. Thus, the next important step is also weed out those customers who are on the Data Controller's "no marketing" stop-list. If a list is brought-in, it is important to obtain a guarantee from the supplier that everyone on the list have agreed to be contacted.

The next step is to square the data protection issues. Firstly, if the information was obtained using a fair processing notice (e.g. this is normally the case with lists sold by a reputable list broker), the notice must be checked (or guarantees obtained) to ensure that the marketing purpose undertaken by the Data Controller and the telemarketing aspects are fully and clearly expressed. This would involve considerations of the following questions: "has a disclosure of personal data to a Third Party for a marketing purpose been described on the notice given to Data Subjects?"; "have Data Subjects been notified that telephone contact would be made?"; "does the notice provide for objectors?"; "are the kinds of products associated with the Controller's marketing campaign appropriate to the fair processing notice which has been issued to Data Subjects?"; and finally, "Is there anything unusual or exceptional about the processing by the Data Controller which needs to be declared to Data Subjects in the notice". If the fair processing notice is deficient in any way, then consider employing another list.

In some cases, personal data can be obtained by a Data Controller without an appropriate fair processing notice being given to the Data Subject; for example, the personal data could be extracted from a publicly available source. In such cases, the Data Controller must first check the wider legal matters associated with the processing of those data. For example, there might be

copyright, contractual restrictions or other statutory limits on the use of these personal data; for instance, in good old "Community Charge days", the Community Charges Register was open to inspection by anyone but **not** for copying (i.e. to use the Register for marketing would be an example of unlawful processing).

Thus assuming these wider legalities are in order, the Data Controller can turn to the question of whether there is an obligation to provide Data Subjects (e.g. in the mail) with all the necessary details about the processing described in a fair processing notice. The notice should also provide the individual with a method of objecting to any further contact or contact by telephone, and provide for a suitable time period so that a Data Subject can register an objection to the marketing purpose in good time before the processing occurs (e.g. the Direct Marketing Association's Code of Practice recommends 30 days to cover these circumstances).

Consideration must then be given as to the circumstances when the Data Controller needs to obtain the response of the Data Subject to the notice **before** commencing the marketing purpose. This brings in all the elements raised in Part 1 with respect to seeking consent and requires consideration of: "what products are marketed?", "who is performing the marketing?", "what kind of personal data are processed to effect the marketing?" and "where does processing occur?". For example, if the Data Controller intends to process Sensitive Personal Data for a marketing purpose, then Data Subjects need to give explicit consent.

If all data protection issues are resolved and the regulatory aspects have been considered, then the marketing campaign can begin. However, because the right to object to marketing can be exercised at any time, ensure that staff involved are trained, and telephone scripts are provided, so that the necessary procedures to take note of an

objection from a Data Subject can take speedy effect.

Finally, note that in very limited circumstances there will be no fair processing notice issued. For example, if someone fills in and returns a coupon in a newspaper asking for further information about a particular product or service, and if the phone number provided was the **only** means of contact.

Finale

It should be clear that whether or not an organisation can process personal data for a marketing purpose, or call its customers or prospects or send them marketing faxes depends upon a number of factors. The most important relate to the content of that fair processing notice, and the screening of lists of objectors such as those organised by the Preference Services. It is worth noting that breaches of the Regulations have been actionable by the Commissioner since 1 May 1999 and compliance procedures should already be in place.

Which they are, for you, of course!

Newsletter

This text was first published in Data Protection and Privacy Practice, a quarterly magazine for privacy practitioners in the UK published by Masons. If any reader wishes a sample copy, please contact the author (details on covers).

Masons is an international law firm. Our aim is to be recognised as the foremost legal advisor to the Information & Technology, Construction & Engineering, Energy & Infrastructure industries, whilst remaining a leading provider of specialist skills.

www.masons.com

London

T +44 (0) 20 7490 4000
F +44 (0) 20 7490 2545

Bristol

T +44 (0) 117 924 5678
F +44 (0) 117 924 6699

Edinburgh

T +44 (0) 131 718 6006
F +44 (0) 131 718 6100

Glasgow

T +44 (0) 141 248 4858
F +44 (0) 141 248 6655

Leeds

T +44 (0) 113 233 8905
F +44 (0) 113 245 4285

Manchester

T +44 (0) 161 234 8234
F +44 (0) 161 234 8235

Brussels

T +32 2 646 02 60
F +32 2 646 73 23

Dublin

T +353 (0) 1 638 3838
F +353 (0) 1 638 3888

Hong Kong

T +852 2521 5621
F +852 2845 2956

Guangzhou

T +86 20 8732 2848
F +86 20 8732 2858

Singapore

T +65 339 8577
F +65 339 5122

MASONS

