Tenth Annual Report of the Data Protection Commissioner 1998

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

PN. 7761

FOREWORD

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

Fergus Glavey
Data Protection Commissioner
October, 1999

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

10 YEARS OF DATA PROTECTION IN IRELAND

Ireland is now very much in the information age. The Data Protection Act, 1988 can rightly be seen as one part of the infrastructure needed to underpin the new 'information society' which is characterised by instant processing of the information flows needed for access to, and delivery of, private and public services. To the extent that people are being asked, and indeed required, to provide personal information in these contexts, it is reasonable that safeguards be put in place to uphold the individual's right to privacy and to control over their personal details, and it is precisely this protection that the Act provides. It must be borne in mind that the Data Protection Act is now over ten years old, and that it was introduced at a time when the potential of computing power was not fully realised, and when the privacy implications of that extra computing power were only partially comprehended. The 1988 Act was drafted in general terms, rather than being couched in terms specific to the technology of the time, and this explains how robustly the Act has retained its relevance even as the applications of computer technology have advanced at a remarkable pace. The basic principles enshrined in the Act are ones that people can identify with, and which provide a broad measure of assurance in any computer-related context: personal data must be obtained fairly; they must be kept for a particular specified purpose; and they must not be disclosed to third parties without the individual's consent. In short, the privacy of the individual, and the authority of individuals over their own personal details, must be respected.

While the rapid technological progress of the past decade has contributed to the development of commercial and public service life in Ireland, it is fair to say that this development has been balanced with personal privacy safeguards. The Data Protection Act has served its purpose very well, and few organisations which deal with computerised personal information are unaware of their privacy obligations. *Appendix 3* of this Report shows that at end-1998, 2,650 persons or organisations dealing with personal data were registered with my Office, setting out clearly what types of personal data they hold, for what purpose, and to whom the data are disclosed. The data protection principles have steadily become ingrained in the decision-making and design processes of the main commercial and non-commercial organisations in Ireland.

The work of my Office has also developed substantially over the ten-year period. The key functions of case-management, maintenance of the Public Register and office administration remain central to the Office, and information technology has helped my staff to improve the effectiveness and efficiency of these operations. In addition, my Office has contributed to practical discussions with data protection authorities at EU and other international levels to an increasing extent. I have been

assigned additional responsibilities as the National Supervisory Body for the purposes of the Europol Act, 1997 and the Europol Convention, and I am likely to be assigned further data protection responsibilities relating to other EU initiatives such as customs information and fingerprinting of asylum seekers. At European level, I had the honour of being elected as the first Chairman of the Joint Supervisory Body of Europol. I also had the honour of bringing the annual Spring Conference of European Data Protection Commissioners to Ireland for the first time in 1998.

THE OUTLOOK FOR DATA PROTECTION IN IRELAND

While the Act has borne up remarkably well in terms of its relevance to changing technologies and practices, it is likely that the personal privacy landscape of Ireland in 2008 will be radically different from that in 1998, dwarfing even the changes of the past ten years. We are only now beginning to see the emergence of novel practices that will have enormous repercussions for personal privacy. Internet-based banking and on-line delivery of other financial services are still in their infancy in Ireland. The forward drive of e-commerce and e-government is only now building momentum. It is likely that devices and services that are today regarded as technological novelties will in future become as ubiquitous as the ATM cards and the mobile phones of today. In such an environment, we must ask whether the protections afforded by the 1988 Act will eventually become out-moded and ineffective.

In my opinion, the sound principles that underlie the Data Protection Act will continue to have relevance into the future. At the same time, the transposition of *EU Directive 95/46/EC* on data protection into Irish law will provide an opportunity to review the working of the Act and to ensure that it is 'future-proofed' as far as possible.

REVIEW OF DEVELOPMENTS IN 1998

This Annual Report gives a comprehensive overview of my activities during 1998. The Report is divided into three Parts and five Appendices.

In **Part 1**, I summarise the day-to-day work of the Office, including statistics on the use of my services by the general public. 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. Included in this section is a reference guide for schools on maintaining data privacy in the internet age. I also outline some developments in international data protection practice. This Part concludes with some details of office administration.

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) on meeting their obligations. These examples are chosen to highlight various aspects of the Act as it applies in real-life situations.

In **Part 3**, I comment on particular issues of policy and practice. I give an account of the 1998 Spring Conference of European Data Protection Commissioners, and I provide details of activities coming within the scope of the 'Third Pillar' of the EU, including work related to Europol. I also comment on the issue of disclosure of telephone billing data to law enforcement agencies, and I provide an overview of modern 'data matching' techniques that have significant implications for data privacy.

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. [13*th July*, 1988]

BE IT ENACTED BY THE OIREACHTAS AS FOLLOWS:

PART 1

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

At the outset of this tenth Annual Report under the Data Protection Act, 1988, I believe it is useful to refer back to the first Annual Report which was presented by my predecessor a decade ago. In that first Report, he identified a number of issues of particular interest to the work of this Office, and he summarised their importance as follows:

- Education and awareness

  The principal aim of any data protection authority must be to make the public aware of the legislation.

- Enquiries and complaints

  The approach I have adopted is to deal with each complaint as informally as possible in the first instance.

- Registration of Data Controllers and Data Processors

  The essence of data protection is transparency.

- International activities

  The importance of the international aspect of data protection cannot be over-stressed.

- Resources

  If all these functions are to be carried out properly, serious consideration will have to be given to providing the resources necessary to ensure that the reputation, already painstakingly built up for the Irish legislation and its supervisory authority, will continue to be maintained and enhanced.

These issues were as relevant in 1998 as in 1988, and in this opening Part of my Report I outline my activities in 1998 under similar headings. This Part also contains some information that may be of interest to schools using the internet and the world wide web as part of their educational programmes. The subsequent Parts of my Report include more in-depth discussion of issues of particular interest.

EDUCATION AND AWARENESS

Before individuals can exercise their rights under the Data Protection Act, it is necessary that they be aware of these rights and understand them properly. Likewise, those who keep information on computer about other people must be aware of their statutory obligations in this regard. My Office provides a free advisory service to both "**data controllers**", as those who keep information on computer about individuals are referred to in the Act, and to "**data subjects**", as the individuals in question are referred to. In addition to dealing with queries raised with my Office, I seek to pro-actively increase awareness of people's rights and responsibilities under the legislation.

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 1998, about 40,000 of these leaflets were distributed throughout the country. There is also a booklet designed for data controllers, which outlines their obligations clearly and explains the criteria for registration. Over

E-mail, the Internet and Data Protection

Some Guidelines for Schools

The following guidelines reflect both the advice issued by the National Centre for Technology in Education (NCTE) and my experience in the light of actual casework in my Office. Schools with specific queries may wish to contact the NCTE, or my Office in respect of data protection issues.

1. The School On-Line Policy

Every school should have a clear, written policy regarding the rights, privileges and responsibilities associated with internet usage. The policy should include a code of conduct to be signed off by all participants, and should be notified to parents/guardians.

2. Child-Friendly Filtering Software

There are a number of software products designed to block access to inappropriate material when browsing the web. Schools should contact the NCTE or their internet service provider for advice on ensuring that such software is installed properly.

3. Monitoring and Supervision

Filtering software is not entirely foolproof, so all internet and web sessions should be monitored to guard against access to harmful material. In particular, chat room sessions should always be supervised, and registration or the signing of visitor s books at web sites should not be generally permitted.

4. Risks with e-mail

Children s full or last names, or any information specific to the child, the child s family, or to the school, should not be transmitted without permission from the teacher. In general, the teacher should not permit disclosure of a child s personal details without prior consent from the parent or guardian.

Any threatening, demeaning or otherwise inappropriate e-mail messages should be reported to the teacher. On no account should such messages be responded to.

The opening of e-mail attachments from unsolicited or unknown sources should not be permitted.

5. Risks with web sites

No images of children should be made available on the school web site without the express permission of the parents or guardians in question. Great care should be exercised when dealing with personal information that could be associated with an identifiable child, including information regarding hobbies, interests and friends.

From the point of view of data protection law, no data relating to children should be used or disclosed by the school without the explicit prior consent of the parents/guardians. Disclosure in this context would include publication on a school web site. If schools are in any doubt on this matter, the proper course is to refer to the parents/guardians to inform them of the proposed use of the personal data, and to obtain their express permission in advance.

32,000 of these were distributed in 1998. A detailed *Guide to the Data Protection Act* is also available for those requiring a fuller understanding of the Act's various provisions. In addition to circulating information literature, my Office placed advertisements in trade and specialist journals over the course of 1998, and my staff made themselves available to give talks and presentations at a number of fora. The demand for these services far outstrips the capacity of my Office to respond and there is clearly a need for a wholetime information officer to co-ordinate these activities and organise them on a professional basis.

Pressure on this front will increase enormously when the 1988 Act is amended to effect the transposition of *EU Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data* into Irish law. This change will of course necessitate a thorough revision of all of the information literature produced by my Office. Experience in other jurisdictions indicates that this is a major task. Planning for this undertaking started in 1998 but real progress must await publication and enactment of the new legislation. I will make every effort to ensure that both data subjects and data controllers are made aware of modifications to their rights and responsibilities as quickly as possible.

Educational and promotional activities accounted for 40% of my Office's non-pay spending in 1998.

SCHOOLS I.T. 2000 — INFORMATION ON DATA PROTECTION

In November 1997, the Government launched *Schools IT 2000*, an initiative to develop the use of information and communication technologies in all schools. The National Centre for Technology in Education (NCTE) was established to manage the implementation of *Schools IT 2000*, and to provide policy advice on this matter to the Department of Education and Science. This initiative will undoubtedly help to foster an appreciation of the benefits of computer-related technologies, as well as equip students with the practical skills they will need in today's world. It is of course important in this context that both students and teachers have a critical awareness of broader issues, including privacy, security and fair information practices. Accordingly, the Director of the NCTE, Mr Jerome Morrissey, and I wrote jointly to the principals of the 4,300 primary and post-primary schools, providing information on data protection, and encouraging the schools to factor this element into their IT education programmes.

The NCTE includes data protection in its ongoing initiatives including the teaching skills initiative, and has also issued specific advice to schools on the appropriate use of the internet and the world wide web in an educational context. It is worthwhile, I believe, to re-state here the key elements of this practical advice for the benefit of school principals and computer teachers, and I have set out this material on the facing page. The case study on page 27 sets out how these data protection principles were applied in a particular real-life situation.

ENQUIRIES

The major part of the day-to-day work of my Office involves dealing with queries. Many different categories of people avail of this service, including individuals, students, researchers, solicitors, accountants and news media, along with a wide range of data controllers (such as financial institutions, Government Departments, small businesses, direct marketing companies, hospitals, medical practitioners and public representatives). My Office strives to deal promptly, efficiently and courteously with all queries. Some are as simple as: am I entitled to get my records from my bank? Others may be as complex as: what new obligations will I have under *Directive 95/46/EC* when exporting genetic data to a country without comprehensive data protection legislation?

I maintain a computer system to track the volume of calls to my Office, and an analysis of the records indicates that my Office dealt with over 2,000 separate contacts in 1998. About 1,500 of these contacts were telephone-based queries. Of the 2,000 contacts, about 600 were from data controllers, and the remainder were from data subjects, the general public and other groups. While the overall number of contacts was similar to that of the previous year, I noted an increased interest in data protection issues from students, teachers and researchers.

DATA SUBJECT QUERIES

Many of the individuals who contacted my Office requested general information on the Data Protection Act, and an 'information pack' was posted to them. Most callers, however, had a query about how their data protection rights applied in specific circumstances, and received appropriate advice from my staff. As in previous years, a large number of callers had questions about how to access their credit rating, and my staff advised such callers to make an access request under ***section 4*** of the Act to the Irish Credit Bureau, which maintains such records on behalf of the main banks and building societies. There were also many requests about the right of access in other situations, and my staff explained that ***section 4*** entitles a data subject to obtain a copy of any information held about him/her on computer, from any data controller in the private or public sector, subject only to some very limited exemptions.

I continue to receive calls from people who have received unwanted direct mailings. My staff inform such callers of their right under ***section 2(7)*** of the Act to have their data removed from direct marketing lists. I also advise such callers of the *'Mailing Preference Service'* (MPS) operated by An Post in conjunction with the Irish Direct Marketing Association (IDMA). By registering with this service (forms are available in post offices), individuals will automatically have their details deleted from any mailing lists operated by the main direct marketing companies. 1998 also saw the launch of the *'Telephone Preference Service'*, a comparable service offered by Eircom in conjunction with the IDMA, whereby individuals can register their wish not to receive unsolicited telephone calls from direct marketing companies. Contact points for these useful services are set out in the box below.

Opting Out of Direct Marketing Contact Points

Mailing Preference Service

Application forms for registering with this service can be obtained from most post offices, and can be returned by Freepost. Further details are available from Freephone 1800 501 000.

Telephone Preference Service

Registration forms are available in Eircom Telecentres, or alternatively you may wish to contact the Irish Direct Marketing Association directly at this address: IDMA, The Powerhouse, Pigeon House Harbour, Dublin 4. Telephone (01) 668 7155 - Fax (01) 668 7945

I should point out that I am now receiving fewer complaints from the general public regarding unsolicited direct marketing material, and I think that this reflects well upon the Irish direct marketing industry, which is increasingly aware of its responsibilities towards individuals under the Act.

DATA CONTROLLER QUERIES

Data controllers and data subjects contact my Office in roughly equal numbers to raise queries. Many responsible data controllers seek advice on meeting their statutory obligations towards individuals, and

I place a particular emphasis on finding privacy-friendly solutions to the issues they raise. Data controllers most commonly enquire about their registration obligations, and my staff explain the provisions of ***section 16*** of the Act which deals with this matter. In addition, data controllers raise a diverse range of issues concerning the practical application of the data protection principles set out in ***section 2*** of the Act. These principles require *inter alia* that a data controller must obtain and use personal data fairly; must ensure that the data are accurate and kept up-to-date; must be kept only for one or more specified and lawful purposes; must not be disclosed in any manner incompatible with that purpose; and must not be kept for longer than is necessary for that purpose.

In many cases, the application of these provisions is straightforward. However, given the pace of technological innovation and the growing technological sophistication of businesses, there will always be areas where data controllers or their legal advisers will refer to this Office for guidance. My Office welcomes such requests for assistance as an opportunity to clarify matters for data controllers, thus hopefully reducing problems for the future — even if this means making clear that a proposed course of action would be contrary to the Act. In my view, it is far better to assist data controllers in complying with their obligations, and to steer them towards fair information practices, than for individuals to suffer an invasion of their privacy and subsequently complain to my Office.

However, I consistently point out to data controllers that any general advice which I provide does not indemnify them against complaints which may be made by data subjects. While my advice should help avoid the problems that give rise to complaints from data subjects, any actual complaints will be investigated impartially and decided on the merits of each particular case.

COMPLAINTS

In 1998, seventy-eight people contacted me complaining that their rights under the Data Protection Act had been infringed. The greater proportion of these complaints were resolved informally, through the intervention of my Office. An example of this type of case is where a data subject is unhappy with the response of a data controller to a subject access request under ***section 4*** of the Act, and where some intervention from my Office is required to ensure that the data controller complies with its obligations. Not all cases can be resolved in this way, and the more complicated cases may need to be subjected to a full investigation by my staff, leading to a formal decision under ***section 10*** of the Act.

While the range of issues raised by complainants is quite wide, it is fair to say that recurring themes are the concerns of individuals with regard to their credit rating, and concerns regarding inappropriate disclosures of personal details by data controllers to third parties. **Part 2** of this Report gives examples of some of the complaints dealt with in 1998.

REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

Most data protection laws provide for the registration of data controllers and data processors. In general terms such schemes may be considered as a cross between company registration procedures and the licensing arrangements applicable to financial institutions. When first-generation data protection laws were being framed in the 1970s, it seemed both practicable and sensible to require all data controllers and processors to register. The dominant form of computing at the time was mainframe-based, and a handful of large organisations in both the public and private sectors accounted for the vast bulk of the processing of personal data. By the time the 1988 Act was introduced significant technological change

was underway and accordingly the Irish legislation provided for a scheme of selective registration. This essentially provides two quite different criteria for assessing whether or not a data controller must register. These are —

- the identity of the data controller, for example all public authorities and financial institutions; and
- the kinds of data kept, for example details of political opinions, medical history or criminal convictions.

This two-prong approach suggests that, on the one hand, certain types of data controller should be registered by virtue of the degree of control they exercise over personal data, and on the other hand, that data controllers who keep particularly sensitive types of data should also be registered. Most modern data protection laws in other administrations provide for a scheme of selective registration similar to ours, although some countries such as New Zealand have dispensed with registration entirely. Registration in the Irish context 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 the number of registrations has increased since the Act came into effect in 1989.

year	1989	1990	1991	1992	1993
no. of registrations	1,194	1,432	1,460	1,536	1,821
annual increase		20%	2%	5%	19%

year	1994	1995	1996	1997	1998
no. of registrations	1,944	2,082	2,353	2,571	2,650
annual increase	7%	7%	13%	9%	3%

Appendix 4 (page 51) gives a breakdown of registered data controllers by sector. Registration levels continue to increase, although the annual rate of increase has slowed to 3%. In part, this slower rate of increase may be due to a ‘saturation effect’, as very many of the organisations and individuals that are required to register have done so by now. It may also be due in part to the limited number of staff available in my Office for registration work, and the increasing pressure of other work priorities. The fact that registration numbers continue to increase steadily, along with fee income from registrations, reflects creditably upon the efficiency and dedication of my staff. I would hope to re-examine the whole question of registration in the context of the new legislation required by the EU Directive.

INTERNATIONAL

EVOLUTION OF DATA PROTECTION IN EUROPE

Europe has a long and distinguished history of concern for privacy and data protection matters. As far back as 1975 it was noted that —

> *The commitment to restrain modern surveillance practices is particularly evident in Europe. War and despotism have left a permanent consciousness that economic progress cannot be isolated from attention to individual rights*[1].

When the 1988 Data Protection Act was passed, the key international instrument dealing with data protection was the 1981 *Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data* (Convention 108), which was ratified by Ireland and effected in Irish law by means of the 1988 Act. While the Council of Europe continues to contribute significantly to data protection, the evolution of the European Union has — in data protection matters as in all other areas of law-making — assumed an ever-growing importance. Thus the focus has shifted from Strasbourg, home of the Council of Europe, to Brussels, the seat of the EU. In practical terms, this means that Irish data protection law will in future be determined in Brussels as part of the European process, in the absence of any uniquely Irish initiatives. Those who recognise and value data privacy as a human rights issue might be inclined to welcome this state of affairs, given that there has been little evidence of any wide-ranging debate of privacy issues in Ireland, particularly in the context of the evolution of the information society. However, a significant event in 1998 was the publication of the *Law Reform Commission Report on Privacy, Surveillance and the Interception of Communications.* I am hopeful that consideration of this report will awaken an awareness that, in the words of the Report —

> *Privacy is at the heart of the implicit social contract in every society by which the terms of peaceful co-existence are set. In short, privacy entails much more than the protection of the person in seclusion; it is a way of organising society.*[2]

In my view, recognition of this fact would ideally lead to the consolidation of several existing or recommended statutory protections on privacy, including data protection provisions, under the heading of a Privacy Act. In the absence of such a development, the dominant influence on Irish data protection law and practice will be found in Brussels for the foreseeable future. In the short term, this will entail the transposition into Irish law of *EU Directive 95/46/EC* on data protection and the related *Directive 97/66/EC*, which deals with telecommunications matters.

Article 29 Working Party

Article 29 of *Directive 95/46/EC* provides for a Working Party, comprised of representatives of the independent data protection authorities in each of the EU member states, to advise on data protection matters at EU level and to work out practical solutions to the issues raised by the Directive. On a day-to-day basis, the ongoing work of this 'Article 29 Group' is one of the most important international influences on my Office. The Group also serves as a sounding board for the European Commission on general data protection matters. During 1998, the Group worked on such diverse topics as the *Platform*

---

[1] *Privacy and Protection of Personal Information in Europe, A Staff Report of the Committee on Government Operations,* United States Senate, March 1975 (Preface)

[2] *Privacy, Surveillance and the Interception of Communications,* Law Reform Commission, June 1998 (Part 1.13)

for Privacy Preferences (P3P) and the *Open Profiling Standard (OPS);* issues associated with Airline Computerised Reservation Systems; transfers of personal data to third countries; the assessment of data protection codes of conduct; and the *'International Safe Harbour Principles'* put forward by the United States Government. A comprehensive list of the Recommendations of the Article 29 Group is given in Appendix 3. In my view, this forum is likely to evolve into the key 'clearing house' for all issues associated with the practical application of the EU Directives relating to data protection.

MEETINGS OF DATA PROTECTION COMMISSIONERS

While *EU Directive 95/46/EC* currently dominates the European data protection agenda, it would be misconceived to consider it the only focus for international developments in data protection. Several other international focal points are of importance. The first of these is the Spring Conference of European Data Protection Commissioners. I had the honour of hosting this annual event in Dublin in 1998. This was the first occasion on which this Conference was held in Ireland and it involved an enormous amount of additional work for the Office. An overview of the topics considered and the conclusions reached is given in **Part 3** of this Report.

The second annual event and importance is the International Conference of Privacy and Data Protection Commissioners, traditionally held in the autumn. A distinguishing feature of this Conference is that it is open not only to data protection authorities but also to representatives of consumer groups, industry groups, Government advisors, academics and information technology specialists. In my experience, it is the participation of these diverse interests which adds real value to this event, along with the contribution of data protection authorities from non-European countries such as Australia, Canada, New Zealand and Hong Kong. This annual Conference truly brings together all those concerned in privacy protection in the global information society. In 1998, the Conference was held in Santiago de Compostela, Spain. Among the issues addressed were concerns relating to the treatment of credit rating data; ethical codes for electronic sales on the internet; and ways of raising the awareness of individuals regarding the protection of their personal data.

Meetings with UK Data Protection Authorities

Meetings between my Office and my counterparts in the United Kingdom, Guernsey, Jersey and the Isle of Man are held twice-yearly. In 1998, these meetings were held in Dublin in June and in the Wilmslow offices of the UK Data Protection Registrar in November. Given the close similarity between our 1988 Act and the UK's Data Protection Act of 1984, and the shared common law foundations of our legal systems, such meetings are of enormous practical benefit to me and my staff. A considerable body of case law and administrative practice has developed in the UK, most of which is directly applicable, with little modification, in an Irish context. The UK Data Protection Registrar and her staff have over the years and throughout 1998 been unsparing in their help and co-operation.

Other International Fora

Before concluding this section on international data protection co-operation, I should mention for reference purposes a number of other fora where important data protection work is concluded, but where there is no active participation at present by my Office. The first of these is the Council of Europe which produced Convention 108. As mentioned earlier, the significance of the data protection work undertaken by the Council of Europe has in recent times been superseded to some extent by the EU initiative, at least insofar as EU members such as Ireland are concerned. The second forum of note is the OECD, whose *Data Protection Guidelines* remain a significant international point of reference. Finally, I should mention the Working Group on Telecommunications which is convened by the Berlin

Data Protection Commissioner. This Group has taken the lead in relation to important questions such as encryption, secondary uses of telephone directories and caller line identification. The Group was very influential in the formulation of the policy underlying *Directive 97/66/EC*. In the past, my Office was able to participate in this Working Group's activities, but such participation has not been possible in recent years owing to pressure on my limited staff resources and the development of other work priorities.

ADMINISTRATION

PAYMENTS AND RECEIPTS

The cost of running the Office in 1998 was £364,171. An analysis of these costs is given in Appendix 5 (pages 52-54). Receipts from registration fees amounted to £220,778 which offset 61% of the cost of running the Office. Income from registration fees increased by 1.2% on 1997.

STAFF

Over the past year, my Deputy, Mr Greg Heylin, the Assistant Commissioner, Mr Michael O'Donovan, and Clerical Officers Ms Catherine Conlon and Ms Marie Finlay moved on from my Office to other posts. I wish to record my sincere gratitude for the immense contribution they have made to the work of the Office in recent years. Mr Heylin has now been replaced by Mr Tom Lynch, Mr O'Donovan has been replaced by Mr Ronnie Downes, and Ms Finlay has been replaced by Ms Irene O'Keeffe. These replacement staff, together with my existing staff Ms Anne-Marie Lynch, Ms Anne Gardner and Ms Avril Brady, brought the total staffing complement of my Office to six people at the end of 1998, still one fewer than the start-up staffing level assigned when the Office of Data Protection Commissioner was established in 1989. I am glad to note that just prior to the publication of this Report, Mr Sean Sweeney was assigned to the Office as an Executive Officer, making good the outstanding vacancy.

My staff deals with a high volume of daily contacts with the public, as well as undertaking investigations of complaints, educational and publicity work, ongoing office administration, and the management of the Register of Data Controllers, which is increasing in size year-on-year. In addition, my Office's EU and other international dealings are becoming increasingly significant. As pointed out elsewhere in this Report, I am the national representative on the Joint Supervisory Board of Europol, and I am likely to be assigned new data protection responsibilities in the area of customs and immigration cooperation at EU level. All of these developments, while positive from a privacy protection point of view, place new demands on the staff of my Office. I am glad to express my appreciation of the highly competent and dedicated team of people who are responding positively to these pressures.

In each of the years 1990, 1991 and 1992 my predecessor indicated in his Annual Reports that the staff resources available were inadequate for the achievement of the tasks assigned to the Office. As far back as 1992, he reported that —

> *The staff complement of my Office was the same as in previous years. The extent to which data protection can be fully effective depends, in the final analysis, on the resources that are made available. Although we are living in an era of public sector cut-backs, many factors are increasing the pressures on existing resources. These include: the increased use of computers and personal*

information; the growing number of privacy issues arising from the demands of administrative efficiency; the need to enforce the Act through the exercise of my legal powers; and the requirement to carry out random searches and inspections of possible defaulters.

All these factors demand a much greater investment in resources to give effect to the original intent of the legislation . An examination of work activities in my Office for 1991 confirms that existing staff levels will not accommodate anticipated increased work loads, and will, accordingly, be insufficient to enable me to carry out the full range of my statutory functions. The higher level of data protection envisaged in the European Community makes the problem of resources more urgent still.

By end-1998 the volume and complexity of the work required to be undertaken by the Office had multiplied in comparison with end-1991 and yet my Office had no more staff than originally provided for in 1989. I have sought a significant increase in the number of staff assigned to the Office in the context of the proposed amendment of the 1988 Act required by *Directive 95/46/EC*. The staffing of the Office has been inadequate for many years now and it is essential that the staff sought should be provided soon if the Office is to be in a position to provide any reasonable level of service to the public, whether they be data controllers or individual data subjects.

SUPPORT SERVICES

I have long recognised the valuable contribution that computer technology can make towards improved efficiency of office administration in a public service office. The computerised registration, case tracking and precedent system which was introduced in 1995 continues to facilitate the smooth running of the Office's business. I will continue to prioritise the improvement and development of my Office's computer capabilities, in those areas where I am satisfied that there is a tangible benefit to be realised in terms of improved service to the public.

The Office's general e-mail address — *info@dataprivacy.ie* — continues to be the contact point used by a significant number of people to raise queries with my Office. My next immediate priority is to develop a comprehensive web site, which will provide answers to the most commonly asked questions, reference material that will be of general interest, as well as providing for customer feedback and for specific queries. The web site will be the key part of my Office's contribution to the development of 'electronic government' in Ireland. In due course, I envisage that all of the key functions of my Office — from accepting registration applications from data controllers, to the filing of complaints from data subjects — will be capable of being effected though the medium of the web site.

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 1998 and I should like to express my appreciation of their helpfulness.

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. [13*th 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

Since the underlying principles of data protection law are couched in general terms, a description of my dealings with practical situations helps to convey the relevance of the Act's provisions in everyday life. In addition, the application of the Act in particular circumstances often raises issues of interpretation that have not been dealt with before. This part of my Report outlines some cases that I feel may be either of general interest, in terms of illustrating the importance of the Act's provisions for individuals, or of relevance to data controllers who may learn from the experience of others. Included among the following case studies are issues regarding the management of access to staff details within a large organisation; the requirement of some telemarketing organisations to register with my Office; obtaining of consent for membership of loyalty card schemes; and data protection considerations with regard to school web sites. Public service bodies should note the limitations on the application of the Act to personal data that is presumed to be in the 'public domain' (*Case Study 6*). I have also included an example of enforcement of data protection on a transnational basis (*Case Study 7*).

CASE STUDY 1 — employee data - appropriate security measures - disclosure

A large organisation, whose staff are employed at several locations throughout the country, used a central database to record information relating to its employees and their work. The complainant questioned the security arrangements in respect of his personal data, and the extent of access to such data throughout the organisation.

The organisation's computer system comprised about a hundred personal computers nationwide connected to a central computer in the Dublin head office. Some sixty laptop computers were also provided for use by employees when away from their offices. These laptops contained a version of the organisation's main database which was downloaded from the main computer and updated periodically. Accordingly, data kept by the organisation on its main database was available to staff in the head office, in the local offices, and at off-site locations.

The complainant, an employee, made his complaint while the computer system was still being developed and implemented by the organisation. He made the following points. First, he alleged there had been a breach of security because the laptops were without any password protection for a period during the development of the system. Second, the complainant objected to certain of his personnel data and details of his work activity being generally available to staff, and argued that such data should only be available to those who needed them to perform their managerial functions.

Section 2(1)(d) of the Data Protection Act provides that *"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."* The question of the security of access to the laptop computers was considered in the light of this provision.

My investigation established that each laptop required use of a password for access to the local version of the database. Where a laptop was establishing a connection to the main computer, another password was needed, and access to the main database itself required the use of a third password. In principle this approach appeared to conform well with the requirements of section 2(1)(d) above. However, the apparent effectiveness of this approach had been compromised. In the interests of simplicity of operation the organisation issued a unique centrally-generated password to each member of staff (so that each staff member would only need to remember one password) thus reducing the effectiveness of the password system as a whole. Furthermore, in the course of training staff on an upgraded version of the software, the password security system was modified to allow trainees ease of access to the system. This modification gave open access to the main database from a number of laptops.

As soon as this fact was discovered, the data controller took steps to rectify the matter. It is not appropriate for a data controller to allow his standards of security to slip, so that personal data becomes more widely accessible than is necessary. However, I noted the prompt action taken by the data controller to put matters right, and — given that my investigation did not discover any evidence of unauthorised access or use of the data during the period when the passwords were not in operation — I did not uphold this part of the complaint.

The second ground for complaint put forward was the alleged wide availability throughout the organisation of details relating to the complainant's work activities including particulars of annual and sick leave. This raised two separate but related issues: first, whether this wide availability constituted *"disclosure"* for the purposes of the Data Protection Act; and second, whether the wide availability of data was consistent with the organisation's duty to take *"appropriate security measures ... against unauthorised access to, or alteration, disclosure or destruction of, the data and against their accidental loss or destruction."*

On the first question, I noted that the only people with access to the main database were the staff of the data controller. The definition of *"disclosure"* given in ***section 1(1)*** of the Act, specifically states that disclosure *"does not include a disclosure made ... to an employee ... for the purpose of enabling the employee ... to carry out his duties"*. In my opinion, these words require a data controller to make an assessment, in respect of particular employees, as to whether such employees need to have access to particular holdings of personal data, and to provide accordingly. Thus, one would expect a Human Resources Manager to have access to personal data not necessarily available to the manager of a client database, and *vice versa*. Data controllers should, in my view, take reasonable steps to prevent personal data from being made available to employees who may have no work-related interest in the data.

On the second question, I consider that sensible restriction of the availability of personal data is one of the *"appropriate security measures"* that data controllers must consider. The more people who have access to personal data, the greater is the risk of unauthorised access or disclosure. These issues were discussed with the data controller in detail. The organisation explained that the wide availability of personnel information and staff operational details was due in part to business requirements, and in part to the culture and tradition of the organisation. Following discussions, the data controller made a number of significant changes to the computer system, at some expense, in order to restrict access to the personal data of employees. It is my view that, in a case such as this, an appropriate balance must be struck between the concerns of the employee as data subject, the real operational requirements of the organisation and the costs to the organisation. I took the view that, following the changes referred to above, the data controller was compliant with the Act.

CASE STUDY 2 — use of telemarketing company in the management of customer accounts - transfer of data to agent not disclosure - obligation of data processors to register

The complainant received an unsolicited telephone call from a telemarketing service company. The call was in connection with the complainant's account with another company (the 'supplier company'), not the telemarketing company. The complainant raised the matter with my Office, expressing concern that details of his name, address, telephone number and certain details of his account (which was in arrears) had been transferred from the supplier company to the telemarketing company, without the complainant's knowledge or consent. He also said that the telemarketing company was not registered with my Office as required under the Data Protection Act, 1988.

In the course of my investigation, the supplier company indicated that it had engaged the telemarketing company under contract to provide a 'courtesy call' service on the supplier company's behalf. To enable the telemarketing company to carry out this service, the supplier company provided it with customers' personal data on a weekly basis. In the case of new customers, the 'courtesy call' service involved telephoning the customers to welcome them and to verify names, addresses and billing details. In the case of customers whose accounts were in arrears, the telemarketing company would operate a 'customer reminder' service, contacting the customers to alert them to the position before the issue of a final demand for payment. All customer responses would be logged by the telemarketing company onto the customer's computer file. The telemarketing company would also offer to take credit card payments over the phone. The supplier company had concluded a confidentiality agreement with the telemarketing company and required all staff involved with the customer courtesy service to sign a non-disclosure agreement.

It was clear from the terms of the contract between the companies that the telemarketing company was providing its services on an agency basis. ***Section 1(1)*** of the Act defines *"disclosure"* as follows —

> *"disclosure", in relation to personal data, includes the disclosure of information extracted from such data and the transfer of such data but does not include a disclosure made directly or indirectly by a data controller or a data processor to an employee or agent of his for the purpose of enabling the employee or agent to carry out his duties ... .*

Consequently, the transfer of data to the telemarketing company for the purpose set out in the contract did not constitute disclosure of data within the meaning of the Data Protection Act, and so this aspect of the complaint was not upheld.

The second issue raised by the complainant related to the alleged failure of the telemarketing company to register as required under the Data Protection Act. The telemarketing company was of the view that, as it was acting as an agent for the supplier company, which was registered as a data controller with the Data Protection Commissioner, the telemarketing company was not itself required to register.

Section 16(2) of the Act provides as follows —

> *The Commissioner shall establish and maintain a register (referred to in this Act as the register) of persons to whom this section applies and shall make, as appropriate, an entry or entries in the register in respect of each person whose application for registration therein is accepted by the Commissioner.*

Persons to whom section 16 applies include at ***subsection (1)(d)*** —

> *data processors whose business consists wholly or partly in processing personal data on behalf of data controllers.*

Section 1 of the Act defines *"data processor"* as —

> *a person who processes personal data on behalf of a data controller but does not include an employee of a data controller who processes such data in the course of his employment.*

It was accepted by all parties that the service provided by the telemarketing company amounted to the processing of personal data on behalf of the supplier company. As the provision of such services was a business activity of the telemarketing company, I decided that the company was clearly a data processor which was required to register with my Office. Accordingly, this aspect of the complainant's case was upheld. The telemarketing company subsequently registered as a data processor.

CASE STUDY 3 — joint bank account - issue of accuracy - disclosure - right of access

The complainant and another person held a joint account with a bank. It came to the complainant's attention that her name was not included in the details of the account kept by the bank. The bank undertook to correct the omission. Subsequently, the complainant found that the name which was recorded on the account was not her own, but a name similar to hers that could be regarded as having a certain public notoriety. In a letter to the bank the complainant alleged that the bank had failed to meet its responsibilities under the Data Protection Act, 1988, in the following respects —

- *maintaining an inaccurate record*
- *disclosing the information to an unauthorised person*
- *failing in its duty of care to her*
- *causing her damage and distress*
- *failing to provide information on request.*

The complainant raised the matter with my Office. This complaint concerned a number of distinct issues, which were considered separately in the light of the various relevant provisions of the Data Protection Act. In the first instance, ***section 2(1)(b)*** of the Act obliges data controllers to ensure that *"the data shall be accurate and, where necessary, kept up to date"*. In addition, ***section 6(1)*** entitles a data subject *"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"*.

The bank acknowledged to me that the complainant's name had initially been omitted from the details of the account and that another name, not that of the complainant, had subsequently been incorrectly entered through a typing error. When this error was brought to the bank's notice it was immediately corrected and a letter of apology was sent to the complainant.

I adjudged the bank to have contravened section 2(1)(b) of the Act in that the complainant's data had not been accurate and up to date, and I upheld this aspect of the complaint. However, in my formal decision on the matter, I acknowledged the fact that the bank had rectified the mistake at the earliest opportunity in compliance with section 6(1) of the Act.

As to the alleged disclosure by the bank of personal details to an unauthorised person, I had regard to ***section 2(1)(c)(ii)*** of the Act, which requires that personal data *"shall be not be used or disclosed in any manner incompatible with [the specified and lawful] purpose [for which the data are kept]"*.

Disclosure, in the case in question, would occur only if data relating to the account-holder were made available to a third party. The complainant made no reference to any specific instance of disclosure. The bank informed me that the only occasion on which the inaccurate information had been made available outside the bank was in a statement to the other joint account holder. The issuing of a bank statement to joint account holders would not ordinarily, in my view, constitute a disclosure in contravention of the Act, and this aspect of the complaint was not upheld.

Finally, I considered the question of the data subject's right of access to her personal data. ***Section 4(1)(a)*** of the Act provides as follows —

> *Subject to the provisions of this Act, an individual shall, if he so requests a data controller in writing —*

(i) be informed by the data controller whether the data kept by him include personal data relating to the individual, and

(ii) be supplied by the data controller with a copy of the information constituting any such data,

as soon as may be and in any event not more than 40 days after compliance by the individual with the provisions of this section.

In her letter to the bank, the complainant had written —

"I want my subject access request under the Data Protection Act to be complied with to the fullest extent to which I am entitled ... I want to know what computer files the name and/or address has been linked to within the bank and I want to see those files."

I am satisfied that this constituted a valid request by the complainant under section 4 of the Act for a copy of her personal data. The bank responded to the complainant, shortly before the expiry of the 40-day reply period, by forwarding to her a copy of its official 'access request application form'. This response did not, in my view, constitute compliance with the individual's access request, and accordingly I upheld this aspect of the complaint against the bank. Data controllers must appreciate that where an individual supplies them in writing with sufficient information to process the access request, and meets the other requirements (for example payment of the processing fee that may apply) set out in the Act, then that request is valid and must be complied with. The bank did eventually provide the individual with a copy of the relevant records.

CASE STUDY 4 — credit record - issue of accuracy - review of credit referencing computer system

The complainant ('person A') was refused a loan to buy a car. He made an access request under ***section 4*** of the Data Protection Act to a credit referencing agency in order to see his credit record. His record showed that he had borrowed a sum of money from a certain financial institution ('Institution X') some years previously, and that this loan had not been repaid. His record also showed that a number of other financial institutions had recently made enquiries about his credit record. Person A immediately recognised that he had never taken out any such loan.

Person A then made enquiries with Institution X. He established that the record of the loan related to a person ('person B') with the same name as his own and a similar address, but with a different date of birth. Person A raised this matter with my Office, requesting that I investigate *"the wrong/misleading information given out by [the agency] to certain financial institutions in relation to loan applications made by [him]"*.

I took the case up with the agency. On checking its archive records, it emerged that the problem had originated several years previously. At that time, the agency had received a request for a credit check of person B from Institution X. The search had shown no record in respect of person B at that time. However, the agency had decided to provide the information it kept in respect of person A to Institution X in view of the similarity of A and B's details. Institution X had erroneously appended the agency's reference number for person A to the details of the loan made to person B. When Institution X subsequently recorded the details of person B's loan with the agency using the erroneous reference number, the agency had automatically appended these details to person A's record. This accounted for the inaccuracy of person A's credit record.

Section 2(1)(b) of the Data Protection Act provides that personal data *"shall be accurate and, where necessary, kept up to date"*. It is clear that in this case, information relating to the complainant was not

accurate in that it included details of a loan which did not relate to him, and accordingly I upheld the complaint. However, I also took note of the fact that the agency immediately rectified its records in respect of the complainant, as required under ***section 6*** of the Act, and also undertook to notify its clients of the rectification of the incorrect data. I also received an assurance from the agency that it had amended its computer systems so that new credit details which contained the agency's customer record numbers would no longer be associated automatically with existing records.

As to the root cause of the difficulties in this case, my decision noted that the credit reference agency was not justified in its original disclosure of person A's details to Institution X in response to a query about person B, who was clearly distinguishable from A.

CASE STUDY 5 — unsolicited loyalty cards - clear consent - fair obtaining

A retail company sought advice from my Office on the extension of its loyalty card scheme to a new outlet. In the normal course of events, customers become members of the loyalty card scheme by making an application at any of the company's retail outlets. It was now proposed to write to potential customers in the catchment area of the new outlet, using a purchased mailing list, inviting them to join the loyalty card scheme. It was further proposed to enclose a loyalty card with the letters of invitation. Use of the card would automatically enrol the potential customers in the loyalty card scheme, with their names being transferred from the mailing list database to the loyalty card membership database.

The main data protection question which arose was whether the triggering of automatic membership of the loyalty card scheme by simply using the card constituted consent to membership by the customer and fair obtaining by the company of the customers' personal data. In particular, I was concerned that a card sent through the post to one member of a household might be used by another member of the household, thus enrolling the first household member in the scheme, possibly without consent. I was of the view that for the scheme to operate as the company envisaged, it would be necessary, when issuing the invitations, to make the implications of the use of the card very clear and to give people a clear opt-out.

In the event, the company agreed to include in the invitation letter a prominent and clear statement that if customers used the loyalty card, their names and addresses would be recorded by the company as part of the loyalty-club membership; and that, if a customer did not wish to become a club member, the card should be destroyed. Given the clear statement of the effect of using the card, the warning to destroy the card if one did not wish to become a member and the prominence given to the statement in the invitation letter, I was satisfied that the automatic triggering of membership by use of the card could, in these particular circumstances, indicate clear consent and thus fair obtaining for the purposes of the Data Protection Act.

CASE STUDY 6 — local authority housing loan - disclosure of personal data by a local authority to a financial institution - whether such data are in the public domain - statutory discretion to make personal data publicly available does not take precedence over data protection law

The complainant received a letter from a bank inviting her to convert her local authority housing loan to a housing loan provided by that bank. The bank informed the complainant that the offer was unique to people who held mortgages from the local authority in question. The complainant queried this matter with her local authority. It admitted that it had passed names and addresses to the bank, in order to allow the bank to advise people of its re-mortgage facilities. The local authority said that no loan account details had been passed to the bank. The complainant raised the matter with my Office, complaining

that her personal details had been disclosed without her knowledge or consent, in contravention of the Data Protection Act.

The local authority confirmed to my Office that it kept data relating to loan account holders for the purpose of administering its loan accounts, and that it had not obtained the complainant's consent to the disclosure of her name and address to the bank. However, the local authority was of the opinion that these details were already in the public domain, because whenever a local authority borrower is approved for a loan, a County Manager's Order is drafted, and all such orders are included as part of the local authority's minutes which are publicly available documents.

In considering this matter, I had regard to ***section 1(4)(b)*** of the Data Protection Act, 1988, which 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"*. This provision would mean that, if the names and addresses of the local authority's housing loan account holders were required by law to be made available to the public, then the disclosure of such data by the local authority could not have been in breach of the Data Protection Act.

Accordingly, the local authority was requested to indicate whether the County Manager's Orders were required by law to be made available to the public. The local authority pointed out that there was a legal obligation to make such orders and to retain records of them, by virtue of the *County Management Acts* of 1940 and 1955. However, while that legislation allowed the County Manager discretion to record the names and addresses of housing loan account holders, the local authority was unable to cite any statutory requirement to place such personal data in the public domain. In the absence of any such statutory requirement, I could only conclude that the data in question were subject to the Data Protection Act, 1988, in the normal way.

Accordingly, I upheld the complaint against the local authority. All data controllers, and in particular those in the public sector, should note that statutory discretion to make personal data publicly available is not the same as a statutory requirement to do so. It is only the latter that takes precedence over the normal application of data protection principles.

CASE STUDY 7 — unsolicited direct mail from abroad - mutual assistance between parties to the 1981 Council of Europe Convention on Data Protection

A number of people complained to me of having received unsolicited mail from a direct mailing company. They wished to establish how the company concerned had obtained their names and addresses and also wished to have their personal data deleted from the company's database. On investigating the case, I noted that the direct mailing company in question was operating in another jurisdiction. I contacted the data protection authority in that jurisdiction in order to have the matter investigated and appropriate action taken.

The 1981 *Council of Europe Convention 108* on data protection provides for mutual assistance between States that are parties to the Convention. In particular, ***Article 14*** of the Convention provides as follows:

1. Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.

2. When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.

3. The request for assistance shall contain all the necessary particulars, relating inter alia to:

(a) the name, address and any other relevant particulars identifying the person making the request;

(b) the automated personal data file to which the request pertains, or its controller;

(c) the purpose of the request.

The foreign data protection authority readily agreed to investigate the case on my behalf. The investigation revealed that the direct mailing company concerned had breached the data protection laws in that jurisdiction. The outcome is that the names of the complainants have been removed from the direct mailing company's database, and the data protection authority is proceeding to take action against the company concerned in accordance with the data protection laws in that jurisdiction. In my opinion, it is likely that international cooperation among data protection authorities will have an increasing role in the future in ensuring that people's privacy rights are respected. My experience to date of securing such cooperation has been most encouraging.

CASE STUDY 8 — bank account details - disclosure to a person listed as a "disclosee" in the bank's entry in the Register of Data Controllers - Register entry not conclusive as to compliance with data protection principles

A person complained to me that details of his bank account had been disclosed to a close relative by his bank. The bank account details had been posted to the relative. The bank acknowledged that the complainant's bank account data had in fact been addressed (as a result of an administrative error) to the relative. However, the bank pointed out in its defence that it was a registered data controller and that the list of disclosees in its entry in the Register of Data Controllers included "current/past/potential relatives", and that therefore the disclosure was not incompatible with the Register entry.

My investigation confirmed that the bank's Register entry was as described. However, the question for consideration was not solely whether the disclosure was of a kind listed in the Register entry, but also whether such disclosure was compatible with the purpose for which the data were obtained. ***Section 2(1)(c)*** of the Act provides *inter alia* that personal data —

(i) shall be kept only 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.

Having examined the case, I noted that the primary purpose for which the bank kept the complainant's data was the administration of his account. When obtaining the data, the bank had informed the complainant that his data would be disclosed to certain bodies which were relevant in the context of the administration of his account. However, the individual was not informed that his data were liable to be disclosed to relatives, and it could not reasonably be maintained that disclosure of the complainant's details to his relatives would be necessary for the administration of the account. Accordingly, I decided that the complainant's data had been disclosed in contravention of section 2 of the Act, and I upheld the complaint.

I would remind data controllers that the inclusion of details in the Register entry is only one aspect of compliance by a data controller with the basic principles of data protection, including the requirement to obtain and use data fairly, and not to disclose such data to other persons inappropriately. The purpose of including details in the Register entry is to describe, in a publicly accessible form, the outer limits of what the data controller may do with personal data, not to provide a 'back door' that would allow a data controller to circumvent its basic data protection responsibilities.

CASE STUDY 9 — telephone-based market research - apparent disclosure of unlisted telephone number

The complainant received a phone call from a market research company carrying out a survey. As his telephone number is ex-directory, the complainant asked how this had been obtained. He was given to understand that his phone number had been obtained from the telephone service provider. When the complainant visited the offices of the telephone service provider to protest about the apparent disclosure of his unlisted number, the provider stated unequivocally that it did not disclose unlisted telephone numbers to third parties. The complainant raised the matter with my Office, saying he was disturbed that his unlisted telephone number had become available to the market research company.

In the course of my investigation, I contacted the market research company to ascertain the source of the telephone numbers which had been used. The market research company explained that it had been contracted by a client company to undertake a continuous survey, which involved contacting a representative sample of the population every four weeks. To achieve this objective, a system of random number dialling was employed whereby a telephone number was taken from the public telephone directory, and then used to generate random telephone numbers by simply adding or subtracting a number. The number initially selected from the directory was not dialled. The market research company informed me that this method of random generation of telephone numbers meant that unlisted numbers and also fax numbers were called from time to time. The company said that it had not been supplied with any ex-directory listings or other personal data by the telephone service provider. Moreover, the company's interviewers did not ask either the names or addresses of the interviewees. Only the answers to the questions which were put to the interviewees were recorded for research purposes. Accordingly, the anonymity of the respondents was not in any way compromised.

A member of my staff visited the offices of the market research company to investigate at first-hand the nature of the processing undertaken by the company. The results of this inspection were consistent with the market research company's account of its activities.

Given the facts that came to light in the course of the investigation, and the lack of any evidence that the complainant's unlisted telephone number had been disclosed by the telephone service company, I did not uphold the complaint.

CASE STUDY 10 — school web site - personal data relating to children - issue of fair obtaining

A parent contacted my Office to complain that the local primary school was publishing personal details of pupils on the school web site, without the knowledge or consent of parents. The details included photographic images of named individual pupils, as well as general details volunteered by pupils regarding their hobbies, likes and dislikes. The parent was concerned that the non-selective publication of children's details in this way was inappropriate, and could expose the children to unnecessary risks. The parent had raised the matter with the school authorities and was very dissatisfied with the response she had received.

I immediately contacted the school principal to arrange that personal details relating to identifiable children would be deleted from the web site, pending an urgent meeting on this matter. At the meeting, the school principal explained that the web site had been set up several weeks previously in order to meet the educational needs of children in relation to computing. The pupils themselves had been quite positive about the development. Photographs of individual pupils in the junior and senior infants classes

had been posted on the web site. Other pupils had been invited to contribute to the web site through other activities, such as filling out questionnaires giving personal information that would be of interest to pupils in other schools, both nationally and internationally. It was noted that the school web site had been given an award by an internet service company in recognition of its merit. As regards parental consent, the principal said that the new web site had been mentioned in a recent school newsletter, and that parents had been invited to come to the school to check it out for themselves.

I pointed out that ***section 2(1)(a)*** of the Data Protection Act requires that personal data "*shall have been obtained, and the data shall be processed, fairly*". When dealing with personal data relating to schoolchildren, "fairness" in my judgement requires that the clear and informed consent of parents or guardians must be obtained before any use is made of the children's data. This is particularly so where the use envisaged involves the posting of data on the worldwide web. The principal accepted these points and undertook not to post personal details of schoolchildren on the web site except with the express authorisation of a parent or guardian.

I have no doubt that forward-looking schools will continue to reflect the growing importance of the internet in their educational programmes in future. Certainly, the internet has the potential to serve as a versatile tool for educators and to yield many benefits for students. However, the posting of personal details on a web site entails a dramatic loss of control over access to and use of such details, in a manner that may be quite incompatible with a school's responsibilities as a data controller. In this case, the vigilance of parents played a key role in ensuring that the school was made aware of its data protection responsibilities. I should also point out that, following the changes made on foot of the parents' concerns, the school web site in question is now, in my opinion, an excellent and a safe educational resource. **Part 1** of this Annual Report gives further information on this general topic under the heading *'Education and Awareness'*.

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. [13*th 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

A useful function of an Annual Report, beyond the presentation of an overview of the year's activities, is to signal and to expand upon developments of particular interest, and to give an indication of my views in relation to evolving issues on the national and international fronts. In this Part of my Report, I give an account of the main activities and outcomes of the 1998 Spring Conference of European Data Protection Commissioners. I also give details on the activities of my Office at European level, where the establishment of Europol and the implementation of the Eurodac Convention involve significant additional responsibilities for my Office, and have implications for the data protection environment in Ireland. I include a discussion of the issue of disclosure of telephone billing data by telecommunications companies to law enforcement agencies, a topic that has been the subject of consideration at EU level. Finally, I include an outline of advanced data-sharing and data-processing techniques which are likely to pose significant challenges for data privacy in the near future, and which have already arisen for consideration in other jurisdictions. The various means adopted for addressing such issues may be of interest in an Irish context.

SPRING CONFERENCE, DUBLIN 1998

A key event in the calendar of European Data Protection Commissioners is the annual Spring Conference. In 1998 this Conference was hosted by my Office in Dublin for the first time. The event was held in Dublin Castle on 23-24 April 1998 and was attended by the data protection authorities of the EU Member States, by those of Iceland and Norway, and by a representative of the EU Commission. All organisational arrangements were undertaken by the staff of my Office, in addition to their day-to-day responsibilities. This collective effort went far beyond the normal call of duty and I am glad to have the opportunity to record my gratitude to all my staff for their enthusiasm and co-operation in making the event a success. Given the importance of the Spring Conference in determining the strategies adopted by European Data Protection Commissioners acting collectively in response to the challenges of the information society, and given the significance of the first hosting of the event in Ireland, I will record the issues discussed and the conclusions reached in greater detail than would normally be the case in this Report.

Strategic Planning

It had been previously been agreed that one of the aims for the Dublin Conference would be an examination of the current mission, organisation and attributes of data protection offices. Such a stock-taking was considered particularly important in 1998, given that the year marked the 25th Anniversary of the establishment of the oldest data protection authority — that of Sweden — and given that the newest authorities — those of Italy and Greece — were less than a year in existence. Much thought was given to how data protection offices could become more responsive to the needs of individual citizens. My Deputy, Mr Heylin, was highly complimented on his contribution to this discussion, based on the detailed analysis of questionnaire responses from the various data protection authorities.

It emerged that almost all authorities are required by law to maintain some form of register of data controllers, although the utility and practicability of this practice in today's world of information technology was questioned. Few participants were enthusiastic about schemes of 'universal registration' (i.e. requiring all data controllers within a jurisdiction to register with the authority), although this type of approach had been popular in an earlier and simpler information age. Most authorities have the power to make decisions on complaints, and all issue recommendations and advice

on good practice. An interesting finding was that several countries operate different data protection regimes for their public and private sectors. Most authorities would wish to increase compliance through education and awareness programmes and follow-up action such as data protection audits. However, such pro-active approaches are resource intensive and most authorities reported being under-resourced in terms of the staff and monetary budgets available. There were wide variations in the backgrounds of the staff of Data Protection Offices. Some national authorities were predominantly staffed by lawyers, with some support from information technologists and administrators, while this proportion was reversed in other authorities. The consensus was that the pace of change required the availability of a mixture of staff. On the question of resources generally, the conclusion reached was that the levels of resources necessary to perform the tasks were quite insufficient, having regard to developments such as implementation of *Directive 95/46/EC;* additional work in respect of Third Pillar matters (i.e. Justice and Home Affairs issues under the Maastricht Treaty); and the need to vindicate the privacy rights of individual EU citizens in an efficient and independent way. A statement to this effect was drafted by the Conference and is set out in Appendix 2.

Police, Customs and related matters

This topic was considered under the headings of Europol, Schengen, Eurodac and the Customs Information System. Mr O'Donovan of my Office took the lead in reporting on developments in the Customs Information System. Following extended discussion of these issues, an Italian proposal for better horizontal co-ordination of Third Pillar data protection issues was adopted and, as Chairman of the Conference, I was asked to write to the President of the Council of Ministers outlining how the Conference felt these matters should be progressed. The Conference's consideration of this question has since become the basis for a work programme at EU level for the reform and simplification of the data protection rules applicable to data protection in the Third Pillar. This debate is dealt with further under the heading 'Europol and Related Matters' below.

Internet Issues

These issues were explored from a number of perspectives. A colleague from the Belgian data protection authority presented a paper examining in detail the technology which underpins web browsers, and demonstrating how this technology uses 'cookies' to collect personal data without either the knowledge or consent of data subjects. He explained how the process could be made more privacy-friendly by changes in default setting and argued that data protection authorities should, as a matter of priority, actively lobby for such improvements. The French data protection commission — *Commission Nationale de l'Informatique et des Libertes (CNIL)* — outlined how it had developed its own web site to demonstrate to individuals how exactly their personal data is handled on the world wide web. The CNIL web site makes transparent the traces a person leaves when visiting the site. A visit to this site, which can be found at *www.cnil.fr,* will provide a worthwhile experience for anyone concerned with privacy on the internet and is a useful online resource for those teaching data protection.

Other Topics

Consideration was also given to the data protection challenges presented by profiling in the financial sector and the difficulties which frequently arise in the consumer credit sector. The conclusion was that there must be some limits to the uses which can legitimately be made by a money transmission service, such as a bank, of the transaction data which will be available to it. However, it is no easy matter to determine where precisely such limits lie, particularly when multipurpose financial institutions are fast becoming the norm in an intensely competitive market place. Finally, the Conference considered the role of privacy audits as part of the proactive role of a data protection office. This topic was presented jointly by the Swedish Data Protection Commissioner and the Dutch Data Protection Office. There was

general agreement that privacy audits will play an essential part in the emerging role of data protection offices in years ahead.

EUROPOL AND RELATED THIRD PILLAR MATTERS

In last year's Report I noted the passage of the Europol Act, 1997 and the role assigned to the Data Protection Commissioner as the National Supervisory Body for the purposes of that Act. The consequences of this designation are two-fold. Firstly, my Office becomes responsible for ensuring that the data protection rules set out in the Europol Act are applied to the transfer of personal data from Ireland to Europol; and secondly, my Office must play its part in the collegiate supervision of the application of the data protection rules to Europol itself. This is undertaken by the Europol Joint Supervisory Body (JSB), consisting of members of the independent data protection authorities in each of the fifteen Europol Convention countries.

So far, my Office's involvement in these tasks has been concentrated on issues associated with the establishment of the JSB rather than supervision at national level. This follows naturally from the fact that, until Europol actually takes up its mandate, no personal data will flow from a Member State to Europol. As soon as such flows commence, national supervision will become an urgent priority. I am aware that the data protection authorities in other countries have been actively planning their strategies for undertaking their responsibilities as National Supervisory Bodies. However, strategic planning of this nature requires staffing resources which were simply not available in my Office in 1998.

My Office's contribution to work associated with Europol in 1998 was devoted to finalising the rules of procedure of the JSB. This proved to be an unusually difficult task, requiring the reconciliation of very different viewpoints as to the nature and functions of a supervisory body for an entity — Europol — which is itself a totally new concept in policing at the level of the European Union. Notwithstanding the work done by the Data Protection Commissioners Working Party on Police and Related Matters (under the auspices of the Spring Conference of European Data Protection Commissioners) in unanimously agreeing draft rules of procedure for the JSB, the issue proved divisive when addressed by the Council of Ministers. The matter reverted to the Data Protection Commissioners, and further compromises were worked out dealing with the innately difficult issue of ensuring fair procedures in the processing of complaints, especially in response to access requests to Europol, without prejudicing Europol's legitimate interests in the non-disclosure of highly sensitive data. These are difficult issues, even in the context of a legislative framework such as our 1988 Act, which gives an individual a right of direct access to data relating to him/her kept by law enforcement agencies, with a right of appeal to the Courts by either party against the Data Protection Commissioner's ruling in the matter. In a European context, where the right of direct access is not recognized in all national laws, and where the Appeals Committee of the Joint Supervisory Body is the final arbiter for both Europol and an aggrieved individual, the sensitivities and difficulties are multiplied. After much deliberation, the Council of Ministers and the JSB were in a position to agree unanimously on the JSB's rules of procedure. This cleared one of the final barriers to Europol taking up its activities. When the JSB met formally for the first time, I had the honour to be elected its first chairman.

Horizontal Co-operation in Third Pillar Data Protection

Experience of the development of a scheme for the data protection supervision of Europol has many lessons to offer for the future of data protection supervision of European institutions. This has been recognised in calls for the greater harmonisation of data protection rules and supervisory mechanisms, in the first instance in respect of Third Pillar matters. In my opinion, the Europol experience will

profoundly influence data protection policy making for the Customs Information System, the Schengen Information System and Eurodac. This process began under the German Presidency of the European Union and is likely to be further advanced under the Finnish Presidency. While it is difficult to predict the ultimate outcome, two broad approaches can currently be identified. The first may be described as a top-down approach which seeks from the outset to harmonise the substantive data protection rules for all Third Pillar institutions. The second approach may be classified as bottom-up and starts with cooperation in more mundane matters, for example by having the same persons involved in the various supervisory bodies and arranging back-to-back meetings in the interests of efficiency and effectiveness. I favour a mixture of both approaches starting with the bottom-up, while acknowledging from the outset that there is need for some harmonisation of the substantive data protection rules that apply in different areas. This is, I suppose, a reflection of my view that there is a core of data protection principles derived from a concern for fundamental human rights which can be applied in both the public and private sectors and to activities as diverse as policing, immigration control and the prevention of fraud.

ADVANCED DATA SHARING TECHNIQUES

Under this heading I will present an overview of some techniques which, although they have not yet come to my attention as being widely practised in Ireland, are well known in other administrations and are a cause of concern to local data protection authorities. Sometimes these techniques are grouped together under the general heading ‘data mining’, which may be described as an application of artificial intelligence and statistical analysis to large-scale databases. These techniques, whether used by public or private sector data controllers, tend to challenge the ‘purpose specification’ or ‘finality’ principle in data protection law and practice. Given the centrality of that principle to the information privacy concept, it is not surprising that data protection authorities are deeply concerned by the growing application of such techniques. But first it may help to describe each of the key techniques in some detail.[1]

Data Matching

This involves the comparison of two or more sets of computerised records to search for individuals who may be included in more than one file. It may take place either within an institution or between different institutions. For example, a financial services conglomerate providing both insurance services and retail banking might wish to data match its customers or, at local government level, a health board and a local authority might wish to data match their records. The New Zealand *Privacy Act* of 1993 defined data or information matching as —

> *The comparison (whether manually or by means of an electronic or other device) of any document that contains personal information about ten or more individuals with one or more other documents that contain personal information about ten or more individuals, for the purpose of producing or verifying information that may be used for the purpose of taking adverse action against an identifiable individual.*

In my view the inclusion of the purpose ‘taking adverse action’ is not an essential ingredient of the technique as such. Indeed the practice may be more insidious from a privacy point of view where it is ostensibly justified on the grounds that it is in an individual’s own best interests. It appears to me that

[1] These descriptions are adapted from a paper, “Privacy Technology, A New Challenge in Cyberspace” presented by Dr John Borking to the 16th International Conference on Data Protection and reproduced in *Privacy Disputed*, ISBN 9034631966

the acid test in all such cases is quite simple: was the data subject afforded an opportunity to freely give his or her informed consent to the proposed data match?

Front-end Verification

Whereas data matching involves comparing pre-existing computer records of an individual, front-end verification is used to certify the accuracy and completeness of personal information by checking it against similar information held in computerised databases, generally of a third party. It may involve certifying information that the individual has supplied, checking a database to determine if there is additional relevant information, or both. Like data matching, any large scale application of front-end verification is dependent on computers and telecommunication systems and creates a *de facto* virtual central national or international database covering many individuals. Information is directly verified on-line on an individual basis for preventive purposes before a transaction will take place and differs from data matching where an electronic search is done on a category or class of people in order to detect discrepancies. During 1998, a number of companies providing specialist services of this kind for the financial services sector held preliminary discussions with my Office on the data protection issues involved.

Computer Profiling

In computer profiling, record systems are searched for a specific combination of historical data elements that together compose the 'profile'. A judgement is made about a particular individual based on the past behaviour of other individuals who appear statistically similar, that is, who have similar demographic, socioeconomic, physical or other characteristics. A profile is developed by a data controller to select characteristics of types of individual and to determine the probabilities of such individuals engaging in activities or behaviours of interest to the searcher. Profiles can be valuable tools for investigative, administrative and marketing purposes, because they reduce the population that is of interest to the searcher, and thus may increase the searcher's efficiency and effectiveness. Computer profiling has important privacy implications because people may be treated differently before they have done anything to warrant such treatment. Discriminatory behaviour may also result from computer profiling. Marketeers developing such profiles often refer to people not fitting the profiles as people living 'below the curve'. Such people may be offered less favourable conditions in respect of services such as insurance and banking. Again, my Office had direct contact for the first time in 1998 with companies proposing to offer such profiling services in the Irish market.

Reactions of other Data Protection Authorities to such developments

My initial response to the likely introduction of these techniques in the Irish environment is to ascertain the approach adopted by my counterparts elsewhere when addressing similar issues. Notwithstanding my comments that the EU is currently the dominant influence in data protection thinking, it is worth looking at the experience of countries such as New Zealand and Canada in relation to data matching in particular. In the first place, the New Zealand experience is informative because that country has attempted to tackle the data matching issues in its 1993 Privacy Act which, coming five years later than the Irish Act, is more in tune with these issues. Secondly, the New Zealand experience has the merit of also being based on a common-law tradition, and the scale of the country and its public administration is similar to our own. Most important of all however is the fact that in 1998 the New Zealand Privacy Commissioner published a major review[2] of the 1993 New Zealand Privacy Act. In this review, he sets out the claims for and against data matching, as shown in the table on the following page.

[2] *Necessary and Desirable - Privacy Act 1993 Review, Report of the Privacy Commissioner on the First Periodic Review of the Operation of the Privacy Act,* 1998, ISBN 0-478-10388-3

Data matching - For & Against

The claims for data matching

- detection and deterrence of fraud and other irregularities, for example fraudulent or multiple claims, unreported income or assets, impersonation;
- verification of information supplied;
- verification of eligibility, for example for a benefit programme;
- identification of corruption or mismanagement, for example conflict of interest; unusual payments; excessive withdrawals;
- construction of comprehensive databases for research purposes;
- identification of suspects through searching on the basis of the characteristics of potential offenders;
- improved efficiency, for example in identifying and concentrating on genuine beneficiaries; locating and rectifying discrepancies and errors;
- cost-effectiveness

The criticisms of data matching

- lack of a general government or public oversight;
- cost/benefits are not thoroughly analysed so as to properly justify data matching programmes;
- poor quality and inaccurate information leads to mismatches and replication of errors;
- information is used out of context and may be untimely, insufficient, or unsuitable for the purpose of the match;
- information flowing from matching should be properly verified;
- machines should not be used as substitutes in qualitative decision-making for human discretion and judgement;
- the assembling of new files of profiles of individuals leads to the replication of inaccuracies and the drawing of what may be unjustifiable conclusions;
- individuals lack knowledge and control over the information about themselves;
- data matching constitutes a fishing expedition without any pre-existing evidence or suspicion of wrongdoing;
- a presumption of innocence is turned into a presumption of guilt;
- individuals are not given an adequate opportunity to contest the results of a match

Having set out the arguments, the New Zealand report notes the position of data protection authorities in other administrations in respect of this technique. To put it mildly, they are at least cautious, as can be seen from the following comments.

> *Computer matching is like investigators entering a home without any warrant or prior suspicion, taking away some or all of the contents, looking at them, keeping what is of interest and returning the rest, all without the knowledge of the occupier.* — *Australian Privacy Commissioner*

> *It is a technique which, unbridled, would present an Orwellian threat which even Orwell would not have imagined. The invasive indiscriminate use of the computer in gathering, storing and comparing personal information for purposes either benign or malign, reduces individuals to commodities, subjugates human values to mere efficiency.* — *Canadian Privacy Commissioner*

> *A traditional investigation is generally triggered by some evidence that a person is possibly engaged in wrongdoing. A computer match is not bound by this limitation. It is directed not at an individual, but at an entire category of persons. It is random in nature as it is not initiated because any person is suspected of misconduct, but because a category is of interest to the Government. What makes computer matching fundamentally different from a traditional investigation is therefore that its very purpose is to generate the evidence of wrong doing required before an investigation can begin.*
> — *Ontario Information and Privacy Commissioner*

Preliminary Conclusions

The preliminary conclusions I draw from the international debate so far are as follows —

- the use of advanced data sharing techniques, particularly data matching, goes to the heart of the kind of relationships which, as a society, we wish to see evolve between individuals (data subjects) and large organisations (data controllers) in the information society, whether the data controllers be private sector organisations such as financial services companies or state agencies such as Government Departments
- in the private sector, increased use of these techniques has the capacity to undermine the ‘purpose specification’ or ‘finality’ principle and, in effect, to curtail drastically the degree of control a person exercises over information relating to him or her
- at the level of state agencies, the debate raises basic questions about the nature of citizenship and the obligations as well as the rights of citizens, and whether or not the relationship between citizen and state is to be based primarily on shared civic values or more on a culture of surveillance
- what is new in the equation is the increased capacity for surveillance as a result of the application of computer and related technologies
- choices as to the extent to which data mining techniques are to be used are ultimately political in nature and we are fortunate to live in a parliamentary democracy where such choices can be subject to public scrutiny and ultimately legislated for by the Oireachtas.

For a Data Protection Commissioner, the position has been set out clearly by my Canadian counterpart in the following terms —

> *A privacy commissioner cannot accept a data search that ignores the presumption of innocence, the need to identify some reasonable grounds for suspicion, and the absence of independent authorization.*

It remains to be seen how these issues will be dealt with in an Irish context.

DISCLOSURE OF TELEPHONE BILLING DATA BY TELECOMMUNICATIONS OPERATORS TO LAW ENFORCEMENT AGENCIES

This issue arose for consideration in 1998 both out of an examination of the relevant provisions of the Data Protection Act, 1988 and in discussions of the underlying issues by the Article 29 Working Party. My view on the matter is that telephone billing information kept on computer by a telecommunications provider is personal data within the meaning of the Act and subject to all the provisions of the Act. These include restrictions on disclosure of personal data unless at least one of the provisions in ***Section 8*** of the Act can be relied upon by the data controller to lift the non-disclosure requirements.

Section 8(b) provides that

> *Any restrictions in this Act on the disclosure of personal data do not apply if the disclosure is-required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders or assessing or collecting any tax, duty or other moneys owed or payable to the State, a local authority or a health board, in any case in which the application of those restrictions would be likely to prejudice any of the matters aforesaid.*

It is this exemption on which a telecommunications data controller is most likely to be entitled to rely when making disclosures of telephone billing data to a law enforcement agency. In this context, I am of the opinion that a data controller, faced with a request for telephone billing data from a law enforcement agency, is required to make a judgement as to whether non-disclosure of the requested data is likely to prejudice at least one of the matters mentioned in section 8(b) above. I am further of the view that for the exemption to apply, there would have to be a substantial risk, rather than a mere chance, that in the particular case being considered at least one of the purposes mentioned would be noticeably damaged by the data controller's failure to provide the information sought. It goes without saying that a data controller cannot rely on section 8(b) to disclose personal data relating to a number of individuals without first making the above assessment in respect of each and every individual concerned. An aggrieved party, either a data subject or a data controller, would of course be entitled to challenge my interpretation of the requirements of section 8(b) in the Courts if a suitable case should arise.

Section 8(b) is of general application in the sense that it applies to all data controllers and to many parties who might legitimately seek disclosure of personal data in reliance on this provision. Data controllers who are telecommunications services providers are also bound by the non-disclosure requirements of *section 98(2A)-(2C)*[3] of the *Postal and Telecommunications Services Act, 1983,* and entitled to rely on the exemptions set out in that section. This raises the question of the relationship between the exemptions found in section 8(b) and section 98(2A)-(2C). It appears to me that nothing in section 98(2A)-(2C) or any other provision of the *Postal and Telecommunications Services Act, 1983* disapplies the provisions of the Data Protection Act, 1988. If I am correct, it follows that a telecommunications services provider, being a data controller which satisfies the exemption from non-disclosure criteria in section 98(2A)-(2C), must also consider and apply section 8(b) of the Data Protection Act when responding to a request from a law enforcement agency for the disclosure of telephone billing data. A data controller cannot automatically assume that, if the requirements of section 98(2A)-(2C) are met, then the requirements of section 8(b) are also satisfied. In this connection, it is worth noting that while the 1983 Act provides a very high level of safeguards in respect of the

[3]Inserted by *section 13* of the *Interception of Postal and Telecommunications Messages (Regulation) Act, 1993.*

interception of the contents of a telecommunications message, the safeguards in respect of the non-disclosure of billing data are less demanding. It is not entirely clear to what extent the privacy protection standards applicable to telephone billing data were considered and debated when either the 1988 Act or 1983 Act (as amended) was being prepared. I recommend that this question be examined and, if necessary, further clarified in the context of the amendment of the 1988 Act required for the transposition of *Directive 95/46/EC* into Irish law. This provides an ideal opportunity to provide in statute a single clear set of legal tests to govern this complex question. Such clarity is in the interests of all — data subjects, data controllers and law enforcement agencies.

Having given my opinion on the requirements of Section 8(b) as currently drafted, and on a possible need for clarification, I should indicate my views on the principles which might guide change. This task is simplified by the fact that the Article 29 Working Party has examined these issues in depth in 1998, albeit in the context of developments at European level as distinct from national level. The Working Party has set out its conclusions in its *Recommendation on the Respect of Privacy in the Context of Interception of Telecommunications* (reproduced in Appendix 1). I urge all concerned with these matters to examine and follow the principles set out in this recommendation.

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. [13*th 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;

Appendix 1

RECOMMENDATION ON THE RESPECT OF PRIVACY IN THE CONTEXT OF INTERCEPTION OF TELECOMMUNICATIONS

Adopted by the Working Party on 3 May 1999

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA,

Instituted by Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995,

Having regard to Articles 29 and 30 paragraphs 1 and 3 of the above-mentioned Directive,

Having regard to its rules of procedure, and in particular Articles 12 and 14 thereof,

Has adopted the present recommendation:

The purpose of this recommendation is to indicate how the principles on the protection of the fundamental rights and freedoms of natural persons, and in particular of their privacy and the secrecy of their correspondence, is to be applied to the measures concerning the interception of telecommunications adopted at European level.

This recommendation covers interception understood in a broad sense, i.e. not only of the contents of telecommunications, but also of any related data, particularly any preparatory measures (such as monitoring and data-mining traffic data) which may be envisaged in order to determine whether intercepting the contents of a telecommunication is advisable.

A. Scope of the provisions on the interception of telecommunications adopted at European level

1. The Council Resolution of 17 January 1995 on the lawful interception of telecommunications lists the technical conditions required for the interception of telecommunications, without going into the conditions under which such interception may be permitted. The Resolution requires network operators or service providers to pass the intercepted data on to the "authorised services" in plain text.

The data concern telephone calls, whether from mobiles or conventional units, e-mail, faxes and telex messages, and Internet data traffic, with regard to both content and any data related to telecommunications (this refers particularly to traffic data, but also to any signal transmitted by the person under surveillance — point 1.4.4. of the Resolution).

Data are to be collected both on the target persons and on any persons with whom they enter into communication.

The Resolution also provides for law enforcement agencies to have access to data on the geographical location of a mobile subscriber.

The Resolution of 18 January 1995 is currently being revised, with one of the main goals being to adapt it to new communication technologies. In particular, the draft text addresses how to apply interception measures to satellite telecommunications.

2. The Working Party is concerned about the scope of the measures envisaged by the Council Resolution of 17 January 1995. An unpublished, more recent version of the document referred to above ("declaration of intent" dated 25 October 1995), provides for the signatories to the text to contact the director of the United States Federal Bureau of Investigation about the requirements for the interception of telecommunications. The text also provides, subject to the approval of the "participants", for other States to take part in the exchange of information and in the revision and updating of the requirements.

The Working Party points out that the legal status of this text is unclear — particularly as regards the actual signing by the countries concerned — and that it does not constitute a measure accessible to the citizen according to the case law of the European Court of Human Rights quoted below, insofar as it has not been published. Secondly, the text notes a desire to develop technical measures for intercepting telecommunications jointly with States which are not subject to the requirements of the European Convention on Human Rights and of Directives 95/46/EC and 97/66/EC.

3. The Working Party notes that the Council Resolution aims to settle technical questions on the means of intercepting communications, without affecting the national provisions which regulate phone tapping in legal terms. Nonetheless, certain measures the resolution provides for, which increase the scope for intercepting telecommunications, conflict with the more restrictive national regulations of certain countries in the European Union (particularly point 1.4, access to data concerning calls, including calls from mobile phones, without considering the anonymous prepaid services now available; point 1.5, geographical location of mobile subscribers, and point 5.1, forbidding operators from disclosing interceptions after the fact.)

4. Although the Council Resolution is in line with an aim of "the protection of national interests, national security and the investigation of serious crimes", the Working Party wishes to draw attention to the risks of abuses with regard to the objectives of tapping, risks which would be increased by an extension to a growing number of countries — some of which are outside the European Union — of the techniques for intercepting and deciphering telecommunications.

A European Parliament resolution of 16 September 1998 relating to transatlantic communications "considers that the increasing importance of the Internet network, and more generally of telecommunications on a world-wide scale and in particular the Echelon system, as well as the risks of their abuse, call for the adoption of measures to protect economic information and effective encoding."

These considerations highlight the risks associated with telecommunication interceptions which go beyond the strict framework of questions of national security — and thus fall outside the European Union's "third pillar". They raise the question of their legitimacy, in particular in the light of the obligations arising from Community legislation on the protection of the fundamental rights and freedoms of natural persons, particularly their privacy.

5. The Working Party emphasises, finally, that as a result of the Treaty of Amsterdam coming into force, the legal basis of provisions for the interception of telecommunications will change at European level. The basis for the Council to draw up the resolution (currently articles K.1 (9) and K.3 (2) of the Treaty on police and judicial co-operation), will include powers of initiative of the European Commission under the new article K.6 (2).

B. General Legal Framework

6. The Working Party points out that each telecommunication interception, defined as a third party acquiring knowledge of the content and/or data relating to private telecommunications between two or more correspondents, and in particular of traffic data concerning the use of telecommunication services, constitutes a violation of individuals' right to privacy and of the confidentiality of correspondence. It follows that interceptions are unacceptable unless they fulfil three fundamental criteria, in accordance with Article 8 (2) of the European Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, and the European Court of Human Rights' interpretation of this provision: a legal basis, the need for the measure in a democratic society and conformity with one of the legitimate aims listed in the Convention.

The legal basis must precisely define the limits and the means of applying the measure through clear and detailed rules which are particularly necessary owing to the continuous improvement of the technical means available. The text of the law must be accessible to the public so that citizens may be informed of the consequences of their behaviour.

In this legal context, exploratory or general surveillance on a large scale must be proscribed.

7. Within the European Union, Directive 95/46/EC establishes the principle of the protection of the right to privacy enshrined in the legal systems of the Member States. This Directive specifies the principles contained in the European Convention for the Protection of Human Rights of 4 November 1950 and in Council of Europe Convention No. 108 of 28 January 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Directive 97/66/EC gives concrete expression to the provisions of this Directive by specifying the Member States' obligation to ensure through national regulations the confidentiality of communications carried out by means of a public telecommunications network or by means of publicly available telecommunication services. According to Article 13 (1) of Directive 95/46/EC, Member States may adopt legislative measures to restrict the scope of certain obligations (for example, concerning the collection of data) and certain rights (for example, the right to be informed of data collection) provided for in the Directive. These exceptions are strictly enumerated: the restriction must constitute a measure needed to safeguard the public interests exhaustively listed in paragraphs a) to g) of this article, which include national security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences.

Article 14 (1) of Directive 97/66/EC similarly states that Member States may only restrict the obligation of the confidentiality of communications on public networks when such a measure is required to safeguard national security, defence, public security or the prevention, investigation, detection and prosecution of criminal offences.

C. Obligations of Telecommunications Operators and Service Providers

8. It must be stressed that the obligations of the security and confidentiality of data to which telecommunication operators, service providers and Member States are subject on the basis of Articles 17 (1) and (2) of Directive 95/46 and Articles 4, 5 and 6 of Directive 97/66/EC respectively are the rule and not the exception.

The Working Party points out that these obligations also apply to operators in general under Article 7 of Council of Europe Convention No. 108 of 28 January 1981 on the Protection of Individuals with regard to Automatic Processing of Personal Data, and Article 4 of the Council of Europe Recommendation No. 4 of 7 February 1995 on the Protection of Personal Data in the Field of Telecommunication Services, with particular regard to telephone services.

9. These obligations imply that telecommunications operators and telecommunications service providers may not process data on telecommunications traffic and billing except under certain conditions: given that traffic data on subscribers and users must be erased or made anonymous as soon as the communication ends, it follows that the purposes for which the data may be processed, the length of time they may be kept (if at all) and access to them must be strictly limited.

10. Telecommunications operators and telecommunications service providers must take the measures needed to make the interception of telecommunications by unauthorised parties impossible, or as technically difficult as the current state of the technology allows.

The Working Party stresses in this respect that the implementation of effective means of intercepting communications, using precisely the most advanced techniques, must not result in a lowering of the level of confidentiality of communication and protection of the privacy of individuals.

These obligations take on a special meaning when telecommunications between individuals located on the territory of the Member States pass or may pass outside European territory, in particular when satellites or the Internet are used.

11. Where Directive 95/46 applies, making such telecommunications accessible outside the European Union could moreover constitute a violation of Article 25 of the Directive, insofar as foreign authorities intercepting them may not be able to ensure an adequate level of data protection.

D. Respect of Fundamental Freedoms by the Authorities with regard to Interceptions

12. Taking into account the above-mentioned provisions, it is important for national law to strictly specify:

- the authorities responsible for permitting the legal interception of telecommunications, those authorised to carry them out and the legal basis for their action,
- the purposes for which such interception may be carried out, which allow an assessment of whether it is proportionate to the national interests at stake,
- the prohibition of all large-scale exploratory or general surveillance of telecommunications,
- the exact circumstances and conditions (for example, facts justifying the measure, duration of the measure) governing the interceptions, without violating the principle of specificity which any interference in the privacy of individuals must respect,
- compliance with the principle of specificity, which is a corollary of forbidding all exploratory or general surveillance. Specifically, as far as traffic data are concerned, it implies that the public authorities may only have access to these data on a case-by-case basis, and never proactively and as a general rule.
- the security measures for the processing and storage of the data, and the length of time data may be kept,
- the guarantees concerning the processing of data concerning individuals affected indirectly or by chance by interceptions, in particular the criteria used to justify the conservation of data, and under what conditions these data may be passed on to third parties,
- that a person under surveillance be informed of this as soon as possible,

- the recourse available to a person under surveillance,
- the arrangements for the monitoring of these services by an independent supervisory authority.
- publication of the policies on the interception of telecommunications as they are actually practised, for example, in the form of regular statistical reports,
- the specific conditions under which the data may be transmitted to third parties under bilateral or multilateral agreements.

Done at Brussels, 3 May 1999

For the Working Party

The Chairman

Peter HUSTINX

Appendix 2

SPRING CONFERENCE OF THE EU DATA PROTECTION COMMISSIONERS, 23-24 APRIL 1998

CONFERENCE STATEMENT ON RESOURCES

The European Data Commissioners Conference meeting in Dublin on 23/24 April 1998,

- considering that the implementation of the European Directive 95/46 on data protection will increase the responsibilities of national data protection authorities, in relation for instance to prior checking, data protection audits and new duties in relation to the transfer of data to third countries outside the European Union,
- considering the critically important new responsibilities envisaged for data protection authorities in the Third Pillar area, including Europol, Eurodac and Customs Information Systems, and
- considering that these authorities require adequate financial and human resources to continue to vindicate the data privacy rights of individual EU citizens in an efficient and independent fashion, through their individual work and their international co-operation in an emerging European legal space in data protection,

strongly urge national Parliaments, Governments and relevant individual Departments of State to give increased priority to the resource requirements of these authorities.

Appendix 3

DOCUMENTS ADOPTED BY THE DATA PROTECTION WORKING PARTY (ARTICLE 29 GROUP)

Reference	Document	Date
5012/97	Recommendation 1/97: Data protection law and the media	25/02/97
5023/97	Opinion 1/97 on Canadian initiatives relating to standardisation in the field of protection of privacy	29/05/97
5025/97	First Annual Report	25/06/97
5020/97	Discussion Document: First Orientations on Transfers of Personal Data to Third Countries — Possible Ways Forward in Assessing Adequacy	26/06/97
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")	03/12/97
5027/97	Working Document: Notification	03/12/97
5022/97	Recommendation 3/97: Anonymity on the Internet	03/12/97
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?	14/01/98
5005/98	Working Document: Preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries	22/04/98
5009/98	Recommendation 1/98 on Airline Computerised Reservation Systems (CRS)	28/04/98

5032/98	Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)	16/06/98
5025/98	Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive	24/07/98
5004/98	Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct	10/09/98
5047/98	Second Annual Report	30/11/98
5092/98	Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the United States Government	26/01/99
5013/98	Working Document: Processing of Personal Data on the Internet	23/02/99
5093/98	Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware	23/02/99
5005/99	Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications	03/05/99
5047/99	Opinion 2/99 on the Adequacy of the “International Safe Harbor Principles” issued by the US Department of Commerce on 19th April 1999	03/05/99
5026/99	Opinion 3/99 on Public Sector Information and Data Protection (English version not yet available)	03/05/99
5066/99	Opinion 4/99 on the Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed “Safe Harbor Principles” on the Adequacy of the “International Safe Harbor Principles”	07/06/99
5054/99	Opinion 5/99 on the level of protection of personal data in Switzerland (English version not yet available)	07/06/99
5085/99	Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes	07/09/99

Appendix 4

REGISTRATIONS 1995 – 1998

	1995	1996	1997	1998
Data controllers by economic sector				
Civil Service Departments/Offices	98	99	97	100
Local Authorities and Vocational Education Committees	121	118	118	114
Health Boards and public hospitals/clinics	39	41	42	40
Third level education	33	31	32	33
Primary and secondary schools	9	14	18	19
Commercial state-sponsored bodies	81	75	74	70
Non-commercial and regulatory public bodies	45	93	116	129
Associated banks	19	22	22	25
Non-associated banks	44	47	52	54
Building societies	8	8	8	8
Insurance and related services	115	120	134	137
Credit Unions and Friendly Societies	431	439	451	457
Credit reference/Debt collection	24	19	20	22
Direct marketing	42	42	45	50
Miscellaneous commercial	17	12	19	34
Private hospitals & clinics/other health	77	81	88	92
Doctors, dentists & other health professionals	180	242	269	306
Pharmacists	349	495	515	511
Political parties & public representatives	28	31	84	78
Religious, voluntary & cultural organisations	29	31	40	42
Subtotal	***1,789***	***2,060***	***2,244***	***2,321***
Data Processors	***293***	***293***	***327***	***329***
Total	**2,082**	**2,353**	**2,571**	**2,650**

[1]A 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.

Appendix 5

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 53 and 54 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, 1998.

Joseph J. Meade

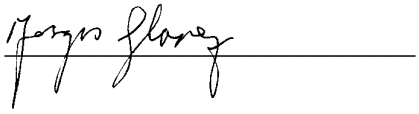
For and on behalf of the Comptroller and Auditor General

6 October 1999

ACCOUNT OF RECEIPTS AND PAYMENTS IN THE YEAR ENDED 31 DECEMBER 1998

1997		1998
£	Receipts	£
313,565	Moneys provided by the Oireachtas (note 1)	309,451
218,216	Fees	220,778
531,781		530,229
	Payments	
215,226	Salaries & Allowances (note 2)	213,498
8,254	Travel & Subsistence	8,012
2,397	Office & Computer Equipment	20,274
2,094	Furniture & Fittings	831
9,529	Equipment Maintenance & Office Supplies	4,628
4,734	Accommodation Costs (note 3)	4,614
12,511	Communication Costs	13,148
6,889	Incidental & Miscellaneous	5,128
46,182	Education & Awareness	38,328
5,749	Legal & Professional Fees	990
313,565		309,451
218,216	Payment of fee receipts to Vote for the Office of the Minister for Justice, Equality and Law Reform	220,778
531,781		530,229

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

Signed  Date 4 Oct 1999

Fergus Glavey
Data Protection Commissioner

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 £309,451

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 1998 was £54,720 (1997 cost £48,143).

NOTES