# Data Protection – An Overview

**By Michael O'Dowd**

**[2004] COLR 14**

## Introduction

Whether it is true or otherwise, people believe that in recent times their privacy has been eroded to a considerable extent. By and large this has been attributed to one thing: the exponential growth in the proliferation and power of computers.

The Data Protection Act 1988 was the result of a fear that personal data would be used recklessly by private and governmental organisations alike. At the time of enactment there was very little debate on the subject. The motivation for the Act came more from both the OECD[1] and The Strasbourg Convention[2] than from within Ireland.

The lack of interest shown in Data Protection in 1988 is however not indicative of today's attitude. Of particular interest to those involved in the area of direct marketing is a survey published by the Data Protection Commissioner on the 13 January 2003. Some of the more salient findings are as follows:

a) Irish people value their privacy of personal information even higher than 'protection of consumer rights' or 'ethics in public office'. 81% of a sample of 1203 people aged 15+ rated their privacy as very important, with a further 17% considering it important.

[1] Organisation for Economic Co-operation and Development Guidelines governing the Protection of Privacy and Transborder flows of Personal Data, 23 September 1980

[2] The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Data, signed by Ireland on the 28 January 1981

b) Financial records are considered more sensitive than medical records. (77% of adults considered their financial details very important, with 18% considering them important.)

c) 76% of people agreed with the statement 'Businesses regularly want to know more about me than they need to'. However, 54% 'trust business to use the information in a fair and proper manner'

d) 56% of people now agree that 'if you use the internet your privacy is threatened'.

e) People are hostile to intrusive direct marketing

    a. Resistance is greatest to marketing over the home telephone. Three in Five overall were opposed to this.

    b. The question of marketing over the internet was relevant only to 40% of respondents, and the level of discontent was 55%.

    c. 54% of respondents were unhappy about direct marketing via SMS.

    d. The least intrusive was post, with 32% of people indifferent.

In light of these findings, it is ever more important for companies engaged in direct marketing to pay particular attention to the legislation governing data protection. The main legislation in this area is:

i. Data Protection Act 1988

ii. EU Data Protection Directive 95/46

iii. European Communities (Data Protection) Regulations, 2001 (SI No. 626 of 2001, which in part implements the Directive)[3]

[3] The regulations part implement the Directive. (When this Essay was composed, the 2003 Data Protection Act had not been passed)

Before analysing some of the more important sections in the Data Protection Act (DPA) it is worth bearing in mind that it applies only to computerised files containing personal data. The directive provides that data not processed automatically will also be within the ambit of the legislation, provided it forms part of a filing system. Personal data is defined in the Act as:

> 'data relating to a living individual who can be identified either from the data or from that data in conjunction with other information in the possession of the data controller'.

**Registration**

All Direct Marketing companies are required to register with the Data Protection Commissioner[4]. Registration involves setting out what kinds of personal information you intend to keep on your computer, why you intend to keep it, and to whom it will be made available. The application is made to the Data Protection Commissioner (DPC), using a form that may be obtained in advance. A fee applies[5], and the registration will have to be renewed each year. It is possible for an application to be refused, the reasons for such refusal are:

a) Particulars in relation to registration are not sufficient, or other information is not being made available.
b) The person applying for registration is likely to contravene the act.[6]

There is a right of appeal in the case of refusal to the circuit court[7]. It should be noted however that it is an offence for a Data controller who is obliged to be registered not to be so[8].

[4] Section 16(1)(b)
[5] 1-5 employees: €25.37; 6-25 employees: €63.49; 26+ employees : €317.43 at http://www.dataprivacy.ie
[6] Section 17(2)

**Data Quality Principles**

Section 2 of the DPA owes it origins directly from the OECD and Strasbourg convention, so it is no surprise it has similarities to the equivalent UK legislation, and of course the directive. Contained within section 2 are the data quality principles, to which all data controllers (direct marketing agencies included) must adhere. The following principles must be followed.

a) The data must be obtained and processed fairly
b) Personal data must be accurate and where necessary, kept up to date
c) The data should be kept for only one or more specified and lawful purposes
d) The data should not be used in any manner incompatible with its original purpose
e) The data should be adequate, relevant and not excessive
f) The data should not be kept longer than is necessary
g) Appropriate security measures should be taken.

*A)* The data must have been obtained and processed fairly

This is arguably the most important rule in the DPA, which has itself been defined as 'fairness legislation, not requiring a balance between data users and data subjects, but simply being fair to an individual'[9]

The DPA does not go any further in defining fairness than the exclusion found in Section 2(5)b – that data shall not be regarded as having been obtained unfairly by reason only that its use for historical, statistical or research purposes was not

[7] Section 26(1)(c)
[8] Section 19(1)

disclosed when it was obtained. Article 10 of the Directive makes a better effort, requiring that data subjects should be informed as to:

a) The Identity of the Controller and his representative, if any.

b) The purposes of the processing for which the data are intended.

c) Any further information as is necessary, examples that are given include

    d) Recipients of the data

    e) Whether replies/answers are obligatory or voluntary

    f) Possible consequences of failure to reply. [10]

These requirements are quite similar to the current standards required by the Irish Direct Marketing Association (IDMA). In their code of practice[11] the IDMA states that to be fairly obtained, individuals at the time of collecting the data should be aware of:

a) The identity of the persons collecting it.

b) To what use(s) it will be put.

c) Secondary uses which might not be so obvious to the individual

d) The persons(s) or category to whom it will be disclosed.

In practice, the principle of fair obtaining and processing is upheld to a higher extent than perhaps many in the direct marketing industry would like. Consent of the data subject is all important, but precisely what constitutes 'consent' is almost as vague as the definition of fairness. The Directive requires that *'the data subject ha*s

[9] UK Office of the Data Protection Deputy Registrar
[10] Directive 95/46/EC Article 10
[11] Although receiving warm words from the Data Protection Commissioner, it is not a statutory code of practice as outlined by Section 13.

*unambiguously given his consent'* [12]. The data subject's consent is defined in Article 2(h)[13]. This is not yet a requirement in Ireland, and it is submitted that something less that absolute consent is currently required. Ian J Lloyd suggests that *'the subject must be given a reasonable notice regarding the purposes for which the data is obtained'.*[14] The line between what constitutes consent, or not, is narrow.

In *Innovations(Mail Order) Ltd. v. Data Protection Registrar*[15] the data subject was sent an acknowledgement after registering their details to purchase goods. This stated that if they did not want their details be used for direct marketing purposes; to complete and return a slip of paper. This was found by the UK Data Protection Tribunal not to come within the ambit of fair obtaining; the subject should be given the opportunity to object to the non-obvious purpose of gathering the data before it was obtained. In any case, such practice is inconsistent with Section 2(7).

While it has been recommended as good practice by the DPC[16], very few companies use an 'opt-in' box. This provides that the data subject will not be enrolled in anything, unless she expressly agrees, and is motivated enough to tick the box. Not many people are so motivated however, and so the 'opt-out' box is a more regular sight. This is tolerated at present, however such passive consent may become a thing of the past when the Directive finally does become law. Silence however should not be taken as an indication of consent[17]. Implied consent is however satisfactory where

[12] Directive 95/46/EC Article 7(a)
[13] 'The data subject's' consent shall mean 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
[14] Ian J Lloyd, *Information Technology Law, 3rd Edition,* (Butterworths, 2000) p112 para. 712
[15] United Kingdom, Case DA/92 31/49/1
[16] http://www.dataprivacy.ie/5b.htm
[17] Case Study 10/1997 (http://www.dataprivacy.ie/97cs10.htm)

*'a person participates in a special promotion, which clearly involves the use of personal data for certain clearly defined marketing purposes'*[18]

The DPC's attitude to consent can be surmised as follows:

*The Direct Marketing company should be clear and upfront about the use of peoples personal data, and not be underhanded or cavalier about obtaining people's consent*[19]

There will be a number of situations where consent will not be required. The most notable of these are where marketing is sent out to people en masse, since there is no personal data involved[20] or where the data is gleaned from a source required to be made available to the public by law[21]. The most pertinent example of this is the electoral register, however, the implementation of the directive may remove this source, Article 3 of the directive makes no exception similar to that found in Irish Law. Section 9 of the UK Representation of People Act 2000 makes provision for two electoral registers, one which will be freely available for marketing purposes, and the other for electoral and law enforcement purposes[22].

B) Personal data must be accurate and where necessary, kept up to date

Section 2(1)b requires that data be accurate and, where necessary, kept up to date. While this provision has much greater resonance with the Insurance and Credit Referencing sectors, it is also important for those engaged in Direct Marketing. For those however in the Direct Marketing sector, the requirement of accurate and up to date data is fundamental to the business. Incorrect data is more likely to have no effect

[18] ibid fn10
[19] ibid
[20] Case Study 09/1996 (http://www.dataprivacy.ie/96cs9.htm)
[21] Section 1(4)b
[22] Ian J Lloyd, *Information Technology Law, 3rd Edition,* (Butterworths, 2000) p127, para. 7.67

whatsoever, than adversely affect the data subject, as may happen with credit referencing.

The requirement of accuracy does not apply to back up data[23]. However, Case Study 11/1997 is on the point; the DPC said data controllers should take measures to ensure the back up copy, if restored accurately reflects the original version. Now that backing up data is far less onerous, it is submitted that the DPC, and ultimately courts will interpret this provision very narrowly.

C) The data should be kept for only one of more specified and lawful purposes

Kelleher and Murray suggest that it is unclear what specified purpose means, and that it will probably be the purpose specified in the register[24]. It suggested however that this is a rather narrow view. More likely is that the data should not be kept for a purpose other than that for which it was collected. Case study 04/2001 gives credence to this view. Here, a customer of a car rental company had his credit card debited because of alleged damage. However on that occasion he had not used a credit card and his details had been gathered on a previous occasion. When the reasons for keeping the data was impugned, the company alleged they had kept the details for auditing and legal purposes. This the DPC was prepared to accept, provided the information was deleted when no longer necessary, but stated that while that information was being held it should not be used for any other purpose without the express consent of the data subject. Ultimately, the subject should be aware why the data about him is being held. Nonetheless, when drafting an application to the register, care should be taken to ensure that all types of prospective data would be covered.

[23] Section 2(4)
[24] Kelleher & Murray, *Information Technology Law in Ireland,* par 20.04 (3)

D) The data should not be used in any manner incompatible with its original purpose

This is very much a follow on from the previous principle, and indeed Article 5(b) of the Strasbourg Convention combined both. This provision tends to attract most controversy, since breaches of it are far more patent. Quite often it happens that data kept for a specified and lawful purpose could be used in a manner incompatible with its original purpose.

Any information coming from a source other than the data subject should be treated with the severest circumspection. There is a very strong possibility it will contravene this section. In Case Study 2/2001, the DPC speaks of how Concern, the respected Irish charity disclosed its donors details to a marketing company for the benefit of a financial institution. In return, the Bank gave Concern a donation for each positive reaction. Here, the DPC found disclosing the information to the marketing company was incompatible with its original purpose.

Case Study 01/2001 also highlights the dangers of accepting data from 3rd parties. A customer from an insurance company received mail advertising a new credit card, by the way issued by the same company. In fact it was being issued by a bank, and when the customer replied to the mail, his details were transferred to the bank. The DPC found the Insurance company had disclosed the details in a manner incompatible with its original purpose[25].

[25] The bank had obtained the information unfairly, contravening Section 2(1)(a)

Article 14(b) of the Directive expands on this point; it requires that the subject will be allowed to object on request before his data is used for direct marketing purposes, or have the right to be informed before personal data is made known to third parties, or even used on their behalf. This is all to be made available free of charge. These provisions, when enacted may have the effect of severely curtailing the use of 'host mailing services', and will increase greatly the cost of compiling mailing lists.

Disclosure does not include the disclosure made to an employee where it is necessary for him to carry out his duties.

E) The data should be adequate, relevant, and not excessive

This is currently one of the less contentious provisions. It could be argued that this is surprising, especially since the majority of people believe, that businesses regularly want to know more about me than they need to.

Microsoft's 'Passport' Online identity system, marketed heavily with Windows XP, has fallen foul of this guideline. The system was designed to allow consumers access online services without having to continually resubmit personal details. Now, when Europeans will sign up for the service, they will have the option of designating themselves as EU citizens, and decide themselves what information to divulge.[26]

It is quite possible that in the future there will be issues concerning loyalty card/store credit card schemes, especially with many alliances being formed of late. Where customers will use these cards in a multitude of shops, and all the information can be

collated there is the possibility for creating exceptionally large and detailed databases. However, like the principle outlined in (C) above, the effects of this provision being contravened are latent, and less likely to provoke an outcry.

F) The data should not be kept longer than necessary

This does not apply to personal data kept for historical or research purposes, subject to it not causing damage or distress to any data subject.[27]

What is longer than necessary is not defined, but case study 04/2001 suggests that details of a contract no longer in dispute should be deleted once the contractual relationship has ceased, nor should there be any need to retain data for auditing purposes once the particular audit period has passed. This would suggest, that, as far as a direct marketing company is concerned, that once the purpose for which the data was collected has been exhausted, the relevant data should be deleted. Case Study 07/1997 considered the issue of a direct marketing company keeping data. The DPC considered it reasonable to keep the data for up to one year after it being collected for a promotional campaign, as it was common for people to query their participation after the promotion has ceased.

G) Appropriate security measures shall be taken

Little was said about this in the 1988 Act, until section 2A was inserted by the Regulation. Here it is provided that the data controller should have regard *inter alia* to; the state of technological development, and cost of implementation; the harm that may result from a breach of security; and the nature of the data concerned. Data of an exceptionally sensitive nature therefore will need more robust security measures than more mundane information. What the directive recognises, is that there is no such

[26] BBC News Online, Thursday, 30 Jan, 2003
[27] Section 2(5)(a)

thing as perfect security, but that privacy cannot be achieved without appropriate security measures.

**Obligations to data subjects**

A number of situations are allowed for in the Act where a company will have direct obligations to certain data subjects.

Section 2(7) specifically concerns direct marketing organisations. It provides that, where requested to do so, the data controller is obliged within 40 days to erase data concerning a particular subject. Also, if unbeknownst to that subject the data was being used for other purposes, that must also cease and the subject must be notified accordingly. This gives people the right to request that a direct marketing company ceases using their details.

Directive 2000/31/EC[28] provides in Article 7(2) provides that those engaged in unsolicited commercial e-mail should consult regularly with opt-out registers where people not wishing to receive 'spam' may register.

Other obligations also exist, but are very unlikely to be used in a direct marketing context. These include a right of access to the information[29], and a right of rectification or erasure[30]. There is no general right to object outside of the direct marketing sphere. The directive will introduce one, but subject to a more stringent test. For these reasons it is unlikely to be availed of by data subjects.

[28] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

**Transfer of Information out of the state**

A separate brief could be written on the complexities of trans-border data flows. It is however worth considering some salient points, especially since the bulk of the 2001 regulations concern this area.

One of the biggest changes introduced by the directive (and subsequently by the regulations) is that there now can be an unimpeded flow of personal data between Member States. It is now the function of the EU Commission to oversee the safe transfer of data to third countries[31]. While third countries are not required to have the same level of protection afforded by the directive, they must have an adequate level[32]. Switzerland and Hungary are examples of two countries that have benefited from this derogation.

There is a separate system for the US, this is known commonly as the USA safe harbour data agreement. It is a voluntary scheme, where companies are required to engage in a self-certification process. While this scheme has been criticised by the Working Party established under Article 29, it does provide a solution for what otherwise would be a disruptive situation for companies attempting to do business in the US. For companies who wish to transmit information outside of the recognised countries, sufficient protection may be attained by contractual clauses[33]

[29] Section 4
[30] Section 6
[31] Section 11(1)
[32] Section 11(3)
[33] Directive 95/46 Article 26.2

The method of banning trans border data flows is by a prohibition notice issued by the DPC. However, it is difficult to see how this can be enforced, save by the goodwill of the company concerned, since there is no obvious way to stop data transmissions out of the state. Data Havens will also continue to exist, and even if every state implements privacy measures there will continue to exist extra-territorial issues[34].

## Conclusion

The EU legislation in the area of Data Protection is thorough. Admittedly by its nature it is a difficult area to police, but by its existence it provides a very strong bargaining tool to ensure that businesses, in particular, do not know more than they have to, and that consumers are adequately protected. For a company involved in the area of direct marketing, this is not such good news. Consumers are less amenable to exploitation, and while the DPC does take a mediatory approach to disputes, companies will have to comply. To be successful, a company engaged in direct marketing will not only have to uphold the law, but be seen to be doing so.

[34] One of the most interesting (and amusing) of these issues has proven to be Haven Co. establishing 'secure' servers on the 'Principality of Sealand', an old WWII anti aircraft platform in the north sea, commandeered by a UK national before Britain extended its territorial waters along with international custom. (www.havenco.com)(www.sealandgov.com)