

**Ninth Annual Report
of the
Data Protection
Commissioner
1997**

**Presented to each House of the Oireachtas pursuant to section 14 of the
Data Protection Act, 1988**

PN. 6398



FOREWORD

I hereby submit my fifth Annual Report to Dáil and Seanad Éireann pursuant to the provisions of section 14 (1) of the Data Protection Act, 1988. This is the ninth Annual Report submitted in relation to the work of the Office of the Data Protection Commissioner since it was established in 1989.

A handwritten signature in black ink, reading "Fergus Glavey". The signature is written in a cursive style with a large initial 'F' and 'G'.

Fergus Glavey
Data Protection Commissioner
November, 1998

MISSION STATEMENT

**To secure respect for the individual's right
to privacy with regard to information
held on computer about him or her by**

- **upholding the rights and**
- **enforcing the obligations**

set out in the Data Protection Act, 1988

Office of the Data Protection Commissioner

Block 4, Irish Life Centre, Talbot Street, Dublin 1

Phone: (01) 874 8544 **Fax:** (01) 874 5405 **E-Mail:** *info@dataprivacy.ie*

CONTENTS

INTRODUCTION	3
PART 1	
SUPERVISING AND MONITORING DATA PROTECTION IN 1997	
Education and Awareness	7
Enquiries	9
Complaints	10
Registration of Data Controllers	11
Survey of Attitudes and Awareness	11
International	15
Administration	17
Protecting Your Privacy in the Information Age — Self-Help	18
PART 2	
CASE STUDIES	23
PART 3	
PARTICULAR ISSUES	
EU Directive on Data Protection	33
Transfer of Data Abroad	34
Registration of Uses and Disclosures	36
Identity Numbers	37
Processing of Medical Data - Smart Cards and Electronic Transmission	37
Credit Records and Credit Referencing	38
Enforced Subject Access	39
Council of Europe Draft Guidelines on the Protection of Privacy on the Internet	40
APPENDICES	
Appendix 1 — Social Welfare Bill, 1998 - Remarks by the Data Protection Commissioner on the Bill to the Dáil Select Committee	45
Appendix 2 — Article 29 Working Party, Index of Documents	49
Appendix 3 — Registrations 1994 - 1997	50
Appendix 4 — Report of the Comptroller and Auditor General and Account of Receipts and Payments in the Year Ended 31 December 1997	51

INTRODUCTION

The Data Protection Act, 1988 is now in its tenth year and while in my view it has served its purpose well the time is clearly opportune to reiterate the respect for privacy as a fundamental human right which is implicit in the 1988 Act while providing for the application of information technology in ways which were never foreseen at the time. In this context the Government's commitment to introduce amending legislation to transpose *EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* is to be welcomed. Exactly how the new legislation will differ from the 1988 Act it is not yet possible to say, as the Government had not published its proposals at the time this Report went to press.

It is now commonplace to remark on the dizzying speed of progress in the application of information technology. Not even those who had the foresight, some thirty years ago, to conceive of the need for data protection law could have anticipated how profoundly computers would change all aspects of everyday life. Realistically, it is no longer possible for anyone to opt out of the Information Society without withdrawing from the world in a way that very few would find possible or appealing. The rapidly shrinking minority unable or unwilling to use computers nevertheless deals, on a daily basis, with public bodies and companies keeping personal information on computer.

I have remarked before that while information technology brings immense benefits it also has the potential to do harm — or rather to be used in a way that does harm, because computers themselves do not make choices. The simplest home computer now comes with the software and the processing power to manipulate information on a scale and at a speed that armies of clerks could never match. The computer systems of public agencies and large companies are far more powerful still. While in many ways this can bring the citizen or the customer a quality of service never dreamed of before, the scope for error, inaccuracy, confusion and downright misuse of information is correspondingly greater.

Data protection law is not an obstacle to progress, even if its prescriptions sometimes seem irksome to those enthused by what information technology can do. On the contrary, it exists to ensure that this technology is used properly and to create the climate of public confidence in which application of the technology can flourish. At the heart of the legislation is an awareness of privacy as a basic human right. A human being is not merely a collection of items of *information in a form which can be processed* — as the Act defines *data*. He or she is a unique individual entitled to be valued as such.

“Human beings are not means to the ends of others but are ends in themselves and are free to choose their own goals in life”¹. Data protection law exists to underscore this point and to redress the very real imbalance in power which might emerge between those who keep information on computer about others, *data controllers*, and those in respect of whom information is kept, *data subjects*.

Most people have an instinctive understanding of the importance of privacy, even if they do not have the capacity or the occasion to articulate such understanding in the context of the application of information technology. I commissioned a survey of attitudes to and awareness of data protection during 1997, and the starting point was a series of questions about how important people thought it was that they should have control over the collection and use of information about them by others. The responses overwhelmingly showed that it was very important indeed.

As yet, many people have no more than an inkling of the part that computers play in their lives. However it is clear, both from the results of the survey and from what I have heard from the thousands of people who have contacted my Office since 1989, that data protection law gives expression to an almost universal human desire to protect privacy — even if this is a right that, like many others, people become aware of only when it is threatened.

Several times in this Report, I refer to the basic data protection principle of *fair obtaining*. More and more, I find that this is at the heart of cases which come to my attention. Fair obtaining is prerequisite to lawfully keeping information about other people on computer. I interpret this principle to mean that a person (*data subject*) whose information is to be kept on computer by another (*data controller*) must be in a position to make an informed choice whether or not to provide such information in the first place unless otherwise required by law. This is an active duty for the data controller and requires among other things that he identify who he is, for what purpose the data will be kept and to whom they will be disclosed. Compliance with this principle would do more than anything else to avoid complaints to my Office.

The work of my Office during 1997 is described in this Report, which is divided into three parts and four appendices.

In **Part 1**, I review the day-to-day work of the Office. I describe the work done in making people aware of their rights and obligations under the Act, and outline the kinds of enquiries and complaints dealt with. I set out in detail the results of the survey of attitudes to information privacy that I commissioned in 1997. There follows a brief description of developments at international level and a section on administration. Finally, I offer some practical tips on how people can protect their privacy in everyday situations in the information society.

Part 2 gives examples of cases I dealt with during the year. Some are complaints; others are cases in which I gave advice to *data controllers* (computer users), either at their request or on my own initiative. These cases are chosen to highlight various aspects of the Act as it applies in real-life situations.

In **Part 3**, I comment on several issues of policy and practice. I look at the increasingly important issue of the transfer of data abroad, and I make recommendations about credit referencing and the practice of compelling individuals to gain access to their own information for the purpose of giving it to others. I also mention the Social Welfare Bill, 1998, smart cards and the electronic transmission of health data, and draft guidelines on the use of the Internet.

¹ Privacy: Surveillance and the Interception of Communication, Law Reform Commission, June 1998 (Part 1.11)



Number 25 of 1988

DATA PROTECTION ACT, 1988

AN ACT TO GIVE EFFECT TO THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA DONE AT STRASBOURG ON THE 28TH DAY OF JANUARY, 1981, AND FOR THAT PURPOSE TO REGULATE IN ACCORDANCE WITH ITS PROVISIONS THE COLLECTION, PROCESSING, KEEPING, USE AND DISCLOSURE OF CERTAIN INFORMATION RELATING TO INDIVIDUALS THAT IS PROCESSED AUTOMATICALLY. [13th July, 1988]

PART 1

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

SUPERVISING AND

Preliminary

Interpretation and application of Act.

1.—(1) In this Act, unless the context otherwise requires—

“appropriate authority” has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

“back-up data” means data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged;

“civil servant” has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

“the Commissioner” has the meaning assigned to it by section 9 of this Act;

“company” has the meaning assigned to it by the Companies Act, 1963;

“the Convention” means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January, 1981, the text of which is set out in the *First Schedule* to this Act;

“the Court” means the Circuit Court;

“data” means information in a form in which it can be processed;

“data controller” means a person who, either alone or with others, controls the contents and use of personal data;

INTRODUCTION

The work of my Office may be listed under five main headings:

- pro-actively spreading awareness of data protection
- dealing with enquiries
- investigating complaints
- maintaining the Public Register of Data Controllers
- liaising and co-operating with privacy protection authorities in other countries.

In this part of my Report I describe what took place in 1997 in these areas of activity. I outline the findings of the first nationwide survey into public perceptions of and attitudes to information privacy (pages 11-14). At the end of this part (pages 17-19) I offer some simple tips on how people can make choices to better safeguard their privacy in everyday situations.

EDUCATION AND AWARENESS

There are two sides to data protection. Individuals have rights, and those who keep information about them have responsibilities. One of my functions is to raise awareness on both sides.

As I have said in previous Annual Reports, what I can achieve in this area depends on the resources made available to me, both human and financial, and the opportunities that present themselves. I get many requests for educational presentations from groups representing both *data subjects* (individuals) and *data controllers* (those who keep information about people in computerised form). During 1997 my staff and I made presentations to groups of data controllers in a range of sectors including civil servants, medical and nursing personnel, market research companies and marketing students. The fact that there are so many requests is encouraging, because it shows that awareness of data protection – and indeed of privacy issues in general – is growing steadily. Time and resources do not allow me, however, to respond to as many requests for educational presentations as I would like.

INFORMATION MATERIAL

Individuals who contact my Office looking for information about their rights are sent a simple leaflet which sets out clearly what their rights are and how they may assert them. During 1997, over 55,000 of these leaflets were distributed, bringing the total distributed to date to over 555,000.

There is also a booklet designed for data controllers, which outlines their obligations clearly and explains the criteria for registration. Over 14,000 of these were distributed in 1997. A more detailed *Guide to the Act* has also been available; this will of course have to be revised in the light of amendments to the 1988 Act necessitated by the transposition of *EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data* into Irish law.

Advertisements were placed in trade and specialist journals as opportunities arose. The use of such advertisements, like most other activities of my Office, is governed by the financial resources I have. While it would be desirable to maintain a regular high level of advertising in the main news media, informing the general public of their rights, that is not practicable at present. In recent years, therefore, my Office has followed a policy of directing publicity at particular groups of data controllers since alerting them to their obligations has a high priority in my view.

Educational and promotional activities accounted for some 47% of my Office's non-pay spending in 1997.

UNIVERSITY COLLEGE DUBLIN ESSAY COMPETITION

In my Annual Report for 1996, I announced that I had agreed to sponsor an essay competition for post-graduate students in University College Dublin (UCD) who were taking their LLM (Commercial Law) in Information Technology Law. I agreed with Professor Robert Clark of UCD that there should be two topics —

- The Data Protection Directive (95/46/EC) will require the Oireachtas to amend the Data Protection Act, 1988. What do you consider to be the key areas that the legislature will have to address?
- The Challenges Posed to Personal Privacy by the Practice of Data Matching

I was very impressed with the quality of the students' entries. The first prize was awarded to Ms Mary Colhoun, who chose to write about the EU Directive and the amendment of the Irish Act, and the second prize went to Mr Jonathan S FitzGerald who wrote about data matching.

The EU Directive and the Data Protection Act

Ms Colhoun's essay was a detailed and outstandingly well-informed examination of the provisions of the Directive set against the existing legislation. She also showed herself to be conversant with the most up-to-date developments in information technology, and she demonstrated a detailed and sophisticated grasp of the human rights issues that lie behind data protection law. At a time when I was formulating my views on the transposition of the Directive into Irish law, I found her insights and suggestions most helpful.

One interesting observation in Ms Colhoun's essay was that the existing Act lacks balance in that it relies too much on the exercise by the individual data subject of his or her rights. To address this, she argued, there was a need for extensive – and adequately funded – publicity activities by my Office to make people aware of those rights. I take her point, though as I have said previously the resources at my disposal have made it necessary for me to concentrate my educational initiatives in recent years on raising the awareness of data controllers of their responsibilities rather than on informing the public of their rights.

Data matching

Mr FitzGerald, dealing with the issue of data matching, identified a difference between the public and private sectors. "In the public sphere personal information privacy is ostensibly threatened by the might and unlimited resources of the state... . Private undertakings do not have access to the same level of information as public bodies nor do their actions impact on the individual to the same degree... . The Data Protection Act achieves a regulatory balance which effectively curtails practices in the private sphere which may impinge upon the information privacy of the data subject without impacting too negatively on the growth of the industry."

In his discussion of the issue in the public sector, Mr FitzGerald identified the introduction of a multi-purpose PINS (Personal Identifying Number System) as the medium through which data matching was most likely to be achieved. Arguing that "instinctively society would not accept ... the state [as] a monolithic data controller", he saw a risk that "governments may be tempted to incrementally make it a reality so society would be faced with a *fait accompli*. This approach ... is to be guarded against, as it would not facilitate the necessary public debate and is in essence anti-democratic." He concluded that "the Government must face this issue head on. PINS-facilitated data matching is such a significant form of invasion of privacy that it should be controlled by clearly enforceable provisions." I am glad to record that this has since happened.

ENQUIRIES

Enquiries to my Office showed a continuing increase during 1997. A new system for tracking telephone queries was introduced and an analysis of the results indicated that such calls numbered over 1,500 during the year as a whole. When other enquiries – by letter or electronic mail, or from people who called to the Office – were added, the total for the year was in the region of 1,850 of which about 1,200 were from individuals and the remainder from data controllers. This total represents an increase of about 10% on 1996.

DATA SUBJECT QUERIES

Individuals who contacted my Office mostly wanted to know what their rights under the Data Protection Act were in particular situations, and how they could go about asserting them. These enquiries covered a wide range of subjects. As in previous years, the greatest number was from people who were concerned about their credit records – often as a result of having been refused credit – and my staff advised them to make a request to the Irish Credit Bureau, under *section 4* of the Act, for a copy of their information. The next largest category of enquiries was about unwelcome direct mail, and in these cases my Office explained the right under *section 2(7)* to have one's data removed from mailing databases.

Consistently, my staff report that enquirers are disappointed and sometimes indignant to find that the Act gives them rights only in respect of information kept in computerised form and has nothing to say about information kept on paper. Several callers who wanted access to their medical records, for example, were unhappy to find that the Act was no help to them in seeking access to much of the information they wanted. In this connection I warmly welcome the passage in April 1997 of the Freedom of Information Act which will radically improve access to personal information kept in paper form by public bodies. The extension of data protection law to information kept on paper is, of course, covered by certain provisions of the 1995 EU Directive on data protection which, at the time of writing, awaits transposition into Irish law.

DATA CONTROLLER QUERIES

Data controllers who contact my Office are usually asking for advice about how they should meet their obligations under the Act. Most of the 600-plus queries in 1997 were about whether they were required to register under *section 16*¹ of the Act and, if so, how they should go about it. A significant number, however, were asking for advice about other obligations. I was pleased to find that in the majority of such cases data controllers were consulting my Office *before* taking a particular course of action. In my contacts with groups of data controllers and their representatives, I have repeatedly stressed that I see giving advice to them as a very important part of the work of my Office, and that I would prefer to advise them before they do something than find myself – and them – having later to try to resolve a situation that has become a problem. I was struck by the sophistication of many of the queries (which frequently came through data controllers' legal advisers); there is evidence now of an increasing awareness of the obligations that the Act places on those who keep personal data on computer, and of a serious attempt to meet these obligations. In **Part 2** of this Report I give some examples of cases in which data controllers sought my advice.

¹ Section 16 of the Act obliges certain data controllers to register with my Office. Broadly speaking, these are public sector bodies, financial institutions, credit referencing or debt collection agencies, those whose business consists mainly of direct marketing, and data controllers who keep data in one of a number of specific "sensitive" categories.

When I advise data controllers about particular courses of action, I always emphasise that my advice is given without prejudice. I cannot indemnify data controllers against subsequent complaints. To carry out properly the function of investigating complaints assigned to me by **section 10** of the Act, I have to examine each case on its merits; it is not possible to foresee all the circumstances which may arise, or the issues they may raise.

COMPLAINTS

During 1997, ninety-one people contacted me to complain that their rights under the Act had been infringed (in 1996 there were eighty-five such complaints). Not all of these cases evolved into formal complaints requiring decisions under **section 10**. As I have explained in previous Annual Reports, I distinguish between cases suggesting a once-off contravention of the Act and those that seem to indicate a systematic contravention, which I view much more seriously. My approach to the first category is to seek to resolve the issue in an informal manner. As this approach is generally successful, the result is that many cases are resolved to the satisfaction of both parties without the need for formal investigation under **section 10**.

The complaints I received in 1997 covered a wide range of issues but, as in previous years, there were two that came up repeatedly. One was the accuracy of credit records; the other was unsolicited direct marketing material. The latter raised a third issue which was an element in several cases — the use of the Electoral Register as a source of names and addresses for mailing lists. In **Part 2** of this Report (pages 23-30), I give examples of some of the complaints I dealt with in 1997.

DATA CONTROLLERS SHOULD NOW BE FAMILIAR WITH THE LAW

The Act is now in its tenth year. I have remarked before that the longer it is in effect the less I am inclined to entertain ignorance as a defence when its provisions are contravened, especially by major data controllers who have the resources to ensure that they are fully advised of their obligations. The Act provides that certain contraventions or offences may entail the forfeiture or destruction of data that have been unfairly obtained or misused. There is every possibility that there will be occasion to invoke such provisions in the future.

REDRESS FOR DATA SUBJECTS

It is not uncommon for data subjects, when complaining to me that their rights have been infringed, to ask me to award them compensation. I explain that the Act does not give me this function. When someone complains to me I will investigate the matter and notify him or her of my findings. On occasion, I may consider it necessary to take action, by issuing an *Enforcement Notice* under **section 10(2)**, to ensure that a data controller changes some practice that constitutes a systematic non-compliance with the Act. My role ends at that point.

A decision or an Enforcement Notice may be appealed to the Courts, but I have no function to award damages or compensation. However, the Act envisages such redress in **section 7**, which provides that

“For the purposes of the law of torts and to the extent that that law does not so provide, a person, being a data controller or a data processor, shall, so far as regards the collection by him of personal data or information intended for inclusion in such data or his dealing with such data, owe a duty of care to the data subject concerned”

REGISTRATION OF DATA CONTROLLERS

As indicated in previous Reports, registration of data controllers serves the following functions:

- it sets out in a publicly available manner the purposes for which personal data are kept by a computer user;
- it brings the more important data controllers into contact with my Office when they initially register and on an annual basis thereafter;
- it provides a mechanism through which some actions of data controllers can be prosecuted as contrary to criminal law; and
- it generates fee income which offsets a significant part of the costs of running my Office.

INCREASES IN REGISTRATION

The following table shows how registrations have increased since the Act came into effect in 1989.

1989	1990	1991	1992	1993	1994	1995	1996	1997
1,194	1,432	1,460	1,536	1,821	1,944	2,082	2,353	2,571
Increase	20%	2%	5%	19%	7%	7%	13%	9%

Appendix 3 (page 50) gives a breakdown of registered data controllers by sector. I am pleased that the higher level of registrations in the medical sector recorded in 1996 was maintained in 1997. I also welcome the fact that the number of public representatives on the register increased by 170%, from 31 to 84. An initiative by the Minister for the Environment, which required that candidates for public office meet their registration obligations before they could obtain a computerised copy of the Electoral Register, appears to have had the effect of alerting a significant number of public representatives to obligations under the Act of which they were previously unaware. I hope to be able to record a further increase in this sector in my next report.

SURVEY OF ATTITUDES AND AWARENESS

From the many thousands of individuals who have contacted my Office for help or advice since it was established in 1989, I have built up a picture of people's concerns about their privacy and about their position in an increasingly computerised society. Those who contact my Office are a self-selecting group, however, and some objective research was needed to measure the privacy concerns of the public as a whole. Therefore I commissioned an opinion survey which was undertaken in the final quarter of 1997.

I was heartened by most of the findings of the survey. It revealed a robust and deeply-felt concern about information privacy. Clear views were expressed by large majorities of respondents as to how they expected persons who keep information about them on computer to behave. The numbers of respondents who considered information privacy unimportant or who expressed no opinion were very small. This reinforces the day-to-day experience of my Office. Again and again my staff and I deal with people who may not speak the technical language of data protection, but who have a clear instinct about their own privacy rights.

In summary, the survey showed that people are very concerned to protect their information privacy and have well defined ideas as to the kinds of actions which would infringe their privacy rights. It identified the kinds of personal information that people regard as most private (financial and health data in particular), and it found that they had clearly held views about what public and private sector organisations should and should not do with information relating to them.

HOW MUCH DO PEOPLE CARE ABOUT PRIVACY?

In order to establish whether people cared about their information privacy, a number of general and specific questions were posed. The conclusion was very clear. A large majority of people felt their privacy was *very important* or *fairly important*, and the numbers who had no opinion or did not care were minuscule. When asked about the importance of “controlling what information is collected about you”, 97% thought it was *very important* or *fairly important* (82% and 15% respectively). Some 95% thought it was *very important* or *fairly important* (77% and 18% respectively) to be “in control of who can get information about you”. When asked about “not having persons watch you or listen to you without your permission”, 94% thought this was *very important* or *fairly important* (74% and 20% respectively). (The responses to this last question highlight the importance of clear signage of areas covered by closed circuit television monitoring, as recommended in my Annual Report for 1996.)

THE MOST SENSITIVE KINDS OF INFORMATION

People were offered a list of seven items of personal information, and asked how important they thought it was to keep each of them private. These were the results.

Table 1: how people ranked the privacy content of different kinds of information

	Very or Fairly important
• Financial history	92%
• Credit card details	85%
• Health information	83%
• RSI number	76%
• Telephone number	71%
• Address	62%
• Date of birth	50%

It is striking that people attached the greatest importance to financial history and credit card details, with 92% and 85% respectively feeling that it was *very important* or *fairly important* to keep them private.

This corresponds with the experience of my Office, where the largest category of queries from the public relates to credit histories. (The Data Protection Act itself recognises the importance of money and credit in people’s lives, by requiring financial institutions, insurance companies and organisations whose

business is wholly or mainly involved with credit referencing and debt collection to register with my Office.)

The respondents ranked health information third in importance, with 83% feeling it was *very important* or *fairly important* to keep such information private. (Under the Act, those who keep information on computer about people's physical or mental health are required to register, unless they are employers keeping it only for personnel administration purposes.)

USE OF DATA BY PUBLIC AGENCIES AND BY BUSINESSES

People were asked some questions about the use of their data by public agencies and businesses. While the result indicated slightly less concern about the use of data by public agencies, the responses nevertheless demonstrated a high degree of concern about privacy. People were asked how concerned they were about a range of propositions and the responses are shown in this table.

Table 2: people were asked how concerned they were about the use of their information by public agencies and businesses

	Very or Fairly concerned
• One company should be allowed to pass your information to another without asking you first	91%
• One public agency organisation should be allowed to pass your information to another without asking you first	88%
• When businesses get information about people, they should be allowed to use it as they please	86%
• When public agencies get information about people, they should be allowed to use it as they please	84%

This part of the survey reveals that people are clearly opposed to the unrestricted use of their information. It ties in with the high degree of concern about privacy shown by the answers to the preliminary general questions. The public's own views are obviously in keeping with the basic data protection principles that personal information must be obtained fairly, for specified and lawful purposes, and may not be used for any incompatible purposes.

IDENTITY NUMBERS

Questions were asked about a possible national identity card. The responses reveal a sophisticated set of views on this issue — while the majority were in favour of an identity card in itself, they distinguished clearly between this and a national identity number and its related uses.

When asked if a compulsory national identity card should be introduced, 53% of respondents *agreed* or *strongly agreed*. A minority – 43% – *agreed* or *strongly agreed* that businesses should be allowed to ask people to produce their identity cards.

But when people were presented with the proposition that public agencies should be allowed to demand a person's national identity number – as opposed to asking them to produce an identity card – the reaction was quite different: 59% *disagreed* or *disagreed strongly* (19% *agreed* or *strongly agreed*). The reaction was even more negative to the proposition that businesses should be allowed to demand a person's national identity number as opposed to asking for their identity card: 72% *disagreed* or *strongly disagreed*.

These responses suggest that while a majority of the public – albeit a narrow one – would support the introduction of a card for use by public agencies as a means of checking identity, they are nevertheless concerned about the use of a national identity number for data sharing or matching, even by public agencies.

SILENCE AS CONSENT?

I took the opportunity of the survey to test the public's attitude to so-called passive consent mechanisms. Such an approach arises when a data controller writes to a data subject saying that he intends to use the data subject's information in some way and saying that if he does not hear otherwise he will assume that the data subject has consented. This approach undermines the data subject's autonomy as a decision maker. It also ignores the fact that silence may simply mean that the data subject has not received the communication from the data controller.

It was striking that when the respondents to the survey were asked how they reacted to the proposition that passive consent was acceptable, 89% were *very concerned*, or were *fairly concerned* (67% and 22% respectively). This confirms the experience of my Office in dealing with individuals who complain about this issue.

AWARENESS OF THE OFFICE OF THE DATA PROTECTION COMMISSIONER

While people would appear to have some appreciation of their legal entitlements under data protection legislation and an instinctive awareness of acceptable and unacceptable information practices in the computer age, awareness of the role of the Office of the Data Protection Commissioner in these matters was very disappointing. Only 2% of respondents spontaneously mentioned the Office when they were asked to name organisations dealing with complaints about privacy. When prompted, one in four had heard of the Data Protection Commissioner and had some awareness of the Commissioner's functions. Clearly there is an overwhelming need to increase public awareness of data protection matters if the legislation is to be effective and the Office truly accessible to data controllers and data subjects alike, though as I have remarked already my efforts to increase awareness are subject to the resources available.

INTERNATIONAL

In my Annual Report for 1996, I commented on the international dimension of data protection law and practice — deriving not only from their foundation in international conventions and more recently EU law, but also from the huge changes which are taking place with the development of the global Information Society. The transposition into national law of the EU Directive 95/46/EC on data protection, to which I refer in **Part 3** of this Report (page 33), will mean that member states of the European Union will have a common standard of data protection law and will, in effect, speak with a single voice in their dealings with other countries.

ARTICLE 29 GROUP

Data protection authorities in European countries have for some years met and communicated regularly to share information and collaborate on the analysis of major issues of common concern. These *ad hoc* structures have been enhanced by a formal system under Article 29 of the EU Data Protection Directive, which established a *Working Party on the Protection of Individuals with regard to the Processing of Personal Data*, consisting of the data protection authorities of the Member States with a secretariat provided by the European Commission. This Working Party, known informally as the Article 29 Group, meets several times a year. It is a forum which provides a focus for the shared activities of the national authorities, and it will increase in importance once the Directive has been given effect in national law in the Member States. The Group has adopted documents on a number of issues including data protection law and the media and transfers of data outside the European Union. Appendix 2 (page 49) gives a list of these documents, copies of which are available on request from my Office.

EUROPOL

The EU Convention of 26 July 1995 establishing a European Police Office (Europol) is one of the most important steps taken at EU level to combat serious crime. The principal tasks of Europol are set out in Article 3 of the Convention as follows:

“(1) to facilitate the exchange of information between the Member States;

(2) to obtain, collate and analyse information and intelligence;

(3) to notify the competent authorities of the Member States without delay via the national units referred to in Article 4 of information concerning them and of any connections identified between criminal offences;

(4) to aid investigations in the Member States by forwarding all relevant information to the national units;

(5) to maintain a computerised system of collected information containing data in accordance with Articles 8,10 and 11.”

Articles 8,10 and 11 provide for:

(1) an Information System with a restricted and precisely defined content which allows rapid reference to the information available to the Member States and Europol;

(2) an Analysis System containing comprehensive information only accessible to personnel with Europol involved in a particular project;

(3) an Index System containing certain particulars from the analysis files.

In preparing the Europol Convention great care was taken to address the data protection issues associated with the operation of Europol and the Convention obliges each Member State to ensure a standard of data protection at least equal to that resulting from the implementation of the principles of the 1981 Council of Europe *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (the convention to which the 1988 Data Protection Act gives effect).

Primary legislation was necessary to put Ireland in a position to ratify the Europol Convention and this was passed in November 1997 as the Europol Act, 1997. Section 6 of this Act makes explicit the application of the Data Protection Act, 1988, to the automatic processing of information relating to individuals arising from the operation of Europol, while Section 7 designates the Data Protection Commissioner as the National Supervisory Body for the purposes of the Europol Act, 1997, and the Europol Convention. In practical terms this means that my Office is responsible for ensuring that general data protection principles and the specific principles of the Europol Convention relating to data protection are observed by An Garda Síochána in transferring data to and from Europol. Secondly, my Office becomes responsible for dealing with complaints alleging contravention of the data protection rules and thirdly, the Office provides the necessary input for the data protection supervision of Europol at a European level. This latter function is exercised through a Joint Supervisory Body consisting of members of the independent data protection authorities in each Member State of the EU. The Europol Convention provides that “The Joint Supervisory Body shall unanimously adopt its rules of procedure, which shall be submitted for the unanimous approval of the Council [of Ministers]”. This striking requirement for double unanimity underlines the importance of the role of the Joint Supervisory Body.

In anticipation of the establishment of the various organisations associated with Europol the Working Party on Police and Related Matters of the European Conference of Data Protection Commissioners met in the Hague on several occasions in 1997 to prepare for the coming into effect of Europol. The principal focus of attention was the preparation of the rules of procedure for the Joint Supervisory Body in accordance with the requirements of Article 24.7 of the Europol Convention. This proved to be a very complex task, not least because of deeply held but different views on the precise nature of the Joint Supervisory Body. Some considered it to be a “court like” body, others an administrative body alone. These differences were accentuated by the fact that under the Europol Convention the findings of the Appeals Committee of the Joint Supervisory Body are final as regards all the parties concerned. This is in marked contrast with the position regarding decisions of data protection authorities at national level which invariably are open to appeal through the courts of the country concerned. The unusual arrangement whereby decisions of the Appeals Committee are not subject to appeal flows from the Europol Convention itself and the inability of the Member States to agree unanimously on the role of the European Court of Justice in respect of Europol. Notwithstanding this I have every confidence that arrangements now in place for the proper supervision of Europol, from a data protection perspective, will in practice be highly effective.

ADMINISTRATION

PAYMENTS AND RECEIPTS

The cost of running the Office in 1997 was £361,708. An analysis of these costs is given in Appendix 4 (pages 51-53). Receipts from registration fees amounted to £218,216 which offset 60% of the cost of running the Office. Income from registration fees increased by 5.3% on 1996.

STAFF

I have seven staff. They have to cope not only with a large number of daily contacts with the public but also with investigations, educational and publicity work and the management of the Register of Data Controllers. I am fortunate in having a team of flexible, committed and highly competent people. I wish to record my gratitude to my Deputy, Mr Greg Heylin, and to my other staff, Mr Michael O'Donovan, Ms Anne Gardner, Ms Anne-Marie Lynch, Ms Marieanne Finlay and Ms Avril Brady. In particular, I would like to thank my secretary, Ms Catherine Conlon, who has contributed so much to the smooth and efficient running of the Office.

SUPPORT SERVICES

The computerised registration, case tracking and precedent system which was introduced in 1995 has now been fully operational for over two years. It provides a means of drawing together information relating to all aspects of the work of the Office and makes a substantial contribution to efficiency and the quality of service that we can provide. I have been fortunate in having among my staff a degree of expertise in information technology which enabled the system to be modified and enhanced when necessary.

Since the Office acquired an electronic mail address – *info@dataprivacy.ie* – early in 1997 it has been used by a wide variety of correspondents both in Ireland and abroad. The commissioning of a web site, which was something I had hoped to do during 1997, had to be deferred because of other priorities but I see this as a necessary service and I hope that 1998 will see progress towards making it a reality.

The Finance Division of the Department of Justice, Equality and Law Reform continued to provide my Office with an excellent service in relation to receipts and payments in 1997 and I should like to express my appreciation of their helpfulness.

PROTECTING YOUR PRIVACY IN THE INFORMATION AGE — SELF HELP

The advice which follows provides answers to some of the questions most frequently put to my staff. The answers emphasise the actions individuals themselves may take to remedy an unsatisfactory situation. People approaching my Office for advice are informed as a matter of course about the steps they can take to vindicate their rights under data protection law. It would be my hope that those complaining to my Office would as a minimum have taken the relevant steps in the guidance before lodging a formal complaint.

PROTECTING YOUR PRIVACY IN THE INFORMATION AGE — SELF-HELP

The Data Protection Act and the Office of the Data Protection Commissioner exist to better secure people's privacy interests as the Information Society evolves. While the Act provides legal safeguards and the Commissioner can assist, there are many ways in which a person can act to better secure his/her information privacy. Here are some hints.

What should I do when ...

- ***I am filling in a form seeking personal data i.e. information about me to be kept on computer?***

Read it carefully. It should tell you how your information will be used and to whom it will be disclosed. Often, these important details will be found in the "small print", perhaps in the terms and conditions on the back — an unsatisfactory practice but widespread nevertheless. Look for any options you may be given, for example to decline direct mail.

- ***I am asked for more information than I think necessary?***

Ask for what purpose the information will be kept and if the goods or service will be provided if a more limited amount of information is given. Often the answer will be yes. If it is no, then press for a clear description of what the information will be used for and to whom it may be disclosed. Whoever is obtaining your data must explain this to you, because they can keep personal data only for specified and lawful purposes and cannot keep more personal data than necessary for those purposes. If you are not happy with what you have been told, ask for a copy of the body's information privacy policy.

- ***I am asked for information about myself over the telephone?***

Ask at the outset whether or not the information will be kept on a computer. Insist on being given an opportunity to review and correct or amend the information at the end of the conversation. Ask what will happen to your information if you decide not to proceed with the proposed transaction. Insist on it being deleted if appropriate. If you proceed with the transaction ask that a copy of all the information being kept be forwarded to you. Do insist on being told *clearly* what the information will be kept for and to whom it will be disclosed.

- *I am using the Internet?*

Be careful! Remember, a certain amount of personal information is always transmitted when you use the Internet unless you use one of the “anonymising” packages that are available. Follow the advice given for Internet users in the Draft Council of Europe Guidelines in part 3 of this report (page 40).

- *I want my name removed from a mailing list?*

Simply write to the company that is sending you direct mail and ask them to remove your details from their mailing list. To make sure they comply with your request, it can be helpful to mention that you are making it under the Data Protection Act. The company has to write back to you within 40 days, confirming that they have done what you asked.

You can be removed from most mailing lists in Ireland in a single step, by using the ***Mailing Preference Service***, a voluntary scheme operated by the Irish Direct Marketing Association (IDMA) and An Post. You can get the necessary form at any Post Office. And a new ***Telephone Preference Service*** has recently been introduced by the IDMA in co-operation with Telecom Éireann to help people avoid unwelcome telephone calls from marketing companies; to use this, telephone the IDMA at 01- 6687155.

- *I want to check my credit record e.g. before seeking a bank loan or a mortgage?*

Make an **access request** under **Section 4 of the Act** in the normal way - write to the Irish Credit Bureau, give them your name and address and any other addresses you have lived at in recent years, ask them for a copy of any information they have about you, and don't forget to enclose the fee of £5 which they are entitled to charge for an access request. The address is: Irish Credit Bureau, ICB House, Newstead, Clonskeagh, Dublin 14.

Most of the main banks and finance houses in Ireland use the ***Irish Credit Bureau*** to check on people's credit records, and when someone borrows money the details of the loan, and the way the borrower keeps the terms, are recorded with the Bureau. The Bureau keeps information about a loan for five years after it is concluded.



Number 25 of 1988

DATA PROTECTION ACT, 1988

AN ACT TO GIVE EFFECT TO THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA DONE AT STRASBOURG ON THE 28TH DAY OF JANUARY, 1981, AND FOR THAT PURPOSE TO REGULATE IN ACCORDANCE WITH ITS PROVISIONS THE COLLECTION, PROCESSING, KEEPING, USE AND DISCLOSURE OF CERTAIN INFORMATION RELATING TO INDIVIDUALS THAT IS PROCESSED AUTOMATICALLY. [13th July, 1988]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

Preliminary

Interpretation and application of Act.

1.—(1) In this Act, unless the context otherwise requires— 15

“appropriate authority” has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

“back-up data” means data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged;

“civil servant” has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958; 20

“the Commissioner” has the meaning assigned to it by section 9 of this Act;

“company” has the meaning assigned to it by the Companies Act, 1963; 25

“the Convention” means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January, 1981, the text of which is set out in the *First Schedule* to this Act;

“the Court” means the Circuit Court; 30

“data” means information in a form in which it can be processed;

“data controller” means a person who, either alone or with others, controls the contents and use of personal data;

INTRODUCTION

This Part of my Report gives examples of cases with which I have dealt in 1997. It includes both complaints from individuals and cases in which I have given advice, either at their request or on my own initiative, to data controllers. These case-studies are chosen to illustrate my approach to issues which arise frequently or are significant in their implications. *Fair obtaining* is fundamental to data protection, and presents itself as an important consideration in a wide variety of circumstances. Case studies 1, 4, 7, 8, 9 and 10 all illustrate this in different ways. The requirement that data shall be *accurate and up to date* is also one that arises often – particularly where people’s credit records are concerned – and case studies 2 and 8 deal with this. Case study 6 describes how I used an Information Notice under section 12 of the Act in the course of an investigation. Case studies 3, 5 and 11 deal with access, use of the Electoral Register for direct marketing and disclosure of personal data respectively.

CASE STUDY 1 — hospital patient’s data disclosed for research – data not obtained fairly for this purpose

The complainant attended the accident and emergency department of a public hospital. A few months later, she was contacted by an organisation carrying out research. The researchers knew when she had attended the hospital and why, and they asked her to answer some questions.

The complainant objected to the fact that the hospital had told the researchers about her visit. She took this up herself with the hospital, but was not happy with the response and she complained to me. She said she had not been informed, when she attended the hospital, that her personal data would be used in this way.

I identified the data protection issue in this case as one of *fair obtaining*. **Section 2(1)(a)** provides that “*data or, as the case may be, the information constituting the data shall have been obtained ... fairly*”. I set out to establish whether, and if so in what way, the complainant’s personal information had been fairly obtained for the purpose of the research. I sought the hospital’s observations.

The hospital was in fact aware of its obligations under the Data Protection Act, but it contended that it had met these in two ways. First of all, it had listed “personnel engaged in medical research” as disclosees in its entry in the Public Register of Data Controllers which is maintained by my Office. Secondly, it had sought to make patients aware of the research project by putting a notice in the waiting area of the accident and emergency department. This notice told patients that the hospital intended to disclose their information to the researchers, and invited them to let the receptionist know if they objected.

I was unable to accept the hospital’s arguments. Its contention about the effects of registration with my Office raised an important issue which I discuss in more detail in **Part 3** of this Report (page 36). A data controller who must register with my Office under section 16 of the Act is legally obliged to provide details of the uses and disclosures of data. However this is a separate obligation from that of obtaining data fairly. I am of the opinion that for personal data to be fairly obtained, a data controller must make the data subject aware, directly and at the time his or her data are being obtained, of how such data may be used and to whom they may be disclosed, in order to get the person’s informed consent to the uses and disclosures described.

The hospital’s second argument related to the notice which it had placed in the waiting area. In my view, the issue to be decided was whether this was an adequate way of informing patients that their information would be disclosed to the researchers. In different circumstances, it might have been. In this case, however, account ought to have been taken of the particular environment in which patients’ data

were obtained. Many patients presenting themselves at the casualty department of a hospital may be expected to be in a state of some anxiety or discomfort. Consequently, they may not be expected to be alert to matters not relating directly to their condition. In such circumstances there is a special need for the data controller to satisfy itself that any uses of the data which are unlikely to be anticipated by the data subject are fully explained. For this reason, I took the view that the intention to disclose should have been brought to the specific attention of the complainant before data relating to her were obtained. This was essential to ensure that she was in a position to make an informed choice whether or not to furnish her information for such a purpose.

I upheld this complaint on the grounds that the measures taken by the hospital did not adequately fulfil its obligation of fair obtaining under section 2(1)(a).

CASE STUDY 2 — data about two people combined in one record kept by a credit referencing agency – issue of accuracy

The complainant looked for a loan to buy a car, but he was refused. He then made an access request under *section 4* of the Data Protection Act to a credit referencing agency.

The record he received in response showed that he had been lent money by a financial institution some years before, and that that loan had not been repaid according to the agreed terms. However the complainant had never had a loan with the institution in question, or any contact with it whatsoever. His record also showed that three other financial institutions had made enquiries about him to the credit referencing agency in the previous few months.

The complainant made his own enquiries to the institution from which he was supposed to have borrowed money previously. This institution confirmed that he had not borrowed money from it. The complainant was informed that the loan had in fact been taken out by a second party with the same name, and an address in the same general area as his own, but with a different date of birth. The complainant then informed the credit referencing agency that the loan related to a different person, and the lending institution confirmed this to the agency. Subsequently the agency wrote to the complainant saying that it had revised his record to delete the reference to the loan, and offering to send copies of its letter to all financial institutions which had accessed his record.

The complainant was aggrieved at what had happened. He asked me to investigate “wrong or misleading information” (i.e. the details of a loan which he had never had) which had been kept by the credit referencing agency and disclosed to those financial institutions which had made enquiries about him.

I sought the views of the credit referencing agency, which explained how the problem had arisen. When the second party had looked for a loan some years previously, the institution that he had approached had made two enquiries about him to the agency. The agency had no record of the second party, but it did have a record of the complainant. I was informed that two men had the same names and they both lived in the same general area, though their house numbers and street names were different. The credit referencing agency, following its practice when there is some similarity in names and addresses, sent the enquiring financial institution a copy of the complainant’s record “to allow them to determine from their greater access to information on their applicant as to whether there was any connection between the individuals of similar name”.

The complainant had been assigned a *customer record number* by the credit referencing agency, and this number was included in the copy of his record sent to the financial institution. The institution, when it subsequently approved a loan for the second party, erroneously associated the complainant’s customer record number with it and submitted the details electronically to the agency. As a result those details

were automatically appended to the complainant's existing record with the agency. (The credit referencing agency told me that some time later it had changed its computer systems so that details of new borrowings which contained customer record numbers were no longer automatically associated with existing records. Henceforth this would only be done by human intervention.)

I accepted that it was the financial institution and not the credit referencing agency which had made an error in assigning the complainant's credit referencing number to the second party's loan. However the agency was not justified in disclosing the complainant's record to the institution in the first place. His address was sufficiently different from that of the second party to clearly suggest that two different persons were involved. I was satisfied that the problems which ensued followed directly from this disclosure.

I upheld this complaint by reference to *section 2(1)(b)* of the Act which provides that information constituting personal data relating to a living individual "*shall be accurate and, where necessary, kept up to date*". I noted, however, that the inaccuracy was rectified when the complainant brought it to the attention of the credit referencing agency, and that the agency offered to clarify the situation to those institutions which had recently accessed the complainant's record.

CASE STUDY 3 — employees sought access to consultants' study

A company engaged consultants to evaluate some of its senior management posts. Knowing that the consultants' reports were kept in computerised form, the occupants of a number of these posts made a request to the consultants, under *section 4* of the Act, for copies of the information relating to themselves. The consultants did not respond within the period of 40 days provided for in *section 4(1)(a)*, and the employees concerned complained to me.

In keeping with my practice – which I have outlined in previous Annual Reports – of seeking in the first instance to resolve cases by agreement between the parties, I invited the consultants to meet me. They explained to me that this was the first time they had encountered a request under the Act for access to data arising from their work. As consultants they acted as agents for other organisations, which made their position sensitive. Furthermore, some of the information they kept – consisting of "scores" assigned according to certain criteria – derived from the application of proprietary methods, and they had some concern that disclosing it would amount to revealing commercial information of their own.

While I appreciated their concerns, I explained to them that *section 4* clearly provided for the complainants' right of access to their personal data. Following my discussions with the consultants they responded to the access requests to the satisfaction of the individuals, who informed me that the matter was resolved as far as they were concerned.

The issue raised by this complaint is one that occurs from time to time. Data controllers, faced with an access request under *section 4*, sometimes argue that there are special circumstances which in some way entitle them to respond either in a limited way or not at all. In such cases, I point out that the only restrictions on the individual's right of access are those laid down specifically in *section 5*. If none of the provisions of that section apply, then the request must be responded to no matter how inconvenient or disagreeable it may be for the data controller to do so.

CASE STUDY 4 — "small print" on application forms – inadequate for fair obtaining

The size of the print used by data controllers to inform data subjects how their information might be used was the subject of two cases dealt with in 1997. One concerned a form being used by a financial institution to collect customer information for a new service. The other related to a form issued through a supermarket chain promoting a product. In each case there was a statement explaining that the

customer's information might be used for direct marketing, and giving him or her the opportunity to decline such use. However the statements on both forms were printed in very small type whereas the details and purported advantages of the product and the service were presented in a much clearer and more attractive way. My Office cautioned the data controllers in these cases that there was a significant risk of contravening the Act in the course of action they had pursued.

Section 2(1)(a) of the Data Protection Act provides that that “*data or, as the case may be, the information constituting the data shall have been obtained ... fairly*”. In **Part 3** of this Report (page 36) I set out in detail the criteria for fair obtaining. It is necessary for the individual to be made aware, clearly and unambiguously, of the purposes for which his or her data are being obtained and the manner in which it is proposed to use and disclose them. I question whether the presentation in “small print” of information which has an important bearing on the information privacy choices of a data subject meets the fair obtaining requirements of the Act. This is especially the case where other information extolling the merits of the product or service on offer uses clear language and striking graphics. I am putting data controllers on notice that such practice, in my view, is unacceptable and in the event of complaints is likely to lead to a finding that the data in question have not been fairly obtained. This in turn may have serious consequences for the data controller concerned, not least being the inability to legally use any personal data obtained in reliance on the small print in question.

CASE STUDY 5 — use of Electoral Register to prepare mailing lists and for other purposes not related to its primary function – concerns about such use of publicly available information

In my Annual Reports for both 1995 and 1996 I referred to cases in which people had complained to me about uses of information about them which had been obtained from the Electoral Register. During 1997 there was again a significant number of complaints from people who had received direct mailings where the names and addresses had come from the Electoral Register. Two of these complaints related to a promotion for an alcoholic drink. Several others were from people who had received direct mailings from a financial institution which was a newcomer to the Irish market.

Once again, I was obliged to tell the complainants that the matter fell outside my remit because **section 1(4)(b)** of the Act provides that the Act does not apply to “*personal data consisting of information that the person keeping the data is required by law to make available to the public*”. The only remedy available to them was to request the companies concerned, under **section 2(7)**, to desist from using their personal data for direct marketing. A number of the complainants expressed in strong terms their disappointment that the Act did not give protection against what they considered to be an inappropriate use of the Electoral Register and an invasion of their privacy.

In another case, a registered adoption agency whose job is to trace birth parents of adopted children sought a copy of the Electoral Register on CD ROM from a local authority. The local authority contacted my Office for advice. In this case also I explained that the the Electoral Register, *in the hands of a local authority*, is excluded from the remit of the Act by **section 1(4)**. However I also explained my concern in principle about uses of the Register by other parties for purposes other than that for which it was compiled. I pointed out that if such uses became widespread then the Register could well be brought into disrepute — perhaps to the point where some people chose not to register to vote at all.

CASE STUDY 6 — ex-directory phone number obtained by insurance broker – Information Notice used to establish circumstances

Two people complained to me, separately, that a particular firm of insurance brokers had obtained their ex-directory telephone numbers and used these to contact them to try to sell insurance products. They

were surprised to be contacted at home, since they had taken the trouble to opt for ex-directory numbers, and they were indignant at what they saw as an aggressive invasion of their privacy. Both complainants speculated that the brokers had got their phone numbers in some illicit way, though neither offered any evidence for this.

I issued an *Information Notice* under **section 12** of the Act to the brokers. In response to the Information Notice, the brokers stated that in the majority of cases they obtained the telephone numbers of prospective clients from the telephone directory, but in some cases they got them from referrals by existing clients (in other words, existing clients were encouraged to suggest other people who might be interested in the company's products and services). However, the brokers indicated that they did not keep records as to who made such referrals and consequently they were unable to explain how they had come into possession of information relating to the complainants.

My decision was that in all the circumstances the investigation had not established that a contravention of the Act had taken place in these cases. In reaching this decision I took into account the fact that the data controller's account of the events had been given to me by way of response to an Information Notice, and that section 12 provides that —

“A person who, without reasonable excuse, fails or refuses to comply with a requirement specified in an information notice or who in purported compliance with such a requirement furnishes information to the Commissioner that the person knows to be false or misleading in a material respect shall be guilty of an offence.”

However I told the brokers that they should in future retain a record of how details of prospective clients were obtained. They agreed to do so.

CASE STUDY 7 — direct mailing to children – complaint by parent – issues of fair obtaining and keeping data longer than necessary

A father complained to me that his children had received direct mail from a company making a product used mainly by children. This complainant took the view that children were more vulnerable than adults to manipulation by marketing and should not be targeted in such a way.

I took the matter up with the company concerned and was referred to the agency which carried out its marketing activities. This agency informed me that as a result of the complaint it had deleted the data relating to the children in question, but in its response it produced material to show that they had responded some time previously to another promotional campaign.

The earlier promotional campaign had been a “once-off”. I told the agency that in these circumstances its actions raised two issues:

- First of all, the earlier campaign had been concluded for some time. **Section 2(1)(c)(iv)** provides that data “shall not be kept for longer than is necessary” for the purpose for which they were obtained in the first place. Consequently I asked the agency to consider whether it should still have the respondents' data at all. The agency explained that when people responded to promotional campaigns their data were generally kept for about a year, because it was quite common for people who had taken part in campaigns, or thought or pretended they had, to contact the promoters again subsequently. I accepted this argument as reasonable in the particular circumstances of the case.
 - Secondly, the children's data had been obtained for a single purpose — the conduct of the earlier campaign. I questioned whether it was open to the agency to use the data for another purpose without
-

first of all seeking the individuals' positive consent to do so. The agency undertook to keep this point in mind in future.

CASE STUDY 8 — credit record indicated that borrower had faced litigation and loan had been partly written off – issue of accuracy – previous concerns about fair obtaining revived

A man who had difficulty in getting a mortgage made an access request under *section 4* to a credit referencing agency. He found that there was a record relating to a hire-purchase agreement that he had entered into some years previously. This record showed that part of the loan had been written off. It also purported to show that before that had happened, litigation had been pending against him. (The credit referencing agency uses codes which show the history of a loan over a period of months.)

The man complained to me, and described what had happened with the hire-purchase agreement. The agreement was for four years, but the payment book he was given was for three years only. Believing that once the book was finished the loan was cleared, he stopped making repayments. Some months later the finance company looked for the remaining twelve monthly instalments, together with additional interest that had accrued since the complainant had stopped his payments. Following negotiations between the parties the data controller agreed to accept the twelve outstanding monthly payments and to write off the accrued interest.

The complainant alleged that his record with the credit referencing agency contravened *section 2(1)(b)* of the Act – which provides that “*data shall be accurate and, where necessary, kept up to date*” – in two respects: he denied that an element of the loan had been written off, or that litigation against him was ever pending.

My investigation of the complaint established that the hire purchase agreement had, in fact, been for four years, not three, and that the complainant had fallen into arrears in the fourth year. At that point, the account could have been transferred to the company's legal department for proceedings to be prepared against him. However this was never done. Accordingly, I found that the complainant's record was inaccurate in stating that litigation had been pending.

My investigation also established that a settlement had been agreed between the complainant and the finance company, in which the company waived the interest due on his late payments. In this respect, I found that the complainant's record was not inaccurate in stating that an element of the loan had been written off. However, this aspect of the complaint raised an issue about which I have expressed concern before — the consequences for a person who settles a loan for less than the full amount owed. *Section 2(1)(a)* of the Act provides that information constituting personal data “*shall be obtained and processed fairly*”. The obligation to obtain data fairly requires a high degree of transparency on the part of a data controller. I have expressed my concern before about whether there is sufficient transparency when loans are settled by agreement with amounts written off.

I reiterated my concern to the finance company in this case. I noted that the company had previously and voluntarily deleted the details of the loan altogether from the credit referencing agency's records. In this Report, however, I think it correct to point out that the practical consequences for a data controller of non-compliance with the fair obtaining requirement are potentially serious. *Section 6(1)* of the Act provides that —

“An individual shall, if he so requests in writing a data controller who keeps personal data relating to him, be entitled to have rectified or, where appropriate, erased any such data in relation to which there has been a contravention by the data controller of section 2(1) of this Act; and the data

controller shall comply with the request as soon as may be and in any event not more than 40 days after it has been given or sent to him”

The implication of this provision, in the context of cases like this, is that a data subject whose personal data have not been obtained fairly may assert his entitlement to have them deleted altogether.

CASE STUDY 9 — Data subjects who previously refused direct mail asked to make new choices – fair obtaining

A major data controller is engaged, as part of its operations, in direct mailing to its customers and also in host-mailing (mailing details of offers and services on behalf of third parties). This data controller, correctly, had previously given all its customers an opportunity to decline to receive such mailings.

The data controller contacted me to say that a certain number of people had complained about not receiving mailings — even though they had previously declined them. The data controller suggested that these people had not clearly understood the full consequences of the choices they were making, and proposed to contact them again to ascertain their true wishes. It was intended to send a letter outlining three options – to receive mail from the data controller alone, to also receive mail handled on behalf of third parties, or to receive no direct mailings at all – and seeking each data subject’s preference among these choices.

I took the view that on this occasion I would not seek to prevent the data controller from making contact – *once only* – with those customers who had previously declined to receive direct mail (though I foresaw a possibility that some customers who had previously declined all direct mailings might take exception to being contacted again and might complain to me, in which case I would of course consider such complaints on their merits). The substance of the proposed approach was that instead of the earlier option of receiving direct mail or not, three options were now being put to customers. In this particular case the balance of advantage appeared to me to lie in giving all customers, including those who had declined any further contact, an opportunity to make a more sophisticated choice. I told the data controller, however, that its proposal was acceptable to me only if it undertook that anyone who did not reply to the letter would be treated as if he or she had positively reiterated the original choice not to receive any mailings at all.

CASE STUDY 10 — Customer satisfaction survey – compatible use – merging of data – fair obtaining

A financial services company proposed to carry out a customer satisfaction survey, and approached my Office for advice. The survey was to be done by telephone, and the company intended to write to customers beforehand telling them about it and inviting them to ring a freephone number if they did not want to be contacted in this way. I told the company that, as a general principle, I resist any contention that silence can be interpreted as consent. However I suggested that the issue of consent might not actually arise in what it was proposing to do. The people it proposed to contact were its customers – people with whom they had an existing ongoing relationship for the purpose of providing a service – and it did not seem to me that a survey designed to find out whether its customers were happy with its service was likely to be a use of customers’ data *incompatible with the purpose for which the data were kept (section 2(1)(c)(ii))*. I had no objection in this case if the company wished to do more than the minimum required by law by contacting customers in writing first.

However, a second issue arose in the course of my discussions with the company about the proposed survey. The company explained that it proposed to collate a customer’s responses to the survey with his or her “product file” — this might show, for instance, that people who held a mortgage had complained about excessive and unintelligible paper work, and the company could review its practices accordingly.

It appeared to me that this proposal, though apparently innocuous, involved a degree of processing of a customer's data that he or she could not foresee. I advised that such processing should not be undertaken unless at the outset of the survey, each customer was informed that information provided in response to the survey would be collated with the customer's existing file. In this way I sought to ensure that respondents would be in a position to make an informed choice as to whether to provide the information sought, in full awareness of all the uses which would be made of that information.

CASE STUDY 11 — Direct mail for previous householder – decline direct marketing – inaccurate data – repeated promises

A man who bought a house found that direct mail, from several sources, arrived regularly for the former owner. My Office advised him to tell each sender that the former owner had moved, and when he did so all but one of them stopped the mailings. Post continued to arrive from a third-level educational institution, although it had made a number of promises that the matter would be rectified. This was a matter of some annoyance to the house-owner and he made a formal complaint to me.

I have had complaints before about mail being sent to an address after the sender has been told that the person concerned has moved. In my view this contravenes the requirement in *section 2(1)(b)* that data “*shall be accurate and, where necessary, kept up to date*”. If a data controller knows that the information he keeps about someone is out of date, he has an obligation to change it whether or not the data subject has asked for this to be done. In this case, the former resident of the house (who had been a student at the institution) had either forgotten or chosen not to tell the institution that she was moving. But the institution knew from the present owner that she was no longer there, and therefore it was wrong to keep that inaccurate address on its mailing lists.

When contacted by my Office, the institution apologised for the continued mailings. It explained that the inaccurate data had indeed been deleted previously from its mailing lists. However, in the course of computer maintenance work an earlier back-up version of the lists had been restored on the computer system.

This case illustrates a point which needs to be borne in mind by data controllers – generally those with sizeable data-holdings – who keep back-up copies. Given the obligation under *section 2(1)(d)* to take “*appropriate security measures*” against the “*accidental loss or destruction*” of data it is of course proper to keep back-up versions in case data are corrupted or erased. However it is necessary for data controllers to consider what measures they can take so that a back-up version, if restored, accurately replicates the live version of data that it has replaced. My Office drew the educational institution's attention to this matter and offered some advice on how it might be dealt with.



Number 25 of 1988

DATA PROTECTION ACT, 1988

AN ACT TO GIVE EFFECT TO THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA DONE AT STRASBOURG ON THE 28TH DAY OF JANUARY, 1981, AND FOR THAT PURPOSE TO REGULATE IN ACCORDANCE WITH ITS PROVISIONS THE COLLECTION, PROCESSING, KEEPING, USE AND DISCLOSURE OF CERTAIN INFORMATION RELATING TO INDIVIDUALS THAT IS PROCESSED AUTOMATICALLY. [13th July, 1988]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

Preliminary

Interpretation and application of Act.

1.—(1) In this Act, unless the context otherwise requires—

“appropriate authority” has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

“back-up data” means data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged;

“civil servant” has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

“the Commissioner” has the meaning assigned to it by section 9 of this Act;

“company” has the meaning assigned to it by the Companies Act, 1963;

“the Convention” means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January, 1981, the text of which is set out in the *First Schedule* to this Act;

“the Court” means the Circuit Court;

“data” means information in a form in which it can be processed;

“data controller” means a person who, either alone or with others, controls the contents and use of personal data;

INTRODUCTION

As information technology develops ever more rapidly and the European Union moves toward closer integration, the international dimension of data protection grows more and more significant. The 1995 EU data protection Directive is due to be transposed into national law in 1998 and in this part of my Report I offer some comments on that process. I also discuss the increasingly important issue of cross-border transfers of data, and I report on some work done at European level on the use of medical smart cards.

Some domestic data protection issues are dealt with in this part as well. More people contact my Office about their credit records than about anything else, and I comment on what I believe may be a significant lack of transparency in this area. I also comment on the final stage of the debate about uses of the RSI number.

Next, I discuss what I believe are two significant issues of principle. I set out to clarify an apparent confusion in the minds of some data controllers between the requirements involved in registering with my Office and their obligations under section 2 of the Act, and I offer my comments on the complex question of enforced subject access to personal data. Finally, I include draft guidelines on the protection of privacy on the Internet.

EU DIRECTIVE ON DATA PROTECTION

I have commented in previous Annual Reports on Directive 95/46/EC *on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, which is required to be transposed into Irish law during 1998. In my Report for 1996, I said that

“Transposition of the Directive into national law is of course a matter for the Oireachtas on the basis of a legislative proposal from the Government; I would advocate that there should be the widest possible consultation with all interested parties in advance of the preparation of the necessary legislation.”

I therefore welcomed the initiative taken by the Department of Justice, Equality and Law Reform in publishing a detailed *Consultation Paper* in November 1997 on the issues raised by the Directive. This document was available not only on paper but also on the Department’s web site with an e-mail facility, making it easier for interested parties to read it and give their observations.

The impending publication of a new Data Protection Bill is an opportunity not only to transpose the requirements of the Directive into Irish law but also to review the existing Act in the light of experience since it came into law in 1989. Discussions have also taken place between the Department and my Office in which I have taken the opportunity to make detailed comments and suggestions on the many complex issues that arise.

I note with interest the recommendation of the *Information Society Commission* that¹ —

“Every effort must be made to ensure that the EC Directive ... is transposed into Irish law before the implementation date in 1998. The objective of the Directive is to protect the fundamental rights and freedoms of individuals and, in particular, a right to privacy in relation to the processing of personal data. The Directive will in general extend the scope of the Data Protection Act, 1988 and in particular will apply the data protection principles to the holding and processing of manually held personal data.”

¹ *Report of Ireland’s Information Society Commission*, 1997, page 30

All Member States of the European Union are required to give effect to the Directive in 1998. In some states the new legislation is already in place; in others it is still in preparation or in the process of being enacted. In the United Kingdom, the Government opted to repeal its existing law (the Data Protection Act, 1984) in its entirety and introduce totally new legislation. Such an approach has its attractions – it allows a fundamental and comprehensive reassessment of all aspects of the law – but it does, of course, demand a very considerable investment of time and resources by all concerned.

TRANSFER OF DATA ABROAD

The Directive has significant implications for the transfer of data abroad, a matter about which a significant number of data controllers consult my Office. Often these data controllers are Irish-based subsidiaries of multi-national corporations.

With the development of electronic commerce and in particular the World-Wide Web, international transfers of data are becoming increasingly commonplace. (In the course of an investigation in 1995, I found that a magazine with an editorial address in the United Kingdom and a mailing address in the Netherlands appeared to be conducting at least part of its data-processing operations in one of the former Soviet Union states.) While the Directive will ensure a common standard of data protection within the European Union, national data protection authorities will find themselves engaged more and more in supervising and monitoring transfers to “third countries” (countries which are not within the EU or are not signatories to the Council of Europe Convention 108 on data protection), many of which may provide little or no legal protection for the privacy of data subjects². The fact that this is a real issue is recognised in *Article 25(1)* of the Directive which provides that —

“Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.”

The current approach: section 11 of the Data Protection Act

The Data Protection Act clearly foreshadowed the Directive’s approach to the transfer of data abroad. *Section 11* provides that

“(3) The Commissioner shall not prohibit a proposed transfer of personal data from the State to a place outside the State unless he is of opinion that the transfer would, if the place were in a state bound by the Convention, be likely to lead to a contravention of the basic principles for data protection set out in Chapter II of the Convention.

(4) In determining whether to prohibit a transfer of personal data under this section, the Commissioner shall also consider whether the transfer would be likely to cause damage or distress to any person and have regard to the desirability of facilitating international transfers of data.”

² For example, a considerable quantity of data is transferred from the EU to the United States. However, while there are some statutory controls in certain areas such as that of credit referencing, the USA does not have data protection legislation like the EU. It advocates instead that the private sector should follow voluntary practices for the protection of individual privacy. The business community in the USA maintains that this is superior to the European legislative approach and the matter is the subject of ongoing debate.

In keeping with section 11, my current practice – which has also been that followed by other national data protection authorities – is to advise data controllers who propose to transfer data abroad to carefully consider the implications of such transfers. It is up to them to take steps to ensure that the data are subject to adequate security provisions, are not used or disclosed in any way incompatible with the purpose or purposes for which they were obtained, and otherwise are treated in accordance with the basic data protection principles. In general, my Office suggests that the best approach is a formal contractual agreement with the person or institution to which the data are being sent. Data controllers are cautioned that if I received a complaint arising from something that had happened to data that had been transferred abroad, the starting-point of my investigation would be an examination of the protective measures that they had taken before making the transfer.

The EU Directive and transfers to third countries

The Directive now in effect puts in place for the European Union as a whole a formal system for policing transfers to third countries. **Article 25(3)** provides that Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure “an adequate level of protection” (essentially, an acceptable set of rules for the protection of information privacy and the means for ensuring their effective application). **Article 25(4)** provides that where the Commission finds that a third country does not ensure an adequate level of protection, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question. In other words, when the Directive has been given effect in national law throughout the EU, situations may arise where a data protection authority, on foot of a determination by the Commission, will have a duty to prohibit the transfer of data to a particular country.

The volume of transfers of data to third countries is already very large and can only increase. Therefore, it seems unlikely that it will be possible for Member States or the Commission to evaluate more than a small number of transfers in detail. **Article 25(6)** envisages a practical response to this situation, in which it could be determined that certain third countries ensured an adequate level of protection. While such determinations would be for guidance only, and therefore would not prejudice particular cases, it may well be that the EU data protection authorities collectively will resort to them as a means of clarifying the situation arising from Article 25.

Article 26 of the Directive provides a framework within which a contractual approach might be appropriate in many cases. This Article provides for certain exemptions to the rule set out in Article 25.

Article 26(2) provides that —

“a Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25(2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.”

Contractual provisions: some issues

If it is proposed to transfer personal data, under a contractual arrangement, to a third country where EU standards of information privacy protection do not exist, then essentially a contract must supply whatever is lacking in that jurisdiction. It must ensure that all the basic principles of data protection law are met. Furthermore, it should provide that the party receiving the personal data imposes similar obligations on future recipients of the data.

Contractual arrangements will not be a solution in every case. Some countries, such as those where the powers of state authorities to access information go beyond those permitted by internationally accepted standards of human rights protection, may not be safe destinations for the transfer of data in any circumstances. In others, the practical or legal difficulty of enforcing contracts may be such that it is pointless to attempt to rely on them. These complex and difficult questions have been the subject of preliminary examination by the Article 29 Group referred to in part 1 of this report and several of the documents referenced in Appendix 2 (page 49) set out the work done to date to resolve the issues.

REGISTRATION OF USES AND DISCLOSURES

Cases have come to my notice from time to time in which people have complained to me that their personal data had been used or disclosed in ways to which they had not consented when the data were first obtained. The data controllers concerned have pointed, in their defence, to the information which they have provided to my Office when they registered under *section 16* of the Act. Other cases have arisen in which registered data controllers have sought to amend their registrations to include new uses or disclosures. These cases raise an important issue.

Fair obtaining

The fundamental obligations governing the obtaining and use of personal data are set out in *section 2(1)* of the Act. *Section 2(1)(a)* provides that information constituting personal data “*shall have been obtained, and the information shall be processed, fairly*”. *Section 2(1)(c)* provides that the information

“(i) *shall be kept for one or more specified and lawful purposes [and]*

“(ii) *shall not be used or disclosed in any manner incompatible with that purpose or those purposes.*”

Fair obtaining is an *active* duty. It is up to the data controller, not the data subject, to make sure that it takes place. A booklet called *Keeping Personal Information on Computer: Your Responsibilities* is distributed widely to data controllers by my Office. In it I explain that for a data controller to satisfy the requirements of fair obtaining and purpose specification he must ensure that —

- (a) *At the time of providing personal information, individuals are made fully aware of:*
 - *the identity of the persons who are collecting it (though this may often be implied)*
 - *to what use it will be put,*
 - *the persons or category of persons to whom it will be disclosed*
- (b) *Secondary or future uses which might not be obvious to individuals should be brought to their attention at the time of obtaining personal data. Individuals should be given the option of saying whether or not they wish their information to be used in these other ways.*

The primary relationship under the Act is that between the data controller and the data subject, and the terms of that relationship are largely governed by what takes place at the time the data controller obtains the data subject’s information (significant subsequent modifications of that relationship require the *positive* and *fully informed* consent of the data subject). Any cases brought to my attention which may involve incompatible uses or disclosures, or unfair processing, will be judged in the light of what has taken place during that transaction.

Registration

Registration is a separate matter. A data controller who, under *section 16*, must register with my Office has to specify in his registration the nature of the data he keeps and the uses and disclosures which he intends to make. He must inform my Office of any subsequent changes to this information.

But registration is mainly a matter between the data controller and my Office, not between him and the data subject. What a data controller does about his obligations in respect of registration has little bearing on the primary relationship with the data subject. If he has not, in the first place, fulfilled his active duty to make the data subject aware of the intended uses and disclosure of personal data in such a way that the data subject can give informed consent, specifying them in the registration does not make up for that and will not, in my opinion, constitute an adequate defence against a complaint in relation to section 2 of the Act.

IDENTITY NUMBERS

In my Annual Reports for 1995 and 1996, I have discussed at length the data protection implications of proposals for changes in the Social Welfare system as a result of new uses of Information Technology. In my 1996 Report I commented in detail on the proposals from the Department of Social Welfare for the RSI number to be used in all dealings between a citizen and state agencies.

I have expressed my concern that the correct balance should be struck between, on the one hand, the need to provide evermore efficient and cost effective service free from fraud on the public purse and, on the other hand, the citizen's right to privacy. I have urged that this is a matter to be decided by the nation's elected representatives in the Oireachtas.

With the passing of the Social Welfare Act, 1998, by the Oireachtas, this debate is now at an end. During 1997, while the Bill was being drafted, I had discussions on it with the Department of Social, Community and Family Affairs. The Department found itself able to accommodate my views on some matters, but not on others. When the Bill was published in 1998 I had the opportunity, which I greatly welcomed, to outline my position to the Dáil Select Committee on Social, Community and Family Affairs. Because I consider that some aspects of the proposal raised major and fundamental privacy issues, I have included a copy of my remarks to the Select Committee in this Report as Appendix 1 (pages 45-48). The issues were considered at Committee Stage of the Bill in Dáil Éireann on 4 March 1998³.

PROCESSING OF MEDICAL DATA — SMART-CARDS AND ELECTRONIC TRANSMISSION

In my Annual Report for 1995 I described how my Office had been involved in lengthy consultations with the Department of Health and the Eastern Health Board before the introduction in Bray of a pilot project on the use of medical smart cards.

Since the pilot projects began in Ireland, France and Italy there have been moves in other European countries, and elsewhere, towards the wider introduction of medical smart cards. The related issue of the electronic transmission of health information, over ISDN lines or by way of the Internet, has also been the subject of some discussion.

³ Dáil Éireann, Parliamentary debates, Select Committee on Family, Community and Social Affairs.

Smart cards

There can be little doubt that before long smart cards will be widely used for many different purposes. They are convenient and cheap, and they can store and process large quantities of information. Advocates of smart card technology foresee a time when everyone will carry a card — possibly containing health information, details of transactions with various state agencies, and banking and insurance information. The same card might also serve as a security pass to a person's workplace, act as a pre-paid public transport ticket and even carry a quantity of electronic cash.

Such things are, of course, perfectly feasible and the advantages are apparent enough. However, whenever information technology develops in a way that makes it easier to collect and exchange information about human beings, there is a need to consider the ethical and legal implications of the application of such technologies as well as their purely technical aspects. I co-chaired with my Dutch counterpart that part of the fourth international conference on Health Cards held in Amsterdam in November 1997 which addressed such questions. The conference heard papers from data protection officials and academic commentators outlining different ways to find a balance which achieves the great benefits which the application of the technology can bring about without compromising the privacy rights of patients and other users of smartcard technology.

Electronic transmission of health data

The Conference on Health Cards also heard expressions of concern by experts about the security of data transmitted by the Internet. The nature of the Internet, where in a transmission from one point to another data may follow the quickest path between computers located in different countries, places a serious obligation on parties transmitting personal data to use the best available forms of encryption and other privacy-enhancing technologies. This is especially true in respect of health information. The obligation derives from one of the fundamental principles of data protection law, which is expressed in **section 2(1)(d)** of the Irish Act — “*appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction.*”

However, recent debates in the USA suggest that in some quarters there is a lack of confidence even in the privacy protection that a combination of legislation and privacy-enhancing technologies would offer. Proposals for a national medical database – with the benign intention of making it easier for people to switch between the many different private-sector providers of medical care and insurance with their histories and payment records intact – have been opposed by those who doubt that the information can be made secure. A report in the London *Times* explained:

*“There are practical worries: with computer hackers roaming the Internet – and, according to reports, the Pentagon mainframes – it is hard to guarantee that an easily operated, quickly established national database would be secure. The main practical safeguard at the moment is that different healthcare plans do not talk to each other. If they link computers, no Congressional Bill will protect the medical secrets of someone's past.”*⁴

CREDIT RECORDS AND CREDIT REFERENCING

Among the enquiries and complaints that I receive, the most common subject has consistently been that of credit records and credit referencing.

In a modern economy the ability to obtain credit is enormously important to most people. Yet many of the people who contact me are unaware, until my Office tells them, that when they take out a loan with one of the major banks or finance houses a record of that loan, and their performance in repaying it, will

⁴ *The Times*, 21 July 1998

be registered promptly with the Irish Credit Bureau and will be kept there for five years after the loan is completed.

This record will be available to any of the other banks and finance houses which are members of the Bureau.

In the course of a number of investigations I have found that the Irish Credit Bureau aspires to, and consistently achieves, a high level of compliance with the Data Protection Act's requirements that information shall be accurate and up to date. There have been comparatively few cases in which these requirements have not been met, and often these have had their origin in errors or faulty procedures on the part of the financial institutions which supply data about borrowers to the Bureau.

However, I believe that the area of credit records and credit referencing raises a more general issue which is for the financial sector as a whole to address. I am concerned to find so many individuals quite unaware that the fact that they are borrowing money, and the way in which they repay it, are not matters between themselves and the lender alone but will be available to most other financial institutions with which they may have dealings in the future. The first time they become aware of this is often when they encounter problems in getting credit and get in touch with my Office.

This situation raises a serious question about what information they were given when they first entered into their dealings with financial institutions. The requirement that information shall be *fairly obtained* (*section 2(1)(a)*) is one of the fundamental principles of data protection and, perhaps, the most important. Fair obtaining – as I have explained in detail on page 36 – means that a data controller must make it clear to an individual, *at the time that his or her information is first obtained*, what it will be used for and to whom it may be disclosed.

Elsewhere in this Report, I mention a case in which my Office advised a data controller that the “small print” on a form was not an acceptable way of informing data subjects about a proposed use or disclosure of their data — that if the question arose in the event of a complaint, I might well be of the opinion that an individual's data had not been fairly obtained in such a manner. (pages 23-24)

I have also, in my Annual Report for 1995, expressed a concern about what happens to an individual's credit record if he settles a loan for less than the full amount owed, or settles it late. In the context of a particular case in which an element of a loan was written off as part of an agreed settlement, and the borrower subsequently found that he had an adverse credit record, I said that the record itself had not been factually inaccurate but I added:

“This case raises questions about a data controller's obligations to notify a data subject of the consequences for his credit rating when he settles a loan agreement for less than the full amount due. I consider that where such settlements occur, the lender should notify the borrower of the consequences for his credit record of the settlement, and the fact that it will result in an unfavourable performance code being notified to credit referencing agencies.”

In future, when considering cases about credit records and credit referencing which come to my attention, I am likely to scrutinise the quality of information given to the individuals concerned when their data were being obtained and subsequently modified or updated. A failure to meet the necessary standard of fair obtaining, in a matter which touches people's lives in such an important way, is a serious matter. If someone's information was not fairly obtained in the first place, then it appears to me that the very entitlement of the data controller to keep it at all must be in question.

ENFORCED SUBJECT ACCESS

Enforced subject access occurs when a third party requires an individual (a) to make a subject access request under **section 4** to a data controller and (b) to present the data controller's response to the third party. It happens most often when someone is applying for a job.

This practice is objectionable in principle. The essence of data protection law is that it enhances privacy by putting the individual in control of his or her own information. The right to get a copy of one's personal data is fundamental to this. Enforced subject access may, I suggest, be said to be an unanticipated use – for totally different purposes – of what was intended to be a key aid for individuals in protecting their privacy. I can find no suggestion, in the record of the Dáil debates on the 1988 Act, that such a use of the right of access was foreseen by the legislature.

The former Data Protection Registrar in the UK was strongly opposed to this practice. In his Fifth Report to Parliament, he said:

*“I do not believe this is a proper use of the Act. I recommend that it should be prohibited with a criminal sanction. There are undoubtedly cases in which, when someone seeks employment or a licence, his criminal record should be available. Those cases should be specifically provided for in other legislation and not achieved by what many see as an abuse of the Data Protection Act.”*⁵

His successor, the present Registrar, has maintained this view. The new UK Data Protection Act, 1998, contains a provision making it an offence – except in cases where other legislation specifically permits it – to compel an individual for employment purposes, or in order to provide a service, or access goods, facilities or services, to obtain access to personal data relating to criminal convictions, police cautions and certain other matters.

In my Annual Report for 1996, I mentioned the case of a young man who had once been convicted of a minor offence but had appealed, and had had the Probation of Offenders Act, 1907, applied to his conviction so that it could not be mentioned if he were ever charged with an offence again. Yet when he made an access request to the Gardaí he found that the conviction remained on his file — correctly, because since Irish law makes no provision for “spent” convictions the Gardaí have no guidance on how long they should retain such records.

In this case the young man needed a copy of his information because he wanted to emigrate, and the Gardaí were able to help him by giving him a *Character Reference for Emigration* which showed, correctly under the terms of the Probation of Offenders Act, that he had no convictions. I see no practical or other reason why such “references” should not be made available in all cases where individuals need to give an assurance of their good character to an employer or some other party. The availability of such references should be enough to meet employers' needs and enforced subject access should then, in my opinion, be made unlawful except in cases where the Oireachtas has specifically chosen to provide otherwise.

COUNCIL OF EUROPE DRAFT GUIDELINES ON THE PROTECTION OF PRIVACY ON THE INTERNET

The Council of Europe has recently published draft guidelines entitled *The Protection of Privacy on the Internet* and has invited comments as part of its public consultation process. It is hoped that these guidelines, amended as necessary, will be presented to the Committee of Ministers for adoption before the end of 1998. Given the explosive increase in the use of the Internet the preparation of guidelines is very timely. They provide practical help for both Internet users and Internet Service Providers (ISPs) and are reproduced on the following pages. I would urge all concerned to consider them carefully and I will be glad to forward any comments received to the Council of Europe secretariat.

⁵ Fifth Report of the Data Protection Registrar (June 1989), para. 240

ESPECIALLY FOR USERS

Draft Guidelines on the Protection of Privacy on the Internet

1. Remember that the Internet is not secure. Use all available means to protect your data and communications, such as legally available encryption for confidential e-mail as well as access codes to your own PC.
2. Remember that every transaction you make, every site you visit on the Internet leaves traces. These “electronic tracks” can be used, without your knowledge, to build a profile of what sort of person you are and your interests. So ask for information about the privacy policy of programmes and sites and give preference to those which record few data or which can be accessed in an anonymous way.
3. Anonymous access to and use of services, and anonymous means of making payments, are the best protection of privacy. Find out about technical means to achieve anonymity, where appropriate.
4. If complete anonymity is impractical and if it is permitted by law you may use a pseudonym so that your personal identity is known only to your Internet Service Provider (ISP).
5. Only give your ISP, or any other person, such data as are necessary in order to fulfil a specific purpose you have been informed about. Be especially careful with credit card and account numbers, which can be used and abused very easily in the context of the Internet.
6. Remember that your e-mail address is personal data, and that others would like to use it for different purposes, such as inclusion in directories or user lists. Do not hesitate to ask about the purpose of the directory or other use. You can request to be omitted if you do not want to be listed.
7. Be wary of sites which request more data than are necessary for accessing the site or for making a transaction or which do not tell you why they want all these data from you.
8. Remember that you are legally responsible for processing of data for example if you illicitly upload or download, and that everything may be traced back to you even if you use a pseudonym.
9. Do not send malicious mail. It can bounce back with legal consequences.
10. Your ISP is responsible for proper use of personal data. Ask your ISP what data he/she collects, processes and stores, in what way and for what purpose. Repeat this request from time to time. Insist that your ISP change them if they are wrong or delete them if they are excessive, out of date or no longer required. Ask the ISP to notify this modification to other parties to whom he/she has communicated your data.
11. If you are not satisfied with the way your current ISP collects, uses, stores or communicates data, and he/she does not change his ways, then consider moving to another ISP. If you believe that the ISP does not comply with data protection rules, you could inform the competent authorities or take legal action.
12. Keep yourself informed of the latest privacy and security risks on the Internet as well as the methods available to reduce such risks.
13. Before you send data to another country ask the competent authorities in your country if the transfer is permissible. You might have to ask the recipient to provide safeguards necessary to ensure protection of the data.

ESPECIALLY FOR INTERNET PROVIDERS

Draft Guidelines on the Protection of Privacy on the Internet

1. Use all available procedures and new technologies to protect the privacy of the people concerned (users or not) especially by ensuring data integrity and confidentiality as well as physical and logical security of the network and of the services provided over the network.
2. Inform users of privacy risks presented by use of the Internet, before they subscribe to start using services. Such risks may concern data integrity, confidentiality, the security of the network or other risks to privacy such as the hidden collection or recording of personal data.
3. Inform the user about technical means which he/she may lawfully use to reduce security risks to data and communications, such as legally available encryption and digital signatures. Offer such technical means at a cost-oriented price, not a deterrent price.
4. Before accepting subscriptions and connecting users to the Internet, inform them about the possibilities of accessing the Internet anonymously and using its services and paying for them in an anonymous way (e.g. pre-paid access cards). If complete anonymity is not appropriate in certain circumstances defined by law, offer the possibility to use pseudonyms. Inform the user about programmes allowing them to search and browse anonymously on the Internet. Design your system in a way that avoids or minimises the use of personal data.
5. Do not read, modify or delete messages sent to others.
6. Do not allow any interference with the contents of communications unless this interference is provided for by law and is carried out by a public authority.
7. Collect, process and store personal data about users only when necessary for explicit, specified and legitimate purposes.
8. Do not communicate personal data unless the communication is provided for by law.
9. Do not store data for longer than is necessary to achieve the purpose of processing.
10. Do not use personal data for your own promotional or marketing purposes unless the person concerned, after having been informed, has not objected or, in the case of processing of traffic data or sensitive data, he/she has given his explicit consent.
11. You are responsible for proper use of personal data. Before the user starts using services, when he/she visits your site, and whenever he/she asks, inform him who you are, what personal data you collect, process and store, in what way, for what purpose and for how long you keep them. If necessary, ask for his consent. At the request of the person concerned, correct inaccurate data immediately and delete them if they are excessive, out of date or no longer required and stop the processing carried out if the user objects to it. Notify the third parties to whom you have communicated the data of modification. Avoid the hidden collection of personal data.
12. Information provided to the user must be accurate and kept up to date.
13. Think twice about publishing personal data on your site! Such publication may infringe other people's privacy and may also be prohibited by law.
14. Before you send data to another country ask the competent authorities in your country if the transfer is permissible. You might have to ask the recipient to provide safeguards necessary to ensure protection of the data.



Number 25 of 1988

DATA PROTECTION ACT, 1988

AN ACT TO GIVE EFFECT TO THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA DONE AT STRASBOURG ON THE 28TH DAY OF JANUARY, 1981, AND FOR THAT PURPOSE TO REGULATE IN ACCORDANCE WITH ITS PROVISIONS THE COLLECTION, PROCESSING, KEEPING, USE AND DISCLOSURE OF CERTAIN INFORMATION RELATING TO INDIVIDUALS THAT IS PROCESSED AUTOMATICALLY. [13th July, 1988]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

APPENDICES

Preliminary

Interpretation and application of Act.

1.—(1) In this Act, unless the context otherwise requires— 15

“appropriate authority” has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958;

“back-up data” means data kept only for the purpose of replacing other data in the event of their being lost, destroyed or damaged;

“civil servant” has the meaning assigned to it by the Civil Service Regulation Acts, 1956 and 1958; 20

“the Commissioner” has the meaning assigned to it by section 9 of this Act;

“company” has the meaning assigned to it by the Companies Act, 1963; 25

“the Convention” means the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data done at Strasbourg on the 28th day of January, 1981, the text of which is set out in the *First Schedule* to this Act;

“the Court” means the Circuit Court; 30

“data” means information in a form in which it can be processed;

“data controller” means a person who, either alone or with others, controls the contents and use of personal data;

SOCIAL WELFARE BILL, 1998

REMARKS BY THE DATA PROTECTION COMMISSIONER ON THE BILL TO THE DÁIL SELECT COMMITTEE ON SOCIAL, COMMUNITY AND FAMILY AFFAIRS, 4 MARCH 1998

Chairman

Thank you for your invitation to meet the Select Committee on Social, Community and Family Affairs about Part IV of the Social Welfare Bill, 1998 as initiated. Since I have the privilege in accordance with Section 14 of the Data Protection Act 1988 to report annually to each House of the Oireachtas on data protection matters, I welcome this opportunity to speak to you about what is undoubtedly the most important data protection issue you have been asked to consider since enacting the 1988 legislation.

International Background

The background, at an international level, to the extended use of personal identification numbers (PINs) is clearly set out in a report from the Council of Europe entitled *The Introduction and Use of Personal Identification Numbers: the Data Protection Issues*, and I would strongly urge you to consider that report as part of your deliberations. It gives an overview of the position on these matters in other countries and shows that they have been subject to the most intense parliamentary scrutiny. I draw your particular attention to a number of points from the report which have been highlighted for ease of reference. In particular:

- In the course of an exchange of views on PINs, the committee noted that they were by no means a neutral issue. Varying degrees of concern were being expressed in Member States with regard to their planned introduction and/or use.
 - There is no doubt that, at least in so far as universal PINs are concerned, real doubts are again being expressed in regard to their introduction and use. For example, the 1989 Privacy Act of Australia was foreshadowed by a vigorous campaign against the surveillance possibilities of a proposed so-called Australia card equipped with a number for each holder of the card. The project was dropped and the new Privacy Act has considerably circumscribed the use of the tax file number. In Canada, successive Privacy Commissioners have sounded warnings in regard to the creeping general application of the social security number.
 - Again in Canada, the 1987 report of the Standing Committee on Justice and of the Solicitor General (*A Review of the Access to Information Act and the Privacy Act*) made strong recommendations on the need to contain the use of the Canadian social insurance number. The report noted that the number was so important, so special and so much a symbol of the need for the data protection that it demands certain controls over its use. In its response to the Parliamentary committee, the Federal Government indicated that it would act to ensure that the SIN did not become a universal identification number.
 - There is no doubt that PINs, in conjunction with automatic data processing, tend to increase the power of the administration. As stated above, file interconnection via the use of unique identifiers allows
-

administrative bodies to match up personal information held in various distinct files. Accumulating data in this way excludes the data subject from the information circuit. It is no longer necessary for a particular administrative body to contact the individual with a view to acquiring information or checking information he has already furnished. The administrative body can conduct checks and controls by referring to other personal data files held by different parts of the administration. The administrative body can also top up the information it holds by borrowing information held by other such bodies for different administrative purposes. A single multi-purpose identifier for each member of the population is a critical part of this administrative process which can lead to an enormous increase in power within the administration.

Social Welfare Bill 1998 as initiated

The proposals in Part IV of this Bill are no ordinary amendments to the Social Welfare Acts. In my opinion what you are considering here is one of the keys to how the information society in Ireland in the 21st century will be implemented. The formulation of these provisions will set the tone for how relations between Government and governed, citizen and State are conducted in that century. To the best of my knowledge this is the first opportunity the Oireachtas will have had to consider such matters. It is of the greatest importance that the underlying issues should be fully explored and debated by the Oireachtas as has occurred in other administrations. I refer specifically to the Parliamentary debates which were associated with proposals for the extended use of the tax file number in Australia and the public consultation and Parliamentary debates on identity cards which took place in the UK in 1995/96 and more recent discussion of these issues in Canada.

It will be clear from what I have said so far that I have doubts as to whether or not a Social Welfare Amendment Bill in respect of which there is great urgency is the ideal vehicle for Parliamentary discussion of these issues. I appreciate that the only proposal before you is the Social Welfare Bill and that consideration of the Bill must be completed very shortly. But I believe that this Bill raises issues which go far beyond the modifications and adjustments to the Social Welfare system which such Bills normally make provision for. Accordingly I will now consider each of the key provisions of Part IV of the Bill against the background set out above. I will suggest ways in which, from a data protection point of view, it might be improved, as an interim solution, if time pressures do not allow the full consideration which the topic of general purpose identity numbers and cards deserves.

Several data protection concerns would be alleviated if the following changes could be accommodated in the Bill:

- a) substitute the words *a benefit, service, payment, allowance or grant mentioned at (a) to (g) in Section 223C(1)* for the words *public funds* in the definition of a transaction at page 13 line 7 and
- b) delete *Oifig and Árd Chláraitheoir* from the definition of a specified body on page 12 line 25.

Let me now explain how I have reached this conclusion.

Firstly I would ask you to consider what precisely is proposed at Section 14(1) of the Bill. I have not found it easy to determine the real purpose and full significance of the various provisions, 223, 223A, 223B and 223C. The Long Title gives no hint that this Bill is anything more than a routine amendment of the Social Welfare and Related Acts and the explanatory memorandum specifically states in respect of Part IV: *“The purpose of these provisions is to provide a legislative framework for the development of an integrated approach to the administration, delivery, management and control of public funded income support services”* (my emphasis).

Public funded income support services

Given this stated purpose I immediately look to the Bill for a definition of these services and I think I find it in Section 223C at page 14 line 37 under the definition *relevant purpose*. Now each of the items listed here with perhaps a little stretching in some cases may readily be perceived as an income support service. If this definition limited the application of Section 223 and Section 223A I would be in the happy position of thanking the Minister and his Department for taking on board several of the points my Office had made, and indeed I am glad to do so in respect of Section 223B and Section 223C.

However I must direct your attention to Section 223 and Section 223A and point out that there is no reference to *relevant purpose* as defined in Section 223C in respect of these sections and as a consequence the vital link and limitation associated with the purpose of all the provisions as set out in Part IV of the explanatory memorandum, i.e. public funded income support services, is missing.

Meaning of *specified body*

I would now draw your attention to Section 223(1) and in particular to the definitions of *specified body* (page 12 line 17) and *transaction* (page 13 line 1) and to their application to each of the Sections 223A, 223B and 223C (page 12 line 10). As regards *specified body* I would point out that it is a very wide ranging definition and covers not only the Minister for Social Welfare and his Department but also Departments such as Foreign Affairs, Agriculture, and Enterprise, Trade and Employment and, more significantly, bodies such as local authorities and An Post which are not accountable to the Oireachtas in the same way as Departments.

I draw your particular attention to the inclusion of Oifig an Árd Chláraitheoir (the Office of the Registrar of Births, Deaths and Marriages) as a specified body.

Meaning of *transaction*

I turn now to the crucial definition of *transaction* (page 13 line 1) and ask you to examine it most carefully. The first thing to note is the all embracing nature of the list (a) to (e): *an application, a claim, a communication, a payment, or a supply of a service*. The second is the phrase *relating to public funds* (line 7). I do not know the intended meaning of this phrase. If it is intended to cover only those items listed (a) to (g) in Section 223C, i.e. publicly-funded income support services (lines 39 onwards) I have few problems. I think this would be entirely in line with the purpose of the provisions as set out in Part IV of the explanatory memorandum and indeed with the long title of the Bill. However it seems to me that the phrase *relating to public funds* is open to a much wider interpretation (as is suggested by the sentence commencing “*It also contains certain provisions for the standardisation of the Revenue and Social Insurance (RSI) number as a unique public sector identifier...*” in the introduction to the explanatory memorandum). For example it may cover items such as industrial development grants, agricultural grants, first time home buyers’ grants and so on. It is also open to the interpretation that it covers items such as television licence fees, passport application fees, public exam fees, parking fines, local authority service charges, dog licence fees etc. **It is arguable that when coupled with the phrase a supply of service (line 6) it covers any service that any specified body provides which is financed from public funds.**

Now it seems to me that if anything beyond what is set out under *relevant purpose* (223C line 37 on page 13) is intended, this should be further clarified for the Oireachtas and is arguably something which should be dealt with in standalone legislation rather than in a Social Welfare Amendment Bill.

In my view clarity in respect of the meaning of *transaction* is of the utmost importance, because it is the foundation on which the powers given to the Minister and the obligations imposed on the citizen are based.

Powers given to the Minister

Examples of powers given to the Minister are:

- to allocate a personal public service number (page 13 line 9)
- to issue a public service card (page 13 line 45).

New obligations imposed on citizens in respect of transactions with all specified bodies (including An Post, local authorities and FÁS)

Examples of the additional obligations imposed on the citizen are:

1. to give a personal public service number in respect of one's self (page 13 line 18)
2. to produce one's public service card (page 14 line 6).

An interim solution

As I have suggested, the issues I have raised might be addressed in the short term as follows:

- a) substitute the words *a benefit, service, payment, allowance or grant mentioned at (a) to (g) in Section 223C(1)* for the words *public funds* in the definition of a transaction at page 13 line 7 and
- b) delete *Oifig an Árd Chláraitheoir* from the definition of a specified body on page 12 line 25.

The reason for a) is to clarify the range of services to which the personal public service number will apply as is already done in respect of the sharing of information and to confirm that the purpose of the provisions relates solely to public funded income support services.

The reason for the suggestion at b) – the deletion of *Oifig and Árd Chláraitheoir* – may at first sight seem puzzling. However the reason is in fact quite straightforward. It appears to me that the inclusion of the agency charged with the issuing of birth, marriage and death certificates has little or nothing to do with a set of provisions whose purpose is to provide a legislative framework for the development of an integrated approach to the administration, delivery, management and control of public funded income support services. However it might have everything to do with the creation of a National Population Register and a National Identity Number System. If this were the intention – and of course I accept the Minister's assurance (as reported in the Irish Times on 26 February 1998) that it is not – the matter should in my opinion be dealt with in standalone legislation, discussion of which might address the pros and cons of the introduction of a national personal identifier. As it is, I am still not entirely clear how a number which would apply to every transaction as defined in Section 223 and might be allocated via *Oifig an Árd Chláraitheoir* might meaningfully be distinguished from a national personal identifier. Hence my suggestion that (a) the definition of *transaction* be modified in the manner suggested above and (b) the deletion of *Oifig an Árd Chláraitheoir* from the list of specified bodies. This in my view would put the matter beyond reasonable doubt. Finally I would draw your attention for example to the extensive consultation process in respect of such proposals which was undertaken in the United Kingdom on this matter in 1996 and to the subsequent abandonment of such proposals at least for the present.

WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA (ARTICLE 29)

Number	Title
5012/97	Data Protection Law and the Media. Recommendation 1/97
5020/97	First Orientations on Transfers of Personal Data to Third Countries-Possible Ways Forward in Assessing Adequacy
5022/97	Recommendation 3/97: Anonymity on the Internet
5023/97	Opinion/97 on Canadian Initiatives Relating to Standardisation in the Field of Protection of Privacy
5025/97	First Annual Report
5057/97	Working Document: Judging Industry Self-Regulation: When Does it Make a Meaningful Contribution to the Level of Data Protection in a Third Country? (Adopted 14.1.1998)
5060/97	Recommendation 2/97: Report and Guidance by the International Working Group on Data Protection in Telecommunications (Budapest-Berlin Memorandum on Data Protection and Privacy on the Internet)
5005/98	Working document: The Use of Contractual Provisions in the Context of Transfers of Personal Data to Third Countries
5009/98	Recommendations 1/98 on Airline Computerised Reservation Systems
5032/98	Opinion 1/98 Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)

REGISTRATIONS 1994 – 1997

	1994	1995	1996	1997
<i>Data controllers by economic sector</i>				
Civil Service Departments/Offices	95	98	99	97
Local Authorities and Vocational Education Committees	121	121	118	118
Health Boards and public hospitals/clinics	39	39	41	42
Third level education	29	33	31	32
Primary and secondary schools	7	9	14	18
Commercial state-sponsored bodies	86	81	75	74
Non-commercial and regulatory public bodies	36	45	93	116
Associated banks	18	19	22	22
Non-associated banks	42	44	47	52
Building societies	8	8	8	8
Insurance and related services	123	115	120	134
Credit Unions and Friendly Societies	276	431	439	451
Credit reference/Debt collection	26	24	19	20
Direct marketing	39	42	42	45
Miscellaneous commercial	15	17	12	19
Private hospitals & clinics/other health	74	77	81	88
Doctors, dentists & other health professionals	163	180	242	269
Pharmacists	359	349	495	515
Political parties & public representatives	30	28	31	84
Religious, voluntary & cultural organisations	27	29	31	40
<i>Subtotal</i>	1,613	1,789	2,060	2,244
<i>Data Processors¹</i>	331	293	293	327
Total	1,944	2,082	2,353	2,571

¹A data processor is defined in section 1(1) of the Act as “a person who processes personal data on behalf of a data controller”. Section 16(1)(d) requires data processors “whose business consists wholly or partly in processing personal data on behalf of data controllers” to register.

REPORT OF THE COMPTROLLER AND AUDITOR GENERAL

In accordance with Paragraph 9 of the Second Schedule to the Data Protection Act, 1988, I have audited the Account on pages 52 and 53 which is in the form approved by the Minister for Justice, Equality and Law Reform.

I have obtained all the information and explanations that I have required.

As the result of my audit it is my opinion that proper accounting records have been kept by the Department of Justice, Equality and Law Reform on behalf of the Data Protection Commissioner and the Account, which is in agreement with them, properly reflects the transactions of the Commissioner for the year ended 31st December, 1997.

Joseph J Meade

For and on behalf of the Comptroller and Auditor General


14 September 1998

ACCOUNT OF RECEIPTS AND PAYMENTS IN THE YEAR ENDED 31 DECEMBER 1997

1996		1997
£	Receipts	£
289,248	Monies provided by the Oireachtas (note 1)	313,565
207,290	Fees	218,216
496,538		531,781
Payments		
208,476	Salaries & Allowances (note 2)	215,226
3,085	Travel & Subsistence	8,254
13,078	Office & Computer Equipment	2,397
5,622	Furniture & Fittings	2,094
7,019	Equipment Maintenance & Office Supplies	9,529
5,080	Accommodation Costs (note 3)	4,734
12,452	Communication Costs	12,511
6,047	Incidental & Miscellaneous	6,889
22,733	Education & Awareness	46,182
5,656	Legal & Professional Fees	5,749
289,248		313,565
207,290	Payment of fee receipts to Vote for the Office of the Minister for Justice, Equality and Law Reform	218,216
496,538		531,781

The statement of accounting policies and principles and notes 1, 2 and 3 form part of these accounts.

Signed



Fergus Glavey
Data Protection Commissioner

Date

10 Aug 1998

ACCOUNT OF THE OFFICE OF THE DATA PROTECTION COMMISSIONER

STATEMENT OF ACCOUNTING POLICIES AND PRINCIPLES

1. GENERAL

The Office of the Data Protection Commissioner was established under the Data Protection Act, 1988. The Commissioner's functions include supervising the implementation of the Act, ensuring compliance with its provisions, investigating complaints, dealing with contraventions of the Act, encouraging the preparation of codes of practice, establishing and maintaining a Register of data controllers and data processors who are required to register, and rendering mutual assistance to other data protection authorities.

2. ACCOUNTING ARRANGEMENTS

2.1 Moneys provided by the Oireachtas

The Commissioner does not operate an independent accounting function. All expenses of the Office are met from subhead F of the Vote for the Office of the Minister for Justice, Equality and Law Reform and, where necessary, from the Vote for Increases in Remuneration and Pensions (No 45). The expenditure figures in these accounts detail the payments made by the Department of Justice, Equality and Law Reform on behalf of the Office.

2.2 Fees

Fees paid to the Data Protection Commissioner in respect of registration and enquiries are transferred intact to the Vote for the Office of the Minister for Justice, Equality and Law Reform as appropriations-in-aid.

NOTES TO THE ACCOUNT

1. Moneys provided by the Oireachtas

Vote 19 - Office of the Minister for Justice, Equality and Law Reform Subhead F €313,565

2. Salaries, allowances and superannuation

(a) The Commissioner is appointed by the Government for terms not exceeding five years and his remuneration and allowances are at rates determined by the Minister for Justice, Equality and Law Reform with the consent of the Minister for Finance.

(b) Staff of the Commissioner's Office are established civil servants. Their superannuation entitlements are governed by the Regulations applying to such officers. A superannuation scheme for the Commissioner as envisaged in the Act was adopted by Statutory Instrument No 141 of 1993.

3. Premises

The Commissioner occupies premises at the Irish Life Centre, Talbot Street, Dublin 1, which are provided by the Office of Public Works, without charge. The provisional cost to the Office of Public Works of the accommodation provided in 1997 was € 48,143 (1996 cost € 51,877).
